Inhaltsverzeichnis

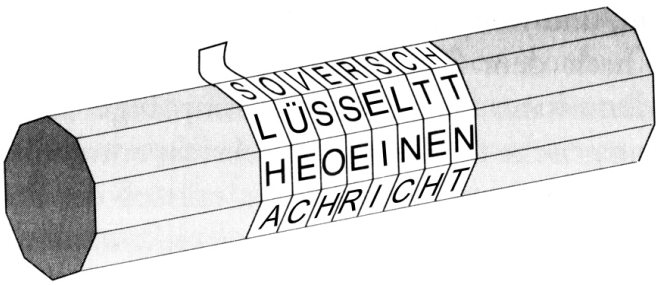
Kurseinheit 1

Symmetrische Kryptosysteme

Studierhinweise

Kryptografie, oder Kryptologie, ist die Lehre von den Geheimschriften. Sie ist sehr alt, denn von jeher ist es von Interesse gewesen zu gewährleisten, dass vertrauliche Nachrichten nur von dazu Befugten gelesen werden konnten.

Eine der ältesten überlieferten Geheimschriften ist die Skytale von Sparta, die im 5. Jahrhundert vor unserer Zeitrechnung von den Spartanern benutzt wurde. Sender und Empfänger besaßen beide Zylinder vom selben Umfang. Der Sender umwickelte seinen Zylinder spiralförmig mit einem schmalen Pergamentstreifen und schrieb seinen Text der Länge nach auf den Zylinder. Den abgewickelten Pergamentstreifen sandte er, und nur jemand, der einen Zylinder des gleichen Umfangs besaß, konnte den Text problemlos rekonstruieren. Ein Beispiel:



Die Nachricht lautet „So verschlüsselt Theo eine Nachricht“. Theo war in der Zeit, als der Kurs geschrieben wurde, Praktikant am Fachbereich Mathematik der FernUni.

Ein weiteres Beispiel für eine überlieferte Geheimschrift stammt von Cäsar. Er „verschob“ die Buchstaben um 23 Positionen. Wir werden Cäsars Idee in Abschnitt 1.1.3 präzisieren.

Bis vor wenigen Jahren war die Kryptografie eine Domäne der Militärs und der Diplomatie. So berichtet etwa F. L. Bauer im Vorwort seines Buches „Entzifferte Geheimnisse“ [Ba]: „Im Sommersemester 1981 kündigte ich eine Vorlesung unter

dem offenen Titel „Kryptologie“ an. ... Ich hielt es für gut möglich, dass die amtlichen Dienste aufmerksam würden; allerdings hatte ich keine Ahnung, wie schnell und in welcher Weise sie sich bemerkbar machen würden. Es geschah nichts. Als ich dann im Wintersemester 1986/87 die Vorlesung wieder hielt, sagte ich trotzdem in der ersten Stunde, als ich über den „heimlichen“ (clandestine) Charakter der Kryptologie sprach, scherzend zu meinen Studenten: „Wenn Sie eines Tages in der Vorlesung die Ihnen bisher unbekannten Gesichter zweier mittelalterlicher Herren mit Anzügen, die sich von den Ihren abheben, bemerken sollten, so denken Sie sich etwas.“ Wie es der Zufall wollte, platzten nach etwa sechs Wochen zwei Gestalten, auf die meine Beschreibung passte, in die Vorlesung - eine Viertelstunde nach Beginn. ... Geistesgegenwärtig begrüßte ich sie mit: „Grüß Gott, die Herren, kommen's direkt aus Pullach?“ Großes Gelächter bei den Studenten und verlegene Gesichter bei den beiden, die mir eine Antwort schuldig blieben. So weiß ich bis heute nicht, ob mein Verdacht gerechtfertigt war.“

Während also bis vor Kurzem der Kryptografie die Romantik und Komik des „Spion gegen Spion“ anhaftete, hat sich dies in den letzten Jahren dramatisch verändert. Mit der Verbreitung der elektronischen Datenverarbeitung, insbesondere der elektronischen Kommunikation bieten sich der Kryptografie völlig neue Aufgabenfelder. Einige Beispiele mögen dies illustrieren:

- Telefongespräche über Satellit kann im Prinzip jeder mithören. Wichtige Telefonate müssen chiffriert werden.
- Geldüberweisungen und andere Bankgeschäfte werden zunehmend elektronisch getätigt. Es muss sicher gestellt werden, dass der Auftrag an die Bank wirklich von dem vorgegebenen Sender stammt, und ein erteilter Auftrag darf nicht von Dritten manipulierbar sein.
- Viele komplexe Multiuser Systeme wie Rechner, Telefonnetze und Banken arbeiten mit Passworten oder PIN's (Personal Identification Number), mit denen sich ein Benutzer gegenüber dem System identifiziert. Diese müssen sicher verwaltet werden.

Zu den klassischen Aufgaben der Kryptografie, der sicheren Nachrichtenübermittlung, kommen also noch die Aufgaben der Authentifikation (stelle sicher, dass eine Nachricht von X wirklich von X ist) und der Integrität (stelle sicher, dass eine Nachricht im Zuge der Übermittlung nicht verändert wurde).

Diesen Aufgaben stellen sich verschiedene Wissenschaften. Gefordert sind die Ingenieurwissenschaften, hier vornehmlich die Elektrotechnik, die Informatik und in

besonderem Maße die Mathematik, denn

- viele kryptografische Algorithmen gehen aus klassischen mathematischen Theorien hervor,
- Mathematik kristallisiert Schwachstellen bei existierenden kryptografischen Algorithmen heraus (ein Beispiel werden Sie in Kurseinheit 7 kennen lernen), und
- im Idealfall kann mit Mathematik bewiesen werden, dass ein bestimmter Algorithmus einen gewissen Sicherheitsstandard erfüllt.

Die Kryptografie ist ein Paradebeispiel dafür, wie klassische Algebra, deren Anfänge vor unsere Zeitrechnung zurückgehen, plötzlich zu einem hochaktuellen Gebiet der angewandten Mathematik wird.

Ziel dieses Kurses ist es, Ihnen die Mathematik, die vielen klassischen und modernen Algorithmen der Kryptografie zu Grunde liegt, sowie die Algorithmen selbst zu erklären.

Kapitel 1

Grundbegriffe

Das Ausgangsproblem der Kryptografie ist es, zwei Personen, die wir Alice und Bob nennen, in die Lage zu versetzen, über einen unsicheren Kanal miteinander zu kommunizieren. Dabei soll es Oscar, der eine Nachricht unerlaubt abfängt, nicht möglich sein, den abgefangenen Text zu verstehen. Unter einem unsicheren Kanal ist etwa der Postweg, das Telefon oder ein Rechnernetz zu verstehen.

Die Information, die Alice an Bob senden will, nennen wir **Klartext**. Dies kann ein deutscher oder ein englischer Text sein; er kann aber auch Zahlen und Sonderzeichen enthalten. Alice chiffriert den Klartext nach einem Schlüssel, den sie und Bob vereinbart haben und schickt den so verschlüsselten Geheimtext über den unsicheren Kanal. Wenn Oscar den Geheimtext ausspioniert hat, kann er den Klartext nicht bestimmen. Bob dagegen, der den Chiffrierschlüssel kennt, kann den Klartext rekonstruieren.

Verschlüsselungen, die nach demselben Prinzip aufgebaut sind, fasst man zu sogenannten Kryptosystemen zusammen.

1.0.1 Definition Ein **Kryptosystem** ist ein 5-Tupel $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, so dass die folgenden Regeln gelten:

(i) $\mathcal{P}$ ist eine endliche Menge von Klartexten (englisch: plain texts).

(ii) $\mathcal{C}$ ist eine endliche Menge von Geheimtexten (englisch: cipher texts).

(iii) $\mathcal{K}$ ist eine endliche Menge von Schlüsseln (englisch: keys).

(iv) Für jedes $K \in \mathcal{K}$ gibt es eine Chiffrierungsregel $e_K \in \mathcal{E}$ (englisch: encryption rule) und eine Dechiffrierungsregel $d_K \in \mathcal{D}$ (englisch: decryption rule). Dabei sind $e_K : \mathcal{P} \to \mathcal{C}$ und $d_K : \mathcal{C} \to \mathcal{P}$ Abbildungen, so dass für alle $x \in \mathcal{P}$ gilt: $d_K(e_K(x)) = x$

Die Elemente aus $\mathcal{P}$ und $\mathcal{C}$ können sowohl einzelne Buchstaben oder Zahlen wie auch ganze Blöcke von Buchstaben oder Zahlen sein. Die Bedingung (iv) der Definition besagt Folgendes: Wenn ein Klartext $x \in \mathcal{P}$ mit Hilfe von e_K verschlüsselt wird, dann muss der Geheimtext $e_K(x) \in \mathcal{C}$ mit Hilfe von d_K wieder nach x entschlüsselt werden. Dies bedeutet, dass die Abbildung e_K injektiv sein muss.

Alice und Bob gehen folgendermaßen vor: Zu einem Zeitpunkt, an dem sie vor Oscar sicher sind, vereinbaren sie ein Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ und einen Schlüssel $K \in \mathcal{K}$. Nehmen wir an, dass Alice zu einem späteren Zeitpunkt eine Nachricht $\mathbf{x} = x_1 x_2 \dots x_n$ an Bob senden möchte. Dabei ist jedes x_i, $1 \leq i \leq n$, ein Klartext in $\mathcal{P}$. Jedes x_i wird durch die Chiffrierungsregel $y_i = e_K(x_i)$ verschlüsselt, und Alice sendet die Geheimtexte $\mathbf{y} = y_1 y_2 \dots y_n$ über den unsicheren Kanal an Bob. Wenn Bob den Text $y_1 y_2 \dots y_n$ erhält, dechiffriert er jedes y_i durch $x_i = d_K(y_i)$ und erhält $x_1 x_2 \dots x_n$, die Klartexte.

Die Kryptosysteme, die wir in dieser Kurseinheit besprechen werden, heißen **symmetrisch**. Der Name rührt daher, dass aus der Chiffrierungsregel e_K die Dechiffrierungsregel d_K leicht berechnet werden kann, und umgekehrt auch. Jeder, der chiffrieren kann, also e_K kennt, kann auch dechiffrieren.

Symmetrische Kryptosysteme haben den Vorteil, dass das Chiffrieren und Dechiffrieren in der Regel sehr schnell durchgeführt werden kann. Es müssen allerdings die Schlüssel häufig ausgetauscht werden, um dem Opponenten Oscar wenig Zeit zu geben, sie herauszufinden.

Nehmen wir aber nun einmal an, wir hätten ein Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, das die folgende Eigenschaft hat:

1. Für alle $K \in \mathcal{K}$ und für alle Klartexte $x \in \mathcal{P}$ lässt sich $e_K(x)$ sehr schnell berechnen.

2. **Ohne** eine geheime Zusatzinformation lässt sich das Urbild eines Geheimtextes $y \in \mathcal{C}$ unter e_K praktisch – das heißt, in angemessener Zeit – nicht berechnen, selbst dann nicht, wenn K und e_K bekannt sind.

3. Dazu Befugte können aus dem Schlüssel K die geheime Zusatzinformation schnell herleiten.

4. **Mit** der geheimen Zusatzinformation lässt sich $d_K(y)$ für alle Geheimtexte y sehr schnell berechnen.

In einer solchen Situation gibt es keine Gründe, die Schlüssel K und die Chiffrierungsregeln e_K zu verheimlichen, es ist ausreichend, die Zusatzinformation zu verbergen.

Kryptosysteme, die diese Eigenschaften haben, werden **Public-Key-Kryptosysteme** oder **asymmetrische Kryptosysteme** genannt. Die Schlüssel $K \in \mathcal{K}$ eines Public-Key-Kryptosystems heißen **öffentliche Schlüssel**, die geheimen Zusatzinformationen werden als **geheime Schlüssel** bezeichnet.

Der Vorteil der Public-Key-Kryptografie besteht darin, dass viele miteinander kommunizieren können, ohne dass fehleranfällige und mit Sicherheitsrisiken behaftete Schlüsselabsprachen nötig sind. So können Personen $A_1, \ldots, A_n$ Schlüssel $K_1, \ldots, K_n$ mit zugehörigen Chiffrierungsregeln wählen und diese quasi wie Einträge in einem Telefonbuch veröffentlichen. Will Bob an A_i eine verschlüsselte Nachricht schicken, so kann er durch Blick in das Telefonbuch feststellen, dass er seine Nachricht an A_i mit der zu K_i gehörenden Regel chiffrieren muss. Mit Eigenschaft 1. ist dies schnell möglich. Die befugte Person A_i hat bereits den geheimen Schlüssel hergeleitet, was mit 3. kein Problem darstellt. Eigenschaft 4. sichert, dass A_i schnell dechiffrieren kann. Der Opponent Oscar, der den geheimen Schlüssel nicht kennt, hat mit 2. ein Problem.

Der Nachteil der Public-Key-Kryptografie liegt darin, dass die Verfahren deutlich mehr Rechenzeit und Speicherplatz erfordern als symmetrische Verfahren. So genannte Hybrid-Verfahren kombinieren die Vorteile beider Varianten. Ein Public-Key-Verfahren wird zur Übermittlung der geheim zu haltenden Schlüssel verwendet und ein symmetrisches Verfahren zur Verschlüsselung der Daten.

Kapitel 2

Monoalphabetische Kryptosysteme

Wir werden in diesem Abschnitt annehmen, dass die Menge der Klartexte $\mathcal{P} = \{x_1, \ldots, x_n\}$ und die Menge der Geheimtexte $\mathcal{C} = \{y_1, \ldots, y_n\}$ gleich sind. In unseren Beispielen werden wir weiterhin annehmen, dass $\mathcal{P}$ und $\mathcal{C}$ nur aus den 26 Buchstaben a, b, ..., y, z bestehen. Klartextbotschaften sind Texte in deutscher Sprache, die als Folge von Kleinbuchstaben, ohne Satzzeichen oder Wortzwischenräume kommen. Die Nachricht „Liebesgrüße aus Moskau“ wird also zu „liebesgruesseausmoskau“. Die Annahme, dass $\mathcal{P} = \mathcal{C} = \{a, b, \ldots, y, z\}$, bedeutet, dass für jedes fest gewählte $K \in \mathcal{K}$ ein Klartextbuchstabe auf genau einen Geheimtextbuchstaben abgebildet wird. Ein Kryptosystem mit diesen Eigenschaften nennt man **monoalphabetisch**.

2.1 Permutationskryptosysteme

Wir behalten die Annahme $\mathcal{P} = \mathcal{C} = \{a, \ldots, z\}$ bei. Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ ein Kryptosystem. Sei $K \in \mathcal{K}$ fest und sei $e_K \in \mathcal{E}$. Wir wissen, dass e_K injektiv ist, und da $\mathcal{P}$ endlich ist, folgt, dass e_K surjektiv, also bijektiv ist. Damit ist e_K eine Permutation der 26 Buchstaben, also eine bijektive Abbildung $e_K : \{a, \ldots, z\} \to \{a, \ldots, z\}$. Eine Permutation $\pi : \{a, \ldots, z\} \to \{a, \ldots, z\}$ veranschaulicht man sich folgendermaßen: Man schreibt die Elemente in alphabetischer Reihenfolge in eine Zeile, dann schreibt man $\pi(a)$ unter a, $\pi(b)$ unter b und so weiter.

2.1.1 Beispiel

$$\pi = \begin{pmatrix} \text{a} & \text{b} & \text{c} & \text{d} & \text{e} & \text{f} & \text{g} & \text{h} & \text{i} & \text{j} & \text{k} & \text{l} & \text{m} & \text{n} & \text{o} & \text{p} & \text{q} & \text{r} & \text{s} & \text{t} & \text{u} & \text{v} & \text{w} & \text{x} & \text{y} & \text{z} \\ \text{x} & \text{n} & \text{y} & \text{a} & \text{h} & \text{p} & \text{o} & \text{g} & \text{z} & \text{q} & \text{w} & \text{b} & \text{t} & \text{s} & \text{f} & \text{l} & \text{r} & \text{c} & \text{v} & \text{m} & \text{u} & \text{e} & \text{k} & \text{j} & \text{d} & \text{i} \end{pmatrix}$$

beschreibt die Permutation

$$\pi : \{a, \ldots, z\} \to \{a, \ldots, z\} \text{ mit}$$

$$\pi(a) = x,\ \pi(b) = n,\ \pi(c) = y, \ldots, \pi(y) = d,\ \pi(z) = i.$$

Die Permutationen bilden mit der Komposition von Abbildungen eine Gruppe mit der identischen Abbildung als neutralem Element. Insbesondere ist jede Permutation invertierbar. Die Inverse π^{-1} zu einer Permutation π ist einfach zu bestimmen: Wir vertauschen in π die beiden Zeilen und ordnen die Spalten so an, dass die Elemente der ersten Zeile in alphabetischer Reihenfolge auftauchen.

2.1.2 Beispiel Zu der Permutation oben ist

$$\begin{pmatrix} \text{a} & \text{b} & \text{c} & \text{d} & \text{e} & \text{f} & \text{g} & \text{h} & \text{i} & \text{j} & \text{k} & \text{l} & \text{m} & \text{n} & \text{o} & \text{p} & \text{q} & \text{r} & \text{s} & \text{t} & \text{u} & \text{v} & \text{w} & \text{x} & \text{y} & \text{z} \\ \text{d} & \text{l} & \text{r} & \text{y} & \text{v} & \text{o} & \text{h} & \text{e} & \text{z} & \text{x} & \text{w} & \text{p} & \text{t} & \text{b} & \text{g} & \text{f} & \text{j} & \text{q} & \text{n} & \text{m} & \text{u} & \text{s} & \text{k} & \text{a} & \text{c} & \text{i} \end{pmatrix}$$

invers.

Das folgende Schema beschreibt das Permutationskryptosystem.

2.1.3 Definition Im **Permutationskryptosystem** sei $\mathcal{P} = \mathcal{C} = \{a, \ldots, z\}$. $\mathcal{K}$ besteht aus allen möglichen Permutationen der Buchstaben $a, \ldots, z$.
Für jede Permutation $\pi \in \mathcal{K}$ sei $e_\pi = \pi$, und $d_\pi = \pi^{-1}$.

2.1.4 Beispiel Nehmen wir an, Alice und Bob hätten sich zum Versenden von Nachrichten auf das Permutationskryptosystem geeinigt und die Permutation π oben als Schlüssel festgelegt. Nehmen wir ferner an, Alice möcht Bob die Nachricht

l i e b e s g r u e s s e a u s m o s k a u

schicken. Sie bildet

$$\pi(l) = b,\ \pi(i) = z,\ \pi(e) = h, \ldots$$

und sendet als chiffrierte Nachricht

b z h n h v o c u h v v h x u v t f v w x u

Zum Dechiffrieren bildet Bob

$$\pi^{-1}(b) = l,\ \pi^{-1}(z) = i, \pi^{-1}(h) = e, \ldots$$

und erhält die Ursprungsnachricht.

Nun werden sich nur wenige Menschen eine Permutation wie die in unserem Beispiel merken können. Daher bedienen sie sich Eselsbrücken, etwa eines Schlüsselworts und eines Schlüsselbuchstaben.

2.1.5 Beispiel Alice und Bob vereinbaren das Schlüsselwort

u n d j i m m y g i n g z u m r e g e n b o g e n

und den Schlüsselbuchstaben e. Zum Chiffrieren macht Alice aus dem Schlüsselwort eine Buchstabenfolge, in der jeder Buchstabe nur einmal vorkommt. Dies erreicht sie dadurch, dass jeder Buchstabe ab seinem zweiten Auftreten gestrichen wird. Das Schlüsselwort u n d j i m m y g i n g z u m r e g e n b o g e n wird also zu der Buchstabenfolge

u n d j i m y g z r e b o.

Diese Buchstabenfolge schreibt Alice unter das Klartextalphabet, und zwar beginnend unter dem Schüsselbuchstaben e:

a b c d e f g h i j k l m n o p q r s t u v w x y z
u n d j i m y g z r e b o

Dann schreibt sie die restlichen Geheimtextbuchstaben in alphabetischer Reihenfolge auf, indem sie nach dem letzten Buchstaben beginnt. Also

a b c d e f g h i j k l m n o p q r s t u v w x y z
t v w x u n d j i m y g z r e b o a c f h k l p q s

Die entsprechende Permutation benutzen Alice und Bob als Schlüssel.

2.1.6 Aufgabe Alice und Bob verabreden das Schlüsselwort „f e l d w a l d u n d w i e s e“ und den Schlüsselbuchstaben t. Wie lautet die entsprechende Permutation?

Berechnen wir, wie viele Schlüssel das Permutationskryptosystem besitzt. Es gibt $n! = n(n-1)(n-2)\cdots 2\cdot 1$ (gelesen wird $n!$ als „n Fakultät“) mögliche Permutationen von n Objekten. In unserem Fall, also $\mathcal{P} = \mathcal{C} = \{a, \ldots, z\}$, sind dies

$$26! = 26 \cdot 25 \cdot \cdots \cdot 2 \cdot 1 = 403\,291\,461\,126\,605\,635\,584000000,$$

also etwa $4 \cdot 10^{26}$ Stück. Durch systematisches Ausprobieren aller Permutationen wird Oscar, selbst mit dem stärksten Rechner, nicht herausfinden, welchen Schlüssel Alice und Bob vereinbart haben. Trotzdem ist die große Zahl von möglichen Schlüsseln keine Garantie für die Sicherheit des Permutationskryptosystems. Wir werden später in Abschnitt 2.6 sehen, dass monoalphabetische Kryptosysteme leicht zu knacken sind.

2.2 Modulare Arithmetik

Der Witz in der Kryptografie besteht darin, an die Elemente der Klartextmenge $\mathcal{P}$ nicht nur als Elemente einer endlichen Menge zu denken, sondern sich vorzustellen, dass $\mathcal{P}$ und $\mathcal{C}$ mit einer mathematischen Struktur versehen sind. Wir stellen uns also vor, dass $\mathcal{P}$ und $\mathcal{C}$ enthalten sind in einer endlichen Gruppe oder einem endlichen Ring oder einem endlichen Körper. In vielen Beispielen werden wir uns $\mathcal{P}$ als endlichen Ring, genauer, als Ring $\mathbb{Z}/26\mathbb{Z}$, vorstellen. Die Ringe $\mathbb{Z}/m\mathbb{Z},\ m > 1$, haben Sie in der Linearen Algebra I kennengelernt. Wir werden sie in diesem Abschnitt wiederholen, denn wir wollen gleichzeitig noch etwas Notation festlegen.

2.2.1 Definition Seien a und b ganze Zahlen, und sei m eine positive ganze Zahl. Wir schreiben $a \equiv b (\bmod m)$, wenn m die Zahl $b - a$ teilt.

Der Satz „$a \equiv b (\bmod m)$“ wird gelesen als „a ist kongruent zu b, modulo m“. Die Zahl m wird der **Modulus** genannt.

Teilen wir a und b durch m mit Rest, so erhalten wir $a = q_1 m + r_1$ und $b = q_2 m + r_2$, wobei $q_1, q_2 \in \mathbb{Z}$ und $0 \leq r_1, r_2 \leq m - 1$ sind. Dann gilt:

2.2.2 Bemerkung $a \equiv b (\bmod m)$ genau dann, wenn $r_1 = r_2$ ist.

Beweis:

$\Rightarrow$ Sei $a \equiv b (\bmod m)$. Dann gibt es eine ganze Zahl x, so dass $b - a = xm$. Setzen wir nun für b und a ein, so folgt $q_2 m + r_2 - q_1 m - r_1 = xm$. Wir formen um und erhalten $(q_2 - q_1 - x)m = r_1 - r_2$. Die Zahl $r_1 - r_2$ ist also durch m teilbar. Da r_1 und r_2 zwischen 0 und $m - 1$ liegen, ist $r_1 - r_2$ eine Zahl, deren Betrag zwischen 0 und $m - 1$ liegt. So eine Zahl kann aber nur dann durch m teilbar sein, wenn sie 0 ist. Also $r_1 - r_2 = 0$, und damit $r_1 = r_2$.

$\Leftarrow$ Für die andere Implikation nehmen wir an, dass $r_1 = r_2$ ist. Dann gilt: $b - a = q_2 m - q_1 m = m(q_1 - q_2)$. Die Zahl m teilt also $b - a$, oder, anders ausgedrückt, $a \equiv b (\bmod m)$.

□

2.2.3 Notation Wenn a durch m mit Rest geteilt wird, also $a = q_1 m + r_1,\ 0 \leq r_1 \leq m - 1$ und $q_1 \in \mathbb{Z}$, so bezeichnet man den Rest r_1 mit $a \bmod m$.

Es ist also $a = q_1 m + a \bmod m$. Die Bemerkung oben besagt gerade, dass $a \equiv b (\bmod m)$ genau dann, wenn $a \bmod m = b \bmod m$.

2.2.4 Definition Wenn wir a durch $a \bmod m$ ersetzen, sagen wir, dass a **reduziert wird** modulo m.

2.2.5 Aufgabe Reduzieren Sie folgende Zahlen modulo 1234. Benutzen Sie dabei den Taschenrechner modulo n, den Sie in der virtuellen Universität zu diesem Kurs finden.

1. $x = -34579$
2. $x = 4711$
3. $x = 7002 \cdot 1489$
4. $x = 12^{64}$

2.2.6 Bemerkung Für alle $a, b \in \mathbb{Z}$ gilt

$$(a + b) \bmod m = (a \bmod m + b \bmod m) \bmod m$$

und

$$(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m.$$

Beweis: Sei $a = xm + a \bmod m$, und $b = ym + b \bmod m$. Dann folgt:

$$\begin{aligned}(a + b) \bmod m &= ((x + y)m + a \bmod m + b \bmod m) \bmod m \\ &= (a \bmod m + b \bmod m) \bmod m\end{aligned}$$

und

$$\begin{aligned}(ab) \bmod m &= ((xym + xr_2 + yr_1)m + a \bmod m \cdot b \bmod m) \bmod m \\ &= ((a \bmod m)(b \bmod m)) \bmod m.\end{aligned}$$

Hier sind $r_1 = a \bmod m$ und $r_2 = b \bmod m$. □

Diese banale Tatsache macht Computern das Leben leichter. Wenn aufwändige Rechnungen gemacht und dann modulo m reduziert werden sollen, können wir bei jedem Rechenschritt modulo m reduzieren und weitermachen. Dabei müssen wir (und der Rechner) mit kleineren Zahlen umgehen.

Das Rechnen in $\mathbb{Z}/m\mathbb{Z}$ lässt sich mit diesen Begriffen nun einfach formulieren: Es ist $\mathbb{Z}/m\mathbb{Z} = \{0, \ldots, m - 1\}$ zusammen mit zwei Verknüpfungen $+$ und $\cdot$. Diese funktionieren genauso wie die Addition und die Multiplikation in $\mathbb{Z}$, nur dass das Ergebnis reduziert wird modulo m.

2.2.7 Aufgabe Sind die folgenden Rechnungen in $\mathbb{Z}/45891\mathbb{Z}$ richtig?

1. $-34701 + 1284566 = -35083$
2. $-34701 + 1284566 = 240263$
3. $-34701 + 1284566 = 11190 + 45509$

In der Linearen Algebra I haben Sie gesehen, dass $\mathbb{Z}/m\mathbb{Z}$ ein Ring ist. Das neutrale Element der Addition ist 0, und zu $a \in \mathbb{Z}/m\mathbb{Z}$, $a \neq 0$ ist $m-a$ das additive Inverse zu a, denn $(a + m - a) \bmod m = m \bmod m = 0$. Das additive Inverse zu 0 ist natürlich 0.

Wie üblich schreiben wir für das additive Inverse von a einfach $-a$, und statt $b + (-a)$ schreiben wir $b - a$.

Den Ausdruck $b-a$ in $\mathbb{Z}/m\mathbb{Z}$ können wir auf zwei Arten ausrechnen: Wir berechnen $b+m-a$ und reduzieren modulo m, oder wir berechnen $b-a$ in $\mathbb{Z}$ und reduzieren modulo m.

2.2.8 Beispiel 11 - 18 soll in $\mathbb{Z}/31\mathbb{Z}$ berechnet werden.

$11 - 18 = 11 + 31 - 18 = 11 + 13 = 24$ in $\mathbb{Z}/31\mathbb{Z}$.

$11 - 18 = -7$ in $\mathbb{Z}$, und $-7 \bmod 31 = 24$.

2.3 Das Verschiebe-Kryptosystem

Wir ordnen den Buchstaben a, b, ..., y, z Zahlen aus $\mathbb{Z}/26\mathbb{Z}$ zu:

2.3.1 Tabelle der numerischen Äquivalente zu Buchstaben:

a $\leftrightarrow$ 0	n $\leftrightarrow$ 13
b $\leftrightarrow$ 1	o $\leftrightarrow$ 14
c $\leftrightarrow$ 2	p $\leftrightarrow$ 15
d $\leftrightarrow$ 3	q $\leftrightarrow$ 16
e $\leftrightarrow$ 4	r $\leftrightarrow$ 17
f $\leftrightarrow$ 5	s $\leftrightarrow$ 18
g $\leftrightarrow$ 6	t $\leftrightarrow$ 19
h $\leftrightarrow$ 7	u $\leftrightarrow$ 20
i $\leftrightarrow$ 8	v $\leftrightarrow$ 21
j $\leftrightarrow$ 9	w $\leftrightarrow$ 22
k $\leftrightarrow$ 10	x $\leftrightarrow$ 23
l $\leftrightarrow$ 11	y $\leftrightarrow$ 24
m $\leftrightarrow$ 12	z $\leftrightarrow$ 25

Das numerische Äquivalent zu dem Wort

a m p e l

ist dann

$$[0, 12, 15, 4, 11].$$

Das Verschiebe-Kryptosystem ist nun durch folgende Daten gegeben:

2.3.2 Definition Im **Verschiebe-Kryptosystem** sind $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}/26\mathbb{Z}$, und für alle $K \in \mathcal{K}$ sind
$e_K : \mathcal{P} \to \mathcal{C},\ e_K(x) = x + K$, und $d_K : \mathcal{C} \to \mathcal{P}, d_K(y) = y - K$.

Alle Rechnungen sind natürlich in $\mathbb{Z}/26\mathbb{Z}$.

2.3.3 Beispiel Alice und Bob vereinbaren zu einem Zeitpunkt, an dem sie sich sicher fühlen, Nachrichten nach dem Verschiebe-Kryptosystem zu übermitteln und wählen 11 als Schlüssel. Zu einem späteren Zeitpunkt möchte Alice an Bob die Botschaft

w i r s e h e n u n s u m m i t t e r n a c h t

schicken. Sie übersetzt den Text in sein numerisches Äquivalent:

$$[22, 8, 17, 18, 4, 7, 4, 13, 20, 13, 18, 20, 12, 12, 8, 19, 19, 4, 17, 13, 0, 2, 7, 19]$$

Dann addiert sie zu jedem Eintrag 11 und reduziert modulo 26. Dies ergibt:

$$[7, 19, 2, 3, 15, 18, 15, 24, 5, 24, 3, 5, 23, 23, 19, 4, 4, 15, 2, 24, 11, 13, 18, 4].$$

Diesen Zahlenstring überführt sie in sein alphabetisches Äquivalent.

h t c d p s p y f y d f x x t e e p c y l n s e

Diesen Text schickt sie an Bob.

Bob übersetzt den Text in sein numerisches Äquivalent

$$[7, 19, 2, 3, 15, 18, 15, 24, 5, 24, 3, 5, 23, 23, 19, 4, 4, 15, 2, 24, 11, 13, 18, 4],$$

subtrahiert in $\mathbb{Z}/26\mathbb{Z}$ von jedem Eintrag 11, beziehungsweise addiert $15 = -11$ zu jedem Eintrag und erhält

$$[22, 8, 17, 18, 4, 7, 4, 13, 20, 13, 18, 20, 12, 12, 8, 19, 19, 4, 17, 13, 0, 2, 7, 19].$$

Zurückübersetzt in Buchstaben ergibt sich der Klartext.

Die Schlüsselmenge $\mathcal{K}$ ist $\mathbb{Z}/26\mathbb{Z}$; es gibt also beim Verschiebe-Kryptosystem nur 26 Schlüssel. Das sind natürlich viel zu wenig. Wenn Oscar eine Nachricht abfängt, muss er nur systematisch probieren. Er übersetzt den Text in sein numerisches Äquivalent $[x_1, \ldots, x_r]$. Dann bildet er $[x_1 + 1, \ldots x_r + 1]$ und übersetzt in Buchstaben. Ergibt dies einen Sinn, wird es wahrscheinlich der Klartext gewesen sein. Andernfalls bildet er $[x_1 + 2, \ldots, x_r + 2]$ und übersetzt in Buchstaben. Dies iteriert er bis er den Klartext gefunden hat.

2.3.4 Aufgabe Welcher Klartext verbirgt sich hinter folgender Nachricht?

o e a p q j a o e i i a n s e a z a n

Geheimschriften des Verschiebe-Kryptosystems nennt man auch Cäsar. Und das aus naheliegendem Grund, denn Cäsar benutzte zur Übermittlung seiner geheimen Nachrichten das Verschiebe-Kryptosystem mit dem Schlüssel 23. Nachlesen kann man dies in [Su], für die Nicht-Lateiner hier eine freie Übersetzung nach [Beu]. „Es existieren auch Briefe von Cäsar an Cicero und an Bekannte über Dinge, in denen er, wenn etwas vertraulich übermittelt werden musste, in Geheimschrift schrieb. Das heißt, er veränderte die Ordnung der Buchstaben derart, dass kein einziges Wort mehr ausgemacht werden konnte. Wenn jemand das entziffern und den Inhalt erkennen wollte, so musste er den vierten Buchstaben des Alphabets, also D, für A einsetzen, und so mit den anderen.“

2.4 Der Euklidische Algorithmus

Beim Verschiebe-Kryptosystem haben wir das Buchstaben-Alphabet mit den Elementen von $\mathbb{Z}/26\mathbb{Z}$ identifiziert und die Ringstruktur von $\mathbb{Z}/26\mathbb{Z}$ dazu benutzt,

Chiffrierungs- und Dechiffrierungsregeln zu definieren. Allerdings haben wir nur benutzt, dass wir in $\mathbb{Z}/26\mathbb{Z}$ eine Addition zur Verfügung haben. Wie gut eignet sich die Multiplikation in $\mathbb{Z}/26\mathbb{Z}$ zum Chiffrieren? Machen wir ein

2.4.1 Beispiel Wir wählen $6 \in \mathbb{Z}/26\mathbb{Z}$ und definieren

$$f : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z} \text{ durch } f(x) = 6x \bmod 26 \text{ für alle } x \in \mathbb{Z}/26\mathbb{Z}.$$

Betrachten wir explizit, auf welche Elemente die Zahlen in $\mathbb{Z}/26\mathbb{Z}$ durch f abgebildet werden:

$$\begin{array}{lllll} f(0) = 0, & f(1) = 6, & f(2) = 12, & f(3) = 18, & f(4) = 24, \\ f(5) = 4, & f(6) = 10, & f(7) = 16, & f(8) = 22, & f(9) = 2, \\ f(10) = 8, & f(11) = 14, & f(12) = 20, & f(13) = 0, & f(14) = 6, \\ f(15) = 12, & f(16) = 18, & f(17) = 24, & f(18) = 4, & f(19) = 10, \\ f(20) = 16, & f(21) = 22, & f(22) = 2, & f(23) = 8, & f(24) = 14, \\ f(25) = 20. & & & & \end{array}$$

Wir sehen, dass $f(0) = f(13) = 0$, und $f(1) = f(14) = 6$, und $f(2) = f(15) = 12$, und so weiter. Insbesondere ist die Abbildung f nicht injektiv, und Bob hat keine Möglichkeit, zu entscheiden, ob er die Zahl 6 als 1 oder als 14 rückübersetzen muss. Zum Chiffrieren ist die Abbildung f also denkbar ungeeignet.

2.4.2 Beispiel Wir wählen $5 \in \mathbb{Z}/26\mathbb{Z}$ und definieren

$$g : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z} \text{ durch } g(x) = 5x \bmod 26 \text{ für alle } x \in \mathbb{Z}/26\mathbb{Z}.$$

Dann gilt:

$$\begin{array}{lllll} g(0) = 0, & g(1) = 5, & g(2) = 10, & g(3) = 15 & g(4) = 20, \\ g(5) = 25, & g(6) = 4, & g(7) = 9, & g(8) = 14 & g(9) = 19, \\ g(10) = 24, & g(11) = 3, & g(12) = 8, & g(13) = 13 & g(14) = 18, \\ g(15) = 23, & g(16) = 2, & g(17) = 7, & g(18) = 12 & g(19) = 17, \\ g(20) = 22, & g(21) = 1, & g(22) = 6, & g(23) = 11 & g(24) = 16, \\ g(25) = 21. & & & & \end{array}$$

Wir sehen, dass g injektiv ist, dass sich die Abbildung g also durchaus zum Chiffrieren eignen würde.

Welche $a \in \mathbb{Z}/m\mathbb{Z}$ wir wählen dürfen, damit die Abbildung $g : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ mit $g(x) = ax \bmod m$ für alle $x \in \mathbb{Z}/m\mathbb{Z}$, injektiv (also bijektiv) ist, wird Thema dieses Abschnitts sein.

2.4.3 Definition Seien a, b ganze Zahlen, die nicht beide Null sind. Eine natürliche Zahl d heißt **größter gemeinsamer Teiler** von a und b (abgekürzt $\mathrm{ggT}(a, b)$), falls die folgenden beiden Eigenschaften gelten:

(i) d teilt a und d teilt b (wir schreiben dafür $d|a$ und $d|b$) und

(ii) wenn c eine ganze Zahl ist, die a und b teilt, dann teilt sie auch d.

2.4.4 Beispiel Sei $a = 210$, und sei $b = -2002$. Die ganzen Zahlen, die a und b teilen, sind

$$-14, -7, -2, -1, 1, 2, 7, 14$$

Die Zahlen $-14, -7, -2$ und -1 kommen als größte gemeinsame Teiler nicht in Frage, denn ein ggT ist per Definition immer positiv. Die Zahl 14 ist positiv, teilt 210 und -2002 und wird von allen Teilern von 210 und -2002 geteilt. Sie ist also ein größter gemeinsamer Teiler von 210 und -2002. Die Zahlen 1, 2 und 7 sind zwar positive Teiler von 210 und -2002, sie werden aber von -14 und 14 nicht geteilt, sind also keine größten gemeinsamen Teiler von 210 und -2002. Wir sehen also: die Zahlen 210 und -2002 besitzen einen größten gemeinsamen Teiler, und dieser ist eindeutig, denn nur 14 ist positiv und erfüllt die Eigenschaften (i) und (ii) der Definition.

Dies liegt natürlich nicht an der speziellen Wahl der Zahlen, wie Sie bereits in der zweiten Kurseinheit der Linearen Algebra I gesehen haben. Wir wiederholen hier, teilweise ohne Beweis, die wichtigsten Ergebnisse.

2.4.5 Bemerkung Seien $a, b \in \mathbb{Z}$ ganze Zahlen, die nicht beide 0 sind. Angenommen, a und b besitzen einen größten gemeinsamen Teiler. Dann ist dieser eindeutig bestimmt.

Beweis: Lineare Algebra I, Kurseinheit 2. □

Die Bemerkung besagt, dass, wenn a und b einen größten gemeinsamen Teiler haben, dieser eindeutig ist. Wir werden also in Zukunft immer von **dem** größten gemeinsamen Teiler von a und b sprechen.

Der folgende Satz besagt, dass diese Annahme immer erfüllt ist (sofern a und b nicht beide 0 sind), und der Beweis liefert einen Algorithmus, wie wir $\mathrm{ggT}(a, b)$ finden können. Die zentrale Idee des Beweises stellen wir als Lemma voraus.

2.4.6 Lemma Seien $x, y \in \mathbb{Z}$, und sei $x \neq 0$. Wir teilen y durch x mit Rest, also $y = qx + r$ mit $q \in \mathbb{Z}$ und $0 \leq r < |x|$. Falls $\mathrm{ggT}(r, x) = d$, so existiert $\mathrm{ggT}(x, y)$ und $\mathrm{ggT}(x, y) = \mathrm{ggT}(x, r) = d$.

Beweis: Lineare Algebra I, Kurseinheit 2. □

2.4.7 Satz Zu zwei ganzen Zahlen a und b, die nicht beide 0 sind, gibt es einen größten gemeinsamen Teiler.

Beweis: (**Euklidischer Algorithmus**)

Sei ohne Einschränkung $a \neq 0$. Dividiere b durch a mit Rest: $b = q_1 a + r_1$, mit $0 \leq r_1 < |a|$. Falls $r_1 = 0$, so ist $|a| = \mathrm{ggT}(a, 0) = \mathrm{ggT}(a, b)$ mit dem Lemma oben. Falls $r_1 \neq 0$, dividiere a durch r_1 mit Rest: $a = q_2 r_1 + r_2,\ 0 \leq r_2 < r_1$. Falls $r_2 = 0$, ist $r_1 = \mathrm{ggT}(r_1, 0) = \mathrm{ggT}(r_1, a) = \mathrm{ggT}(a, b)$ mit dem Lemma. Falls $r_2 \neq 0$ dividieren wir r_1 durch r_2 mit Rest, und so weiter. Wir erhalten eine absteigende Folge von Resten $|a| > r_1 > r_2 > \cdots \geq 0$, und da es nur endlich viele positive Zahlen zwischen $|a|$ und 0 gibt, gibt es ein $n \geq 1$, so dass $r_n \neq 0$ und $r_{n+1} = 0$ ist. Mit dem Lemma gilt:

$$r_n = \mathrm{ggT}(r_n, 0) = \mathrm{ggT}(r_{n-1}, r_n) = \cdots = \mathrm{ggT}(r_1, a) = \mathrm{ggT}(a, b).$$

□

2.4.8 Beispiel Wir wissen bereits, dass $\mathrm{ggT}(210, -2002) = 14$ ist und errechnen dieses Ergebnis erneut mit dem Euklidischen Algorithmus:

$$\begin{array}{rcrcrcl} -2002 & = & -10 \cdot 210 + 98 & , & r_1 & = & 98 \\ 210 & = & 2 \cdot 98 + 14 & , & r_2 & = & 14 \\ 98 & = & 7 \cdot 14 & , & r_3 & = & 0 \end{array}$$

Das r_n des Euklidischen Algorithmus ist hier $r_2 = 14 = \mathrm{ggT}(210, -2002)$. In diesem Beispiel hatten wir $b = -2002$ und $a = 210$ gesetzt. Wir hätten dies auch umgekehrt machen können, also $a = -2002$ und $b = 210$:

$$\begin{array}{rcrcrcl} 210 & = & 0 \cdot (-2002) + 210 & , & r_1' & = & 210 < |-2002| \\ -2002 & = & -10 \cdot 210 + 98 & , & r_2' & = & 98 \\ 210 & = & 2 \cdot 98 + 14 & , & r_3' & = & 14 \\ 98 & = & 7 \cdot 14 & , & r_4' & = & 0 \end{array}$$

Das r_n des Euklidischen Algorithmus ist hier $r_3' = 14 = \mathrm{ggT}(210, -2002)$.

Der folgende Satz, dessen Beweis wieder ein Algorithmus ist, ist in der Kryptografie sehr wichtig.

2.4.9 Satz Seien $a, b \in \mathbb{Z}$ und sei $d = \mathrm{ggT}(a, b)$. Dann gibt es ganze Zahlen s und t, so dass $d = sa + tb$ ist.

Beweis: (**Erweiterter Euklidischer Algorithmus**)

Sei $a \neq 0$. Falls $b = q_1 a$ mit $q_1 \in \mathbb{Z}$, so ist $|a| = \mathrm{ggT}(a, b)$. Dann sind $t = 0$ und $s = 1$ oder $s = -1$ die gesuchten Zahlen. Andernfalls führen wir den Euklidischen Algorithmus durch und erhalten die Gleichungen:

$$\begin{array}{rcll} b & = & q_1 a + r_1 & , \quad 0 < r_1 < |a| \\ a & = & q_2 r_1 + r_2 & , \quad 0 < r_2 < r_1 \\ r_1 & = & q_3 r_2 + r_3 & , \quad 0 < r_3 < r_2 \\ & & \vdots & \\ r_{n-2} & = & q_n r_{n-1} + r_n & , \quad 0 < r_n < r_{n-1} \\ r_{n-1} & = & q_{n+1} r_n & \end{array}$$

Es ist $r_n = \mathrm{ggT}(a, b) = d$. Wir stellen die Gleichung um:

$$\begin{array}{rcl} r_1 & = & b - q_1 a \\ r_2 & = & a - q_2 r_1 \\ r_3 & = & r_1 - q_3 r_2 \\ & & \vdots \\ r_n & = & r_{n-2} - q_n r_{n-1} \end{array}$$

Wir zeigen mit Induktion, dass für alle $1 \leq i \leq n$ gilt: $r_i = s_i a + t_i b$ für gewisse ganze Zahlen s_i und t_i. Für r_1 und r_2 ist dies richtig, setze $s_1 = -q_1$ und $t_1 = 1$, und Einsetzen von r_1 in die Gleichung $r_2 = a - q_2 r_1$ liefert $s_2 = 1 + q_2 q_1$ und $t_2 = -q_2$.

Für den Induktionsschritt sei $1 < i < n$. Es ist $r_{i+1} = r_{i-1} - q_{i+1} r_i$. Nach Induktionsvoraussetzung sind $r_{i-1} = s_{i-1} a + t_{i-1} b$ und $r_i = s_i a + t_i b$. Setzen wir dies in die Gleichung $r_{i+1} = r_{i-1} - q_{i+1} r_i$ ein, so erhalten wir $r_{i+1} = (s_{i-1} - q_{i+1} s_i) a + (t_{i-1} - q_{i+1} t_i) b$. Wir setzen nun $s_{i+1} = s_{i-1} - q_{i+1} s_i$ und $t_{i+1} = t_{i-1} - q_{i+1} t_i$. Die gesuchten Zahlen s und t sind dann $s = s_n$ und $t = t_n$. □

2.4.10 Beispiel Wir suchen ganze Zahlen s und t so, dass $14 = s210 + t(-2002)$ ist.

Der Euklidische Algorithmus lieferte

$$\begin{array}{rcll} -2002 & = & -10 \cdot 210 + 98 & , \quad r_1 = 98 \\ 210 & = & 2 \cdot 98 + 14 & , \quad r_2 = 14 = \mathrm{ggT}(a, b). \end{array}$$

Wir stellen um:

$$\begin{array}{rcl} 98 & = & -2002 + 10 \cdot 210 \\ 14 & = & 210 - 2 \cdot 98 \end{array}$$

Wir setzen die erste Gleichung in die zweite ein:

$$\begin{aligned} 14 &= 210 - 2(-2002 + 10 \cdot 210) = \\ &= -19 \cdot 210 - 2(-2002). \end{aligned}$$

Zahlen s und t, die die Behauptung des Satzes erfüllen, sind also $s = -19$ und $t = -2$.

Auch $s' = 1983$ und $t' = 208$ erfüllen die Gleichung $14 = s'210 + t'(-2002)$. Allerdings hat auch niemand behauptet, dass die Zahlen s und t des Satzes eindeutig sind.

2.4.11 Aufgabe Bestimmen Sie den größten gemeinsamen Teiler von $a = 7356$ und $b = 2112$ und ganze Zahlen s und t mit $\mathrm{ggT}(a, b) = sa + tb$. Überprüfen Sie Ihre Rechnung mit dem Taschenrechner modulo n in der VU.

Wir wollen einige wichtige Folgerungen aus den Sätzen 2.4.7 und 2.4.9 festhalten.

2.4.12 Korollar Sei $a \in \mathbb{Z}/m\mathbb{Z},\ m > 1$. Genau dann gibt es ein $a' \in \mathbb{Z}/m\mathbb{Z}$ mit $aa' \bmod m = 1$, wenn $\mathrm{ggT}(a, m) = 1$.

Beweis: Lineare Algebra I, Kurseinheit 2. □

Wichtig ist Folgendes! Wenn $\mathrm{ggT}(a, m) = 1$, so kann man $a' \in \mathbb{Z}/m\mathbb{Z}$ mit $(aa') \bmod m = (a'a) \bmod m = 1$ ganz einfach berechnen (oder berechnen lassen). Man bestimmt s und t so, dass $sa + tm = 1$ sind. Dies geschieht mit Hilfe des erweiterten Euklidischen Algorithmus 2.4.9. Dann reduziert man s modulo m und setzt $a' = s \bmod m$.

2.4.13 Korollar Seien $a, b, d \in \mathbb{Z}$, und es gelte $d|ab$ und $\mathrm{ggT}(d, a) = 1$. Dann gilt $d|b$.

Beweis: Laut 2.4.9 gibt es ganze Zahlen s und t, so dass $sd + ta = 1$. Wir multiplizieren die Gleichung mit b und erhalten $sdb + tab = b$. Nach Voraussetzung teilt d die linke Seite der Gleichung, also auch die rechte. Damit gilt $d|b$. □

2.4.14 Korollar Seien $a, b, c \in \mathbb{Z}$, und es gelte $a|c$ und $b|c$. Wenn $\mathrm{ggT}(a, b) = 1$, so folgt $ab|c$.

Beweis: Sei $c = ax = by$ für $x, y \in \mathbb{Z}$. Da $b|by$, folgt $b|ax$. Da $ggT(a, b) = 1$ folgt $b|x$, also $ab|c$. □

2.4.15 Korollar Seien $a, b \in \mathbb{Z}$, und sei $p \in \mathbb{N}$ eine Primzahl. Wenn p ein Teiler von ab ist, so gilt $p|a$ oder $p|b$.

Beweis: Sei p ein Teiler von ab. Da p eine Primzahl ist, gilt $\mathrm{ggT}(p, a) = p$ oder $\mathrm{ggT}(p, a) = 1$. Im ersten Fall ist p ein Teiler von a, im zweiten Fall ist p mit Korollar 2.4.13 ein Teiler von b. □

Wir kommen nun zur Ausgangsfrage dieses Kapitels zurück:

2.4.16 Korollar Sei $a \in \mathbb{Z}/m\mathbb{Z}$, und sei $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ definiert durch $f(x) = (ax) \bmod m$. Die Abbildung f ist genau dann injektiv, wenn $\mathrm{ggT}(a, m) = 1$ ist.

Beweis:

⇒ Sei $\mathrm{ggT}(a, m) = d > 1$. Dann gibt es ein $0 \neq s \in \mathbb{Z}/m\mathbb{Z}$ mit $sd = m$ und ein $t \in \mathbb{Z}/m\mathbb{Z}$ mit $td = a$. Dann gilt

$$\begin{aligned} f(s) = as \bmod m &= tds \bmod m \\ &= tm \bmod m = 0. \end{aligned}$$

Also $f(s) = f(0) = 0$, das heißt, f ist nicht injektiv.

⇐ Sei $\mathrm{ggT}(a, m) = 1$. Seien $x, y \in \mathbb{Z}/m\mathbb{Z}$ mit $ax \bmod m = ay \bmod m$. Mit der Bemerkung 2.2.2 folgt $ax \equiv ay (\mathrm{mod} m)$. Sei $a' \in \mathbb{Z}/m\mathbb{Z}$ so, dass $a'a \bmod m = 1$. Ein solches a' existiert, da $\mathrm{ggT}(a, m) = 1$. Dann gilt $a'ax \equiv a'ay (\bmod m)$, und wieder mit der Bemerkung 2.2.2 folgt $a'ax \bmod m = a'ay \bmod m$, also $x \bmod m = y \bmod m$. Da $x, y \in \mathbb{Z}/m\mathbb{Z}$, folgt $x = y$, also ist f injektiv.

□

2.4.17 Definition Seien $a, b \in \mathbb{Z}$. Wenn $\mathrm{ggT}(a, b) = 1$, so nennt man a und b **teilerfremd**.

2.4.18 Beispiel Korollar 2.4.16 beantwortet die Frage, für welche $a \in \mathbb{Z}/26\mathbb{Z}$ die Abbildung $f : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}$ mit $f(x) = ax \bmod 26$ injektiv ist. Die Zahlen a und 26 müssen teilerfremd sein. Die zu 26 teilerfremden Zahlen in $\mathbb{Z}/26\mathbb{Z}$ sind $1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$.

2.5 Das affine Kryptosystem

Wir beginnen mit einer Verallgemeinerung von Korollar 2.4.16 im letzten Abschnitt.

2.5.1 Proposition Seien $a, b \in \mathbb{Z}/m\mathbb{Z}$ und sei $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ definiert durch $f(x) = (ax + b) \bmod m$. Die Abbildung f ist genau dann injektiv, wenn $\mathrm{ggT}(a, m) = 1$ ist.

Beweis: Die Abbildung f ist die Komposition der Abbildungen $g : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, mit $g(x) = ax \bmod m$ und $h : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, mit $h(x) = (x + b) \bmod m$ für alle $x \in \mathbb{Z}/m\mathbb{Z}$. Dann gilt $f = h \circ g$, denn

$$\begin{aligned} f(x) &= h(g(x)) = h(ax \bmod m) = (ax \bmod m + b) \bmod m \\ &= (ax + b) \bmod m. \end{aligned}$$

Die Abbildung h ist injektiv, und $h \circ g = f$ ist genau dann injektiv, wenn g injektiv ist. Dies ist genau dann der Fall, wenn $\mathrm{ggT}(a, m) = 1$ ist. □

Seien $a, b \in \mathbb{Z}/m\mathbb{Z}$ und sei $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},\ f(x) = (ax + b) \bmod m$, injektiv. Dann ist f bijektiv, und es gibt eine zu f inverse Abbildung f^{-1}. Diese ist folgendermaßen definiert: $f^{-1} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},\ f^{-1}(x) = (a'x - a'b) \bmod m$, wobei $a'a \bmod m = aa' \bmod m = 1$ ist, denn es gilt für alle $x \in \mathbb{Z}/m\mathbb{Z}$:

$$\begin{aligned} f^{-1}(f(x)) &= f^{-1}((ax + b) \bmod m) &&= (a'(ax + b) - a'b) \bmod m \\ &= x, \text{ und} \\ f(f^{-1}(x)) &= f((a'x - a'b) \bmod m) &&= (a(a'x - a'b) + b) \bmod m \\ &= x. \end{aligned}$$

Sei $(\mathbb{Z}/m\mathbb{Z})^\times = \{a \in \mathbb{Z}/m\mathbb{Z} \,|\mathrm{ggT}(a, m) = 1\}$ die Menge der invertierbaren Elemente des Ringes $\mathbb{Z}/m\mathbb{Z}$. Sie haben in der Linearen Algebra I, Kurseinheit 2 gesehen, dass $(\mathbb{Z}/m\mathbb{Z})^\times$ mit der Multiplikation in $\mathbb{Z}/m\mathbb{Z}$ eine Gruppe bildet. Wir werden auf diese Gruppen in 4.4 näher eingehen.

2.5.2 Notation Ist $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, so bezeichnen wir mit a^{-1} das zu a inverse Element in $\mathbb{Z}/m\mathbb{Z}$.

2.5.3 Beispiel Wir hatten die zu 26 teilerfremden Zahlen in Beispiel 2.4.18 bestimmt, es ist also

$$(\mathbb{Z}/26\mathbb{Z})^\times = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\},$$

und $|(\mathbb{Z}/26\mathbb{Z})^\times| = 12$.

Wir können nun das affine Kryptosystem definieren.

2.5.4 Definition Im **affinen Kryptosystem** sind $\mathcal{P} = \mathcal{C} = \mathbb{Z}/26\mathbb{Z}$, und $\mathcal{K} = (\mathbb{Z}/26\mathbb{Z})^\times \times \mathbb{Z}/26\mathbb{Z}$. Zu $K = (a, b) \in \mathcal{K}$ sei

$$\begin{array}{rcl} e_K & : & \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z} \quad , \quad e_K(x) = (ax + b) \bmod 26 \text{ und} \\ d_K & : & \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z} \quad , \quad d_K(y) = a^{-1}(y - b) \bmod 26. \end{array}$$

2.5.5 Beispiel Alice und Bob vereinbaren, Nachrichten mit Hilfe des affinen Kryptosystems zu übermitteln und wählen als Schlüssel $K = (3, 12)$.

Alice will an Bob die Nachricht h e u t e n i c h t senden. Sie bildet das numerische Äquivalent zu der Nachricht, also $[7, 4, 20, 19, 4, 13, 8, 2, 7, 19]$. Sie berechnet zu jeder Zahl x die Zahl $(3x + 12) \bmod 26$, also $[7, 24, 20, 17, 24, 25, 10, 18, 7, 17]$, und übersetzt diese Zahlenfolge in ihr alphabetisches Äquivalent, also h y u r y z k s h r. Dieses sendet sie an Bob.

Das numerische Äquivalent zu h y u r y z k s h r ist $[7, 24, 20, 17, 24, 25, 10, 18, 7, 17]$. Bob berechnet mit Hilfe des erweiterten Euklidischen Algorithmus s und t so, dass $s3 + t26 = 1$ ist, also etwa $s = 9,\ t = -1$. Es ist $3^{-1} = 9$ in $\mathbb{Z}/26\mathbb{Z}$. Nun berechnet er für jede Zahl x die Zahl $9(x-12) \bmod 26 = 9(x+14) \bmod 26 = (9x+22) \bmod 26$:

$$\begin{array}{rcl} (9 \cdot 7 + 22) \bmod 26 & = & 7 \\ (9 \cdot 24 + 22) \bmod 26 & = & 4 \\ (9 \cdot 20 + 22) \bmod 26 & = & 20 \\ & \vdots & \\ (9 \cdot 17 + 22) \bmod 26 & = & 19. \end{array}$$

Wenn er die Zahlenfolge $[7, 4, 20, 19, 4, 13, 8, 2, 7, 19]$ in ihr alphabetisches Äquivalent übersetzt, erhält er die Klartextbotschaft.

2.5.6 Aufgabe Sie sind Bob. Sie haben mit Alice den Schlüssel $(7, 18)$ abgesprochen, und Sie erhalten die Nachricht

f w u c f n f w y y u h

Was möchte Alice Ihnen sagen?

Berechnen wir abschließend wie viele Schlüssel wir beim affinen Kryptosystem zur Verfügung haben. Die Mächtigkeit $|\mathcal{K}|$ der Schlüsselmenge ist $|(\mathbb{Z}/26\mathbb{Z})^\times \times \mathbb{Z}/26\mathbb{Z}| = 12 \cdot 26 = 312$. Dies ist für die brutale Methode der Kryptoanalyse, das systematische Ausprobieren, schon eine ziemlich große Zahl, allerdings für den Rechner eine zu kleine. Es gibt aber geschicktere Möglichkeiten der Kryptoanalyse, wie wir im folgenden Abschnitt sehen werden.

Das Verschiebe-Kryptosystem ist übrigens ein Spezialfall des affinen Kryptosystems. Die Zahl $a \in (\mathbb{Z}/26\mathbb{Z})^\times$ ist $a = 1$.

2.6 Kryptoanalyse monoalphabetischer Kryptosysteme

In diesem Abschnitt werden wir Oscars Rolle übernehmen. Die Philosophie der Kryptoanalyse wird durch das Prinzip von Kerckhoff beschrieben, der dies 1883 in seinem Buch „La cryptographie militaire“ erstmalig formulierte.

Prinzip von Kerckhoff: Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung der Chiffrierungsregel abhängen, sondern darf nur auf der Geheimhaltung des Schlüssels beruhen.

Mit anderen Worten: Entwickler von Kryptosystemen sollten Oscar ernst nehmen. Man wird die Chiffrierungsregel über kurz oder lang erkennen. Moderne Kryptosysteme wie DES und asymmetrische Kryptosysteme gehen mit Kerckhoffs Prinzip sehr offensiv um. Jeder darf den Chiffrierungsalgorithmus kennen, nur der Schlüssel wird geheim gehalten.

Bei der Kryptoanalyse sieht sich Oscar von Fall zu Fall unterschiedlichen Ausgangssituationen gegenüber. Man unterscheidet folgende Typen von Attacken:

2.6.1 Attacken auf Kryptosysteme:

1. **Known-ciphertext-attack**:

   Oscar kennt ein relativ großes Stück des Geheimtextes.

2. **Known-plaintext-attack**:

   Oscar kennt ein vergleichsweise kleines Stück von zusammengehörigem Klartext und Geheimtext. Dies könnten beispielsweise Standardgrußformeln zu Beginn oder Ende der abgefangenen Nachricht sein.

3. **Chosen-plaintext-attack**: Oscar hat Zugang zu einem Chiffrieralgorithmus und möchte die sich dahinter verbergende Chiffrierungsregel und den Schlüssel erkennen.

2.6.2 Beispiel Es gibt Mailsysteme, bei denen die Möglichkeit zum Chiffrieren von Mails voreingestellt ist. Oscar kann einen Klartext, etwa die Buchstabenfolge e e e e e e .... e e an sich selbst, verschlüsselt, schicken und so versuchen, hinter

den Schlüssel zu kommen. Gelingt ihm dies, kann er später chiffrierte Nachrichten versenden, und vorgeben, ein autorisierter Benutzer des Kryptosystems zu sein.

Wir werden die Kryptoanalyse von monoalphabetischen Geheimschriften unter der schwächsten Annahme, nämlich der einer Known-ciphertext-attack durchführen. Die stehende Annahme dieses Abschnitts ist also die folgende:

Oscar besitzt ein großes Stück des abgefangenen Geheimtextes, von dem er weiß, dass die Klartextnachricht in deutscher Sprache verfasst ist, wobei die Klartextsymbole die 26 Buchstaben (keine Satzzeichen, keine Zwischenräume) sind, und dass das benutzte Kryptosystem monoalphabetisch ist. Wir folgen bei der Beschreibung der Kryptoanalyse im Wesentlichen [Beu].

Jede natürliche Sprache hat ihre Eigenheiten. So werden in einem deutschen Text die Buchstaben e und n am häufigsten auftreten, wohingegen Sie die Buchstaben q, x, y selten finden werden. Genauer, die zehn häufigsten Buchstaben e, n, i, s, r, a, t, d, h, u machen bereits drei Viertel eines Standardtextes in deutscher Sprache aus. Wenn ein deutscher Text mit Hilfe eines monoalphabetischen Kryptosystems verschlüsselt wird, werden diese Spezifika auch im Geheimtext auftreten. Das ist die Basis der Kryptoanalyse. Die folgende Tabelle gibt Ihnen die Häufigkeit der verschiedenen Buchstaben in Prozent an.

2.6.3 Tabelle Buchstabenhäufigkeiten eines deutschen Textes:

Buchstabe	Häufigkeit (in %)	Buchstabe	Häufigkeit (in %)
a	6,51	n	9,78
b	1,89	o	2,51
c	3,06	p	0,79
d	5,08	q	0,02
e	17,4	r	7,00
f	1,66	s	7.27
g	3.01	t	6,15
h	4,76	u	4,35
i	7,55	v	0,67
j	0,27	w	1,89
k	1,21	x	0.03
l	3,44	y	0.04
m	2,53	z	1,13

Wir teilen die Buchstaben in vier Gruppen ein, entsprechend der Häufigkeit ihres Auftretens in einem Text:

2.6.4 Tabelle Prozentualer Anteil von Buchstaben in einem deutschen Text:

Gruppe	Anteil der Buchstaben dieser Gruppe an einem Text
e, n	27,18 %
i, s, r, a, t	34,48 %
d, h, u, l, c, g, m, o, b, w, f, k, z	36,52 %
p, v, j, y, x, q	1,82 %

Die folgende Tabelle listet die häufigsten **Bigramme**, das sind Paare aufeinanderfolgender Buchstaben, in der deutschen Sprache auf:

2.6.5 Tabelle Die häufigsten Bigramme in einem deutschen Text:

Bigramm	Häufigkeit
en	3,88 %
er	3,75%
ch	2,75 %
te	2,26 %
de	2,00 %
nd	1,99 %
ei	1,88 %
ie	1,79 %
in	1,67 %
es	1,52%

Bei der Kryptoanalyse geht Oscar in drei Schritten vor:

(1) Er stellt die Häufigkeiten der Buchstaben des Geheimtextes fest. Damit kann er die Äquivalente der Buchstaben e und n lokalisieren, und welche Menge von Geheimtextbuchstaben der Menge {i, s, r, a, t} von Klartextbuchstaben entspricht. Dabei kann er in der Regel bei den Buchstaben der Gruppe 2 der Tabelle oben noch keine klare Zuordnung zwischen Geheim- und Klartextbuchstaben herstellen. Dazu dient

(2) Oscar zählt die Bigramme, damit kann er die Buchstaben der Gruppe 2 den entsprechenden Geheimtextbuchstaben zuordnen. Nehmen wir etwa an, er kennt die Äquivalente zu e und n, dann kann er den zu r gehörigen Geheimtextbuchstaben leicht ausmachen, denn dieser tritt oft in Verbindung mit dem Äquivalent zu e auf. Das Äquivalent zu i findet er beispielsweise dadurch, dass er die Bigramme mit e mit ihren inversen Bigrammen vergleicht. Die Bigramme ei und ie treten fast gleich oft auf. ea ist selten. Damit kann er a lokalisieren. Außerdem wird ihm die Analyse der Bigramme c und h liefern: Diese sind als

Bigramm häufig, isoliert aber selten. Auf diese Weise kann Oscar die Buchstaben e, n, i, s, r, a, t, h, c identifizieren. Diese bilden zusammen schon zwei Drittel des Gesamttextes.

(3) Oscar setzt die erkannten Buchstaben im Text ein, die noch nicht erkannten werden markiert. Nun ist Oscars Pfiffigkeit gefragt. Vielleicht ist klar, dass irgendwo ein Vokal eingesetzt werden muss. Es bleiben nur noch u und o. Vielleicht tritt häufig _ ie, _ er, _ as auf. Dies liefert d. Nach wenigen Versuchen wird Oscar einen gut lesbaren Text erhalten.

2.6.6 Aufgaben Versetzen Sie sich in die Rolle von Oscar.

1. Sie haben eine Nachricht abgefangen, von der Sie wissen, dass die Verschlüsselung mit Hilfe des Verschiebekryptosystems erfolgte. Buchstaben zählen lässt Sie vermuten, dass der Geheimtextbuchstabe u dem Klartextbuchstaben e entspricht. Wie lautet die Dechiffrierabbildung?

2. Sie haben eine lange Nachricht abgefangen, von der Sie stark vermuten, dass sie mit Hilfe des affinen Kryptosystems verschlüsselt wurde. Buchstabenzählen liefert als häufigsten Buchstaben r und dann g. Welchen Schlüssel hatten Alice und Bob verabredet?

Wir schließen diesen Abschnitt mit einem Beispiel der Kryptoanalyse. (Die einzelnen Schritte der Kryptoanalyse wurden mit dem Computer gemacht.)

2.6.7 Beispiel Oscar hat sich folgenden Geheimtext verschafft:

```
mwokypyzuzvjamzjkeoryzzcxywpylzyuzjyhzhuzvylrxkyluzvokypjkerlmrvmoxcwtmzv
rmezclvlhykzayorbmtyzpyoshtcooyzyeyoyrjjulyllkshruzeykzylbylzuzkxylokrmyrw
krvywokrjkzhmeyzkzqlmbrmwbuyzbryzvyjywpylvyooytpyznmhlyopylkybvmowkzkorylk
uwbuylakooyzoshmbruzvbcloshuzevyzeluyzvuzeomuooshuoovylvkymubpmufhmoypyety
kryzocttryuzvvylokshmuobmshakooyzoshmbrtylzwyvkyzryshzkqylzuzvwyvkyzvkvmqr
kqylzjuomwwyzoyrjryyoemtrykzymurczcwyuzkxylormyrmubjupmuyzvkykhlytyhlyzksh
rwyhlkwhcylommtuzvoywkzmloczvylzkzyloryltkzkyuypylwyvkyzxylwkrrytryaytrayk
rhmrryokshpylykroykzxkytjmhtxczbylzoruvkyzogorywyzkzormttkylrvkyuypylwyvky
zxylwkrrytrytyhlyylwcyetkshryyouzmphmyzekevmxczacvylvkyoruvkylyzvytypruzvm
lpykryrtyhlyjurlmzofclrkylyzwkrvyluypylwyvkyzxylwkrrytryztyhlyaklvmuovylby
lzyykzoytporkzorlukylyzvyovulshflmyoyzjfhmoyzkzoruvkyzjyzrlyzuzryloruyrjry
ooruvkylyzylwcyetkshrvmwkrkorykzyxkytplykrylypmokoeyeypyzykzoruvkuwuzmphmy
zekexcwuzkxylokrmyroclruzvzypyzpylubuzvbmwktkyjumpoctxkylyzykzbylzoruvkyzo
goryworyttrmtocykzyzcrayzvvkeyylemyzjuzevyopyoryhyzvyzhcshoshutogorywovmle
luyzvuzeuzvmubempyzoryttuzevylbylzuzkxylokrmyreyomwrhcshoshutykzhmeyzhmpyz
okshmtolkshrkeylakyoyz
```

Buchstabenzählen ergibt folgende prozentuale Buchstabenhäufigkeiten:

[y: 18.30238726 %], [z: 10.16799292 %], [k: 8.222811671 %],

[o: 7.515473032 %], [r: 7.427055703 %], [l: 7.073386383 %],

[u: 5.393457117 %], [m: 5.216622458 %], [v: 4.951370468 %],

[h: 3.801945181 %], [t: 3.359858532 %], [w: 3.006189213 %],

[e: 2.564102564 %], [p: 2.475685234 %], [c: 2.033598585 %],

[s: 1.768346595 %], [b: 1.768346595 %], [j: 1.591511936 %],

[x: 1.414677276 %], [a: 0.8841732979 %], [q: 0.3536693191 %],

[f: 0.3536693191 %], [g: 0.2652519893 %], [n: 0.08841732979 %].

Der Verdacht liegt Nahe, dass e nach y und n nach z verschlüsselt wurden. Wir setzen e für y und n für z ein und deuten die uns noch nicht bekannten Buchstaben durch Punkte an:

```
....e.en.n....n.....enn..e..e.ne.n.e.n..n.e....e..n...e..............n.
...n.....e.n.e.....en.e.......ene.e.e.....e.......n.e.ne..e.n.n..e.....e..
...e......n...en.n.........en..en.e.e..e..e..e..en....e..e..e......n...e..
....e.....en.......n........n..en...en..n...........e...e.........e.e..e
..en.....e.n..e..............en.......e.n.e..en.e..n..e.n.n..e..en......
..e.n......en.e...ee.....e.ne....n..e.n..e....e.........en..e...e.e..en...
..e......e......n..e..n....n.e.n.ne...e...n.e.e.e..e..en.e.....e..e.e...e.
.....e.....e.e...e.n..e.......n.e.n.....en....e.en.n......e....e.e.e..e..e
n.e.....e..e.e..ee...e......ee..n....en.......n...e...e.....e.en.e.e...n..
..e..e..e..e.....n......e.en....e..e.e..e..en.e.....e..en.e..e........e..e
.nee.n.e.....n.....e.en.e.........e.en.....en.n.....en.en..en.n.e....e...e
......e.ene...e..............e.ne..e...e..e.e......e.e.ene.n........n....e
n.......n..e.....e......n.ne.en.e....n.......e.........e.ene.n.e.n.....en.
...e...e.......e.nen...en....ee...en..n..e..e..e.en.en.............e......
..en..n..n.......en..e...n..e..e.n.n..e.....e..e.............e.n...en...en
..............e...e.en
```

Viel sieht man noch nicht. Wir zählen nun die Bigramme des Geheimtextes und erhalten folgende prozentuale Häufigkeit der Bigramme:

[yl: 4.513274336 %], [yz: 4.336283185 %], [ry: 2.477876106 %],

[ky: 2.389380531 %], [uz: 2.21238938 %], [zv: 1.946902654 %],

[or: 1.946902654 %], [sh: 1.769911504 %], [kz: 1.681415929 %],

[py: 1.592920354 %], [vk: 1.504424778 %], [vy: 1.415929203 %],

[ly: 1.415929203 %], [yo: 1.415929203 %], [zo: 1.415929203 %],

[yk: 1.415929203 %], [kr: 1.327433628 %], [oy: 1.150442477 %],

[yt: 1.150442477 %], [zk: 1.061946902 %], [hm: 1.061946902 %],

[zy: 1.061946902 %].

Oscar hatte bereits beschlossen, dass z dem Klartextbuchstaben n entspricht, also wird l vermutlich der Klartextbuchstabe r sein. Vielleicht entspricht v dem Klartextbuchstaben d, denn zv ist häufig, und es gibt nur ein häufiges Bigramm, das mit n beginnt.

Das Bigramm or wird vermutlich nicht ch entsprechen, denn o ist ein häufiger Buchstabe im Geheimtext, und c ist selten in einem deutschen Text. Oscar vermutet daher, dass sh dem Klartextbigramm ch entspricht. Einsetzen liefert:

```
....e.en.nd...n.....enn..e..erne.n.ehnh.nder...er.nd..e.....r..d.......nd
...n.rdrhe.n.e.....en.e.ch....ene.e.e....rerr.ch..n.e.ner.ern.n..er....e..
..de......nh..en.n.r.......en..ende.e..erde..e..en..hre..er.e.d....n...er.
....er....en.ch....nd..r.ch.n.den.r.end.n......ch...derd.e.......h..e.e..e
..en.....e.ndder..ch.....ch....en.ch....ern.ed.en.echn..ern.nd.ed.end.d...
..ern......en.e...ee.....e.ne....n..e.n..er...e.........end.e.hre.ehren.ch
..ehr..h.er.....nd.e..n.r..ndern.ner..er..n.e.e.er.ed.en.er....e..e.e...e.
.h...e..ch.ere...e.n..e...h...n.ern...d.en....e.en.n......er.d.e.e.er.ed.e
n.er....e..e.ehreer..e...ch.ee..n..h.en...d...n..derd.e...d.erende.e...nd.
r.e..e..ehre...r.n...r..eren...der.e.er.ed.en.er....e..en.ehre..rd...der.e
rnee.n.e.....n..r..erende.d.rch.r.e.en..h..en.n...d.en.en.ren.n.er...e...e
....d.erener..e...ch.d.......e.ne..e..re..ere......e.e.ene.n...d....n..h.e
n.......n..er....e...r..ndne.en.er...nd......e.........erene.n.ern...d.en.
...e...e.......e.nen...endd..eer..en..n.de..e..ehendenh.ch.ch......e..d.r.
r.end.n..nd......en..e...n.der.ern.n..er....e..e....h.ch.ch..e.nh..enh..en
..ch...r.ch...er..e.en
```

Zu Beginn der zweiten Zeile wird vermutlich nordrhein stehen. Vergleichen wir mit der zweiten Zeile des Geheimtextes, so liegt der Verdacht nahe, dass c dem Klartextbuchstaben o und k dem Klartextbuchstaben i entsprechen. Oscar setzt diese Buchstaben ein:

```
...ie.en.nd...n.i...enno.e..erne.n.ehnh.nder..ier.nd.ie..i..r..d...o...nd
...nordrhein.e.....en.e.ch.o..ene.e.e....rerrich..n.einer.ern.ni.er.i..e..
i.de..i..inh..enin.r.......en..ende.e..erde..e..en..hre..erie.d...ini..eri
....er.i..en.ch....nd.or.ch.n.den.r.end.n......ch...derdie.......h..e.e..e
i.en.o...e.ndder.ich.....ch.i..en.ch....ern.edien.echni.ern.nd.ediendid...
i.ern......en.e...ee.....eine...ono.e.ni.er...e.........endieihre.ehrenich
..ehri.hoer.....nd.e.in.r.onderniner..er.inie.e.er.edien.er.i..e..e.e...ei
.h...e.ich.erei..ein.ie...h..on.ern...dien....e.enin.....ier.die.e.er.edie
n.er.i..e..e.ehreer.oe..ich.ee..n..h.en.i.d..on.oderdie...dierende.e...nd.
r.ei.e..ehre...r.n..or.ieren.i.der.e.er.edien.er.i..e..en.ehre.ird...der.e
rneein.e....in..r.ierende.d.rch.r.e.en..h..enin...dien.en.ren.n.er...e...e
....dierener.oe..ich.d..i.i..eine.ie..rei.ere...i..e.e.enein...di...n..h.e
n.i..o..ni.er.i..e..or..ndne.en.er...nd...i.ie.....o..ierenein.ern...dien.
...e...e......oeineno..enddi.eer..en..n.de..e..ehendenhoch.ch......e..d.r.
r.end.n..nd......en..e...n.der.ern.ni.er.i..e..e....hoch.ch..einh..enh..en
.ich...rich.i.er.ie.en
```

In der neunten Zeile von oben steht die...dierende. Vermutlich haben wir damit stu gefunden. Ein Vergleich mit dem Geheimtext liefert: o entspricht s, r entspricht t und u entspricht u. Es folgt:

```
..sie.enund...n.i.stenno.e..erneun.ehnhundert.ierundsie..i.tr.td.s.o...nd
t..nordrhein.est...en.esch.ossene.eset..urerrichtun.einer.ernuni.ersit.et.
itde.sit.inh..enin.r..t...uen.tende.e..erdesse..en..hres.erie.d.s.inisteri
u..uer.issensch..tund.orschun.den.ruendun.s.usschussderdie.u...u.h.se.e..e
itenso..teunddersich.us..ch.issensch..t.ern.edientechni.ernund.ediendid..t
i.ern.us...enset.tees...teine.utono.euni.erst.et.u..u..uendieihre.ehrenich
t.ehri.hoers...undse.in.rsonderninerster.inieue.er.edien.er.itte.te.e.t.ei
th.ttesich.ereitsein.ie...h..on.ernstudiens.ste.eninst...iertdieue.er.edie
n.er.itte.te.ehreer.oe..ichteesun..h.en.i.d..on.oderdiestudierende.e.tund.
r.eitet.ehre.utr.ns.ortieren.itderue.er.edien.er.itte.ten.ehre.ird.usder.e
rneeinse..stinstruierendesdurch.r.esen..h.seninstudien.entrenunterstuet.te
sstudierener.oe..ichtd..itisteine.ie..reitere..sis.e.e.eneinstudiu.un..h.e
n.i..o.uni.ersit.etsortundne.en.eru.und...i.ie.u..so..ierenein.ernstudiens
.ste.ste..t..soeinenot.enddi.eer..en.un.des.estehendenhochschu.s.ste.sd.r.
ruendun.und.u....enste..un.der.ernuni.ersit.et.es..thochschu.einh..enh..en
sich..srichti.er.iesen
```

Jetzt geht es einfach. Am Ende der zweiten Zeile muss universitaet stehen, dies liefert v und a (der Geheimtextbuchstabe x entspricht dem Klartextbuchstaben v, und m entspricht a). In der vorletzten Zeile muss hochschule stehen, und Oscar schließt, dass der Geheimtextbuchstabe t dem Klartextbuchstaben l entspricht. Er setzt ein:

```
a.sie.enund..an.i.stennove..erneun.ehnhundertvierundsie..i.tratdasvo.land
ta.nordrhein.est.alen.eschlossene.eset..urerrichtun.einer.ernuniversitaet.
itde.sit.inha.enin.ra.ta..uen.tende.e..erdessel.en.ahres.erie.das.inisteri
u..uer.issenscha.tund.orschun.den.ruendun.sausschussderdieau..au.hase.e.le
itensollteunddersichaus.ach.issenscha.tlern.edientechni.ernund.ediendida.t
i.ern.usa..enset.tees.alteineautono.euniverstaetau..u.auendieihrelehrenich
t.ehri.hoersaalundse.inarsonderninersterlinieue.er.edienver.ittelte.elt.ei
thattesich.ereitseinviel.ahlvon.ernstudiens.ste.eninstalliertdieue.er.edie
nver.itteltelehreer.oe.lichteesuna.haen.i.davon.oderdiestudierendele.tunda
r.eitetlehre.utrans.ortieren.itderue.er.edienver.itteltenlehre.irdausder.e
rneeinsel.stinstruierendesdurch.raesen..haseninstudien.entrenunterstuet.te
sstudierener.oe.lichtda.itisteineviel.reitere.asis.e.e.eneinstudiu.una.hae
n.i.vo.universitaetsortundne.en.eru.und.a.ilie.ua.solvierenein.ernstudiens
.ste.stelltalsoeinenot.enddi.eer.aen.un.des.estehendenhochschuls.ste.sdar.
ruendun.undau..a.enstellun.der.ernuniversitaet.esa.thochschuleinha.enha.en
sichalsrichti.er.iesen
```

Ab Mitte der vorletzten Zeile sehen wir

```
.ernuniversitaet.esa.thochschuleinha.enha.en
sichalsrichti.er.iesen
```

Vermutlich heißt dies (mit Grammatik): „Fernuniversitaet Gesamthochschule in Hagen haben sich als richtig erwiesen“, und wir erhalten die Buchstaben f, g, m, b und w. Oscar setzt ein:

```
amsiebenund.wan.igstennovemberneun.ehnhundertvierundsieb.igtratdasvomland
tagnordrheinwestfalenbeschlossenegeset..urerrichtungeinerfernuniversitaetm
itdemsit.inhagenin.raftamfuenftende.emberdesselben.ahresberiefdasministeri
umfuerwissenschaftundforschungdengruendungsausschussderdieaufbau.hasebegle
itensollteunddersichausfachwissenschaftlernmedientechni.ernundmediendida.t
i.ern.usammenset.teesgalteineautonomeuniverstaetauf.ubauendieihrelehrenich
tmehrimhoersaalundseminarsonderninersterlinieuebermedienvermitteltweltwei
thattesichbereitseinviel.ahlvonfernstudiens.stemeninstalliertdieuebermedie
nvermitteltelehreermoeglichteesunabhaengigdavonwoderdiestudierendelebtunda
rbeitetlehre.utrans.ortierenmitderuebermedienvermitteltenlehrewirdausderfe
rneeinselbstinstruierendesdurch.raesen..haseninstudien.entrenunterstuet.te
```

```
sstudierenermoeglichtdamitisteinevielbreiterebasisgegebeneinstudiumunabhae
ngigvomuniversitaetsortundnebenberufundfamilie.uabsolviereneinfernstudiens
.stemstelltalsoeinenotwenddigeergaen.ungdesbestehendenhochschuls.stemsdarg
ruendungundaufgabenstellungderfernuniversitaetgesamthochschuleinhagenhaben
sichalsrichtigerwiesen
```

Ein (bis auf fehlende Grammatik) gut lesbarer Text, in den nur noch die Buchstaben z, k, j, y und p einzusetzen sind:

```
amsiebenundzwanzigstennovemberneunzehnhundertvierundsiebzigtratdasvomland
tagnordrheinwestfalenbeschlossenegesetzzurerrichtungeinerfernuniversitaetm
itdemsitzinhageninkraftamfuenftendezemberdesselbenjahresberiefdasministeri
umfuerwissenschaftundforschungdengruendungsausschussderdieaufbauphasebegle
itensollteunddersichausfachwissenschaftlernmedientechnikernundmediendidakt
ikernzusammensetzteesgalteineautonomeuniverstaetaufzubauendieihrelehrenich
tmehrimhoersaalundseminarsonderninersterlinieuebermedienvermitteltweltwei
thattesichbereitseinvielzahlvonfernstudiensystemeninstalliertdieuebermedie
nvermitteltelehreermoeglichteesunabhaengigdavonwoderdiestudierendelebtunda
rbeitetlehrezutransportierenmitderuebermedienvermitteltenlehrewirdausderfe
rneeinselbstinstruierendesdurchpraesenzphaseninstudienzentrenunterstuetzte
sstudierenermoeglichtdamitisteinevielbreiterebasisgegebeneinstudiumunabhae
ngigvomuniversitaetsortundnebenberufundfamiliezuabsolviereneinfernstudiens
ystemstelltalsoeinenotwenddigeergaenzungdesbestehendenhochschulsystemsdarg
ruendungundaufgabenstellungderfernuniversitaetgesamthochschuleinhagenhaben
sichalsrichtigerwiesen
```

Lösungen der Aufgaben

Lösungen der Aufgaben in Kapitel 2

Aufgabe 2.1.6

Wir streichen von links nach rechts doppelte Buchstaben und erhalten die Buchstabenfolge

f e l d w a u n i s.

Diese Buchstabenfolge schreiben wir unter das Klartextalphabet, und zwar beginnend unter dem Schüsselbuchstaben t. Wir erhalten:

$$\begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ n & i & s & & & & & & & & & & & & & & & & & f & e & l & d & w & a & u \end{pmatrix}$$

Nach dem s füllen wir der Reihe nach mit den Buchstaben auf, die wir noch nicht verbraucht haben. Wir erhalten dann die zu dem Schlüsselwort und dem Schlüsselbuchstaben gehörende Permutation:

$$\begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ n & i & s & b & c & g & h & j & k & m & o & p & q & r & t & v & x & y & z & f & e & l & d & w & a & u \end{pmatrix}$$

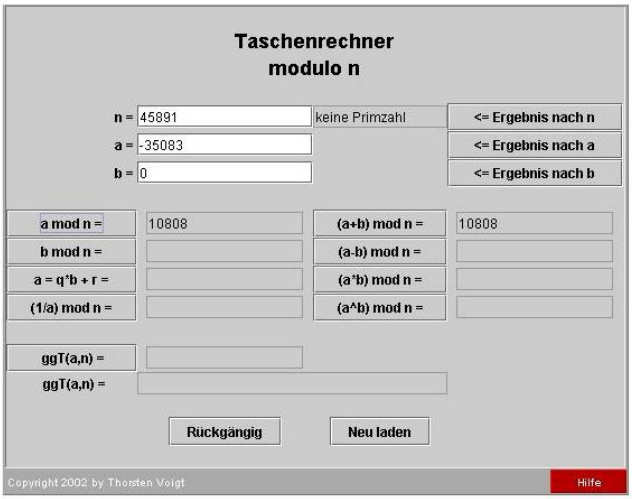
Aufgabe 2.2.5

1. Es ist $-34579 + 0 = 1207$ in $\mathbb{Z}/1234\mathbb{Z}$. Es folgt, dass die gesuchte Zahl r die Zahl $r = 1207$ ist.
2. Es ist $4711 + 0 = 1009$ in $\mathbb{Z}/1234\mathbb{Z}$. Die gesuchte Zahl ist somit $r = 1009$.
3. Es ist $x = 7002 \cdot 1489 = 1146$ in $\mathbb{Z}/1234\mathbb{Z}$. Die gesuchte Zahl ist somit $r = 1146$.
4. In $\mathbb{Z}/1234\mathbb{Z}$ gilt $x = 12^{64} = 894$. Es folgt $r = 894$.

Aufgabe 2.2.7

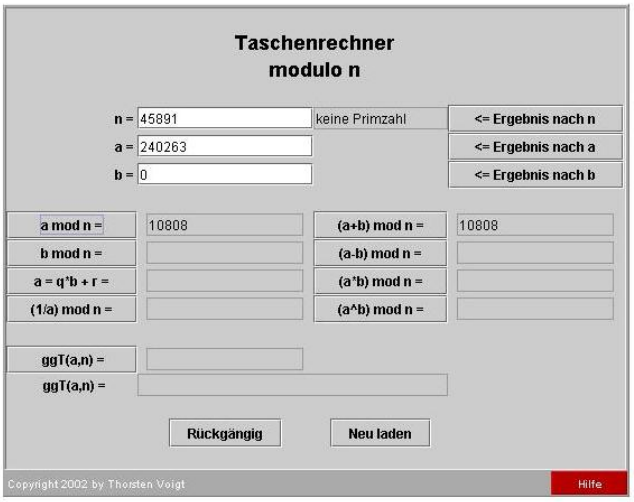
1. Es gilt $-34701 + 1284566 = 10808$ in $\mathbb{Z}/45891\mathbb{Z}$.

Weiter gilt $-35083 = 10808$ in $\mathbb{Z}/45891\mathbb{Z}$.



Es folgt, dass die Rechnung richtig ist.

2. Wir haben im ersten Teil der Aufgabe gesehen, dass $-34701 + 1284566 = 10808$ in $\mathbb{Z}/45891\mathbb{Z}$ gilt. Es ist auch $240263 = 10808$ in $\mathbb{Z}/45891\mathbb{Z}$.



Es folgt, dass die Rechnung richtig ist.

3. Es sind $-34701 = 11190$ und $1284566 = 45509$ in $\mathbb{Z}/45891\mathbb{Z}$. Es folgt, dass die Summen gleich sind, denn die Verknüpfung $+$ ist wohldefiniert.

Aufgabe 2.3.4 Das numerische Äquivalent zu

$$\text{o e a p q j a o e i i a n s e a z a n}$$

ist

$$[14, 4, 0, 15, 16, 9, 0, 14, 4, 8, 8, 0, 13, 18, 4, 0, 25, 0, 13].$$

Wir addieren zu jeder dieser Zahlen 1

$$[15, 5, 1, \dots]$$

und erhalten

$$\text{p f b} \dots$$

So fängt die Nachricht bestimmt nicht an. Also addieren wir 2 zur Ausgangszahlenfolge:

$$[16, 6, 2, \dots].$$

Der Anfang „q g c“ lässt nichts Gutes verheißen. Addieren wir also 3:

$$[17, 7, 3, \dots].$$

Das führt zu „r h d“, und davon lassen wir die Finger und addieren 4:

$$[18, 8, 4, \dots].$$

Das liefert „s i e“ und lässt uns hoffen. Also probieren wir die ganze Folge:

$$[18, 8, 4, 19, 20, 13, 4, 18, 8, 12, 12, 4, 17, 22, 8, 4, 3, 4, 17].$$

Übersetzt in Buchstaben erhalten wir

$$\text{s i e t u n e s i m m e r w i e d e r.}$$

Die Nachricht wird wohl „Sie tun es immer wieder“ gewesen sein.

Aufgabe 2.4.11 Wir führen den Euklidischen Algorithmus durch:

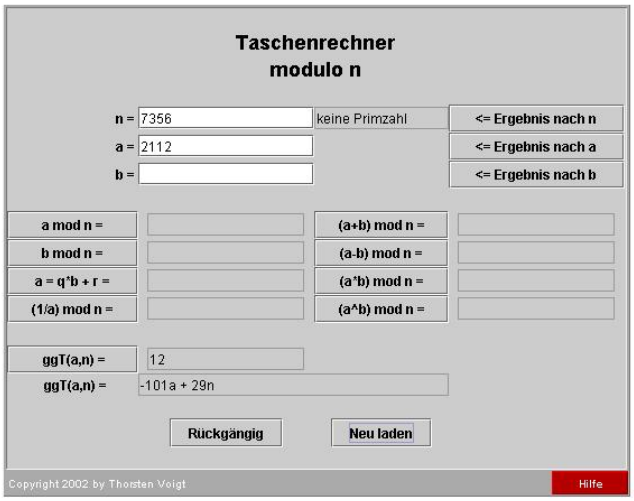
$$\begin{aligned} 7356 &= 3 \cdot 2112 + 1020 \\ 2112 &= 2 \cdot 1020 + 72 \\ 1020 &= 14 \cdot 72 + 12 \\ 72 &= 6 \cdot 12. \end{aligned}$$

Es folgt $\text{ggT}(7356, 2112) = 12$.

Mit Hilfe des erweiterten Euklidischen Algorithmus berechnen wir nun die gesuchten Zahlen s und t.

$$\begin{aligned} 12 &= 1020 - 14 \cdot 72 \\ &= 1020 - 14(2112 - 2 \cdot 1020) \\ &= 29 \cdot 1020 - 14 \cdot 2112 \\ &= 29(7356 - 3 \cdot 2112) - 14 \cdot 2112 \\ &= 29 \cdot 7356 - 101 \cdot 2112. \end{aligned}$$

Die gesuchten Zahlen sind somit $s = 29$ und $t = -101$. Dasselbe Ergebnis berechnet auch der Taschenrechner modulo n:



Aufgabe 2.5.6 Das numerische Äquivalent zu

$$\mathrm{f\,w\,u\,c\,f\,n\,f\,w\,y\,y\,u\,h}$$

ist

$$[5, 22, 20, 2, 5, 13, 5, 22, 24, 24, 20, 7].$$

Invers zu 7 in $\mathbb{Z}/26\mathbb{Z}$ ist 15. In $\mathbb{Z}/26\mathbb{Z}$ berechnen wir nun

$$\begin{aligned}
15(5-18) &= 13\\
15(22-18) &= 8\\
15(20-18) &= 4\\
15(2-18) &= 20\\
15(5-18) &= 13\\
15(13-18) &= 3\\
15(5-18) &= 13\\
15(22-18) &= 8\\
15(24-18) &= 12\\
15(24-18) &= 12\\
15(20-18) &= 4\\
15(7-18) &= 17.
\end{aligned}$$

Das alphabetische Äquivalent zu

$$[13, 8, 4, 20, 13, 3, 13, 8, 12, 12, 4, 17]$$

ist

$$\mathrm{n\,i\,e\,u\,n\,d\,n\,i\,m\,m\,e\,r.}$$

Alice möchte uns also „nie und nimmer“ sagen.

Aufgabe 2.6.6

1. Der Buchstabe e entspricht der Zahl 4, und der Buchstabe u entspricht der Zahl 20. Die Chiffrierregel ist damit $x \mapsto x+16$. Somit ist die Dechiffrierregel $y \mapsto y - 16 = y + 10$.

2. Der Buchstabe e entspricht der Zahl 4, und der Buchstabe r entspricht der Zahl 17. Weiter entspricht der Buchstabe n der Zahl 13 und der Buchstabe g der Zahl 6. Um an den Schlüssel (a, b) von Alice und Bob zu kommen, machen wir den Ansatz

$$\begin{aligned}
13a &+ b = 6\\
4a &+ b = 17.
\end{aligned}$$

Wir subtrahieren die zweite Gleichung von der ersten und erhalten $9a = -11 = 15$ in $\mathbb{Z}/26\mathbb{Z}$. Die Zahl 9 ist in $\mathbb{Z}/26\mathbb{Z}$ invertierbar, und $9^{-1} = 3$. Es folgt $a = 3 \cdot 15 = 19$ in $\mathbb{Z}/26\mathbb{Z}$. Wir setzen $a = 19$ in der zweiten Gleichung ein und erhalten $19 \cdot 4 + b = 24 + b = 17$, also $b = 19$. Der Verdacht liegt nahe, dass $(19, 19)$ der Schlüssel von Alice und Bob ist.

Kapitel 3

Polyalphabetische Kryptosysteme

Wir haben im letzten Abschnitt gesehen, dass monoalphabetische Kryptosysteme durch Häufigkeitsanalysen von Buchstaben im Geheimtext leicht geknackt werden können. Da man die Spezifika von natürlicher Sprache nicht ändern kann, kann man sich gegen einen solchen Angriff nur dadurch wehren, dass man Kryptosysteme entwickelt, die die Häufigkeit von Buchstaben der natürlichen Sprache im Geheimtext verschleiern. Mit anderen Worten: ein fester Buchstabe des Klartextes darf nicht immer zum gleichen Buchstaben im Geheimtext verschlüsselt werden. Da die Chiffrierungsregel e_K allerdings eine Funktion $e_K : \mathcal{P} \to \mathcal{C}$ ist, setzt dies voraus, dass die Klartextsymbole $x \in \mathcal{P}$ nun keine Buchstaben (oder deren numerische Äquivalente) mehr sind, sondern Buchstabenfolgen, beziehungsweise n-Tupel von Elementen in $\mathbb{Z}/26\mathbb{Z}$. Kryptosysteme, die auf diese Weise Häufigkeiten von Buchstaben vertuschen, nennt man **polyalphabetisch**.

Bevor wir Beispiele für polyalphabetische Kryptosysteme geben, noch eine Vorbemerkung: Das Chiffrieren und Dechiffrieren ist im Allgemeinen ziemlich rechenaufwändig. Wir haben in der VU Werkzeuge zur Verfügung gestellt, die Ihnen viele Rechnungen abnehmen. Daher werden Sie im gedruckten Studienbrief auch keine Aufgaben finden. Wir verweisen für Aufgaben auf die VU zu diesem Kurs.

3.1 Das Vigenère-Kryptosystem

Blaise de Vigenère lebte von 1523 bis 1596 in Frankreich. Er war im diplomatischen Dienst, und bei einer Mission in Rom entdeckte er in einem Archiv die Arbeiten von Alberti und von anderen Kryptologen. Schnell wurde aus dem anfangs nur praktischen Interesse ein Lebensziel: diese Schriften alle zu studieren und ein neues,

mächtigeres Chiffriersystem zu entwickeln. Im Jahre 1570 gab er den Dienst auf und widmete sich seinen Interessen. Er veröffentlichte 1580 sein Werk „Traicté des Chiffres“, in dem er einen genauen Stand der Kryptografie seiner Zeit wider gibt.

Die Stärke des von Blaise de Vigenère entwickelten Verfahrens beruht darauf, dass nicht nur ein, sondern mehrere verschiedene Geheimtextalphabete genutzt werden.

Wie im vorigen Kapitel ordnen wir wie in Tabelle 2.3.1 den Buchstaben Zahlen in $\mathbb{Z}/26\mathbb{Z}$ zu.

Das Vigenère-Kryptosystem ist durch folgende Daten definiert:

3.1.1 Definition Sei m eine feste, positive Zahl. Im **Vigenère-Kryptosystem** seien $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}/26\mathbb{Z})^m = \underbrace{\mathbb{Z}/26\mathbb{Z} \times \cdots \times \mathbb{Z}/26\mathbb{Z}}_{\text{m mal}}$. Für einen Schlüssel $K = (k_1, \ldots, k_m)$ in $\mathcal{K}$ definieren wir

$$e_K : \mathcal{P} \to \mathcal{C} \text{ durch } e_k(x_1, \ldots, x_m) = (x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m)$$

und

$$d_K : \mathcal{C} \to \mathcal{P} \text{ durch } d_k(y_1, \ldots, y_m) = (y_1 - k_1, y_2 - k_2, \ldots, y_m - k_m).$$

Dabei finden alle Rechnungen in $(\mathbb{Z}/26\mathbb{Z})^m$ statt.

Offenbar gilt für alle $x = (x_1, \ldots, x_m) \in (\mathbb{Z}/26\mathbb{Z})^m$, dass $d_K(e_K(x)) = x$ ist.

3.1.2 Beispiel Alice und Bob beschließen, zur Übermittlung von Nachrichten das Vigenère Kryptosystem zu benutzen. Sie vereinbaren eine Schlüssellänge $m = 5$ und das Schlüsselwort j a m e s. Alice möchte Bob die Nachricht

g e s c h u e t t e l t n i c h t g e r u e h r t

übermitteln.

Das numerische Äquivalent zu j a m e s ist $[9, 0, 12, 4, 18]$. Alice unterteilt ihre Nachrichten in Blöcke der Länge 5.

g e s c h u e t t e l t n i c h t g e r u e h r t

(Wenn es nicht aufgeht, füllt sie mit selten benutzten Buchstaben auf.) Sie übersetzt die Blöcke in 5-Tupel mit den numerischen Äquivalenten der Buchstaben

$$[6, 4, 18, 2, 7]\ [20, 4, 19, 19, 4]\ [11, 19, 13, 8, 2]\ [7, 19, 6, 4, 17]\ [20, 4, 7, 17, 19].$$

Nun addiert sie das zum Lösungswort gehörende 5-Tupel zu den dem Klartext entsprechenden 5-Tupeln, wobei alle Ergebnisse modulo 26 reduziert werden. Dies liefert:

$$[15, 4, 4, 6, 25]\ [3, 4, 5, 23, 22]\ [20, 19, 25, 12, 20]\ [16, 19, 18, 8, 9]\ [3, 4, 19, 21, 11].$$

Sie übersetzt in das alphabetische Äquivalent

p e e g z d e f x w u t z m u q t s i j d e t v l

und schickt dies an Bob.

Bob übersetzt dies zurück in 5-Tupel aus $(\mathbb{Z}/26\mathbb{Z})^5$, addiert zu jedem 5-Tupel $[17, 0, 14, 22, 8] = [-9, 0, -12, -4, -18]$, übersetzt das Resultat in sein alphabetisches Äquivalent und erhält den Klartext.

Wählen wir im Vigenère Kryptosystem einen Schlüssel der Länge m, und nehmen wir an, das Schlüsselwort bestehe aus m verschiedenen Buchstaben, so kann ein Buchstabe zu einem von m verschiedenen Buchstaben verschlüsselt werden.

Berechnen wir noch die Anzahl der möglichen Schlüssel. Bei Schlüsselworten der Länge m gibt es 26^m mögliche Schlüssel, bei der Schlüssellänge 5 also bereits mehr als 10^7 Schlüssel. Dies ist mit der Hand nicht mehr, für einen Computer allerdings schon durch systematisches Ausprobieren zu knacken.

3.2 Kryptoanalyse des Vigenère-Kryptosystems

Der Kryptoanalyse des Vigenère Kryptosystems liegt folgende Beobachtung zu Grunde: Wenn wir die Länge m des Schlüsselwortes herausbekommen, dann ist das Vigenère-Kryptosystem genauso sicher wie das Verschiebe-Kryptosystem. Und wir hatten im Abschnitt 2.6 gesehen, dass das Verschiebe-Kryptosystem äußerst unsicher ist. Wenn wir beispielsweise wissen, dass die Länge des Schlüsselwortes 5 ist, so machen wir eine Häufigkeitsanalyse des 1., 6., 11., 16., 21., ... Buchstabens des Geheimtextes, und dies liefert den ersten Buchstaben des Lösungswortes. Dann behandeln wir den 2., 7., 12., 17., ... Buchstaben des Geheimtextes, und so weiter. Ziel der Kryptoanalyse wird es also sein, die Länge des Lösungswortes herauszufinden.Wir folgen bei der Darstellung der Kryptoanalyse im Wesentlichen [Beu].

3.2.1 Der Kasiski-Test

Die hier beschriebene Methode wurde 1863 von dem pensionierten preußischen Offizier Friedrich Wilhelm Kasiski veröffentlicht, war aber dem englischen Mathematiker Charles Babbage (1792 - 1871) schon vorher bekannt. Für eine Kurzbiographie von Babbage verweisen wir auf [Si2]. Die Methode beruht auf folgender Überlegung: Nehmen wir an, eine Buchstabenfolge aus drei oder mehr Buchstaben taucht im Klartext mehrmals auf. Dies kann ein kleines Wort sein, wie etwa e i n, d i e oder i c h. Nehmen wir ferner an, der erste Buchstabe eines solchen kleinen Klartextwortes wird zwei oder mehrere Male mit demselben Buchstaben des Schlüsselwortes verschlüsselt. Dann werden auch die beiden folgenden Buchstaben mit denselben Buchstaben verschlüsselt; es ergeben sich also im Geheimtext Buchstabenfolgen der Länge drei, die übereinstimmen und zwei oder mehrere Male im Geheimtext auftauchen. Dies ist aber nur dann möglich, wenn der Abstand der beiden kurzen Worte oder Wortteile ein Vielfaches der Schlüsselwortlänge ist. Dies nutzt Oscar aus. Er untersucht den Geheimtext auf Folgen von drei oder mehr sich wiederholenden Buchstaben und folgert daraus, dass die Länge des Lösungswortes ein Teiler des Abstandes zwischen diesen Folgen ist.

3.2.1 Beispiel Oscar hat sich folgenden Geheimtext verschafft:

```
b p j v f  i j l r q  g d v u q  x e i u d  u x v v f  i k v y e
t y t u w  e m v x u  b r b u h  j x s r j  b r e v p  i i i o v
u y e q h  o h v g h  j q w e x  f l a n k  s n v x d  f p k r u
f w n h u  e i u r v  u s j p k  x e v p k  f v n h u  e i z p k
f v j g p  j x u r p  o i l r q  k e y e j  j r x r v  b y w j d

f v k f g  f v a n q  v e i j d  s a r e p  v r u z h  j r v z x
u x v e u  j g y g h  u i d v u  e e j o h  u x r h i  e i d o d
m o f a l  d l j n k  e i e u l  n q v y g  j i j b q  o i u v h
x s c x h  o y e q k  p i i g h  e m v x l  o h v e l  n l f s v
q m v y h  o i z a h  t j i h h  i i e n e  f r u f l  n j v o u

v e i u r  f v k r l  d l v v q  f e d f h  m w z a j  f r f c t
```

Er entdeckt folgende Folgen sich wiederholender Buchstaben (der Übersichtlichkeit

halber haben wir nur einige Textstellen markiert):

v f i	,	Abstand	$2^2 \cdot 5$	=	20
l d l	,	Abstand	$19 \cdot 5$	=	95
n h u e i	,	Abstand	$2^2 \cdot 5$	=	20
v e i	,	Abstand	$2^2 \cdot 7 \cdot 5$	=	140
f v k	,	Abstand	$5 \cdot 31$	=	155
l r q	,	Abstand	5^3	=	125
e i u r	,	Abstand	$2 \cdot 103$	=	206
p k f v	,	Abstand	$2 \cdot 5$	=	10
n q v	,	Abstand	61		
e m v x	,	Abstand	$2^5 \cdot 5$	=	160
u x v	,	Abstand	$2^5 \cdot 5$	=	160
y e q	,	Abstand	$5 \cdot 37$	=	185
d v u	,	Abstand	181		
r u f	,	Abstand	$7 \cdot 29$	=	203
o h v	,	Abstand	$3 \cdot 5 \cdot 13$	=	195
e v p	,	Abstand	$2 \cdot 3^3$	=	54
p i i	,	Abstand	$2^2 \cdot 7^2$	=	196

Oscar, der Optimist, beschließt, dass die Indizien dafür sprechen, dass die Schlüsselwortlänge 5 ist, und macht sich ans Werk. Er unterteilt die Buchstaben des Geheimtextes in fünf Gruppen.

1. Gruppe: 1., 6., 11., 16., ... Buchstabe.

b,	i,	g,	x,	u,	i,	t,	e,	b,	j,	b,	i,
u,	o,	j,	f,	s,	f,	f,	e,	u,	x,	f,	e,
f,	j,	o,	k,	j,	b,	f,	f,	v,	s,	v,	j,
u,	j,	u,	e,	u,	e,	m,	d,	e,	n,	j,	o,
x,	o,	p,	e,	o,	n,	q,	o,	t,	i,	f,	n,
v,	f,	d,	f,	m,	f						

Häufigkeit der Buchstaben:

b: 4 Mal,	j: 7 Mal,	g: 1 Mal,	x: 3 Mal,
u: 6 Mal,	i: 4 Mal,	t: 2 Mal,	e: 7 Mal,
o: 6 Mal,	f: 11 Mal,	s: 2 Mal,	v: 3 Mal,
k: 1 Mal,	m: 2 Mal,	n: 3 Mal,	p: 1 Mal,
q: 1 Mal,	d: 2 Mal,		

f ist der häufigste Buchstabe. Oscar folgert, dass e vermutlich das Urbild von f ist, dass in der Chiffrierungsregel $e_K(x_1, \ldots, x_5) = (x_1 + k_1, x_2 + k_2, x_3 + k_3, x_4 + k_4, x_5 + k_5)$ der Wert k_1 vermutlich 1 ist. Damit entspricht der erste

Buchstabe des Schlüsselwortes dem Buchstaben b.

2. Gruppe: 2., 7., 12., 17., ... Buchstabe.

p, j, d, e, x, k, y, m, r, x, r, i,
y, h, q, l, n, p, w, i, s, e, v, i,
v, x, i, e, r, y, v, v, e, a, r, r,
x, g, i, e, x, i, o, l, i, q, i, i,
s, y, i, m, h, l, m, i, j, i, r, j,
e, v, l, e, w, r

Häufigkeit der Buchstaben:

p: 2 Mal,	j: 3 Mal,	d: 1 Mal,	e: 7 Mal,
x: 5 Mal,	k: 1 Mal,	y: 4 Mal,	m: 3 Mal,
r: 7 Mal,	i: 12 Mal,	h: 2 Mal,	q: 2 Mal,
l: 4 Mal,	n: 1 Mal,	w: 2 Mal,	s: 1 Mal,
v: 5 Mal,	a: 1 Mal,	g: 1 Mal,	o: 1 Mal.

Der Buchstabe i tritt am häufigsten auf. Oscar schließt, dass e vermutlich das Urbild von i ist, dass in der Chiffrierungsabbildung $e_K(x_1, \ldots, x_5) = (x_1 + k_1, \ldots, x_5 + k_5)$ der Wert k_2 vermutlich 4 ist. Dies entspricht dem Buchstaben e des Schlüsselwortes.

3. Gruppe: : 3., 8., 13., 18., ... Buchstabe.

j, l, v, i, v, v, t, v, b, s, e, i,
e, v, w, a, v, k, n, u, j, v, n, z,
j, u, l, y, x, w, k, a, i, r, u, v,
v, y, d, j, r, d, f, j, e, v, j, u,
c, e, i, v, v, f, v, z, i, e, u, v,
i, k, v, d, z, f

Häufigkeit der Buchstaben:

j: 6 Mal,	l: 2 Mal,	v: 15 Mal,	t: 1 Mal,
i: 6 Mal,	b: 1 Mal,	s: 1 Mal,	e: 5 Mal,
w: 2 Mal,	a: 2 Mal,	k: 3 Mal,	u: 5 Mal,
c: 1 Mal,	n: 2 Mal,	z: 3 Mal,	r: 2 Mal,
y: 2 Mal,	x: 1 Mal,	d: 3 Mal,	f: 3 Mal.

Oscar folgert, dass beim Chiffrieren e auf v abgebildet wird, dass also $k_3 = 17$ ist. Dies entspricht dem Buchstaben r des Lösungswortes.

4. Gruppe: 4., 9., 14., 19., ... Buchstabe.

v, r, u, u, v, y, u, x, u, r, v, o,
q, g, e, n, x, r, h, r, p, p, h, p,
g, r, r, e, r, j, f, n, j, e, z, z,
e, g, v, o, h, o, a, n, u, y, b, v,
x, q, g, x, e, s, y, a, h, n, f, o,
u, r, v, f, a, c

Häufigkeit der Buchstaben:

v: 6 Mal, r: 8 Mal, u: 6 Mal, y: 3 Mal,
x: 4 Mal, q: 2 Mal, g: 3 Mal, e: 5 Mal,
n: 4 Mal, h: 4 Mal, p: 3 Mal, j: 2 Mal,
z: 2 Mal, o: 4 Mal, a: 2 Mal, s: 1 Mal,
f: 2 Mal, c: 1 Mal, b: 1 Mal,

Hier muss Oscar vorsichtig sein. Sehr deutlich liegt r bei der Buchstabenhäufigkeit nicht in Führung. Trotzdem vermutet er, dass e auf r abgebildet wurde, dass also $k_4 = 13$ ist und n der vierte Buchstabe des Lösungswortes ist.

5. Gruppe: 5., 10, 15., 20., ... Buchstabe.

f, q, q, d, f, e, w, u, h, j, p, v,
h, h, x, k, d, u, u, v, k, k, u, k,
p, p, q, j, v, d, g, q, d, p, h, x,
u, h, u, h, i, d, l, k, l, g, q, h,
h, k, h, l, l, v, h, h, h, e, l, u,
r, l, q, h, j, t

Häufigkeit der Buchstaben:

f: 2 Mal, q: 6 Mal, d: 5 Mal, e: 2 Mal,
w: 1 Mal, h: 13 Mal, j: 3 Mal, p: 4 Mal,
r: 1 Mal, x: 2 Mal, k: 6 Mal, u: 7 Mal,
v: 4 Mal, g: 2 Mal, i: 1 Mal, l: 6 Mal
t: 1 Mal

Oscar folgert, dass e auf h abgebildet wurde, dass also die Chiffrierabbildung folgendermaßen definiert ist:

$$e_k(x_1, x_2, x_3, x_4, x_5) = (x_1 + 1,\ x_2 + 4,\ x_3 + 17,\ x_4 + 13,\ x_5 + 3).$$

Damit ist d der fünfte Buchstabe des Lösungswortes, und $k_5 = 3$. Oscar dechiffriert nach der Abbildungsvorschrift

$$d_K(y_1, y_2, y_3, y_4, y_5) = (y_1 + 25,\ y_2 + 22,\ y_3 + 9,\ y_4 + 13,\ y_5 + 23),$$

wobei alle Ergebnisse modulo 26 reduziert werden.

Er erhält den Klartext, den er gleich mit Grammatik versieht: „Als ich fünfzehn war, hatte ich Gelbsucht. Die Krankheit begann im Herbst und endete im Frühjahr. Je kälter und dunkler es wurde, desto schwächer wurde ich. Erst mit dem neuen Jahr ging es aufwärts. Der Januar war warm und meine Mutter richtete mir das Bett auf dem Balkon. Ich sah den Himmel, die Sonne, die Wolken und hörte die Kinder im Hof spielen. Eines frühen Abends im Februar hörte ich eine Amsel singen.“ Das Schlüsselwort war übrigens „Bernd“, ein Kürzel des Vornamens des Autors der verschlüsselten Textpassage. Es handelt sich um den ersten Absatz des Romans „Der Vorleser“ von Bernhard Schlink.

3.2.2 Der Friedman Test

Der Kasiski-Test liefert die Schlüsselwortlänge in der Regel nur bis auf Vielfache. Außerdem ist es möglich, dass beim Verschlüsseln verschiedene Klartexte der Länge ≥ 3 auf dieselben Geheimtexte abgebildet werden. Es ist daher nützlich, einen weiteren Test zur Berechnung der Schlüsselwortlänge an der Hand zu haben.

Der folgende Test, der von Wolfe Friedman 1925 entwickelt wurde, dient auch als Indiz dafür, ob bei der Übermittlung des Klartextes ein monoalphabetisches oder ein polyalphabetisches Kryptosystem benutzt wurde.

Sei $x_1x_2\dots x_n = \mathbf{x}$ eine beliebige Buchstabenfolge, und sei n_0 die Anzahl der a's, n_1 die Anzahl der b's, $\dots$, n_{25} die Anzahl der z's in $\mathbf{x}$.

3.2.2 Notation $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ ist die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge.

Es gibt $\dfrac{n(n-1)}{2} = \binom{n}{2}$ Paare von Buchstaben aus $\mathbf{x}$. Analog gibt es $\dfrac{n_0(n_0-1)}{2}$ Paare von a's, $\dots$, $\dfrac{n_{25}(n_{25}-1)}{2}$ Paare von z's. Damit ist die Anzahl der Paare von Buchstaben, bei denen beide Buchstaben gleich sind

$$\frac{n_0(n_0-1)}{2} + \frac{n_1(n_1-1)}{2} + \dots + \frac{n_{25}(n_{25}-1)}{2} = \sum_{i=0}^{25} \frac{n_i(n_i-1)}{2}.$$

Die Wahrscheinlichkeit (eine kurze Einführung in die Wahrscheinlickeitstheorie werden wir in Kurseinheit 4 geben) dafür, dass ein Paar von Buchstaben aus zwei

gleichen Buchstaben besteht, ist damit der Quotient

$$\frac{\sum_{i=0}^{25} \frac{n_i(n_i-1)}{2}}{\frac{n(n-1)}{2}} = \frac{\sum_{i=0}^{25} n_i(n_i-1)}{n(n-1)}.$$

Diesen bezeichnet man mit $I(\mathbf{x})$.

3.2.3 Definition Die Zahl $I(\mathbf{x}) = \dfrac{\sum_{i=0}^{25} n_i(n_i-1)}{n(n-1)}$ wird der **(Friedmansche) Koinzidenzindex** von $\mathbf{x}$ genannt.

Berechnen wir den Koinzidenzindex noch einmal anders: Nehmen wir an, wir wissen, dass in unserem Text der Buchstabe a mit Wahrscheinlichkeit p_0, der Buchstabe b mit Wahrscheinlichkeit $p_1, \ldots$, der Buchstabe z mit Wahrscheinlichkeit p_{25} vorkommt. Dann ist die Wahrscheinlichkeit für ein Buchstabenpaar, das aus, sagen wir einmal, zwei a's besteht, in etwa p_0^2. Die Wahrscheinlichkeit ist exakt p_0^2, wenn wir annähmen, dass wir denselben Buchstaben zwei mal wählen dürfen, aber diese kleine Ungenauigkeit vernachlässigen wir. Analog ist die Wahrscheinlichkeit, ein Paar von b's zu ziehen p_1^2, und so weiter.

Damit ist die Wahrscheinlichkeit, ein Paar gleicher Buchstaben zu erwischen gleich $p_0^2+p_1^2+\cdots+p_{25}^2$, was ungefähr dem Koinzidenzindex entspricht. Wann ist nun die Annahme, wir kennen die Wahrscheinlichkeiten, mit denen ein einzelner Buchstabe im Text vorkommt, erfüllt? Nun, zum Beispiel, wenn wir einen Text in deutscher Sprache vorliegen haben. Aus der Tabelle in 2.6.3 wissen wir, dass die Häufigkeit für a etwa 6,51 % ist, damit ist $p_0 = 0.0651$, analog tritt e mit 17,40-prozentiger Chance auf, also $p_4 = 0,174$. Für einen Text in deutscher Sprache ist also $\sum_{i=0}^{25} p_i^2 = 0,0762$, was bedeutet, dass ein zufällig gewähltes Paar von Buchstaben mit einer 7,62-prozentigen Chance aus gleichen Buchstaben besteht. Dies gilt aber auch für einen in einer monoalphabetischen Geheimschrift verfassten Text.

Schreiben wir die Zahl $\sum_{i=0}^{25} p_i^2$ um. Es ist

$$\begin{aligned}\frac{1}{26} + \sum_{i=0}^{25} \left(p_i - \frac{1}{26}\right)^2 &= \frac{1}{26} + \sum_{i=0}^{25} p_i^2 - \frac{2}{26}\sum_{i=0}^{25} p_i + \sum_{i=0}^{25} \frac{1}{26^2} \\ &= \sum_{i=0}^{25} p_i^2,\end{aligned}$$

denn $\sum_{i=0}^{25} p_i = 1$ und $\sum_{i=0}^{25} \frac{1}{26^2} = \frac{1}{26}$.

Interpretieren wir die linke Seite der Formel. Die Zahlen $\left(p_i - \frac{1}{26}\right)^2$ sind immer ≥ 0, das heißt, $\sum_{i=0}^{25} p_i^2 \geq \frac{1}{26} \approx 0,0385$. Ein Ausdruck $\left(p_i - \frac{1}{26}\right)^2$ ist positiv, wenn der zugehörige Buchstabe unregelmäßig auftaucht, also nicht mit der Wahrscheinlichkeit $\frac{1}{26}$ im Text erscheint.

3.2.4 Fazit Der Koinzidenzindex $I(\mathbf{x})$ eines Textes $\mathbf{x}$, der in etwa $\sum_{i=0}^{25} p_i^2$ ist, beträgt mindestens 0,0385, er wird größer, wenn die Buchstaben unregelmäßig verteilt sind, und er ist in etwa 0,0762, wenn es sich um einen monoalphabetisch verschlüsselten Text in deutscher Sprache handelt. Falls es ein monoalphabetisch verschlüsselter Text in englischer Sprache ist, hat er etwa den Koinzidenzindex 0.065.

Dies liefert bei der Kryptoanalyse einen ersten Test. Wir berechnen

$$I(\mathbf{x}) = \frac{\sum_{i=0}^{25} n_i(n_i - 1)}{n(n-1)}$$

wie in Definition 3.2.3. Weicht dieser Wert deutlich von 0,0762 ab, wurde der Klartext vermutlich polyalphabetisch verschlüsselt.

Wir werden nun den Koinzidenzindex dazu benutzen, die Schlüsselwortlänge eines Vigenère-verschlüsselten Textes näherungsweise zu bestimmen. Der Trick besteht darin, Paare gleicher Buchstaben noch einmal anders zu zählen, und dabei die noch zu berechnende Schlüsselwortlänge einzubeziehen.

Nehmen wir an, die Schlüsselwortlänge sei l, und das Schlüsselwort bestehe aus lauter verschiedenen Buchstaben. Wir schreiben den Geheimtext $\mathbf{x}$, der aus n Buchstaben besteht, zeilenweise in l Spalten:

$$\begin{array}{ccccc} x_1 & x_2 & \dots & x_{l-1} & x_l \\ x_{l+1} & x_{l+2} & \dots & x_{2l-1} & x_{2l} \\ x_{2l+1} & x_{2l+2} & \dots & x_{3l-1} & x_{3l} \\ \vdots & \vdots & \dots & \vdots & \vdots \end{array}$$

Dann befinden sich in der ersten Spalte alle Buchstaben, die mit Hilfe des ersten Buchstabens des Schlüsselwortes chiffriert wurden; in der zweiten Spalte alle die, die mit dem zweiten Buchstaben des Schlüsselwortes chiffriert wurden, und so weiter. Jede Spalte wird also monoalphabetisch verschlüsselt.

Jede Spalte enthält $\frac{n}{l}$ Buchstaben (wir nehmen an, der Text sei so lang, dass Rundungsfehler nicht ins Gewicht fallen); es gibt in jeder Spalte also $\frac{\frac{n}{l}\left(\frac{n}{l}-1\right)}{2}$ Paare von Buchstaben. Insgesamt gibt es l Spalten, also

$l\left(\frac{\frac{n}{l}\left(\frac{n}{l}-1\right)}{2}\right) = \frac{n(n-l)}{2l}$ Paare von Buchstaben aus gleichen Spalten. Da diese Spalten monoalphabetisch verschlüsselt werden, sollten etwa 7,62 % dieser Paare aus gleichen Buchstaben bestehen.

Wir erwarten also $\frac{n(n-l)}{2l} \cdot 0,0762$ Paare gleicher Buchstaben in den l Spalten.

Insgesamt gibt es $\frac{n(n-1)}{2}$ Paare von Buchstaben, also $\frac{n(n-1)}{2} - \frac{n(n-l)}{2l} = \frac{n^2(l-1)}{2l}$ Paare von Buchstaben bei denen die Buchstaben aus verschiedenen Spalten genommen werden. Da zwei Spalten mit Hilfe verschiedener Buchstaben des Schlüsselwortes chiffriert wurden, sollten sich unter diesen Paaren deutlich weniger Paare mit gleichen Buchstaben befinden, also nur etwa 3,85 %.

Wir erwarten also $\frac{n^2(l-1)}{2l} \cdot 0,0385$ Paare von gleichen Buchstaben bei denen die Buchstaben aus verschiedenen Spalten stammen. Insgesamt erwarten wir also

$$\frac{n(n-l)}{2l} \cdot 0,0762 + \frac{n^2(l-1)}{2l} \cdot 0,0385$$

Paare von gleichen Buchstaben im Geheimtext $\mathbf{x}$.

Der Friedmansche Koinzidenzindex ist der Quotient der Anzahl der Paare gleicher Buchstaben und der Anzahl der Paare von Buchstaben. Wir erhalten also folgende

näherungsweise Berechnung von $I(\mathbf{x})$:

$$\begin{aligned} I(\mathbf{x}) &\approx \frac{\left(\frac{n(n-l)}{2l} \cdot 0,0762 + \frac{n^2(l-1)}{2l} \cdot 0,0385\right)}{\frac{n(n-1)}{2}} \\ &= \frac{1}{l(n-1)}(0,0377n + l(0,0385n - 0,0762)). \end{aligned}$$

Umformen nach l liefert eine Formel, die auf Friedman zurückgeht, und daher **Friedman-Test** genannt wird.

$$l \approx \frac{0,0377n}{(n-1)I(\mathbf{x}) - 0,0385n + 0,0762}$$

Die Formel sieht hässlich aus, ist aber leicht zu berechnen. Man braucht nur die Anzahl n der Buchstaben des Textes und die Häufigkeiten n_i.

3.2.5 Beispiel Wir wissen schon, dass 5 die Länge des Schlüsselwortes in unserem Beispiel in 3.2.1 war. Wir berechnen die Länge nun mit dem Friedman-Test.

Der Geheimtext bestand aus $n = 330$ Buchstaben. Die Häufigkeiten der einzelnen Buchstaben sind:

$n_0 = 6$ = Anzahl der a's	$n_{13} = 10$ = Anzahl der n's
$n_1 = 6$ = Anzahl der b's	$n_{14} = 11$ = Anzahl der o's
$n_2 = 2$ = Anzahl der c's	$n_{15} = 10$ = Anzahl der p's
$n_3 = 11$ = Anzahl der d's	$n_{16} = 11$ = Anzahl der q's
$n_4 = 26$ = Anzahl der e's	$n_{17} = 18$ = Anzahl der r's
$n_5 = 19$ = Anzahl der f's	$n_{18} = 6$ = Anzahl der s's
$n_6 = 8$ = Anzahl der g's	$n_{19} = 4$ = Anzahl der t's
$n_7 = 19$ = Anzahl der h's	$n_{20} = 24$ = Anzahl der u's
$n_8 = 23$ = Anzahl der i's	$n_{21} = 33$ = Anzahl der v's
$n_9 = 21$ = Anzahl der j's	$n_{22} = 5$ = Anzahl der w's
$n_{10} = 11$ = Anzahl der k's	$n_{23} = 15$ = Anzahl der x's
$n_{11} = 12$ = Anzahl der l's	$n_{24} = 9$ = Anzahl der y's
$n_{12} = 5$ = Anzahl der m's	$n_{25} = 5$ = Anzahl der z's

Damit ist der Friedmansche Koinzidenzindex $I(x) = 0,049995$. Der Verdacht liegt nahe, dass eine polyalphabetische Chiffrierung vorliegt.

Der Friedman-Test liefert $l \approx 3,26$, also ein kurzes Schlüsselwort und gemeinsam mit dem Kasiski-Test, der als Schlüsselwortlänge ein Vielfaches von 5 lieferte, scheint sich zu bestätigen, dass 5 die Schlüsselwortlänge ist, und so war es dann ja auch.

3.3 Das Hill-Kryptosystem

Das folgende polyalphabetische Kryptosystem wurde 1929 von Lester S. Hill erfunden. Es benutzt Matrizenrechnung über endlichen Ringen, speziell über $\mathbb{Z}/26\mathbb{Z}$. Sie haben das Hill-Kryptosystem bereits in der Linearen Algebra I, als Anwendungen des Adjunktensatzes kennen gelernt, und wir werden es hier nur noch einmal kurz wiederholen.

3.3.1 Chiffrieren im Hill-Kryptosystem

Sei $m \in \mathbb{N}$, und sei R ein kommutativer Ring. Wir nehmen an, dass R ein neutrales Element der Multiplikation besitzt, das wir mit 1 bezeichnen. Sei $\mathrm{M}_{nm}(R)$ die Menge der $n \times m$-Matrizen über R, also der Matrizen mit n Zeilen und m Spalten mit Einträgen aus R. Für $A \in \mathrm{M}_{nm}(R)$ und $B \in \mathrm{M}_{ml}(R)$ definieren wir das Matrizenprodukt $A \cdot B$ als Matrix in $\mathrm{M}_{nl}(R)$ durch:

$$A \cdot B = C = (c_{ij})_{\substack{1 \le i \le n \\ 1 \le j \le l}} \in \mathrm{M}_{nl} \text{ mit } c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

Das Matrizenprodukt wird also wie gewohnt berechnet, es ist nur zu beachten, dass alle Rechnungen in R durchgeführt werden. Sei $\mathrm{M}_{mm}(R)$ der Ring der $m \times m$-Matrizen mit Einträgen in R. Die Menge der invertierbaren Elemente in $\mathrm{M}_{mm}(R)$ bezeichnen wir mit $\mathrm{Gl}_m(R)$. Sie bilden mit der Multiplikation von Matrizen eine Gruppe. Das neutrale Element in $\mathrm{Gl}_m(R)$ ist die $m \times m$ Einheitsmatrix I_m.

Wenn der Ring R ein Körper K ist, können wir mit Hilfe des Gaußalgorithmus leicht entscheiden, ob eine Matrix $A \in \mathrm{M}_{mm}(K)$ invertierbar ist, und, falls dies der Fall ist, können wir A^{-1} berechnen. Dies Hilfsmittel steht uns allerdings bei Matrizen über beliebigen kommutativen Ringen nicht zur Verfügung. Allerdings haben wir zum Invertieren von Matrizen über kommutativen Ringen ein anderes Hilfsmittel, nämlich den Adjunktensatz. Dazu erinnern wir an den Begriff der Adjunkten A^{Ad} einer Matrix A:

Sei $A = (a_{ij}) \in \mathrm{M}_{mm}(R)$. Dann ist $A^{Ad} = (a'_{ij}) \in \mathrm{M}_{mm}(R)$, wobei für alle $1 \le i, j \le m$ gilt: $a'_{ij} = (-1)^{i+j} \det A_{ji}$ und $A_{ji} \in \mathrm{M}_{m-1,m-1}(R)$ ist die Matrix, die aus A entsteht, indem wir die j-te Zeile und die i-te Spalte aus A streichen.

Es gilt der folgende, wichtige Adjunktensatz:

3.3.1 Satz Sei $A \in \mathrm{M}_{mm}(R)$. Dann gilt $A \cdot A^{Ad} = A^{Ad} \cdot A = \det A \cdot I_m$.

Beweis: Lineare Algebra I, Kurseinheit 4. □

Sei $A \in \mathrm{M}_{mm}(R)$ invertierbar. Der Adjunktensatz ermöglicht uns, die zu A inverse Matrix zu berechnen, denn $A^{-1} = (\det A)^{-1} \cdot A^{Ad}$.

Das Hill-Kryptosystem ist durch folgende Daten gegeben:

3.3.2 Definition Sei m eine natürliche Zahl. Im **Hill-Kryptosystem** sind $\mathcal{P} = \mathcal{C} = (\mathbb{Z}/26\mathbb{Z})^m$ (Zeilenvektoren). Es ist $\mathcal{K} = \mathrm{Gl}_m(\mathbb{Z}/26\mathbb{Z})$. Für ein $K \in \mathcal{K}$ sei

$$\begin{array}{ll} & e_K : (\mathbb{Z}/26\mathbb{Z})^m \to (\mathbb{Z}/26\mathbb{Z})^m \quad e_K(x) = xK, \\ \text{und} & d_K : (\mathbb{Z}/26\mathbb{Z})^m \to (\mathbb{Z}/26\mathbb{Z})^m \quad d_K(y) = yK^{-1}. \end{array}$$

3.3.3 Beispiel Alice und Bob vereinbaren eine natürliche Zahl m und eine in $\mathrm{M}_{mm}(\mathbb{Z}/26\mathbb{Z})$ invertierbare Matrix K, beispielsweise $m = 2$ und $K = \begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix}$.

Alice möchte Bob die geheime Nachricht

j a m e s h a t l o n d o n v e r l a s s e n

schicken. Sie übersetzt die Buchstaben in ihre numerischen Äquivalente in $\mathbb{Z}/26\mathbb{Z}$ und erhält [9, 0, 12, 4, 18, 7, 0, 19, 11, 14, 13, 3, 14, 13, 21, 4, 17, 11, 0, 18, 18,4, 13].

Sie unterteilt die Zahlenfolge in Tupel der Länge 2:

[9, 0], [12, 4], [18, 7], [0, 19], [11, 14], [13, 3], [14, 13], [21, 4], [17, 11], [0, 18], [18, 4], [13,23].

Bei dem letzten Tupel hat sie, da die Botschaft aus einer ungeraden Anzahl von Buchstaben besteht, das numerische Äquivalent zu x eingefügt. Sie berechnet nun für jedes Tupel $[x_1, x_2]$ das Tupel $[x_1, x_2]K$. Dies macht sie, um Schreibarbeit zu minimieren, indem sie die Tupel zeilenweise in eine Matrix schreibt:

$$\begin{pmatrix} 9 & 0 \\ 12 & 4 \\ 18 & 7 \\ 0 & 19 \\ 11 & 14 \\ 13 & 3 \\ 14 & 13 \\ 21 & 4 \\ 17 & 11 \\ 0 & 18 \\ 18 & 4 \\ 13 & 23 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 9 & 9 \\ 16 & 2 \\ 25 & 20 \\ 19 & 24 \\ 25 & 15 \\ 16 & 25 \\ 1 & 14 \\ 25 & 11 \\ 2 & 9 \\ 18 & 20 \\ 22 & 8 \\ 10 & 1 \end{pmatrix}.$$

Sie bildet das alphabetische Äquivalent zu

[9, 9], [16, 2], [25, 20], [19, 24], [25, 15], [16, 25], [1, 14], [25, 11], [2, 9], [18, 20], [22, 8], [10, 1], also

j j q c z u t y z p q z b o z l c j s u w i k b

und schickt dies an Bob.

Bob berechnet $\det K = 3$. Es ist $\mathrm{ggT}(3, 26) = 1$, also ist K invertierbar. Es ist

$$K^{Ad} = \begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix}^{Ad} = \begin{pmatrix} 4 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 25 \\ 25 & 1 \end{pmatrix} \in \mathrm{M}_{22}(\mathbb{Z}/26\mathbb{Z}).$$

Mit dem erweiterten Euklidischen Algorithmus berechnet Bob $\det(K)^{-1} = 3^{-1} = 9$ in $\mathbb{Z}/26\mathbb{Z}$.

Nun berechnet Bob $9 \cdot \begin{pmatrix} 4 & 25 \\ 25 & 1 \end{pmatrix} = \begin{pmatrix} 10 & 17 \\ 17 & 9 \end{pmatrix} \in M_{22}(\mathbb{Z}/26\mathbb{Z})$ und hat damit K^{-1} bestimmt. Er übersetzt nun Alices Botschaft in Tupel der Länge 2 von Zahlen in $\mathbb{Z}/26\mathbb{Z}$ und bildet für $[y_1, y_2]$ dann $[y_1, y_2]K^{-1}$. Übersetzt in das alphabetische Äquivalent erhält er den Klartext.

3.3.2 Lester Hill

Lester Hill (1891-1961) war einer der Begründer der algebraischen Kryptografie. Er veröffentlichte 1929 und 1931 zwei Artikel, in denen er Matrizen als Schlüssel zum Chiffrieren vorschlug. Beide Kryptosysteme haben sich nicht durchgesetzt. Der Grund dafür war vermutlich, dass die Rechenoperationen in einer Zeit ohne Computer sehr zeitaufwändig waren. Hill selbst erkannte dies und entwarf Maschinen, die die benötigten Rechnungen durchführen konnten. Hills wirklicher Beitrag zur Kryptografie war ein anderer. Er wies den Weg hin zu einer Kryptografie, die nicht mehr auf die Genialität zweier Individuen angewiesen ist, sondern auf mathematische Theorien zurückgreift, in denen Rechner die komplexen mathematischen Operationen des Chiffrierens und Dechiffrierens durchführen können.

3.4 Kryptoanalyse des Hill-Kryptosystems

Das Hill-Kryptosystem ist mit einem Known-Ciphertext-Angriff allein nicht leicht zu brechen. Anders ist es dagegen mit einem Known-Plaintext-Angriff. (Vergleichen Sie die verschiedenen Angriffe auf Kryptosysteme in 2.6.1.)

Angenommen, Oscar würde m kennen und hätte sich mindestens m verschiedene m-Tupel

$$x_1 = (x_{11}, \ldots, x_{1m}), \ldots, x_m = (x_{m1}, \ldots, x_{mm})$$

und

$$y_1 = (y_{11}, \ldots, y_{1m}), \ldots, y_m = (y_{m1}, \ldots, y_{mm})$$

verschafft, so dass $e_K(x_i) = y_i$ für alle $1 \leq i \leq m$.

Wir definieren zwei Matrizen

$$X = (x_{ij}) = \begin{pmatrix} x_{11} & \ldots & x_{1m} \\ \vdots & & \vdots \\ x_{m1} & \ldots & x_{mm} \end{pmatrix} \quad \text{und} \quad Y = (y_{ij}) = \begin{pmatrix} y_{11} & \ldots & y_{1m} \\ \vdots & & \vdots \\ y_{m1} & \ldots & y_{mm} \end{pmatrix}.$$

Es gilt dann $XK = Y$, wobei $K \in \mathrm{M}_{mm}(\mathbb{Z}/26\mathbb{Z})$ die uns nicht bekannte Schlüsselmatrix ist. Wenn X invertierbar ist, so berechnet Oscar X^{-1} in $\mathrm{M}_{mm}(\mathbb{Z}/26\mathbb{Z})$ und erhält $K = X^{-1}Y$. Wenn X nicht invertierbar ist, so kennt Oscar vielleicht ein weiteres Paar von Klartext-Geheimtext m-Tupeln. Er ersetzt die Zeilen in X und Y systematisch durch das weitere Klartext-Geheimtextpaar und wenn er Glück hat, erhält er Matrizen X' und Y', deren Determinanten teilerfremd zu 26, also invertierbar sind.

Wenn dies nicht möglich ist, wird er K nicht präzise bestimmen können. Trotzdem wird er vielleicht Informationen über K erhalten, die ihn die richtige Matrix mit etwas Experimentieren finden lassen. Das folgende Beispiel ist im Wesentlichen in [K] enthalten.

3.4.1 Beispiel Oscar hat die Nachricht

j z s e q b e k e x l v y k m f o v m l

von Mata Hari abgefangen. Mata Hari pflegt ihre Nachrichten zu unterschreiben. Oscar ahnt, dass der Klartext mit Hilfe einer 2×2-Matrix in $\mathrm{M}_{22}(\mathbb{Z}/26\mathbb{Z})$ verschlüsselt wurde. Der Klartext

m a t a h a r i

entspricht also dem Geheimtext

y k m f o v m l.

Die Zahlentupel zu m a t a h a r i sind

$$[12, 0], [19, 0], [7, 0], [17, 8],$$

und die zu y k m f o v m l sind

$$[24, 10], [12, 5], [14, 21], [12, 11].$$

Wie es Oscar auch anstellt, er wird aus den Tupeln [12, 0], [19, 0], [7, 0] und [17, 8] keine über $\mathbb{Z}/26\mathbb{Z}$ invertierbare Matrix basteln können, denn die Determinante einer solchen Matrix ist 0 oder gerade, also in $\mathbb{Z}/26\mathbb{Z}$ nicht invertierbar.

Oscar geht nun folgendermaßen vor:

Er betrachtet die Matrix $X = \begin{pmatrix} 7 & 0 \\ 17 & 8 \end{pmatrix}$ deren Zeilen aus Zahlentupeln oben besteht. Es ist $\det X \neq 0$, allerdings ist $X \in \mathrm{M}_{22}(\mathbb{Z}/26\mathbb{Z})$ nicht invertierbar. Es gilt $XK = \begin{pmatrix} 14 & 21 \\ 12 & 11 \end{pmatrix} = Y$. Sei $K = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$.

Nun fasst Oscar die Matrizen X und Y als Elemente in $\mathrm{M}_{22}(\mathbb{Z}/13\mathbb{Z})$ auf, es sind also

$$\begin{pmatrix} 7 & 0 \\ 17 & 8 \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 4 & 8 \end{pmatrix} \in \mathrm{M}_{22}(\mathbb{Z}/13\mathbb{Z}) \text{ und } \begin{pmatrix} 14 & 21 \\ 12 & 11 \end{pmatrix} = \begin{pmatrix} 1 & 8 \\ 12 & 11 \end{pmatrix} \in \mathrm{M}_{22}(\mathbb{Z}/13\mathbb{Z}).$$

Die Matrizengleichung

$$\begin{pmatrix} 7 & 0 \\ 17 & 8 \end{pmatrix} \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} = \begin{pmatrix} 14 & 21 \\ 12 & 11 \end{pmatrix} \in \mathrm{M}_{22}(\mathbb{Z}/26\mathbb{Z})$$

schreibt sich in $\mathrm{M}_{22}(\mathbb{Z}/13\mathbb{Z})$ dann als

$$\begin{pmatrix} 7 & 0 \\ 4 & 8 \end{pmatrix} \begin{pmatrix} \overline{k_{11}} & \overline{k_{12}} \\ \overline{k_{21}} & \overline{k_{22}} \end{pmatrix} = \begin{pmatrix} 1 & 8 \\ 12 & 11 \end{pmatrix},$$

wobei die Einträge $\overline{k_{ij}}$ die modulo 13 reduzierten k_{ij} sind. In $\mathrm{M}_{22}(\mathbb{Z}/13\mathbb{Z})$ ist $\begin{pmatrix} 7 & 0 \\ 4 & 8 \end{pmatrix}$ invertierbar, denn $\det \begin{pmatrix} 7 & 0 \\ 4 & 8 \end{pmatrix} \bmod 13 = 4$, und $\mathrm{ggT}(4, 13) = 1$.

Invers zu 4 ist 10 in $\mathbb{Z}/13\mathbb{Z}$ und es ist $\begin{pmatrix} 7 & 0 \\ 4 & 8 \end{pmatrix}^{Ad} = \begin{pmatrix} 8 & 0 \\ 9 & 7 \end{pmatrix}$ in $\mathrm{M}_{22}(\mathbb{Z}/13\mathbb{Z})$. Damit ist

$$\begin{pmatrix} 7 & 0 \\ 4 & 8 \end{pmatrix}^{-1} = 10 \begin{pmatrix} 8 & 0 \\ 9 & 7 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 12 & 5 \end{pmatrix} \in \mathrm{M}_{22}(\mathbb{Z}/13\mathbb{Z}).$$

Damit gilt

$$\begin{pmatrix} \overline{k_{11}} & \overline{k_{12}} \\ \overline{k_{21}} & \overline{k_{22}} \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 12 & 5 \end{pmatrix} \begin{pmatrix} 1 & 8 \\ 12 & 11 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}.$$

Oscar kennt also K bis auf Vielfache von 13, die er möglicherweise zu den Einträgen $\overline{k_{ij}}$ addieren muss. Da die k_{ij} Elemente in $\mathbb{Z}/26\mathbb{Z}$ sind, folgt:

$$\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} = \begin{pmatrix} \overline{k_{11}} & \overline{k_{12}} \\ \overline{k_{21}} & \overline{k_{22}} \end{pmatrix} + 13 \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

und die Einträge a_{ij} sind 0 oder 1. Sei $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$. Für A stehen folgende $2^4 = 16$ Möglichkeiten zur Verfügung:

$$A_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

$$A_5 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_6 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad A_7 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \quad A_8 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix},$$

$$A_9 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \quad A_{10} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_{11} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_{12} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$A_{13} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_{14} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad A_{15} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad A_{16} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Falls $A = A_3$, so ist $\det K$ gerade, also $\mathrm{ggT}(\det K, 26) \neq 1$, und K ist nicht invertierbar. Dies ist ein Widerspruch, und Oscar kann die Möglichkeit $A = A_3$ ausschließen. Analog kann er $A_4, A_6, A_7, A_8, A_9, A_{10}, A_{11}, A_{13}$ und A_{15} ausschließen.

Damit bleiben also nur noch die Fälle $A = A_1$, oder $A = A_2$, oder $A = A_5$, oder $A = A_{12}$, oder $A = A_{14}$ oder $A = A_{16}$ übrig. Diese 6 Fälle muss Oscar durchprobieren, jeweils K^{-1} bestimmen und überprüfen, ob er einen sinnvollen Text erhält. Das ist immerhin weniger als alle 157 248 möglichen invertierbaren Matrizen in $\mathrm{M}_{22}(\mathbb{Z}/26\mathbb{Z})$. Und Oscar hat Glück. Schon mit $A = A_1$ erhält er den Text

f l i e h e s o f o r t m a t a h a r i ,

und das wird auch wohl der Klartext gewesen sein.

3.5 Stromchiffren

Bei den bisher vorgestellten Kryptosystemen wurde der Klartext (beziehungsweise dessen numerisches Äquivalent) in Blöcke einer festen Länge m unterteilt, und jeder Block wurde unter der Verwendung des gleichen Schlüssels chiffriert. Solche Kryptosysteme nennt man auch **Blockchiffren**. Für diese gilt also: Sei $K \in \mathcal{K}$ ein Schlüssel, und sei $\mathbf{x} = x_1\ x_2\ x_3\ \ldots$ eine Folge von Klartextsymbolen, wobei

jedes x_i ein Block der Länge m ist. Sei e_K die Chiffrierungsregel. Dann hat der Geheimtext $y = y_1\ y_2\ y_3 \ldots$ die Form $y = e_K(x_1)\ e_K(x_2)\ e_K(x_3) \ldots$.

3.5.1 Definition und Beispiele

Bei Stromchiffren wählt man für jedes Klartextsymbol einen eigenen Schlüssel.

Die Idee bei Stromchiffren ist es, einen Schlüsselstrom $\mathbf{z} = z_1\ z_2\ z_3\ \ldots$ zu erzeugen, und mit diesem eine Folge $\mathbf{x} = x_1\ x_2\ x_3\ \ldots$ von Klartextsymbolen folgendermaßen zu verschlüsseln:

$$\mathbf{y} = e_{z_1}(x_1)\ e_{z_2}(x_2)\ e_{z_3}(x_3)\ \ldots$$

Eine Funktion f_i wird benutzt, um das i-te Element z_i des Schlüsselstroms zu erzeugen. Dabei hängt f_i ab von einem gewählten Schlüssel $K \in \mathcal{K}$ und den ersten $i-1$ Klartextsymbolen. Es ist also $z_i = f_i(K,\ x_1, \ldots, x_{i-1})$. Das Schlüsselstromelement z_i wird benutzt um x_i zu verschlüsseln, also $y_i = e_{z_i}(x_i)$.

Um den Klartext $x_1\ x_2\ x_3 \ldots$ zu verschlüsseln, berechnet Alice nacheinander z_1, y_1, z_2, y_2, $\ldots$. Bob dechiffriert $y_1\ y_2\ y_3 \ldots$ indem er nacheinander $z_1,\ x_1,\ z_2,\ x_2,\ \ldots$ berechnet.

Eine formale Definition von Stromchiffren ist wie folgt:

3.5.1 Definition Eine **Stromchiffre** ist ein Tupel $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{L}, \mathcal{F}, \mathcal{E}, \mathcal{D})$, so dass folgende Regeln gelten:

(i) $\mathcal{P}$ ist eine endliche Menge von Klartexten.

(ii) $\mathcal{C}$ ist eine endliche Menge von Geheimtexten.

(iii) $\mathcal{K}$ ist eine endliche Menge von Schlüsseln.

(iv) $\mathcal{L}$ ist eine endliche Menge, genannt das Schlüsselstromalphabet.

(v) $\mathcal{F} = (f_1, f_2, \ldots)$ ist der Schlüsselstrom-Erzeuger. Für $i \geq 1$ ist f_i eine Abbildung, $f_i : \mathcal{K} \times \mathcal{P}^{i-1} \to \mathcal{L}$.

(vi) Für jedes $z \in \mathcal{L}$ gibt es eine Chiffrierungsregel $e_z \in \mathcal{E}$, $e_z : \mathcal{P} \to \mathcal{C}$ und eine Dechiffrierungsregel $d_z \in \mathcal{D}$, $d_z : \mathcal{C} \to \mathcal{P}$, so dass für alle $x \in \mathcal{P}$ gilt: $d_z(e_z(x)) = x$.

3.5.2 Beispiel Als Beispiel betrachten wir das sogenannte **Selbstschlüssel-Kryptosystem**:

Es ist $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathcal{L} = \mathbb{Z}/26\mathbb{Z}$. Sei $z_1 = K$, und sei $z_i = x_{i-1}$ für $i \geq 2$. Für $0 \leq z \leq 25$ definieren wir

$$\begin{aligned} e_z(x) &= x + z \bmod 26 \text{ und} \\ d_z(y) &= y - z \bmod 26. \end{aligned}$$

Zur Illustration: Nehmen wir an, Alice und Bob hätten vereinbart, das Selbstschlüssel Kryptosystem zur Übermittlung von Nachrichten zu benutzen, und sie hätten als Schlüssel $K = 8$ gewählt. Alice möchte an Bob die Nachricht

r e n d e z v o u s

schicken. Sie übersetzt den Text in sein numerisches Äquivalent

17, 4, 13, 3, 4, 25, 21, 14, 20, 18.

Der Schlüssselstrom ist $z_1 = 8$, $z_2 = x_1 = 17$, $z_3 = x_2 = 4$, $z_4 = x_3 = 13$, $\ldots$, $z_{10} = x_9 = 20$, also

8, 17, 4, 13, 3, 4, 25, 21, 14, 20.

Sie bildet nun

$$\begin{aligned} y_1 &= 17 + 8 \bmod 26 = 25 \\ y_2 &= 4 + 17 \bmod 26 = 21 \\ y_3 &= 13 + 4 \bmod 26 = 17 \\ y_4 &= 3 + 13 \bmod 26 = 16 \\ y_5 &= 4 + 3 \bmod 26 = 7 \\ y_6 &= 25 + 4 \bmod 26 = 3 \\ y_7 &= 21 + 25 \bmod 26 = 20 \\ y_8 &= 14 + 21 \bmod 26 = 9 \\ y_9 &= 20 + 14 \bmod 26 = 8 \\ y_{10} &= 18 + 20 \bmod 26 = 12. \end{aligned}$$

Sie übersetzt $\mathbf{y} = y_1 y_2 \ldots y_{10}$ in sein alphabetisches Äquivalent z v r q h d u j i m und schickt dies an Bob.
Bob übersetzt den Geheimtext in sein numerisches Äquivalent 25, 21, 17, 16, 7, 3, 20, 9, 8, 12. Er bildet

$$\begin{aligned} x_1 &= d_{z_1}(25) = 25 - 8 \bmod 26 = 17, \text{ denn } z_1 = z = 8 \\ x_2 &= d_{z_2}(21) = 21 - 17 \bmod 26 = 4, \text{ denn } z_2 = x_1 = 17 \\ x_3 &= d_{z_3}(17) = 17 - 4 \bmod 26 = 13, \text{ denn } z_3 = x_2 = 4 \end{aligned}$$

und so weiter. Mit jedem Schritt erhält er ein neues Klartextsymbol, welches ihm ein neues Schlüsselstromelement liefert.

Natürlich ist das Selbstschlüssel Kryptosystem unsicher. Da es nur 26 mögliche

Schlüssel gibt, wird Oscar durch systematisches Probieren einen abgefangenen Geheimtext schnell dechiffrieren können.

3.5.3 Definition Eine Stromchiffre heißt **synchron**, wenn der Schlüsselstrom unabhängig vom Klartext ist.

3.5.4 Beispiele
1. Wir können das Vigenère Kryptosystem als eine synchrone Stromchiffre interpretieren. Wenn $k = (k_1, \ldots, k_m)$ das Schlüsselwort ist, so ist $z = k_1 \ldots k_m k_1 \ldots k_m \ldots$ ein Schlüsselstrom mit $z_1 = k_1, \ldots, z_m = k_m$, und $z_j = k_i$ falls $i \bmod m = j$.
2. Das Selbstschlüssel Kryptosystem ist ein Beispiel für eine nicht synchrone Stromchiffre.

3.5.5 Definition Eine Stromchiffre heißt **periodisch** mit Periode d, falls $z_{i+d} = z_i$ für alle $i \geq 1$.

3.5.6 Beispiel Eine Vigenère Chiffre, deren Schlüsselwort die Länge m hat, kann als periodische Stromchiffre der Periode m interpretiert werden.

3.5.2 Zahlen zu verschiedenen Basen

In Lehrbüchern der Kryptografie werden Stromchiffren in der Regel in dem Kontext erklärt, wo Klartext und Geheimtext aus Folgen von 0 und 1 bestehen, und das Schlüsselstromalphabet ist $\mathbb{Z}/2\mathbb{Z}$. In dieser Situation ist chiffrieren und dechiffrieren gerade Addition modulo 2, also

$$e_z(x) = x + z \bmod 2, \text{ und } d_z(y) = y + z \bmod 2.$$

Wir überprüfen kurz, dass $d_z(e_z(x)) = x$ für alle $x \in \{0, 1\}$ und alle $z \in \{0, 1\}$.

Fall 1: $z = 0$. Dann gilt für alle $x \in \{0, 1\}$:
$d_z(e_z(x)) = d_z(x + 0) = d_z(x) = x + 0 = x$.

Fall 2: $z = 1$. Dann gilt für alle $x \in \{0, 1\}$
$d_z(e_z(x)) = d_z(x + 1) = x + 1 + 1 = x + 0 = x$.

Die Annahme, dass Klar- und Geheimtext als Folge von 0 und 1 vorliegen, ist nicht ungewöhnlich. Wir können jede ganze Zahl ≥ 0 zur Basis 2 darstellen. Machen wir dies gleich allgemeiner:

3.5.7 Definition Sei $n \in \mathbb{Z},\ n \geq 0$, und sei $b \in \mathbb{Z},\ b > 1$. Wir sagen, dass n eine **k-stellige Zahl** $(d_{k-1}d_{k-2}\ldots d_1 d_0)_b$ **zur Basis** b ist, falls $n = d_{k-1}b^{k-1} +$

$d_{k-2}b^{k-2} + \cdots + d_1 b + d_0$ ist, und falls für alle $0 \leq i \leq k-1$ gilt: $0 \leq d_i < b$, und $d_{k-1} \neq 0$.

3.5.8 Definition Zahlen zur Basis 2 werden **Binärzahlen**, und Zahlen zur Basis 10 werden **Dezimalzahlen** genannt.

3.5.9 Beispiele (a)

$$\begin{aligned} (11001001)_2 &= 201, \text{ denn} \\ 201 &= 1 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2 + 1 \\ &= 128 + 64 + 8 + 1 \end{aligned}$$

(b)

$$\begin{aligned} (4123)_5 &= 538, \text{ denn} \\ 538 &= 4 \cdot 5^3 + 1 \cdot 5^2 + 2 \cdot 5 + 3 \\ &= 500 + 25 + 10 + 3 \end{aligned}$$

Um eine Zahl n als k-stellige Zahl zur Basis b darzustellen, teilen wir n durch b mit Rest, und $n \bmod b$ liefert die Stelle d_0. Also $n = a_1 b + d_0$. Die Stelle d_1 erhalten wir, indem wir a_1 durch b mit Rest teilen, also $a_1 = a_2 b + d_1,\ d_1 = a_1 \bmod b$. Die Stelle d_2 bekommen wir, indem wir $a_2 \bmod b$ berechnen, und so weiter. Dieses Verfahren wird **Divisions-Rest-Methode** genannt.

3.5.10 Beispiel Wir wollen $n = 1\,000\,000$ zur Basis 2 bestimmen.

$$\begin{array}{rcrcl}
1\,000\,000 & = & 500\,000 \cdot 2 & + & 0 \\
500\,000 & = & 250\,000 \cdot 2 & + & 0 \\
250\,000 & = & 125\,000 \cdot 2 & + & 0 \\
125\,000 & = & 62\,500 \cdot 2 & + & 0 \\
62\,500 & = & 31\,250 \cdot 2 & + & 0 \\
31\,250 & = & 15\,625 \cdot 2 & + & 0 \\
15\,625 & = & 7\,812 \cdot 2 & + & 1 \\
7\,812 & = & 3\,906 \cdot 2 & + & 0 \\
3\,906 & = & 1\,953 \cdot 2 & + & 0 \\
1\,953 & = & 976 \cdot 2 & + & 1 \\
976 & = & 488 \cdot 2 & + & 0 \\
488 & = & 244 \cdot 2 & + & 0 \\
244 & = & 122 \cdot 2 & + & 0 \\
122 & = & 61 \cdot 2 & + & 0 \\
61 & = & 30 \cdot 2 & + & 1 \\
30 & = & 15 \cdot 2 & + & 0 \\
15 & = & 7 \cdot 2 & + & 1 \\
7 & = & 3 \cdot 2 & + & 1 \\
3 & = & 1 \cdot 2 & + & 1 \\
1 & = & 0 \cdot 2 & + & 1.
\end{array}$$

Damit ist $n = (11110100001001000000)_2$.

Tools zum Umschreiben von Dezimalzahlen in Binärzahlen und von Binärzahlen in Dezimalzahlen finden Sie in der virtuellen Universität. Aber machen wir es einmal von Hand:

3.5.11 Aufgabe Stellen Sie die Dezimalzahl 7891 zur Basis 2 dar.

3.5.3 Der ASCII-Code

Eine weitere Methode, einen Text in $0, 1$ Folgen zu übertragen, ist die folgende:

Jedem Symbol des Klartextes (Buchstaben, Zahlen, Sonderzeichen) wird ein bestimmtes Muster aus 8 Bits (Nullen und Einsen) zugeordnet. Dazu benutzt man meistens den sogenannten ASCII Code. Gesprochen wird dies Asskie, und ASCII ist eine Abkürzung für „American Standard Code for Information Interchange“.

Als Beispiele einige ASCII-Zeichen (Vergleiche [Beu]).

ASCII-Zeichen	Binäre Form	ASCII-Zeichen	Binäre Form
Zwischenraum	00100000	H	01001000
!	00100001	I	01001001
0	00110000	J	01001010
1	00110001	K	01001011
2	00110010	L	01001100
3	00110011	M	01001101
4	00110100	N	01001110
5	00110101	O	01001111
6	00110110	P	01010000
7	00110111	Q	01010001
8	00111000	R	01010010
9	00111001	S	01010011
A	01000001	T	01010100
B	01000010	U	01010101
C	01000011	V	01010110
D	01000100	W	01010111
E	01000101	X	01011000
F	01000110	Y	01011001
G	01000111	Z	01011010

Wenn Klar- und Geheimtext Folgen von 0 und 1 sind, und wenn auch das Schlüsselstromalphabet $\mathcal{L} = \{0, 1\}$ ist, so lässt sich das Chiffrieren $e_z(x) = x + z \bmod 2$ und Dechiffrieren $d_z(y) = y + z \bmod 2$ sehr effektiv in die Hardware eines Computers implementieren. Mit anderen Worten: Chiffrieren und Dechiffrieren mit dem Rechner kann schnell erfolgen.

3.6 Das One-time Pad

Das One-time Pad ist ein Beispiel für eine synchrone Stromchiffre, das heißt, der Schlüssel ist unabhängig vom Klartext. Es handelt sich im Wesentlichen um eine Vigenère-Verschlüsselung, bei der die Schlüsselwortlänge gleich der Länge des Klartextes ist. Wir werden dabei annehmen, dass Klar- und Geheimtext Folgen von 0 und 1 sind. Eine formale Beschreibung des Kryptosystems ist wie folgt:

3.6.1 Definition Im **One-time Pad** sei $n \geq 1$, und sei $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}/2\mathbb{Z})^n$. Sei $K = (K_1, \ldots, K_n) \in \mathcal{K}$ und sei $\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{P}$. Dann ist

$$\begin{aligned} e_K(x) &= (x_1 + K_1, \ldots, x_n + K_n) \bmod 2 \text{ und} \\ d_K(y) &= (y_1 + K_1, \ldots, y_n + K_n) \bmod 2 \end{aligned}$$

Dabei bedeutet die Schreibweise $(x_1 + K_1, \ldots, x_n + K_n) \bmod 2$, dass jeder Eintrag $x_i + K_i$ modulo 2 reduziert wird.

Alice und Bob gehen also folgendermaßen vor: Sie verabreden einen Schlüssel $K = (K_1, \ldots, K_n) \in (\mathbb{Z}/2\mathbb{Z})^n$, wobei n mindestens so groß wie die Anzahl der Buchstaben einer zu verschlüsselnden Nachricht ist. Dabei ist es für die Sicherheit der Nachrichtenübermittlung wichtig, dass die Einträge in K zufällig gewählt werden, also alle mit derselben Wahrscheinlichkeit vorkommen. Alice oder Bob könnten etwa für die Absprache des Eintrags K_i eine Münze werfen, und bei Kopf $K_i = 1$, bei Zahl $K_i = 0$ setzen. Verschlüsseln und Entschlüsseln erfolgt dann wie oben beschrieben.

Man könnte beim One-time Pad den Eindruck gewinnen, dass man den Teufel (die Übermittlung einer Nachricht der Länge n) gegen den Belzebub (die Verabredung eines Schlüssels der Länge n) eingetauscht hat. Dies ist aber nicht richtig, denn im Normalfall können Alice und Bob den Zeitpunkt zur Schlüsselverabredung frei wählen, also wenn sie sich vor Oscar sicher fühlen, wohingegen sie auf den Zeitpunkt der Nachrichtenübermittlung oft keinen Einfluss haben.

Das One-time Pad ist eines der wenigen Kryptosysteme, von denen man beweisen kann, dass sie sicher sind. Dabei bedeutet Sicherheit, dass Oscar keine Chance hat, seine Kenntnisse über das Kryptosystem zu vergrößern, selbst wenn ihm alle Rechenkapazität der Welt zur Verfügung steht. (Für eine formale Definition von Sicherheit und den Beweis dafür, dass das One-time Pad sicher ist verweisen wir für Interessierte z. B. auf [St].)

Allerdings beruht die Sicherheit darauf, dass die Einträge von K zufällig gewählt werden, und dass jeder Schlüssel nur für eine zu übermittelnde Nachricht benutzt wird. Daher kommt der Name One-time Pad. Die Vorstellung ist die, dass der Schlüssel auf einem Abreißblock notiert ist, und wenn mit ihm eine Nachricht chiffriert wurde, wird der Zettel abgerissen und vernichtet.

Das One-time Pad Kryptosystem wurde erstmalig 1917 von Gilbert Vernam beschrieben, der es zum Patent anmeldete und hoffte, dass es kommerziell benutzt werden würde. Dies war nicht der Fall. Die Probleme sind zu offensichtlich. Es sind die Längen der Schlüssel (mindestens so groß wie die Länge der Nachricht), die sicher aufbewahrt werden müssen, und es ist die Tatsache, dass jeder Schlüssel nur ein Mal verwendet werden darf. Dies erfordert ein sehr aufwändiges Schlüssel-Management, was in der Regel nicht zu leisten ist.

Im zweiten Weltkrieg wurde das One-time Pad von der englischen Entschlüsselungstruppe vom Betchley Park benutzt, um dem Premierminister die Nachrichten zu übermitteln, die von den Deutschen mit Hilfe der Chiffriermaschine Enigma

verschlüsselt worden waren [Beu]. Die Chiffrierung der Enigma war von den Briten 1940 geknackt worden, und bis 1944 wussten die maßgeblichen deutschen Stellen nicht, dass der britische Geheimdienst seit Jahren die geheimen Nachrichten mitlas (vergleiche [Ba]).

Elektronische One-time Pads sind angeblich bis vor wenigen Jahren dazu benutzt worden, Gespräche über den „heißen Draht“ zwischen dem Weißen Haus und dem Kreml zu verschlüsseln [Beu].

Lösungen der Aufgaben

Lösungen der Aufgaben in Kapitel 3

Aufgabe 3.5.11

Wir wollen die Dezimalzahl 7891 zur Basis 2 darstellen. Dabei gehen wir vor wie im Beispiel:

$$\begin{array}{rcrcl}
7891 & = & 2 \cdot 3945 & + & 1 \\
3945 & = & 2 \cdot 1972 & + & 1 \\
1972 & = & 2 \cdot 986 & + & 0 \\
986 & = & 2 \cdot 493 & + & 0 \\
493 & = & 2 \cdot 246 & + & 1 \\
246 & = & 2 \cdot 123 & + & 0 \\
123 & = & 2 \cdot 61 & + & 1 \\
61 & = & 2 \cdot 30 & + & 1 \\
30 & = & 2 \cdot 15 & + & 0 \\
15 & = & 2 \cdot 7 & + & 1 \\
7 & = & 2 \cdot 3 & + & 1 \\
3 & = & 2 \cdot 1 & + & 1 \\
1 & = & 2 \cdot 0 & + & 1.
\end{array}$$

Damit gilt $7891 = (1111011010011)_2$.

Kurseinheit 2

Gruppen

Studierhinweise

In Kurseinheit 1 haben Sie etliche symmetrische Kryptosysteme kennen gelernt. Der Rest des Kurses wird sich asymmetrischer Kryptosysteme und der Mathematik hinter ihnen widmen. Dabei ist diese Kurseinheit die einzige, die nicht unmittelbar erkennbar einen Bezug zur Kryptografie hat.

Wir haben bereits angedeutet, dass der Trick der modernen Kryptografie darin besteht, das zu Grunde liegende Alphabet mit einer mathematischen Struktur zu versehen und diese geschickt beim Chiffrieren, Dechiffrieren oder Brechen des Kryptosystems einzusetzen. Eine wichtige mathematische Struktur ist die einer Gruppe.

Sie haben Gruppen bereits in der Linearen Algebra I studiert, allerdings nur sehr oberflächlich und nur in Beispielen. In dieser Kurseinheit werden wir Grundlagen der Gruppentheorie bereitstellen, die in den folgenden Kurseinheiten für kryptografische Verfahren benötigt werden. Dabei wird - aus dem oben genannten Grund - unser Hauptaugenmerk auf der Theorie endlicher Gruppen liegen.

Sie werden klassische Sätze der Gruppentheorie kennen lernen, wie etwa den Satz von Lagrange, den „Kleinen Satz von Fermat“ und den Satz von Euler. Diese Sätze wurden vor 250-350 Jahren bewiesen, sind aber alles andere als „Schnee von gestern“. Sie gehen an zentralen Stellen in moderne kryptografische Verfahren ein.

Diejenigen endlichen Gruppen, die im Verlauf des Kurses die wichtigste Rolle spielen werden, sind so genannte zyklische Gruppen. Diese Gruppen haben eine ganz besonders einfache Struktur. Eine Gruppe $(G, *)$ heißt zyklisch, wenn es ein $g \in G$ so gibt, dass jedes Element $h \in G$ von der Form $h = g * \cdots * g$ ist. Zyklische Gruppen werden wir im Detail in den letzten beiden Abschnitten dieser Kurseinheit untersuchen.

Kapitel 4

Gruppen

4.1 Notation und Beispiele

In den ganzen Zahlen $\mathbb{Z}$ gibt es zwei „mathematische Verknüpfungen“: Wir können zwei ganze Zahlen addieren und multiplizieren. Dieses Konzept lässt sich auf beliebige Mengen S verallgemeinern.

4.1.1 Definition Eine **Verknüpfung** auf S ist eine Abbildung $f : S \times S \to S$.

Bei einer Verknüpfung wird also zwei Elementen a, b in S wieder ein Element $f(a, b)$ in S zugeordnet. Verknüpfungen bezeichnen wir in der Regel nicht, wie sonst bei Abbildungen üblich, mit Buchstaben, sondern mit Symbolen wie $+, \cdot, \circ, * \ldots$, also

$$\begin{aligned} + &: \ S \times S \to S \\ \cdot &: \ S \times S \to S \\ \circ &: \ S \times S \to S \\ * &: \ S \times S \to S. \end{aligned}$$

Das Bild eine Paares (a, b) unter einer Verknüpfung $*$ wird dann mit $a*b$ bezeichnet, also

$$\begin{aligned} + &: \ S \times S \to S, \quad (a, b) \mapsto a + b \\ \cdot &: \ S \times S \to S, \quad (a, b) \mapsto a \cdot b \\ \circ &: \ S \times S \to S, \quad (a, b) \mapsto a \circ b \\ * &: \ S \times S \to S, \quad (a, b) \mapsto a * b. \end{aligned}$$

Unter den mathematischen Strukturen, bei denen Mengen mit einer Verknüpfung untersucht werden, ist die am häufigsten studierte und am weitesten entwickelte die einer Gruppe. Gruppen sind Ihnen bereits in der Linearen Algebra I in Kurseinheit 2 begegnet. Wir wiederholen die Definition.

4.1.2 Definition Eine **Gruppe** ist eine Menge G mit einer Verknüpfung $*$, so dass die folgenden drei Bedingungen gelten:

(i) $*$ ist **assoziativ**, das heißt, für alle $a, b, c \in G$ gilt

$$a * (b * c) = (a * b) * c.$$

(ii) Es gibt ein **neutrales Element** e in G, so dass für alle $a \in G$ gilt

$$a * e = e * a = a.$$

(iii) Für jedes a in G gibt es ein **inverses Element** $a^{-1} \in G$, so dass

$$a * a^{-1} = a^{-1} * a = e.$$

Wenn die Gruppe noch die Bedingung

(iv) Für alle $a, b \in G$ gilt

$$a * b = b * a.$$

erfüllt, so wird G **abelsch** oder **kommutativ** genannt.

4.1.3 Definition Ist G eine Gruppe, und ist die Mächtigkeit $|G| < \infty$, so wird G eine **endliche Gruppe** genannt. Die Anzahl der Elemente in G wird dann die **Ordnung** von G genannt. Ist $|G| = \infty$, so nennt man G eine **unendliche Gruppe** und sagt, dass die Ordnung von G **unendlich** ist.

Sie haben in der Linearen Algebra I gesehen, dass das neutrale Element e einer Gruppe G und das zu einem Element a inverse Element eindeutig bestimmt ist. Weiterhin gelten $(a * b)^{-1} = b^{-1} * a^{-1}$ für alle $a, b \in G$. Dabei bezeichnen wir mit a^{-1} das zu a inverse Element.

4.1.4 Vereinbarung Die am häufigsten benutzten Schreibweisen für Verknüpfungen in Gruppen sind $\cdot$ und $+$. Im ersten Fall sagen wir, dass wir die Gruppe G **multiplikativ** geschrieben haben, im zweiten Fall, dass wir sie **additiv** geschrieben haben. Das bedeutet aber keinesfalls, dass $\cdot$ und $+$ die übliche Addition und Multiplikation sind. Die additive Schreibweise von Gruppen wird in der Regel dann verwendet, wenn G abelsch ist. Wir treffen folgende Vereinbarungen zur Vereinfachung der Schreibweisen:

1. Statt $a \cdot b$ schreiben wir in der Regel nur ab.

2. Wenn wir Gruppen multiplikativ schreiben, so bezeichnen wir das zu einem Element a inverse Element mit a^{-1} und das neutrale Element mit e oder 1.

   Wenn wir Gruppen additiv schreiben, bezeichnen wir das zu einem Element a inverse Element mit $-a$ und das neutrale Element mit 0.

3. Das Assoziativgesetz in einer Gruppe G mit Verknüpfung $*$ garantiert, dass wir in Ausdrücken der Form $a_1 * \cdots * a_n$ mit $a_i \in G$, $1 \leq i \leq n$, Klammern beliebig setzen dürfen. Wenn wir G multiplikativ schreiben und ausdrücken wollen, dass wir ein Element a n Mal mit sich selbst verknüpfen, so schreiben wir

   $$a^n = a \cdots a \quad (n \text{ Faktoren } a).$$

   Wenn wir G additiv schreiben und denselben Sachverhalt ausdrücken wollen, so schreiben wir

   $$na = a + \cdots + a \quad (n \text{ Summanden } a).$$

   Für $n = 0$ benutzen wir die Notation $a^0 = e$, falls wir die Gruppe multiplikativ schreiben, und $0a = 0$, falls wir sie additiv schreiben. Außerdem sei $a^{-n} = (a^{-1})^n$ beziehungsweise $(-n)a = n(-a)$.

   Wenn wir diese Notationen benutzen, ergeben sich folgende Regeln für alle $m, n \in \mathbb{Z}$:

Multiplikative Notation			**Additive Notation**		
$a^n a^m$	$=$	a^{n+m}	$na + ma$	$=$	$(n+m)a$
$(a^n)^m$	$=$	a^{nm}	$m(na)$	$=$	$(mn)a$.

4.1.5 Beispiele (a) Mit der üblichen Addition + ist $\mathbb{Z}$ eine abelsche Gruppe. Das neutrale Element ist 0, und zu $a \in \mathbb{Z}$ ist $-a$ invers. □

(b) Sei $n \in \mathbb{N}$, $n > 1$. Dann ist $\mathbb{Z}/n\mathbb{Z}$ mit der Verknüpfung

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \ (a, b) \mapsto a + b = (a + b) \mathrm{mod} n$$

eine abelsche Gruppe. Das neutrale Element ist 0, und zu einem $a \in \mathbb{Z}/n\mathbb{Z}$ ist $n - a$ invers. □

(c) Sei $n \in \mathbb{N}$, und sei $G = \mathrm{Gl}_n(\mathbb{K})$ die Menge aller invertierbaren $n \times n$-Matrizen über einem Körper $\mathbb{K}$. Mit der Matrizenmultiplikation als Verknüpfung ist G eine Gruppe, die für $n \geq 2$ nicht abelsch ist. Das neutrale Element in G ist die $n \times n$ Einheitsmatrix I_n. □

(d) Sei M eine nicht leere Menge, und sei S_M die Menge der bijektiven Abbildungen von M nach M. Wie Sie in der Linearen Algebra I, Kurseinheit 2, gesehen haben, ist S_M mit der Komposition von Abbildungen eine Gruppe. Das neutrale Element ist die identische Abbildung id_M auf M. □

(e) Ein Spezialfall der Gruppe unter (d) ist die symmetrische Gruppe S_n der bijektiven Abbildungen (Permutationen) von $\{1, \ldots, n\}$ nach $\{1, \ldots, n\}$, die wir in der Linearen Algebra I, Kurseinheit 2, genauer untersucht haben.

(f) Sei $\mathbb{K}$ ein Körper, und sei $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$. Dann ist $\mathbb{K}^\times$ mit der Multiplikation in $\mathbb{K}$ eine abelsche Gruppe. □

4.2 Untergruppen

4.2.1 Definition Sei G mit der Verknüpfung $*$ eine Gruppe. Eine Teilmenge H von G heißt **Untergruppe** von G, wenn H das neutrale Element e enthält, und wenn H mit der Verknüpfung $*$ wieder eine Gruppe ist.

4.2.2 Notation Wenn H eine Untergruppe einer Gruppe G ist, so schreiben wir $H < G$.

4.2.3 Beispiele (a) Sei G eine Gruppe mit Verknüpfung $*$ und neutralem Element e. Dann sind G und $\{e\}$ Untergruppen von G. Diese Untergruppen werden **triviale Untergruppen** von G genannt.

(b) Sei $G = \mathbb{Z}$ mit der Verknüpfung $+$. Sei $n \in \mathbb{Z}$, und sei $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$. Für zwei Elemente $nz, nz' \in n\mathbb{Z}$ gilt $nz + nz' = n(z + z') \in n\mathbb{Z}$, also ist $+$ eine Verknüpfung auf $n\mathbb{Z}$.

Das Assoziativgesetz gilt in $n\mathbb{Z}$, denn es gilt für alle ganzen Zahlen.

Es ist $0 = n0 \in n\mathbb{Z}$, somit enthält $n\mathbb{Z}$ das neutrale Element.

Zu $nz \in n\mathbb{Z}$ ist $-nz = n(-z)$ invers, und $n(-z) \in n\mathbb{Z}$. Es folgt, dass $n\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$ ist. □

(c) Sei $G = \mathrm{Gl}_n(\mathbb{K})$ die Menge der invertierbaren $n \times n$-Matrizen über einem Körper $\mathbb{K}$, und sei H die Teilmenge der Matrizen $A \in \mathrm{Gl}_n(\mathbb{K})$ mit $\det(A) = 1$.

Mit dem Determinantenmultiplikationssatz gilt für alle $A, B \in H$, dass $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$ ist, und es folgt, dass die Matrizenmultiplikation eine Verknüpfung auf H ist.

Das Assoziativgesetz gilt für alle Matrizen in $\mathrm{Gl}_n(\mathbb{K})$, also gilt es auch für die Matrizen in H.

Es ist $I_n \in H$, denn $\det(I_n) = 1$.

Sei $A \in H$, und sei $A^{-1} \in \mathrm{Gl}_n(\mathbb{K})$. Dann gilt

$$1 = \det(AA^{-1}) = \det(A)\det(A^{-1}) = 1 \cdot \det(A^{-1}),$$

also $\det(A^{-1}) = 1$ und $A^{-1} \in H$. Es folgt, dass H eine Untergruppe von $\mathrm{Gl}_n(\mathbb{K})$ ist. □

(d) Sei $G = S_n$, $n \geq 2$. Sei $A_n \subseteq S_n$ die Teilmenge der Permutationen σ mit $\mathrm{sgn}(\sigma) = 1$. Zur Erinnerung: Es ist sgn die Signatur, und für eine Permutation $\sigma \in S_n$ gilt

$$\mathrm{sgn}(\sigma) = \begin{cases} 1 & \text{gerade ist} \\ & \text{falls die Anzahl der Paare } (i,j) \\ & \text{mit } i > j \text{ und } \sigma(i) < \sigma(j) \\ -1 & \text{ungerade ist.} \end{cases}$$

Seien $\sigma, \tau \in A_n$. Mit der Signaturformel (Lineare Algebra I, Kurseinheit 2) gilt

$$\mathrm{sgn}(\sigma \circ \tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau) = 1 \cdot 1 = 1,$$

und es folgt, dass $\circ$ eine Verknüpfung auf A_n ist.

Da die Komposition von Abbildungen assoziativ ist, gilt das Assoziativgesetz in A_n.

Das neutrale Element in A_n ist die identische Permutation.

Sei $\sigma \in A_n$, und sei $\sigma^{-1} \in S_n$. Wieder mit der Signaturformel gilt

$$1 = \mathrm{sgn}(\sigma \circ \sigma^{-1}) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\sigma^{-1}) = 1 \cdot \mathrm{sgn}(\sigma^{-1}),$$

also $\sigma^{-1} \in A_n$. Es folgt, dass A_n eine Gruppe ist. A_n wird die **alternierende Gruppe** genannt. □

(e) Sei $G = \mathbb{C}^\times$, und sei $H = \{-1, 1, i, -i\} \subseteq \mathbb{C}^\times$. Das Produkt von zwei Elementen in H liegt in H, somit ist die Multiplikation eine Verknüpfung auf H.

Das Assoziativgesetz gilt für alle Elemente in H.

Das neutrale Element 1 liegt in H.

Invers zu 1 ist $1 \in H$, invers zu -1 ist $-1 \in H$, invers zu i ist $-i \in H$, und invers zu $-i$ ist $i \in H$. Es folgt, dass H eine Untergruppe von $\mathbb{C}^\times$ ist. □

Zur Überprüfung, ob eine Teilmenge einer Gruppe G eine Untergruppe ist, ist folgendes Kriterium nützlich.

4.2.4 Proposition (Untergruppenkriterium)

Sei $(G, \cdot)$ eine Gruppe, und sei H eine nicht leere Teilmenge von G. Dann gilt

$$H < G \Leftrightarrow ab^{-1} \in H \text{ für alle } a, b \in H.$$

Beweis:

$\Rightarrow$ Seien $a, b \in H$. Da H eine Gruppe ist, folgt $b^{-1} \in H$. Da $\cdot$ eine Verknüpfung auf H ist, gilt $ab^{-1} \in H$.

$\Leftarrow$ Sei $H \neq \emptyset$, und sei $ab^{-1} \in H$ für alle $a, b \in H$. Da $H \neq \emptyset$ gibt es ein $a \in H$. Nach Voraussetzung liegt $aa^{-1} = e$ in H, somit hat H ein neutrales Element.

Nach Voraussetzung liegt mit $a \in H$ auch $ea^{-1} = a^{-1}$ in H. Es folgt, dass jedes Element in H ein inverses Element in H besitzt.

Das Assoziativgesetz gilt für alle Elemente in H, denn $H \subseteq G$, und es gilt für alle Elemente in G.

Da mit $b \in H$ auch $b^{-1} \in H$, gilt nach Voraussetzung $a(b^{-1})^{-1} = ab \in H$, und dies zeigt, dass $\cdot$ eine Verknüpfung auf H ist. Somit ist $(H, \cdot)$ eine Gruppe.

□

4.2.5 Aufgaben (1) Formulieren Sie das Untergruppenkriterium und dessen Beweis für Gruppen, die additiv geschrieben sind.

(2) Sei G eine Gruppe, und seien K, H Untergruppen von G. Beweisen Sie, dass $K \cap H$ eine Untergruppe von G ist.

4.2.6 Beispiel Sei $(G, \cdot)$ eine Gruppe, und sei $a \in G$. Sei

$$\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}.$$

Da $a \in \langle a \rangle$, ist $\langle a \rangle \neq \emptyset$. Seien $a^r, a^s \in \langle a \rangle$. Es ist $(a^s)^{-1} = a^{-s}$, und $a^r a^{-s} = a^{r-s} \in \langle a \rangle$. Es folgt mit dem Untergruppenkriterium, dass $\langle a \rangle$ eine Untergruppe von G ist.

4.2.7 Definition Die in 4.2.6 definierte Untergruppe wird die **von a erzeugte Untergruppe** von G genannt. Wenn $\langle a \rangle$ eine endliche Gruppe ist, so nennen wir $|\langle a \rangle|$ die **Ordnung** von a und schreiben $\text{ord}(a) = |\langle a \rangle|$. Ist $\langle a \rangle$ eine unendliche Gruppe, so sagen wir, dass a von **unendlicher Ordnung** ist und schreiben $\text{ord}(a) = \infty$.

4.2.8 Aufgaben (1) Sei $G = \mathbb{Z}$ mit der Addition. Sei $m \in \mathbb{Z}$. Bestimmen Sie alle Elemente in $\langle m \rangle$ und die Ordnung von m.

(2) Sei $G = S_3$, also

$$G = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}.$$

Seien $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ und $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. Bestimmen Sie $\langle \sigma \rangle$, $\langle \tau \rangle$, $\mathrm{ord}(\sigma)$ und $\mathrm{ord}(\tau)$.

4.2.9 Proposition (Ordnungen von Gruppenelementen)

Sei G eine Gruppe.

(a) Sei $a \in G$ mit $\mathrm{ord}(a) = k < \infty$. Dann ist k die kleinste natürliche Zahl mit $a^k = e$, und es ist $\langle a \rangle = \{a^0, \ldots, a^{k-1}\}$. Wenn $a^r = e$ ist für ein $r \in \mathbb{Z}$, dann ist k ein Teiler von r.

(b) Sei $a \in G$ mit $\mathrm{ord}(a) = \infty$. Genau dann gilt $a^r = a^s$ für $r, s \in \mathbb{Z}$, wenn $r = s$ ist.

Beweis:

(a) Sei m die kleinste natürliche Zahl, so dass $a^0, a^1, \ldots, a^{m-1}$ verschieden sind und $a^m = a^l$ ist für ein $0 \leq l < m$. Dann gilt

$$a^m (a^l)^{-1} = a^{m-l} = a^0 = e.$$

Wenn $l \neq 0$, so ist $0 < m - l < m$, ein Widerspruch zur Minimalität von m. Es folgt $l = 0$, also $a^m = e$. Es bleibt zu zeigen, dass $m = k$ ist.

Offenbar gilt $\{a^0, \ldots, a^{m-1}\} \subseteq \langle a \rangle$.

Sei $a^s \in \langle a \rangle$. Wir teilen s durch m mit Rest: $s = tm + r$ und $0 \leq r < m$. Dann gilt

$$a^s = a^{mt+r} = (a^m)^t a^r = e^t a^r = a^r \in \{a^0, \ldots, a^{m-1}\},$$

also $\langle a \rangle = \{a^0 \ldots, a^{m-1}\}$. Da k die Ordnung von $\langle a \rangle$ ist, folgt $k = m$.

Sei nun $r \in \mathbb{Z}$ mit $a^r = e$. Wir teilen r durch k mit Rest und erhalten $r = tk + s$ mit $t \in \mathbb{Z}$ und $0 \leq s < k$. Es folgt

$$e = a^r = a^{kt+s} = (a^k)^t a^s = e^t a^s = a^s.$$

Da $s < k$, folgt $s = 0$. Somit ist k ein Teiler von r.

(b) Sei $\mathrm{ord}(a) = \infty$. Wenn $r = s$, so gilt offenbar $a^r = a^s$. Sei umgekehrt $r \neq s$, und sei ohne Einschränkung $r > s$. Angenommen, es gilt $a^r = a^s$. Dann gilt $a^r(a^s)^{-1} = a^{r-s} = e$, und $r - s \in \mathbb{N}$. Es gibt also eine natürliche Zahl t mit $a^t = e$. Sei k die kleinste natürliche Zahl mit dieser Eigenschaft. Wie im Beweis von (a) gilt $\langle a \rangle \subseteq \{a^0 \ldots, a^{k-1}\}$, ein Widerspruch zur Annahme, dass $\mathrm{ord}(a) = \infty$ ist.

□

4.3 Der Satz von Lagrange

4.3.1 Definition Sei $(H, \cdot)$ eine Untergruppe der Gruppe $(G, \cdot)$. Wir definieren eine Äquivalenzrelation $R_H \subseteq G \times G$ auf G durch

$$(a, b) \in R_H \quad \Leftrightarrow \quad a = bh \text{ für ein } h \in H.$$

Wir überzeugen uns zunächst davon, dass R_H wirklich eine Äquivalenzrelation auf G definiert.

Für alle $a \in G$ liegt (a, a) in R_H, denn $a = ae$ und $e \in H$. Somit gilt die Reflexivität.

Sei $(a, b) \in R_H$, also $a = bh$ für ein $h \in H$. Dann gilt $b = ah^{-1}$, und $h^{-1} \in H$. Es folgt $(b, a) \in R_H$, die Symmetrie.

Seien $(a, b) \in R_H$ und $(b, c) \in R_H$. Dann gibt es $h, h' \in H$ mit $a = bh$ und $b = ch'$. Es folgt $a = bh = (ch')h = c(h'h)$, und $h'h \in H$. Somit gilt $(a, c) \in R_H$, die Transitivität.

Somit ist R_H eine Äquivalenzrelation auf G, und sie wird **Linkskongruenz modulo** H genannt. Völlig analog wird durch $L_H \subseteq G \times G$ mit

$$(a, b) \in L_H \quad \Leftrightarrow \quad a = hb \text{ für ein } h \in H$$

eine Äquivalenzrelation auf G definiert. Diese wird **Rechtskongruenz modulo** H genannt.

Sie haben in der Linearen Algebra I, Kurseinheit 1, gesehen, dass die Menge G durch eine Äquivalenzrelation in disjunkte Teilmengen, die Äquivalenzklassen, zerlegt wird. Die Äquivalenzklassen bezüglich R_H sind

$$aH = \{ah \mid h \in H\},\ a \in G$$

beziehungsweise

$$a + H = \{a + h \mid h \in H\},\ a \in G,$$

wenn G additiv geschrieben wird.

Analog sind

$$Ha = \{ha \mid h \in H\},\ a \in G$$

beziehungsweise

$$H + a = \{h + a \mid h \in H\},\ a \in G,$$

die Äquivalenzklassen bezüglich L_H.

4.3.2 Definition Die Äquivalenzklassen bezüglich R_H werden **Linksnebenklassen modulo** H, die bezüglich L_H **Rechtsnebenklassen modulo** H genannt. Ist aH eine Linksnebenklasse, beziehungsweise Ha eine Rechtsnebenklasse, so wird a ein **Vertreter** oder **Repräsentant** der Nebenklasse genannt.

4.3.3 Beispiel Sei $G = (\mathbb{Z}/6\mathbb{Z}, +)$. Es ist $H = \{0, 3\}$ eine Untergruppe von G. Wir bestimmen die verschiedenen Linksnebenklassen modulo H.

$$\begin{array}{rcccc} H & = & 0 + H & = & 3 + H \\ & & 1 + H & = & 4 + H \\ & & 2 + H & = & 5 + H. \end{array}$$

Es sind also

$$\begin{array}{rcl} 0 + H & = & \{0, 3\} \\ 1 + H & = & \{1, 4\} \\ 2 + H & = & \{2, 5\} \end{array}$$

die verschiedenen Linksnebenklassen modulo H.

4.3.4 Aufgaben (1) Sei $G = S_3$, und sei $H = A_3$ die Untergruppe der Permutationen σ mit $\operatorname{sgn}(\sigma) = 1$. Bestimmen Sie die verschiedenen Linksnebenklassen modulo H.

(2) Sei $G = \mathbb{Z}$, und sei $H = n\mathbb{Z}$ für ein $n \in \mathbb{Z}$. Bestimmen Sie die verschiedenen Linksnebenklassen modulo H.

4.3.5 Definition Sei $H < G$. Wenn es nur endlich viele verschiedene Linksnebenklassen modulo H gibt, dann wird die Anzahl dieser Linksnebenklassen der **Index** von H in G genannt und mit $[G : H]$ bezeichnet.

4.3.6 Lemma Sei G eine Gruppe, und sei H eine endliche Untergruppe von G. Dann haben alle Linksnebenklassen modulo H die Mächtigkeit $|H|$.

Beweis: Sei $a \in G$. Wir definieren eine Abbildung

$$f : aH \to H \text{ durch } f(ah) = a^{-1}ah = h \text{ für alle } ah \in aH.$$

Offenbar ist f surjektiv, denn zu jedem $h \in H$ gibt es $ah \in aH$ mit $f(ah) = h$.

Seien $ah, ah' \in aH$ mit $f(ah) = f(ah')$. Dann gilt $f(ah) = h = h' = f(ah')$, also $ah = ah'$. Somit ist f auch injektiv, also bijektiv. Da aH und H endliche Mengen sind, folgt $|aH| = |H|$ für alle $a \in G$. □

4.3.7 Aufgabe Sei $(G, +)$ eine Gruppe, und sei H eine endliche Untergruppe von G. Beweisen Sie, dass alle Rechtsnebenklassen modulo H die Mächtigkeit $|H|$ haben.

4.3.8 Satz (Lagrange, 1736-1813)

Sei G eine endliche Gruppe, und sei H eine Untergruppe von G. Dann gilt

$$|G| = [G : H] \cdot |H|.$$

Beweis: Sei $[G : H] = k$, und seien $g_1H, \ldots, g_kH$ die verschiedenen Linksnebenklassen modulo H. Da R_H eine Äquivalenzrelation auf G ist, folgt

$$G = \bigcup_{i=1}^{k} g_iH.$$

Da $g_iH \cap g_jH = \emptyset$ für alle $i \neq j$, $1 \leq i, j \leq k$, denn Äquivalenzklassen sind disjunkt oder gleich, folgt

$$|G| = \sum_{i=1}^{k} |g_iH|.$$

Da $|g_iH| = |H|$ mit dem Lemma, erhalten wir

$$|G| = \sum_{i=1}^{k} |H| = k|H| = [G : H] \cdot |H|,$$

die Behauptung. □

Der Satz von Lagrange hat viele Folgerungen, die in der Kryptografie wichtig sind.

4.3.9 Korollar Sei G eine endliche Gruppe, und sei H eine Untergruppe von G. Dann ist die Ordnung von H ein Teiler der Ordnung von G. □

4.3.10 Korollar Sei G eine endliche Gruppe, und sei $|G| = p$ eine Primzahl. Dann hat G nur die trivialen Untergruppen $\{e\}$ und G.

Beweis: Sei $H \neq \{e\}$ eine Untergruppe von G. Dann gibt es ein Element $a \neq e$ in H, und da $e \in H$, folgt $|H| \geq 2$. Da $|H|$ ein Teiler von $|G| = p$ ist, folgt $|H| = p$, also $H = G$. □

4.3.11 Korollar Sei G eine endliche Gruppe, und sei $|G| = p$ eine Primzahl. Sei $a \in G$, $a \neq e$. Dann gilt $G = \langle a \rangle$.

Beweis: Da $a \neq e$, folgt $\langle a \rangle \neq \{e\}$. Mit Korollar 4.3.10 folgt $\langle a \rangle = G$. □

4.3.12 Korollar Sei G eine endliche Gruppe, und sei $a \in G$. Dann ist $\mathrm{ord}(a)$ ein Teiler der Ordnung von G. □

4.3.13 Korollar Sei G eine endliche Gruppe, und sei $a \in G$. Dann gilt $a^{|G|} = e$.

Beweis: Es ist $\mathrm{ord}(a)$ ein Teiler von $|G|$, also $|G| = \mathrm{ord}(a) \cdot n$ für ein $n \in \mathbb{N}$. Weiter gilt $a^{\mathrm{ord}(a)} = e$ mit Proposition 4.2.9. Es folgt

$$a^{|G|} = a^{\mathrm{ord}(a)n} = (a^{\mathrm{ord}(a)})^n = e^n = e,$$

die Behauptung. □

4.4 Die Eulersche φ-Funktion

Sei R ein Ring. Sie haben in der Linearen Algebra I, Kurseinheit 2, gesehen, dass die invertierbaren Elemente in R mit der Multiplikation eine Gruppe bilden. Diese Gruppe wird **Einheitengruppe** von R genannt und mit $R^\times$ bezeichnet. Die Elemente $a \in R^\times$ heißen **Einheiten** von R.

Wir werden in diesem Abschnitt die Einheitengruppe von $\mathbb{Z}/m\mathbb{Z}$, $m > 1$, näher untersuchen. Als Folgerung des Euklidischen Algorithmus haben wir in 2.4, Korollar 2.4.16, die Einheiten in $\mathbb{Z}/m\mathbb{Z}$ bereits charakterisiert: Genau dann ist a eine Einheit in $\mathbb{Z}/m\mathbb{Z}$, wenn $\mathrm{ggT}(a, m) = 1$ ist. Die Frage, wie viele Elemente in $\mathbb{Z}/m\mathbb{Z}$ diese Eigenschaft haben, führt zu folgender Definition:

4.4.1 Definition Sei $m \in \mathbb{N}$, $m > 1$. Die Ordnung der Gruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ wird mit $\varphi(m)$ bezeichnet. Zusätzlich definieren wir $\varphi(1) = 1$. Die Funktion

$$\varphi : \mathbb{N} \to \mathbb{N},\ n \mapsto \varphi(n) \text{ für alle } n \in \mathbb{N}$$

wird die **Eulersche φ-Funktion** genannt.

Der griechische Buchstabe φ wird „fi“ ausgesprochen.

Die φ-Funktion wurde 1760 von Leonhard Euler (geboren 1707 in Basel, gestorben 1783 in Petersburg) eingeführt. Sie gehört, wie wir zeigen werden, zu einer wichtigen Klasse zahlentheoretischer Funktionen, den so genannten multiplikativen Funktionen.

4.4.2 Definition Eine Abbildung $f : \mathbb{N} \to \mathbb{N}$ heißt eine **multiplikative Funktion**, falls $f(mn) = f(m)f(n)$ für alle $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$.

Zum Beweis, dass φ multiplikativ ist, benötigen wir noch folgende Hilfsmittel:

4.4.3 Lemma Sei $d \in \mathbb{N}$, $d > 1$. Dann gibt es eine Primzahl, die d teilt.

Beweis: Wir beweisen die Behauptung mit Induktion nach d. Ist $d = 2$, so ist d eine Primzahl. Da d ein Teiler von d ist, folgt die Behauptung.

Sei nun $d > 2$. Ist d eine Primzahl, so sind wir wie im Induktionsanfang schon fertig. Wir können also annehmen, dass d keine Primzahl ist. Somit hat d einen Teiler t mit $2 \leq t < d$. Mit der Induktionsannahme hat t einen Teiler, der eine Primzahl ist. Dieser teilt auch d, und es folgt die Behauptung. □

4.4.4 Lemma Seien $a, m, n \in \mathbb{N}$. Es gilt

$$\mathrm{ggT}(a, mn) = 1 \quad \Leftrightarrow \quad \mathrm{ggT}(a, m) = 1 \text{ und } \mathrm{ggT}(a, n) = 1.$$

Beweis: Sei $\mathrm{ggT}(a, mn) = 1$. Sei $d = \mathrm{ggT}(a, m)$. Es folgt $d|m$, also $d|mn$, somit $d = 1$. Analog folgt $\mathrm{ggT}(a, n) = 1$.

Sei nun umgekehrt $\mathrm{ggT}(a, m) = \mathrm{ggT}(a, n) = 1$. Angenommen, $\mathrm{ggT}(a, mn) = d > 1$. Mit Lemma 4.4.3 gibt es eine Primzahl p, die d und damit auch a teilt. Es folgt $p|mn$, und mit Korollar 2.4.15 in 2.4 gilt $p|m$ oder $p|n$, ein Widerspruch zur Voraussetzung, dass $\mathrm{ggT}(a, m) = \mathrm{ggT}(a, n) = 1$ ist. □

4.4.5 Satz Die Eulersche φ-Funktion ist multiplikativ.

Beweis: Seien $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m,n) = 1$. Wir schreiben die mn Zahlen $1, \ldots, mn$ folgendermaßen in ein Schema:

$$\begin{array}{cccccc} 1 & m+1 & \cdots & (n-2)m+1 & (n-1)m+1 \\ 2 & m+2 & \cdots & (n-2)m+2 & (n-1)m+2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ m-1 & 2m-1 & \cdots & (n-1)m-1 & nm-1 \\ m & 2m & \cdots & (n-1)m & nm. \end{array}$$

In der k-ten Zeile, $1 \leq k \leq m$, steht $am + k$, $0 \leq a \leq n-1$. Falls $\mathrm{ggT}(k,m) = d > 1$, so sind alle Zahlen in der k-ten Zeile durch d teilbar. Zu mn teilerfremde Zahlen finden wir also nur in den $\varphi(m)$ Zeilen, deren erstes Element ein zu m teilerfremdes k ist. Sei k so, dass $\mathrm{ggT}(k,m) = 1$ ist. Mit der Proposition 2.5.1 in 2.5 ist die Abbildung $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $f(a) = (am + k) \mathrm{mod} n$ bijektiv. Somit sind die Reste modulo n der Elemente in der k-ten Zeile gerade $\{0, \ldots, n-1\}$. Da $\mathrm{ggT}(x,n) = \mathrm{ggT}(x \mathrm{mod} n, n)$ mit Lemma 2.4.6, gibt es in der k-ten Zeile genau $\varphi(n)$ Elemente, die zu n teilerfremd sind. Insgesamt erhalten wir genau $\varphi(m)\varphi(n)$ Elemente, die sowohl zu m als auch zu n teilerfremd sind. Mit Lemma 4.4.4 sind dieses die zu mn teilerfremden Zahlen, also $\varphi(mn) = \varphi(m)\varphi(n)$. □

Zur Berechnung von $\varphi(n)$ für eine natürliche Zahl n benötigen wir noch ein Ergebnis, das Ihnen vermutlich seit der Mittelstufe geläufig ist, das aber trotzdem eines Beweises bedarf. Dieses Ergebnis ist so wichtig, dass man es den „Hauptsatz der elementaren Zahlentheorie“ nennt, und es besagt, dass jede natürliche Zahl bis auf Anordnung eindeutig als Produkt von Primzahlen geschrieben werden kann. Der Beweis dieses Resultates wird unser nächstes Etappenziel sein.

Wir benötigen zunächst eine Verallgemeinerung von Korollar 2.4.15 in 2.4.

4.4.6 Lemma Sei p eine Primzahl, und seien $a_1 \ldots, a_n$ natürliche Zahlen. Teilt p das Produkt $\prod_{i=1}^{n} a_i$, so teilt p einen der Faktoren.

Beweis: Wir beweisen die Behauptung mit Induktion nach n. Ist $n = 1$ so ist die Behauptung richtig. Sei $n > 1$, und sei p ein Teiler von $\prod_{i=1}^{n} a_i$. Wenn p die Zahl a_n teilt, so sind wir fertig. Wir können also annehmen, dass p kein Teiler von a_n ist. Sei $a = \prod_{i=1}^{n-1} a_i$. Dann gilt $p | a a_n$, und mit Korollar 2.4.15 in 2.4 folgt $p|a$. Mit der Induktionsannahme teilt p einen der Faktoren $a_1, \ldots, a_{n-1}$. □

4.4.7 Satz (Hauptsatz der elementaren Zahlentheorie)

Jede natürliche Zahl $n > 1$ kann als Produkt von Primzahlen geschrieben werden, und je zwei solcher Produkte sind bis auf die Anordnung der Faktoren gleich.

Beweis: Wir zeigen die Existenz mit Induktion nach n. Ist $n = 2$, so ist 2 das Produkt von einer Primzahl. Sei $n > 2$. Wenn n eine Primzahl ist, so sind wir fertig. Wenn n keine Primzahl ist, so gibt es mit Lemma 4.4.3 eine Primzahl p, die n teilt. Sei $n = pt$. Es ist $t < n$, und mit der Induktionsannahme ist $t = \prod_{i=1}^{r} p_i$ ein Produkt von Primzahlen. Dann ist $n = p\prod_{i=1}^{r} p_i$ ein Produkt von Primzahlen.

Wir zeigen nun, dass ein solches Produkt von Primzahlen bis auf Anordnung der Faktoren eindeutig ist. Dazu sei $n > 1$, und es gelte

$$n = \prod_{i=1}^{r} p_i = \prod_{j=1}^{s} q_j \text{ für Primzahlen } p_1, \ldots, p_r, q_1, \ldots q_s.$$

Wir beweisen die Eindeutigkeit mit Induktion nach r. Ist $r = 1$, so ist n eine Primzahl, hat also keine Teiler bis auf 1 und n. Es folgt $s = 1$ und $q_1 = p_1 = n$. Sei nun $r > 1$. Der Faktor p_r teilt $\prod_{j=1}^{s} q_j$, und mit Lemma 4.4.6 folgt $p_r | q_k$ für ein $1 \leq k \leq s$. Da q_k eine Primzahl ist, folgt $p_r = q_k$. Wir nummerieren die Faktoren $q_1, \ldots, q_s$ so um, dass $p_r = q_s$ gilt. Es folgt $\prod_{i=1}^{r-1} p_i = \prod_{j=1}^{s-1} q_j$. Mit der Induktionsannahme folgt $r - 1 = s - 1$ und $p_i = q_{\sigma(i)}$ für eine Permutation σ von $\{1, \ldots, r-1\}$. Es folgt $r = s$, und da $p_r = q_r$, gilt die Behauptung. □

4.4.8 Bemerkung Sei p eine Primzahl, und sei $n \in \mathbb{N}$. Dann gilt $\varphi(p^n) = p^{n-1}(p-1)$.

Beweis: Die Anzahl der Elemente in $\mathbb{Z}/p^n\mathbb{Z}$ ist p^n. Von diesen Elementen sind p^{n-1} nicht teilerfremd zu p^n, nämlich $0, p, 2p, \ldots, p^n - p$. Es folgt $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$. □

Mit diesen Ergebnissen können wir $\varphi(n)$, also die Ordnung von $(\mathbb{Z}/n\mathbb{Z})^\times$ bestimmen:

4.4.9 Korollar Sei $n > 1$, und sei $n = \prod_{i=1}^{r} p_i^{m_i}$, wobei $p_1, \ldots, p_r$ Primzahlen sind mit $p_i \neq p_j$ für alle $i \neq j$, $1 \leq i, j \leq r$, und $m_i \geq 1$ für alle $1 \leq i \leq r$. Dann gilt

$$\varphi(n) = \prod_{i=1}^{r} p_i^{m_i - 1}(p_i - 1).$$

Beweis: Für alle $i \neq j$, $1 \leq i, j \leq r$ gilt $\mathrm{ggT}(p_i^{m_i}, p_j^{m_j}) = 1$. Da φ multiplikativ ist, folgt $\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{m_i})$. Die Bemerkung 4.4.8 impliziert die Behauptung. □

4.4.10 Aufgabe Berechnen Sie die Anzahl der zu 200 teilerfremden Zahlen x mit $0 < x \leq 200$.

Die folgenden klassischen Ergebnisse spielen in der modernen Kryptografie eine große Rolle.

4.4.11 Satz (Euler 1760)

Seien $x, n \in \mathbb{N}$, und sei $\mathrm{ggT}(x, n) = 1$. Dann gilt $x^{\varphi(n)} \equiv 1 (\mathrm{mod} n)$, also $n | (x^{\varphi(n)} - 1)$.

Beweis: Es ist $\mathrm{ggT}(x, n) = \mathrm{ggT}(x \mathrm{mod} n, n) = 1$, also $x \mathrm{mod} n \in (\mathbb{Z}/n\mathbb{Z})^{\times}$. Mit Korollar 4.3.13 aus dem Satz von Lagrange in 4.2 folgt $(x \mathrm{mod} n)^{\varphi(n)} \mathrm{mod} n = 1$, denn 1 ist das neutrale Element in $(\mathbb{Z}/n\mathbb{Z})^{\times}$. Es folgt $x^{\varphi(n)} \mathrm{mod} n = 1$, also $n | (x^{\varphi(n)} - 1)$ und damit $x^{\varphi(n)} \equiv 1 (\mathrm{mod} n)$. □

4.4.12 Satz (Fermat 1637)

Sei p eine Primzahl, und sei $a \in \mathbb{N}$ mit $\mathrm{ggT}(a, p) = 1$. Dann gilt $a^{p-1} \equiv 1 (\mathrm{mod} p)$, also $p | a^{p-1} - 1$.

Beweis: Es ist $\varphi(p) = p^0(p - 1) = p - 1$. Die Behauptung folgt nun aus dem Satz von Euler, 4.4.11. □

Dieser Satz ist auch unter dem Namen „der kleine Satz von Fermat“ bekannt. Was natürlich sofort die Frage nach dem „großen Satz von Fermat“ aufwirft. Der große Satz (eigentlich benutzt niemand diesen Begriff) ist die so genannte „Fermatsche Vermutung“. Diese besagt, dass die Gleichung $x^n + y^n = z^n$ für $n \geq 3$ keine Lösung x, y, z in $\mathbb{Z} \setminus \{0\}$ besitzt. Fermat schrieb 1637 an den Rand seines privaten

Exemplares eines Mathematikbuches von Diophant, dass er einen wunderbaren Beweis für diese Tatsache habe, dass aber der Rand des Buches zu klein sei, ihn darauf zu notieren. Die Fermatsche Vermutung hat über 350 Jahre lang die Mathematikgeschichte bestimmt, neue Teilgebiete der Mathematik initiiert, neue Fragen aufgeworfen und die Entwicklung der Mathematik entscheidend beeinflusst. Die Fermatsche Vermutung wurde 1994 von dem englischen Mathematiker Andrew Wiles bewiesen. Ein wunderschönes Buch zur Geschichte der Fermatschen Vermutung ist [Si1].

Wir werden in Kurseinheit 3 eine Verallgemeinerung des kleinen Satzes von Fermat benötigen:

4.4.13 Korollar Seien p und q verschiedene Primzahlen. Sei c eine natürliche Zahl mit $c \bmod \varphi(pq) = 1$. Dann gilt $pq|(a^c - a)$ für alle $a \in \mathbb{Z}$. Insbesondere gilt $a^c \bmod pq = a \bmod pq$ für alle $a \in \mathbb{Z}$.

Beweis: Wir werden zeigen, dass $p|(a^c - a)$ und $q|(a^c - a)$ gelten. Da p und q verschiedene Primzahlen sind, folgt dann $pq|(a^c - a)$.

Fall 1: Wenn p ein Teiler von a ist, so folgt $p|(a^c - a)$.

Fall 2: Angenommen, p teilt nicht a. Sei $c = k\varphi(pq)+1$ für ein $k \in \mathbb{Z}$. Mit Korollar 4.4.9 gilt $\varphi(pq) = (p-1)(q-1)$. Dann gilt

$$a^c = a^{k(p-1)(q-1)+1} = a(a^{p-1})^{k(q-1)}.$$

Es folgt

$$a^c \bmod p = a(a^{p-1})^{k(q-1)} \bmod p = a \bmod p,$$

denn mit dem kleinen Satz von Fermat gilt $a^{p-1} \bmod p = 1$. Es folgt $a^c \bmod p = a \bmod p$, also $p|(a^c - a)$.

In beiden Fällen gilt also $p|(a^c - a)$. Nun lassen wir p und q die Rollen tauschen und erhalten $q|(a^c - a)$. □

4.5 Gruppenhomomorphismen

In der Linearen Algebra haben wir Abbildungen zwischen Vektorräumen untersucht, die die Struktur der Vektorräume respektierten. Wir haben uns für die linearen Abbildungen interessiert, und diese werden auch Vektorraumhomomorphismen genannt. Wenn wir mit Gruppen arbeiten, interessieren wir uns für Abbildungen, die die Gruppenstruktur respektieren. Diese werden Gruppenhomomorphismen, oder kurz Homomorphismen genannt. Präziser:

4.5.1 Definition Seien $(G, *)$ und $(H, \circ)$ Gruppen. Eine Abbildung $\phi : G \to H$ heißt **Gruppenhomomorphismus** oder kurz **Homomorphismus**, wenn $\phi(g * g') = \phi(g) \circ \phi(g')$ für alle $g, g' \in G$ gilt. Ein surjektiver Gruppenhomomorphismus wird **Epimorphismus**, und ein bijektiver Gruppenhomomorphismus wird **Isomorphismus** genannt. Wenn ϕ ein Isomorphismus ist, so sagt man, dass G und H **isomorph** sind und schreibt $G \simeq H$. Ein Gruppenhomomorphismus $\phi : G \to G$ heißt **Endomorphismus**, ein bijektiver Endomorphismus heißt **Automorphismus**.

Der griechische Buchstabe ϕ wird, wie φ, „fi“ ausgesprochen.

Die Bedingung $\phi(g * g') = \phi(g) \circ \phi(g')$ für alle $g, g' \in G$ formuliert man auch als „ϕ ist strukturverträglich“.

4.5.2 Beispiele (a) Sei $G = \mathbb{Z}$, und sei $H = \mathbb{Z}/n\mathbb{Z}$ für ein $n > 1$. Wir definieren $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ durch $\phi(a) = a \mathrm{mod} n$ für alle $a \in \mathbb{Z}$. Dann ist ϕ ein Homomorphismus, denn für alle $a, b \in \mathbb{Z}$ gilt

$$\phi(a + b) = (a + b)\mathrm{mod} n = a\mathrm{mod} n + b\mathrm{mod} n = \phi(a) + \phi(b). \quad \square$$

(b) Sei $G = (\mathbb{Z}/4\mathbb{Z}, +)$, und sei $H = \{-1, 1, i, -i\} \subseteq \mathbb{C}$ mit der Multiplikation komplexer Zahlen. Wir definieren $\phi : G \to H$ durch $\phi(0) = 1, \phi(1) = i, \phi(2) = -1$ und $\phi(3) = -i$.

Behauptung ϕ ist ein Isomorphismus.

Beweis: Offenbar ist ϕ bijektiv. Wir müssen also nur noch zeigen, dass ϕ strukturverträglich ist.

$$\phi(0 + 0) = \phi(0) = 1 = 1 \cdot 1 = \phi(0) \cdot \phi(0)$$

$$\phi(0 + 1) = \phi(1) = i = 1 \cdot i = \phi(0) \cdot \phi(1)$$

$$\phi(0 + 2) = \phi(2) = -1 = 1 \cdot (-1) = \phi(0) \cdot \phi(2)$$

$$\phi(0 + 3) = \phi(3) = -i = 1 \cdot (-i) = \phi(0) \cdot \phi(3).$$

Da G und H abelsch sind, folgt $\phi(z + 0) = \phi(z) \cdot \phi(0)$ für alle $z \in \mathbb{Z}/4\mathbb{Z}$.

$$\phi(1 + 1) = \phi(2) = -1 = i \cdot i = \phi(1) \cdot \phi(1)$$

$$\phi(1 + 2) = \phi(3) = -i = i \cdot (-1) = \phi(1) \cdot \phi(2)$$

$$\phi(1 + 3) = \phi(0) = 1 = i \cdot (-i) = \phi(1) \cdot \phi(3).$$

Wieder folgt $\phi(z+1) = \phi(z) \cdot \phi(1)$ für alle $z \in \mathbb{Z}/4\mathbb{Z}$.

$$\phi(2+2) = \phi(0) = 1 = (-1) \cdot (-1) = \phi(2) \cdot \phi(2)$$

$$\phi(2+3) = \phi(1) = i = (-1) \cdot (-i) = \phi(2) \cdot \phi(3).$$

Wieder gilt $\phi(z+2) = \phi(z) \cdot \phi(2)$ für alle $z \in \mathbb{Z}/4\mathbb{Z}$.

$$\phi(3+3) = \phi(2) = -1 = (-i) \cdot (-i) = \phi(3) \cdot \phi(3).$$

Da $\phi(a+b) = \phi(a) \cdot \phi(b)$ für alle $a, b \in \mathbb{Z}/4\mathbb{Z}$, ist ϕ strukturverträglich. Es folgt, dass ϕ ein Isomorphismus ist. □

(c) Sei G eine Gruppe, und sei $a \in G$. Wir definieren $\phi_a : G \to G$ durch $\phi_a(b) = aba^{-1}$ für alle $b \in G$. Dann gilt

$$\phi_a(bb') = abb'a^{-1} = (aba^{-1})(ab'a^{-1}) = \phi_a(b)\phi_a(b'),$$

und es folgt, dass ϕ_a strukturverträglich ist. Die Abbildung ϕ_a ist auch bijektiv, denn $\phi_{a^{-1}}$ ist invers zu ϕ_a. Es folgt, dass ϕ_a ein Automorphismus ist. □

4.5.3 Aufgaben Seien G, H und ϕ wie in Beispiel 4.5.2 (b).

(1) Definieren Sie einen Isomorphismus $\phi' : G \to H$ mit $\phi' \neq \phi$.

(2) Definieren Sie eine bijektive Abbildung h von G nach H, die kein Isomorphismus ist.

Die folgende Proposition listet Eigenschaften von Gruppenhomomorphismen auf:

4.5.4 Proposition (Eigenschaften von Gruppenhomomorphismen)

Seien G, H, K Gruppen mit neutralen Elementen e_G, e_H, e_K. Seien $\phi : G \to H$ und $\psi : H \to K$ Homomorphismen. Dann gilt:

(a) $\phi(e_G) = e_H$.

(b) Für alle $g \in G$ gilt $(\phi(g))^{-1} = \phi(g^{-1})$.

(c) Die Abbildung $\psi \circ \phi : G \to K$ ist ein Homomorphismus.

(d) Wenn ϕ ein Isomorphismus ist, dann ist die zu ϕ inverse Abbildung ebenfalls ein Isomorphismus.

(e) Wenn ϕ und ψ Isomorphismen sind, dann ist $\psi \circ \phi$ ein Isomorphismus.

(f) Die identische Abbildung $\mathrm{id}_G : G \to G$, $\mathrm{id}_G(g) = g$ für alle $g \in G$, ist ein Isomorphismus.

(g) Sei ϕ ein Isomorphismus. Genau dann ist G abelsch, wenn H abelsch ist.

Der griechische Buchstabe ψ wird „psi“ ausgesprochen.

Beweis:

(a) Da ϕ ein Homomorphismus ist, gilt

$$\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G).$$

Wir multiplizieren die Gleichung mit $(\phi(e_G))^{-1}$ und erhalten $e_H = \phi(e_G)$.

(b) Es gilt

$$\begin{array}{rclcrcl} \phi(g)\phi(g^{-1}) & = & \phi(gg^{-1}) & = & \phi(e_G) & = & e_H \\ \phi(g^{-1})\phi(g) & = & \phi(g^{-1}g) & = & \phi(e_G) & = & e_H. \end{array}$$

Somit ist $\phi(g^{-1})$ invers zu $\phi(g)$, die Behauptung.

(c) Seien $g, g' \in G$. Dann gilt

$$\begin{array}{rclcl} (\psi \circ \phi)(gg') & = & \psi(\phi(gg')) & = & \psi(\phi(g)\phi(g')) \\ & = & \psi(\phi(g))\psi(\phi(g')) & = & (\psi \circ \phi)(g)(\psi \circ \phi)(g'). \end{array}$$

Somit ist $\psi \circ \phi$ eine strukturverträgliche Abbildung von G nach K, also ein Homomorphismus.

(d) Sei ϕ^{-1} die zu ϕ inverse Abbildung. Diese ist bijektiv, denn ϕ ist invers zu ϕ^{-1}. Seien $h, h' \in H$. Da ϕ bijektiv ist, gibt es $g, g' \in G$ mit $h = \phi(g)$, $h' = \phi(g')$, $\phi^{-1}(h) = g$ und $\phi^{-1}(h') = g'$. Es folgt

$$\begin{array}{rclcl} \phi^{-1}(hh') & = & \phi^{-1}(\phi(g)\phi(g')) & = & \phi^{-1}(\phi(gg')) \\ & = & (\phi^{-1} \circ \phi)(gg') & = & gg' \\ & = & \phi^{-1}(h)\phi^{-1}(h'). & & \end{array}$$

Es folgt, dass ϕ^{-1} strukturverträglich, also ein Isomorphismus ist.

(e) Wenn ϕ und ψ Isomorphismen sind, ist $\psi \circ \phi$ bijektiv. Die Behauptung folgt nun mit (c).

(f) Die Behauptung ist offenbar richtig.

(g) Sei G abelsch, und sei ϕ ein Isomorphismus. Seien $h, h' \in H$. Dann gibt es $g, g' \in G$ mit $\phi(g) = h$ und $\phi(g') = h'$. Es folgt

$$hh' = \phi(g)\phi(g') = \phi(gg') = \phi(g'g) = \phi(g')\phi(g) = h'h.$$

Es folgt, dass H abelsch ist.

Sei nun umgekehrt H abelsch. Auch ϕ^{-1} ist ein Isomorphismus. Wie bei der ersten Implikation folgt, dass G abelsch ist.

□

4.5.5 Definition Sei $\phi : G \to H$ ein Gruppenhomomorphismus, und sei e_H das neutrale Element in H. Das **Bild** und der **Kern** von ϕ sind folgende Teilmengen von H beziehungsweise G:

$$\text{Bild}(\phi) = \{h \in H \mid \text{ es gibt ein } g \in G \text{ mit } \phi(g) = h\} \subseteq H$$

$$\text{Kern}(\phi) = \{g \in G \mid \phi(g) = e_H\} \subseteq G.$$

4.5.6 Beispiel Sei $n > 1$ und sei $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ definiert durch $\phi(k) = k \bmod n$. Wir haben in Beispiel 4.5.2 (a) oben gesehen, dass ϕ ein Homomorphismus ist.

Behauptung $\text{Kern}(\phi) = n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$.

Beweis: Sei $k \in \mathbb{Z}$ mit $\phi(k) = 0$. Dann gilt $k \bmod n = 0$, also $k = nz$ für ein $z \in \mathbb{Z}$. Es folgt $\text{Kern}(\phi) \subseteq n\mathbb{Z}$. Sei umgekehrt $nz \in n\mathbb{Z}$. Dann gilt $\phi(nz) = nz \bmod n = 0$, also $n\mathbb{Z} \subseteq \text{Kern}(\phi)$. □

4.5.7 Proposition Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Dann gilt:

(a) $\text{Bild}(\phi)$ ist eine Untergruppe von H.

(b) $\text{Kern}(\phi)$ ist eine Untergruppe von G.

(c) Der Homomorphismus ϕ ist genau dann injektiv, wenn $\text{Kern}(\phi) = \{e_G\}$.

Beweis:

(a) Wir benutzen zum Beweis das Untergruppenkriterium. Da $e_H = \phi(e_G)$, gilt $e_H \in \text{Bild}(\phi)$, also ist das Bild von ϕ nicht die leere Menge. Seien $h, h' \in \text{Bild}(\phi)$. Dann gibt es $g, g' \in G$ mit $\phi(g) = h$ und $\phi(g') = h'$. Dann gilt

$$hh'^{-1} = \phi(g)(\phi(g'))^{-1} = \phi(g)\phi(g'^{-1}) = \phi(gg'^{-1}),$$

also $hh'^{-1} \in \text{Bild}(\phi)$. Mit dem Untergruppenkriterium folgt die Behauptung.

(b) Da $e_G \in \text{Kern}(\phi)$, ist $\text{Kern}(\phi) \neq \emptyset$. Seien $g, g' \in \text{Kern}(\phi)$, also $\phi(g) = \phi(g') = e_H$. Es folgt $(\phi(g'))^{-1} = e_H = \phi(g'^{-1})$. Damit gilt

$$\phi(gg'^{-1}) = \phi(g)\phi(g'^{-1}) = e_H e_H = e_H.$$

Somit liegt $gg'^{-1} \in \text{Kern}(\phi)$, und mit dem Untergruppenkriterium folgt die Behauptung.

(c) $\Rightarrow$ Sei ϕ injektiv, und sei $x \in \text{Kern}(\phi)$. Es folgt $\phi(x) = e_H = \phi(e_G)$, also $x = e_G$. Somit gilt $\text{Kern}(\phi) \subseteq \{e_G\}$, und es folgt $\text{Kern}(\phi) = \{e_G\}$.

$\Leftarrow$ Sei $\mathrm{Kern}(\phi) = \{e_G\}$. Seien $g, g' \in G$ mit $\phi(g) = \phi(g')$. Es folgt

$$\phi(g)(\phi(g'))^{-1} = e_H = \phi(g)\phi(g'^{-1}) = \phi(gg'^{-1}).$$

Somit gilt $gg'^{-1} \in \mathrm{Kern}(\phi)$, also $gg'^{-1} = e_G$. Es folgt $g = g'$, das heißt, ϕ ist injektiv.

□

4.6 Normalteiler und Faktorgruppen

Sei G eine Gruppe, und sei S eine Untergruppe von G. Wir hatten in Abschnitt 4.2, Definition 4.3.2, bereits das Konzept von Rechts- beziehungsweise Linksnebenklassen kennen gelernt. Dieses Thema werden wir in diesem Abschnitt wieder aufgreifen und vertiefen.

Betrachten wir zunächst ein

4.6.1 Beispiel Sei $G = S_3$, also

$$G = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}.$$

Sei $S = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$. Es ist S eine Untergruppe von G.

Die Rechtsnebenklassen modulo S sind

$$\begin{aligned}
S \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} &= S \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} &&= S \\
S \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} &= S \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} &&= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} \\
S \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} &= S \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} &&= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}
\end{aligned}$$

Die Linksnebenklassen modulo S sind

$$\begin{aligned}
\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \circ S &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ S &&= S \\
\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ S &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ S &&= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\} \\
\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ S &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ S &&= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}
\end{aligned}$$

Zunächst einmal zeigt dieses Beispiel, dass Vertreter von Nebenklassen nicht eindeutig sind. Wann Nebenklassen gleich sind, besagt folgendes Kriterium:

4.6.2 Proposition (Kriterium für Gleichheit von Nebenklassen)

Sei S eine Untergruppe von G. Seien $a, b \in G$. Dann gilt

(a) $Sa = Sb \Leftrightarrow ab^{-1} \in S$.

(b) $aS = bS \Leftrightarrow a^{-1}b \in S$.

Beweis:

(a) $\Rightarrow$ Sei $Sa = Sb$. Da $a \in Sa$, folgt $a \in Sb$. Es gibt also ein $s \in S$ mit $a = sb$. Es folgt $ab^{-1} \in S$.

$\Leftarrow$ Sei $ab^{-1} = s$ für ein $s \in S$. Dann folgt $a = sb$, und damit $Sa = S(sb) = Sb$.

(b) Der Beweis erfolgt analog zu (a).

□

Weiter zeigt das Beispiel 4.6.1, dass Rechtsnebenklassen in der Regel keine Linksnebenklassen sind, etwa ist $S \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ keine Linksnebenklasse. Weiter sehen wir, dass im Allgemeinen $Sa \neq aS$ gilt. Falls $Sa = aS$ für alle $a \in G$, so ist das schon eine sehr spezielle Situation, die zu folgender Definition führt:

4.6.3 Definition Sei S eine Untergruppe von G. Wenn $Sa = aS$ für alle $a \in G$ gilt, so wird S ein **Normalteiler** von G genannt, und wir schreiben $S \lhd G$.

4.6.4 Proposition (Charakterisierung von Normalteilern)

Sei S eine Untergruppe von G. Die folgenden Aussagen sind äquivalent:

(i) $S \lhd G$.

(ii) Für alle $a \in G$ gilt $aSa^{-1} \subseteq S$.

(iii) Für alle $a \in G$ gilt $aSa^{-1} = S$.

Beweis:

(i)$\Rightarrow$(ii) Sei $Sa = aS$ für alle $a \in G$. Sei $asa^{-1} \in aSa^{-1}$. Da $as \in aS = Sa$, gibt es ein $s' \in S$ mit $as = s'a$. Es folgt $asa^{-1} = s'aa^{-1} = s' \in S$, also $aSa^{-1} \subseteq S$.

(ii)⇒(iii) Für alle $a \in G$ gelte $aSa^{-1} \subseteq S$. Dann gilt $a^{-1}Sa \subseteq S$, denn $a^{-1} \in G$. Es folgt $S = a(a^{-1}Sa)a^{-1} \subseteq aSa^{-1}$, also $S = aSa^{-1}$.

(iii)⇒(i) Für alle $a \in G$ gelte $aSa^{-1} = S$. Es folgt $Sa = (aSa^{-1})a = aS$, die Behauptung.

□

4.6.5 Beispiele (a) Für jede Gruppe G ist $\{e_G\}$ eine Untergruppe von G, und $\{e_G\}$ ist ein Normalteiler von G. □

(b) Sei S ein Normalteiler einer Gruppe G, und sei H eine Untergruppe von G, die S enthält. Dann ist S auch eine Untergruppe von H, und wegen $aSa^{-1} = S$ für alle $a \in H$, ist S auch ein Normalteiler von H. □

(c) Sei G eine abelsche Gruppe. Dann gilt $aSa^{-1} = S$ für alle Untergruppen von G, das heißt, alle Untergruppen von G sind Normalteiler von G. □

(d) Sei $\mathrm{Gl}_n(\mathbb{K})$ die Gruppe der invertierbaren $n \times n$-Matrizen über einem Körper $\mathbb{K}$. Sei $\mathrm{Sl}_n(\mathbb{K})$ die Untergruppe der $n \times n$-Matrizen mit Determinante 1. Dann gilt für alle $A \in \mathrm{Gl}_n(\mathbb{K})$ und alle $X \in \mathrm{Sl}_n(\mathbb{K})$

$$\det(AXA^{-1}) = \det(A)\det(X)\det(A^{-1}) = \det(A) \cdot 1 \cdot (\det(A))^{-1} = 1,$$

also $A(\mathrm{Sl}_n(\mathbb{K}))A^{-1} \subseteq \mathrm{Sl}_n(\mathbb{K})$, und damit $\mathrm{Sl}_n(\mathbb{K}) \lhd \mathrm{Gl}_n(\mathbb{K})$. □

(e) Seien G und H Gruppen, und sei $\phi : G \to H$ ein Gruppenhomomorphismus.

Behauptung $\mathrm{Kern}(\phi)$ ist ein Normalteiler von G.

Beweis: Wie wir in 4.5.7 gesehen haben, ist $\mathrm{Kern}(\phi)$ eine Untergruppe von G. Sei $a \in G$, und sei $x \in \mathrm{Kern}(\phi)$. Dann gilt

$$\phi(axa^{-1}) = \phi(a)\phi(x)\phi(a^{-1}) = \phi(a)e_H(\phi(a))^{-1} = e_H.$$

Es folgt $a(\mathrm{Kern}(\phi))a^{-1} \subseteq \mathrm{Kern}(\phi)$ für alle $a \in G$. Somit ist $\mathrm{Kern}(\phi)$ ein Normalteiler von G. □

Sei G eine Gruppe, und sei S ein Normalteiler von G. Wir bezeichnen mit

$$G/S = \{aS \mid a \in G\}$$

die Menge aller Linksnebenklassen (= Rechtsnebenklassen) von G modulo S. Auf dieser Menge definieren wir

$$\begin{array}{rccc} \cdot : & G/S \times G/S & \to & G/S \\ & (aS, bS) & \mapsto & (ab)S \end{array}$$

für alle $a, b \in G$. Wir zeigen, dass diese Zuordnung wohldefiniert, also unabhängig von der Wahl der Repräsentanten der Nebenklassen ist.

Dazu seien $aS = a'S$ und $bS = b'S$. Wir müssen zeigen, dass $(ab)S = (a'b')S$ ist. Wir verwenden Proposition 4.6.2.

Da $aS = a'S$, gilt $a^{-1}a' \in S$, und da $bS = b'S$ gilt $b^{-1}b' \in S$. Es folgt

$$\begin{array}{rcll} (ab)^{-1}(a'b') & = & b^{-1}(a^{-1}a')b' & \\ & = & b^{-1}sb', & \text{denn } a^{-1}a' = s \text{ für ein } s \in S \\ & = & b^{-1}b's', & \text{denn } Sb' = b'S, \text{ also } sb' = b's' \text{ für ein } s' \in S \\ & \in & S, & \text{denn } b^{-1}b' \in S. \end{array}$$

Mit dem Kriterium für Gleichheit von Nebenklassen, Proposition 4.6.2, folgt, dass die oben definierte Zuordnung eine Verknüpfung auf G/S ist. Es ist nun einfach zu zeigen, dass G/S mit dieser Verknüpfung eine Gruppe bildet. Das neutrale Element ist $S = e_G S$, und zu einem Element $aS \in G/S$ ist $a^{-1}S$ invers.

4.6.6 Definition Sei G eine Gruppe, und sei S ein Normalteiler von G. Dann wird G/S die **Faktorgruppe** oder **Quotientengruppe** von G nach S genannt.

Wir haben in 4.6.5 (e) gezeigt, dass der Kern eines Gruppenhomomorphismus' $\phi : G \to H$ ein Normalteiler von G ist. Der folgende Satz untersucht die Faktorgruppe $G/\mathrm{Kern}(\phi)$.

4.6.7 Satz (Homomorphiesatz für Gruppen)

Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Dann ist $G/\mathrm{Kern}(\phi)$ isomorph zu $\mathrm{Bild}(\phi)$. Genauer, es ist

$$\begin{array}{rccc} \Phi : & G/\mathrm{Kern}(\phi) & \to & \mathrm{Bild}(\phi) \\ & g\mathrm{Kern}(\phi) & \mapsto & \phi(g) \end{array}$$

ein Isomorphismus von Gruppen.

Der griechische Buchstabe Φ wird „groß fi“ ausgesprochen.

Beweis:

1. Wir zeigen zunächst, dass Φ wohldefiniert ist. Sei $g\mathrm{Kern}(\phi) = g'\mathrm{Kern}(\phi)$, also $g^{-1}g' \in \mathrm{Kern}(\phi)$. Es folgt

$$e_H = \phi(g^{-1}g') = \phi(g^{-1})\phi(g') = (\phi(g))^{-1}\phi(g'),$$

   also $\phi(g') = \phi(g)$, und damit $\Phi(g\mathrm{Kern}(\phi)) = \Phi(g'\mathrm{Kern}(\phi))$.

2. Wir zeigen nun, dass Φ ein Homomorphismus ist. Dazu seien $g\text{Kern}(\phi)$, $g'\text{Kern}(\phi) \in G/\text{Kern}(\phi)$. Dann gilt

$$\begin{aligned}\Phi((g\text{Kern}(\phi))(g'\text{Kern}(\phi))) &= \Phi((gg')\text{Kern}(\phi)) \\ &= \phi(gg') \\ &= \phi(g)\phi(g') \\ &= \Phi(g\text{Kern}(\phi))\Phi(g'\text{Kern}(\phi)).\end{aligned}$$

3. Wir zeigen mit Proposition 4.5.7, dass Φ injektiv ist. Sei $g\text{Kern}(\phi) \in \text{Kern}(\Phi)$, also $\phi(g) = e_H$. Dann liegt g im Kern von ϕ, also $g\text{Kern}(\phi) = \text{Kern}(\phi)$, und das ist das neutrale Element in $G/\text{Kern}(\phi)$. Mit 4.5.7 folgt, dass Φ injektiv ist.

4. Sei $h \in \text{Bild}(\phi)$. Dann gibt es ein $g \in G$ mit $\phi(g) = h$. Es folgt

$$\Phi(g\text{Kern}(\phi)) = \phi(g) = h,$$

also ist Φ surjektiv.

Es folgt, dass Φ ein Isomorphismus ist. □

4.6.8 Aufgaben (1) Vergleichen Sie den Homomorphiesatz für Gruppen mit dem Homomorphiesatz für Vektorräume in der Linearen Algebra I, Kurseinheit 6.

(2) Sei $G = \mathbb{Z}$, und sei $H = \mathbb{Z}/n\mathbb{Z}$ für ein $n \geq 2$. Sei $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ wie in 4.5.2 definiert durch $\phi(a) = a \bmod n$ für alle $a \in \mathbb{Z}$. Bestimmen Sie alle Elemente von $\mathbb{Z}/\text{Kern}(\phi)$.

(3) Sei G eine endliche Gruppe, und sei S ein Normalteiler von G. Beweisen Sie, dass G/S eine endliche Gruppe ist, und bestimmen Sie die Ordnung von G/S.

Sei G eine Gruppe, und sei S ein Normalteiler von G. Wir definieren

$$\pi : G \to G/S \text{ durch } \pi(g) = gS \text{ für alle } g \in G.$$

Die Abbildung π ist ein surjektiver Gruppenhomomorphismus, also ein Epimorphismus. Man nennt π den **kanonischen Epimorphismus** von G nach G/S.

4.6.9 Aufgabe Bestimmen Sie den Kern von π.

Wir hatten in den Beispielen 4.6.5 gesehen, dass $\text{Kern}(\phi)$ ein Normalteiler von G ist, sofern $\phi : G \to H$ ein Homomorphismus von Gruppen ist. Im gewissen Sinne gilt auch die Umkehrung:

4.6.10 Proposition Sei S ein Normalteiler einer Gruppe G. Dann gibt es eine Gruppe H und einen Homomorphismus $\phi : G \to H$, so dass $S = \text{Kern}(\phi)$ ist.

Beweis: Sei $H = G/S$, und sei $\phi = \pi$. Sie haben in Aufgabe 4.6.9 gezeigt, dass $\text{Kern}(\pi) = S$ ist. Dies impliziert die Behauptung. □

4.7 Die Klassengleichung

Sei G eine Gruppe, und sei $a \in G$ ein festes Element. Wir definieren $f_a : G \to G$ durch $f_a(b) = aba^{-1}$. Dann ist f_a ein Homomorphismus, denn

$$f_a(bb') = a(bb')a^{-1} = (aba^{-1})(ab'a^{-1}) = f_a(b)f_a(b')$$

für alle $b, b' \in G$. Der Homomorphismus f_a ist auch bijektiv, denn $f_{a^{-1}}$ ist invers zu f_a. Somit ist f_a ein Automorphismus. (Vergleichen Sie mit Definition 4.5.1 und Beispiel 4.5.2(c).)

4.7.1 Definition Automorphismen der Form $f_a : G \to G$, $f_a(b) = aba^{-1}$ werden **innere Automorphismen** genannt. Elemente a und b in G heißen **konjugiert**, wenn es ein $g \in G$ mit $a = gbg^{-1}$ gibt. Für eine nicht leere Teilmenge S von G wird $\{aSa^{-1} \mid a \in G\}$ die Menge der **Konjugierten** von S genannt.

In der Regel gilt $aSa^{-1} \neq S$. Wenn beispielsweise S eine Untergruppe von G ist, so haben wir in Proposition 4.6.4 gesehen, dass $aSa^{-1} = S$ für alle $a \in G$ genau dann gilt, wenn S ein Normalteiler von G ist.

4.7.2 Aufgabe Sei $G = S_3$. Bestimmen Sie ein Element τ und ein Element σ in S_3, so dass $\sigma \circ \tau \circ \sigma^{-1} \neq \tau$ ist.

4.7.3 Definition Sei S eine nicht leere Teilmenge einer Gruppe G. Der **Normalisator** von S ist die Menge $N(S) = \{a \in G \mid aSa^{-1} = S\}$.

4.7.4 Aufgabe Sei $G = S_3$. Sei $\tau \in S_3$ das Element, das Sie in Aufgabe 4.7.2 bestimmt haben. Berechnen Sie $N(\{\tau\})$.

4.7.5 Proposition Für jede nicht leere Teilmenge S einer Gruppe G ist $N(S)$ eine Untergruppe von G. Es gibt eine bijektive Abbildung zwischen den Linksnebenklassen modulo $N(S)$ und den verschiedenen Konjugierten aSa^{-1} von S.

Beweis: Sei e das neutrale Element in G. Dann gilt $eSe^{-1} = S$, das heißt, $N(S) \neq \emptyset$. Seien $a, b \in N(S)$. Dann gilt $b^{-1} \in N(S)$, denn

$$b^{-1}Sb = b^{-1}(bSb^{-1})b = (b^{-1}b)S(b^{-1}b) = S,$$

also

$$ab^{-1}S(ab^{-1})^{-1} = ab^{-1}Sba^{-1} = aSa^{-1} = S,$$

somit $ab^{-1} \in N(S)$. Mit dem Untergruppenkriterium, 4.2.4, folgt, dass $N(S)$ eine Gruppe ist.

Weiter gilt

$$\begin{aligned} aSa^{-1} = bSb^{-1} &\Leftrightarrow S = a^{-1}bSb^{-1}a = (a^{-1}b)S(a^{-1}b)^{-1} \\ &\Leftrightarrow a^{-1}b \in N(S) \\ &\Leftrightarrow bN(S) = aN(S) \text{ mit Proposition 4.6.2.} \end{aligned}$$

Dies impliziert den zweiten Teil der Behauptung. □

Sei G eine Gruppe, und seien $a, b \in G$. Wir schreiben $a \sim b$, wenn a und b konjugiert sind.

Es gilt $a \sim a$, denn $a = eae^{-1}$, und damit ist $\sim$ reflexiv.

Wenn $a \sim b$, also $a = gbg^{-1}$ für ein $g \in G$, so gilt $b = g^{-1}ag$. Es folgt $b \sim a$, also ist $\sim$ symmetrisch.

Seien $a \sim b$ und $b \sim c$. Dann gibt es $g, g' \in G$ mit $a = gbg^{-1}$ und $b = g'cg'^{-1}$. Es folgt

$$a = gbg^{-1} = gg'cg'^{-1}g^{-1} = (gg')c(gg')^{-1},$$

also $a \sim c$.

Somit ist $\sim$ eine Äquivalenzrelation auf G, und $\sim$ liefert eine Zerlegung von G in eine Vereinigung der verschiedenen Äquivalenzklassen bezüglich $\sim$.

4.7.6 Definition Die Äquivalenzklasse

$$C_a = \{b \in G \mid \text{ es gibt ein } g \in G \text{ mit } a = gbg^{-1}\}$$

eines Elementes a bezüglich Konjugation wird **Konjugationsklasse** von a genannt.

4.7.7 Definition Sei G eine Gruppe, und sei

$$C(G) = \{a \in G \mid ag = ga \text{ für alle } g \in G\}.$$

Dann wird $C(G)$ das **Zentrum** von G genannt.

4.7.8 Aufgabe Beweisen Sie, dass das Zentrum von G ein Normalteiler von G ist.

4.7.9 Bemerkung Sei G eine Gruppe mit Zentrum $C(G)$. Dann gilt

$$a \in C(G) \Leftrightarrow C_a = \{a\}.$$

Beweis: Sei $a \in C(G)$, und sei $b \in C_a$. Dann gilt $a = gbg^{-1}$ für ein $g \in G$, also

$$b = g^{-1}ag = g^{-1}ga = a,$$

also $C_a \subseteq \{a\}$ und damit $C_a = \{a\}$.

Sei umgekehrt $C_a = \{b \in G \mid b = gag^{-1} \text{ für ein } g \in G\} = \{a\}$. Dann gilt $a = gag^{-1}$, also $ag = ga$ für alle $g \in G$. Es folgt, dass a im Zentrum von G liegt. □

Wir kommen nun zum Hauptergebnis dieses Abschnitts:

4.7.10 Proposition (Klassengleichung endlicher Gruppen)

Sei G eine endliche Gruppe mit Zentrum $C(G)$. Dann gilt

$$|G| = |C(G)| + \sum_{i=1}^{k} n_i,$$

wobei $n_i \geq 2$ für alle $1 \leq i \leq k$, und jedes n_i ist ein Teiler von $|G|$. Genauer, $n_1, \ldots, n_k$ sind die Anzahlen der Elemente der verschiedenen Konjugationsklassen in G, die mehr als ein Element enthalten.

Beweis: Da Konjugation eine Äquivalenzrelation auf G ist, ist $|G|$ die Anzahl der Elemente der verschiedenen Konjugationsklassen in G. Es gibt genau $|C(G)|$ Konjugationsklassen mit genau einem Element. Diese korrespondieren zu den Elementen des Zentrums von G, die Zahlen $n_1, \ldots, n_k$ gehören zu den übrigen Konjugationsklassen. Dies beweist die Klassengleichung. Es bleibt zu zeigen, dass n_i ein Teiler von $|G|$ ist für alle $1 \leq i \leq k$. Mit Proposition 4.7.5 ist die Anzahl der zu einem Gruppenelement a konjugierten Elemente gleich der Anzahl der Linksnebenklassen modulo $N(\{a\})$. Da $N(\{a\})$ eine Untergruppe von G ist, ist die Anzahl der Linksnebenklassen modulo $N(\{a\})$ gleich dem Index von $N(\{a\})$ in G. Aus dem Satz von Lagrange folgt die Behauptung. □

4.8 Zyklische Gruppen

4.8.1 Definition Eine Gruppe G heißt **zyklisch**, wenn es ein $a \in G$ gibt, so dass $\langle a \rangle = G$ ist. So ein Element wird **erzeugendes Element** von G genannt.

Sei G eine zyklische Gruppe mit erzeugendem Element a. Wie Sie in Proposition 4.2.9 gesehen haben, ist $G = \{a^0, \ldots, a^{n-1}\}$, falls G die Ordnung $n < \infty$ hat. Dabei ist n die kleinste natürliche Zahl, für die $a^n = e$ gilt. Falls G eine zyklische Gruppe von unendlicher Ordnung ist, so ist $a^n \neq e$ für alle $n \in \mathbb{Z} \setminus \{0\}$.

4.8.2 Beispiele (a) Jede Gruppe, deren Ordnung eine Primzahl ist, ist zyklisch. Das war eine Folgerung aus dem Satz von Lagrange 4.3.8. Genauer, jedes Element $a \neq e$ ist ein erzeugendes Element von G.

(b) Sei $G = \{-1, 1, i, -i\} \subseteq \mathbb{C}$ mit der Multiplikation komplexer Zahlen. Es ist

$$G = \langle i \rangle = \{i, i^2 = -1, i^3 = -i, i^4 = 1\}.$$

Somit ist G zyklisch mit erzeugendem Element i. Auch $-i$ ist ein erzeugendes Element von G, denn

$$G = \{-i, (-i)^2 = -1, (-i)^3 = i, (-i)^4 = 1\}.$$

Die Elemente 1 und -1 sind keine Erzeugenden von G, denn $\langle 1 \rangle = \{1\}$ und $\langle -1 \rangle = \{1, -1\}$.

(c) Sei $G = \mathbb{Z}$. Es ist $\mathbb{Z} = \langle 1 \rangle = \{n1 \mid n \in \mathbb{Z}\}$. Es folgt, dass $\mathbb{Z}$ zyklisch ist. Es ist auch $\mathbb{Z} = \langle -1 \rangle = \{n(-1) \mid n \in \mathbb{Z}\}$. Also sind 1 und -1 erzeugende Elemente von $\mathbb{Z}$.

4.8.3 Aufgaben (1) Beweisen Sie, dass 1 und -1 die einzigen erzeugenden Elemente von $\mathbb{Z}$ sind.

(2) Beweisen Sie, dass S_3 nicht zyklisch ist.

(3) Beweisen Sie, dass A_3 zyklisch ist.

(4) Beweisen Sie, dass zyklische Gruppen abelsch sind.

4.8.4 Proposition (Klassifikation zyklischer Gruppen)

Sei $G = \langle a \rangle$ eine zyklische Gruppe.

(a) Ist $|G| = \infty$, so ist G isomorph zu $(\mathbb{Z}, +)$.

(b) Ist $|G| = n < \infty$, so ist G isomorph zu $(\mathbb{Z}/n\mathbb{Z}, +)$.

Beweis:

(a) Wir definieren eine Abbildung $\phi : G \to \mathbb{Z}$ durch $\phi(a^i) = i$ für alle $a^i \in G$. Da $a^r = a^s$ genau dann, wenn $r = s$ ist (mit Proposition 4.2.9), ist ϕ eine Abbildung. Diese Abbildung ist auch bijektiv. Seien $a^i, a^j \in G$. Dann gilt

$$\phi(a^i a^j) = \phi(a^{i+j}) = i + j = \phi(a^i) + \phi(a^j),$$

und es folgt, dass ϕ ein Isomorphismus ist.

(b) Sei $G = \{a^0, \ldots, a^{n-1}\}$. Wir definieren $\phi : G \to \mathbb{Z}/n\mathbb{Z}$ durch $\phi(a^i) = i$ für alle $a^i \in G$. Dann ist ϕ bijektiv. Seien $a^i, a^j \in G$. Wir teilen $i+j$ durch n mit Rest und erhalten $i + j = sn + (i + j)\mathrm{mod}n$. Dann gilt

$$a^i a^j = a^{i+j} = (a^n)^s a^{(i+j)\mathrm{mod}n} = e^s a^{(i+j)\mathrm{mod}n} = a^{(i+j)\mathrm{mod}n},$$

also

$$\phi(a^i a^j) = (i + j)\mathrm{mod}n = \phi(a^i) + \phi(a^j),$$

und es folgt, dass ϕ ein Isomorphismus ist.

□

Je zwei zyklische Gruppen G und H mit $|G| = |H|$ sind also isomorph. Man spricht daher auch von **der** zyklischen Gruppe der Ordnung n (beziehungsweise der Ordnung ∞) und bezeichnet sie mit C_n beziehungsweise C_∞.

Die folgende Proposition beschreibt die Struktur der Untergruppen zyklischer Gruppen.

4.8.5 Proposition (Untergruppen zyklischer Gruppen)

Sei $G = \langle a \rangle$ eine zyklische Gruppe. Dann gilt:

(a) Alle Untergruppen von G sind zyklisch.

(b) Sei $|G| = n < \infty$, und sei $k \in \mathbb{Z}$. Dann ist $\langle a^k \rangle$ eine Untergruppe der Ordnung $\frac{n}{\mathrm{ggT}(n,k)}$ von G.

(c) Sei $|G| = n < \infty$, und sei d ein positiver Teiler von n. Dann hat G genau eine Untergruppe vom Index d und genau eine Untergruppe der Ordnung d.

(d) Sei $|G| = n < \infty$, und sei f ein positiver Teiler von n. Dann enthält G genau $\varphi(f)$ Elemente der Ordnung f. Hierbei bezeichnet φ die Eulersche φ-Funktion.

(e) Sei $|G| = n < \infty$. Dann enthält G genau $\varphi(n)$ erzeugende Elemente. Diese sind von der Form a^r mit $\mathrm{ggT}(n, r) = 1$.

Beweis:

(a) Sei H eine Untergruppe von G mit $H \neq \{e_G\}$. Dann gibt es ein $a^k \in H$, und $k \neq 0$. Da mit a^k auch a^{-k} in H liegt, enthält H also mindestens ein Element a^m mit $m > 0$. Sei d die kleinste positive Zahl, so dass a^d in H liegt, und sei a^s ein beliebiges Element in H. Wir teilen s durch d mit Rest und erhalten $s = td + r$ mit $0 \leq r < d$. Es folgt

$$a^r = a^s a^{-td} = a^s (a^{-d})^t \in H,$$

denn a^s und a^{-d} sind Elemente in H. Da d minimal gewählt wurde, folgt $r = 0$, das heißt, d ist ein Teiler von s. Es folgt $H \subseteq \langle a^d \rangle$, also $H = \langle a^d \rangle$.

(b) Sei $d = \mathrm{ggT}(k, n)$. Die Ordnung von a^k ist mit Proposition 4.2.9 die kleinste positive Zahl m mit $a^{km} = e$. Es folgt $n | km$, also $\frac{n}{d} | \frac{k}{d} m$. Da $\frac{n}{d}$ und $\frac{k}{d}$ teilerfremd sind, folgt mit Korollar 2.4.13, dass $\frac{n}{d}$ ein Teiler von m ist. Die kleinste positive Zahl m mit dieser Eigenschaft ist $m = \frac{n}{d}$.

(c) Sei d ein positiver Teiler von n. Mit (b) hat die Untergruppe $\langle a^d \rangle$ die Ordnung $\frac{n}{d}$. Mit dem Satz 4.3.8 von Lagrange ist d der Index von $\langle a^d \rangle$ in G. Sei $\langle a^k \rangle$ eine weitere Untergruppe von G vom Index d. Wieder mit dem Satz von Lagrange folgt, dass $\langle a^k \rangle$ die Ordnung $\frac{n}{d}$ hat. Mit (b) folgt $\mathrm{ggT}(n, k) = d$, insbesondere, $d | k$. Somit gilt $a^k \in \langle a^d \rangle$, und $\langle a^k \rangle$ ist eine Untergruppe von $\langle a^d \rangle$. Da beide Gruppen dieselbe Ordnung haben, folgt $\langle a^k \rangle = \langle a^d \rangle$. Die zweite Behauptung folgt nun aus dem eben Bewiesenen, denn die Untergruppen der Ordnung d sind genau die Untergruppen vom Index $\frac{n}{d}$.

(d) Sei $n = df$. Mit (b) ist a^k genau dann ein Element der Ordnung f, wenn $d = ggT(n, k)$ ist. Somit ist die Anzahl der Elemente in G der Ordnung f gleich der Anzahl der Zahlen k mit $1 \leq k \leq n$, für die $d = ggT(k, n)$ gilt. Sei $k = dh$, $1 \leq h \leq f$. Dann gilt

$$\mathrm{ggT}(k, n) = \mathrm{ggT}(dh, df) = d \quad \Leftrightarrow \quad \mathrm{ggT}(h, f) = 1.$$

Die Anzahl der Zahlen $1 \leq h \leq f$ mit $\mathrm{ggT}(h, f) = 1$ ist aber gerade $\varphi(f)$.

(e) Die Anzahl der erzeugenden Elemente von G ist die Anzahl der Elemente der Ordnung n. Mit (d) sind dieses $\varphi(n)$ Elemente. Mit (b) haben sie die Form a^r mit $\mathrm{ggT}(r, n) = 1$.

□

Im Beweis des folgenden Satzes benötigen wir noch einen Begriff aus der elementaren Zahlentheorie.

4.8.6 Definition Seien $a, b \in \mathbb{N}$. Eine ganze Zahl, die sowohl von a als auch von b geteilt wird, heißt ein **Vielfaches** von a und b. Sind $a, b \in \mathbb{N}$, so heißt eine Zahl $v \in \mathbb{Z}$ ein **kleinstes gemeinsames Vielfaches** von a und b, wenn gilt:

(i) $v \geq 0$ und $a|v$ und $b|v$, und

(ii) für jedes Vielfache c von a und b gilt $v|c$.

Wenn v und v' kleinste gemeinsame Vielfache von a und b sind, so gilt $v|v'$ und $v'|v$. Da $v, v' \geq 0$ impliziert dies $v = v'$. Das heißt, wenn a und b ein kleinstes gemeinsames Vielfaches haben, dann ist dieses eindeutig bestimmt und wird mit $\mathrm{kgV}(a, b)$ bezeichnet.

Wir werden nun zeigen, dass es zu $a, b \in \mathbb{N}$ immer ein kleinstes gemeinsames Vielfaches gibt. Dazu führen wir zunächst folgende Notation ein.

4.8.7 Notation Sei $c \in \mathbb{N}$, und sei $\prod_{i=1}^{n} p_i^{t_i} = c$ die Primfaktorzerlegung von c, wobei $p_i \neq p_j$ für alle $i \neq j$ gilt. Sei p eine Primzahl. Wir schreiben $w_p(c) = 0$, falls $p \notin \{p_1, \ldots, p_n\}$ und $w_p(c) = t_i$ falls $p = p_i$ ist. Insbesondere gilt $p^{w_p(c)} = 1$ für $p \notin \{p_1, \ldots, p_n\}$.

Seien nun $a, b \in \mathbb{N}$, und sei P_{ab} die Menge aller Primzahlen, die a oder b teilen. Es gilt dann $a = \prod_{p \in P_{ab}} p^{w_p(a)}$ und $b = \prod_{p \in P_{ab}} p^{w_p(b)}$. Wenn c ein Vielfaches von a und b ist, so folgt aus dem Hauptsatz der elementaren Zahlentheorie, 4.4.7, dass $w_p(c) \geq w_p(a)$ und $w_p(c) \geq w_p(b)$ für alle $p \in P_{ab}$ ist. Es gilt also $w_p(c) \geq \max(w_p(a), w_p(b))$. Damit ist

$$v = \prod_{p \in P_{ab}} p^{\max(w_p(a), w_p(b))}$$

ein Vielfaches von a und b, das jedes Vielfache von a und b teilt. Es folgt

4.8.8 Proposition Für $a, b \in \mathbb{N}$ ist $\mathrm{kgV}(a, b) = \prod_{p \in P_{ab}} p^{\max(w_p(a), w_p(b))}$. □

Der folgende Satz ist in der Kryptografie wichtig und liefert darüberhinaus eine interessante Klasse zyklischer Gruppen.

4.8.9 Satz Sei $\mathbb{K}$ ein Körper. Jede endliche Untergruppe von $\mathbb{K}^\times$ ist zyklisch.

Beweis: Sei G eine endliche Untergruppe von $\mathbb{K}^\times$, und sei $q = |G|$.

Sei $S = \{1 \leq k \leq q \mid \text{es gibt ein } a \in G \text{ mit } \mathrm{ord}(a) = k\}$. Wir werden in mehreren Schritten beweisen, dass q in S liegt. Wenn uns das gelungen ist, sind wir fertig. Denn dann gibt es ein $a \in G$ mit $\mathrm{ord}(a) = |G|$, und das bedeutet, dass G zyklisch ist mit erzeugendem Element a.

1. Wenn $m, n \in S$ und $\mathrm{ggT}(m, n) = 1$, so gilt $mn \in S$.

   Beweis Seien $a, b \in G$ mit $\mathrm{ord}(a) = m$ und $\mathrm{ord}(b) = n$. Dann gilt

   $$\begin{aligned} (ab)^{mn} &= a^{mn}b^{mn}, \text{ denn } G \text{ ist abelsch} \\ &= (a^m)^n(b^n)^m \\ &= e. \end{aligned}$$

   Somit ist $\mathrm{ord}(ab)$ ein Teiler von mn. Sei $\mathrm{ord}(ab) = k$.

   Es ist $e = (ab)^{km} = (a^m)^k b^{km} = b^{km}$, also $n|km$. Da m und n teilerfremd sind, folgt $n|k$.

   Analog gilt $e = (ab)^{kn} = a^{kn}(b^n)^k = a^{kn}$, also $m|kn$, und damit $m|k$. Da $\mathrm{ggT}(m, n) = 1$, folgt $mn|k$. Es gilt also $k|mn$ und $mn|k$, also $k = mn$.

2. Sei $m \in S$, und sei d ein Teiler von m. Dann folgt $d \in S$.

   Beweis Da $m \in S$, gibt es ein $a \in G$ mit $|\langle a \rangle| = m$. Mit 4.8.5 gibt es genau eine zyklische Untergruppe der Ordnung d von $\langle a \rangle$. Diese ist eine zyklische Untergruppe von G, es gibt also ein $b \in G$ mit $\mathrm{ord}(b) = d$.

3. Wenn $m, n \in S$, so gilt $\mathrm{kgV}(m, n) \in S$.

   Beweis Mit Proposition 4.8.8 gilt $\mathrm{kgV}(m, n) = \prod_{p \in P_{mn}} p^{\max(w_p(m), w_p(n))}$.

   Mit Schritt 2 gilt $p^{\max(w_p(m), w_p(n))} \in S$ für alle $p \in P_{mn}$. Mit Schritt 1 folgt $\mathrm{kgV}(m, n) \in S$.

4. Sei n das größte Element in S. Dann ist jedes $m \in S$ ein Teiler von n.

   Beweis Sei $m \in S$. Es ist $n \leq \mathrm{kgV}(n, m)$. Mit Schritt 3 liegt $\mathrm{kgV}(n, m)$ in S. Da n maximal ist, folgt $n = \mathrm{kgV}(n, m) \in S$. Es folgt $m|n$.

5. Sei n das größte Element in S. Dann gilt $n = q$.

   Beweis Sei $a \in G$ mit $\mathrm{ord}(a) = m$. Mit Schritt 4 gilt $n = mm'$. Es folgt $a^n = (a^m)^{m'} = e$ für alle $a \in G$. Das neutrale Element e in G ist aber das neutrale Element 1 der Multiplikation in $\mathbb{K}$. Somit sind alle q Elemente von G Nullstellen des Polynoms $T^n - 1 \in \mathbb{K}[T]$. In der Linearen Algebra II, Kurseinheit 1, haben Sie gesehen, dass ein Polynom vom Grad n maximal n Nullstellen hat.

Es folgt $n \geq q$. Andererseits liegt n in S, also $n \leq q$. Es folgt $n = q$, und dies impliziert die Behauptung.

□

Das war ein trickreicher Beweis, der die Existenz eines erzeugenden Elementes von G zeigte, ohne dass der Beweis einen Hinweis darauf gab, wie man ein solches finden kann. Kombinieren wir den Satz mit Proposition 4.8.5 (e), so erhalten wir:

4.8.10 Korollar Sei $\mathbb{K}$ ein Körper, und sei G eine endliche Untergruppe von $\mathbb{K}^\times$. Sei $|G| = q$. Dann gibt es $\varphi(q)$ erzeugende Elemente von G. □

4.8.11 Korollar Sei $\mathbb{F}$ ein endlicher Körper mit q Elementen. Dann ist $\mathbb{F}^\times$ zyklisch, und es gibt $\varphi(q-1)$ erzeugende Elemente von $\mathbb{F}^\times$.

Beweis: Es ist $\mathbb{F}^\times$ eine endliche Gruppe mit $q-1$ Elementen, denn nur $0 \notin \mathbb{F}^\times$. Die Behauptung folgt nun aus 4.8.10. □

Die erzeugenden Elemente von $\mathbb{F}^\times$, $|\mathbb{F}| < \infty$ sind so wichtig, dass sie eine eigene Bezeichnung erhalten.

4.8.12 Definition Sei $\mathbb{F}$ ein endlicher Körper. Ein erzeugendes Element von $\mathbb{F}^\times$ wird ein **primitives Element** in $\mathbb{F}$ genannt.

Eine weitere Klasse zyklischer Gruppen liefert die folgende Proposition:

4.8.13 Proposition Sei $p > 2$ eine Primzahl, und sei $m \in \mathbb{N}$. Dann ist $(\mathbb{Z}/p^m\mathbb{Z})^\times$ zyklisch.

Beweis: Wenn $m = 1$, so sind wir fertig, denn $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper. Wir nehmen also an, dass $m > 1$ gilt. Sei g ein erzeugendes Element von $(\mathbb{Z}/p\mathbb{Z})^\times$. Wir unterscheiden zwei Fälle:

Fall 1: Es ist $g^{p-1} \bmod p^2 \neq 1$.

Behauptung g ist ein erzeugendes Element von $(\mathbb{Z}/p^m\mathbb{Z})^\times$.

Beweis Mit Bemerkung 4.4.8 gilt $\varphi(p^m) = p^{m-1}(p-1)$, also $|(\mathbb{Z}/p^m\mathbb{Z})^\times| = p^{m-1}(p-1)$. Mit Korollar 4.3.13 aus dem Satz von Lagrange folgt

$$g^{p^{m-1}(p-1)} \bmod p^m = 1$$

Sei s die Ordnung von g in $(\mathbb{Z}/p^m\mathbb{Z})^\times$. Wir sind fertig, wenn wir zeigen können, dass $s = p^{m-1}(p-1)$ ist. Zunächst wissen wir nur, dass s ein Teiler von $p^{m-1}(p-1)$ ist.

Aus der Annahme, dass g ein erzeugendes Element von $(\mathbb{Z}/p\mathbb{Z})^\times$ ist, folgt, dass $g^{p-1} \bmod p = 1$, also $g^{p-1} = ap + 1$ für ein $a \in \mathbb{Z}$. Da $g^{p-1} \bmod p^2 \neq 1$, folgt, dass p kein Teiler von a ist, also $\mathrm{ggT}(a, p) = 1$.

Da s ein Teiler von $p^{m-1}(p-1)$ ist, folgt $s = p^r t$ mit $r \leq m-1$, und t ist ein Teiler von $p-1$. Wir schreiben die Zahl $p^r t$ jetzt anders:

$$p^r t = (p^{r-1}(p-1) + p^{r-1})t = p^{r-1}(p-1)t + p^{r-1}t.$$

Dann gilt

$$1 = g^{p^r t} \bmod p = (\underbrace{g^{p-1}}_{=1})^{p^{r-1}t} \cdot g^{p^{r-1}t} \bmod p = g^{p^{r-1}t} \bmod p.$$

Es gilt also $1 = g^{p^r t} \bmod p = g^{p^{r-1}t} \bmod p$, und indem wir dieses Verfahren induktiv fortsetzen, erhalten wir $g^t \bmod p = 1$. Da $p-1$ die Ordnung von g in $(\mathbb{Z}/p\mathbb{Z})^\times$ ist, folgt $t = p-1$. Somit gilt $s = p^r(p-1)$.

Es gilt

$$\begin{aligned} 1 &= g^{p^r(p-1)} \bmod p^m \\ &= (g^{p-1})^{p^r} \bmod p^m \\ &= (ap+1)^{p^r} \bmod p^m \\ &= (1 + p^{r+1}a + \text{ Vielfache von } p^l) \bmod p^m, \text{ wobei } l > r+1. \end{aligned}$$

Das letzte Gleichheitszeichen folgt mit der Binomischen Formel (Lineare Algebra II, Kurseinheit 3). Wie die Vielfachen von p^l genau aussehen, wird uns in dem Beweis nicht weiter interessieren.

Es folgt, dass p^m ein Teiler von ($p^{r+1}a +$ Vielfache von p^l) ist. Dann muss p^m ein Teiler von $p^{r+1}a$ sein. Da a und p teilerfremd sind, folgt $p^m | p^{r+1}$, also $m = r+1$. Somit gilt $s = p^{m-1}(p-1)$, und es folgt, dass g ein erzeugendes Element von $(\mathbb{Z}/p^m\mathbb{Z})^\times$ ist.

Fall 2: Es gilt $g^{p-1} \bmod p^2 = 1$.

Sei $h = (p+1)g$. Es folgt $h \bmod p = (pg + g) \bmod p = g \bmod p$, das heißt, h

ist ein erzeugendes Element von $(\mathbb{Z}/p\mathbb{Z})^\times$. Weiter folgt

$$\begin{aligned} h^{p-1} \bmod p^2 &= ((p+1)g)^{p-1} \bmod p^2 \\ &= (p+1)^{p-1} \cdot g^{p-1} \bmod p^2 \\ &= (p+1)^{p-1} \bmod p^2 \\ &= (1 + (p-1)p + \text{ Vielfache von } p^2) \bmod p^2 \\ &\quad \text{mit der Binomischen Formel} \\ &= (1 - p + p^2 + \text{ Vielfache von } p^2) \bmod p^2 \\ &= (1-p) \bmod p^2 \\ &\neq 1 \bmod p^2. \end{aligned}$$

Wir ersetzen g durch h, und wie im Fall 1 ist h ein erzeugendes Element von $(\mathbb{Z}/p^m\mathbb{Z})^\times$.

□

4.8.14 Aufgabe (1) Finden Sie ein Beispiel für eine Zahl n, so dass $(\mathbb{Z}/n\mathbb{Z})^\times$ nicht zyklisch ist.

(2) Geben Sie ein Beispiel für ein erzeugendes Element von $(\mathbb{Z}/81\mathbb{Z})^\times$.

4.9 Produkte von Gruppen

Seien $(G_1, *_1), \ldots, (G_n, *_n)$ Gruppen. Das **cartesische Produkt** von $G_1, \ldots, G_n$ ist die Menge

$$G_1 \times \cdots \times G_n = \{(g_1, \ldots, g_n) \mid g_i \in G_i, 1 \leq i \leq n\}$$

der n-Tupel von Elementen in $G_1, \ldots, G_n$. Das cartesische Produkt wird auch mit $\prod_{i=1}^{n} G_i$ bezeichnet.

Auf $G_1 \times \cdots \times G_n$ definieren wir eine Verknüpfung

$$\begin{array}{rccccc} * : & (G_1 \times \cdots \times G_n) & \times & (G_1 \times \cdots \times G_n) & \to & (G_1 \times \cdots \times G_n) \\ & ((g_1, \ldots, g_n), & & (g'_1, \ldots, g'_n)) & \mapsto & (g_1 *_1 g'_1, \ldots, g_n *_n g'_n). \end{array}$$

Mit dieser Verknüpfung ist $G_1 \times \cdots \times G_n = \prod_{i=1}^{n} G_i$ eine Gruppe. Das neutrale Element in $\prod_{i=1}^{n} G_i$ ist $(e_{G_1}, \ldots, e_{G_n})$, und invers zu einem Element $(g_1, \ldots, g_n)$ ist $(g_1^{-1}, \ldots, g_n^{-1})$.

4.9.1 Definition Die Gruppe $\prod_{i=1}^{n} G_i$ wird das **direkte Produkt** von $G_1, \ldots, G_n$ genannt.

4.9.2 Bemerkung Seien $G_1, \ldots, G_n$ Gruppen, und sei $G = \prod_{i=1}^{n} G_i$.

(a) Wenn es ein $1 \leq i \leq n$ mit $|G_i| = \infty$ gibt, so ist $|G| = \infty$.

(b) Wenn $|G_i| < \infty$ für alle $1 \leq i \leq n$, so ist $|G| = \prod_{i=1}^{n} |G_i|$.

Beweis:

(a) Sei ohne Einschränkung $|G_1| = \infty$. Dann gibt es eine unendliche Indexmenge J, so dass g_{1j}, $j \in J$, unendlich viele verschiedene Elemente in G_1 sind. Dann sind $(g_{1j}, e_{G_2}, \ldots, e_{G_n})$, $j \in J$, unendlich viele verschiedene Elemente in G.

(b) Wir beweisen die Behauptung mit Induktion nach n. Für $n = 1$ ist die Behauptung richtig. Sei $n > 1$. Es ist $G = \prod_{i=1}^{n} G_i = \prod_{i=1}^{n-1} G_i \times G_n$. Nach Induktionsvoraussetzung gilt $\left|\prod_{i=1}^{n-1} G_i\right| = \prod_{i=1}^{n-1} |G_i|$. Da $|M \times N| = |M| \cdot |N|$ für alle endlichen Mengen M und N, folgt die Behauptung.

□

4.9.3 Aufgaben Seien G und H Gruppen.

(1) Beweisen Sie, dass $G \times H$ genau dann abelsch ist, wenn G und H abelsch sind.

(2) Sei $G \simeq G'$, und sei $H \simeq H'$. Beweisen Sie, dass $G \times H$ und $G' \times H'$ isomorph sind.

Wir werden in diesem Abschnitt untersuchen, wann direkte Produkte von zyklischen Gruppen zyklisch sind. Dazu betrachten wir zunächst zwei Beispiele.

4.9.4 Beispiele (a) Sei $C_2 = (\mathbb{Z}/2\mathbb{Z}, +)$, und sei $G = C_2 \times C_2$. Es ist $G =$

$\{(0,0),(1,0),(0,1),(1,1)\}$. Weiter gilt

$$\begin{array}{rcl}\langle(0,0)\rangle & = & \{(0,0)\}\\ \langle(1,0)\rangle & = & \{(1,0),(0,0)\}\\ \langle(0,1)\rangle & = & \{(0,1),(0,0)\}\\ \langle(1,1)\rangle & = & \{(1,1),(0,0)\}.\end{array}$$

Es folgt, dass G nicht zyklisch ist.

(b) Seien $C_2 = (\mathbb{Z}/2\mathbb{Z},+)$ und $C_3 = (\mathbb{Z}/3\mathbb{Z},+)$. Sei $G = C_2 \times C_3$. Es ist $G = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$. Betrachten wir die von $(1,1)$ erzeugte Untergruppe, so erhalten wir

$$\langle(1,1)\rangle = \{(1,1),(0,2),(1,0),(0,1),(1,2),(0,0)\}.$$

Somit ist G zyklisch mit erzeugendem Element $(1,1)$.

4.9.5 Aufgabe Sei G wie in Beispiel 4.9.4 (b). Bestimmen Sie $\langle(1,2)\rangle$.

4.9.6 Proposition Seien C_m und C_n zyklisch mit $|C_m| = m$ und $|C_n| = n$. Genau dann ist $C_m \times C_n$ zyklisch, wenn $\mathrm{ggT}(m,n) = 1$ ist.

Beweis:

$\Rightarrow$ Sei $\mathrm{ggT}(m,n) = d > 1$. Seien $m' = \frac{m}{d}$ und $n' = \frac{n}{d}$. Dann gilt $m'dn' < mn$.

Sei $(x,y) \in C_m \times C_n$. Mit Korollar 4.3.13 aus dem Satz von Lagrange folgt $x^m = e_{C_m}$ und $y^n = e_{C_n}$. Dann gilt

$$(x,y)^{m'dn'} = (x^{m'dn'}, y^{m'dn'}) = ((x^{m'd})^{n'}, (y^{dn'})^{m'}) = (e_{C_m}^{n'}, e_{C_n}^{m'}) = (e_{C_m}, e_{C_n}).$$

Da es kein Element $(x,y) \in C_m \times C_n$ mit der Ordnung mn gibt, ist $C_m \times C_n$ nicht zyklisch.

$\Leftarrow$ Sei $\mathrm{ggT}(m,n) = 1$. Sei a ein erzeugendes Element von C_m, und sei b ein erzeugendes Element von C_n. Wir zeigen, dass (a,b) ein erzeugendes Element von $C_m \times C_n$ ist.

Sei k die Ordnung von (a,b), also $(a,b)^k = (a^k, b^k) = (e_{C_m}, e_{C_n})$. Es folgt $m|k$ und $n|k$. Da $\mathrm{ggT}(m,n) = 1$ folgt $mn|k$. Somit ist k ein positives Vielfaches von mn. Da $|G| = mn$ und $k \leq |G|$, folgt $k = mn$.

□

4.9.7 Satz (Struktursatz endlicher zyklischer Gruppen)

Sei C_n eine zyklische Gruppe der Ordnung n. Sei $n = \prod_{i=1}^{r} p_i^{s_i}$ die Primfaktorzerlegung von n mit $p_i \neq p_j$ für alle $1 \leq i, j \leq n$, $i \neq j$. Dann gilt

$$C_n \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}.$$

Beweis: Wir beweisen die Behauptung mit Induktion nach r. Ist $r = 1$, also $n = p^s$ für eine Primzahl p, so gilt $C_n \simeq \mathbb{Z}/p^s\mathbb{Z}$ mit Proposition 4.8.4.

Sei $r > 1$. Für den Induktionsschritt nehmen wir an, dass jede zyklische Gruppe $C_{n'}$ mit Primfaktorzerlegung $n' = \prod_{i=1}^{r-1} p_i^{s_i}$, $p_i \neq p_j$ für $i \neq j$, isomorph zu $\prod_{i=1}^{r-1} \mathbb{Z}/p^{s_i}\mathbb{Z}$ ist.

Sei C_n zyklisch mit $n = \prod_{i=1}^{r} p_i^{s_i}$ und $p_i \neq p_j$ für $i \neq j$. Mit Proposition 4.8.4 gibt es einen Isomorphismus

$$\phi : C_n \to \mathbb{Z}/n\mathbb{Z}.$$

Sei $n' = \prod_{i=1}^{r-1} p_i^{s_i}$. Da $\mathrm{ggT}(n', p_r^{s_r}) = 1$, ist $\mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/p_r^{s_r}\mathbb{Z}$ zyklisch mit Ordnung $n' p_r^{s_r} = n$. Wieder mit Proposition 4.8.4 gibt es einen Isomorphismus

$$\psi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/p_r^{s_r}\mathbb{Z}.$$

Mit der Induktionsannahme gibt es einen Isomorphismus

$$g : \mathbb{Z}/n'\mathbb{Z} \to \prod_{i=1}^{r-1} \mathbb{Z}/p^{s_i}\mathbb{Z}.$$

Mit Aufgabe 4.9.3 gibt es einen Isomorphismus

$$h : \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/p_r^{s_r}\mathbb{Z} \to (\prod_{i=1}^{r-1} \mathbb{Z}/p^{s_i}\mathbb{Z}) \times \mathbb{Z}/p_r^{s_r}\mathbb{Z}.$$

Es folgt, dass $h \circ \psi \circ \phi : C_n \to \prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ ein Isomorphismus ist. □

Insbesondere gilt für die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$:

4.9.8 Korollar $\mathbb{Z}/n\mathbb{Z}$ ist isomorph zu $\prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$, wobei $n = \prod_{i=1}^{r} p_i^{s_i}$ mit $p_i \neq p_j$ für $i \neq j$ die Primzahlzerlegung von n ist. □

Lösungen der Aufgaben

Lösungen der Aufgaben in Kapitel 4

Aufgabe 4.2.5

(1) **Behauptung** Sei $(G, +)$ eine Gruppe, und sei H eine nicht leere Teilmenge von G. Dann gilt

$$H < G \Leftrightarrow a - b \in H \text{ für alle } a, b \in H.$$

Beweis:

$\Rightarrow$ Seien $a, b \in H$. Da H eine Gruppe ist, folgt $-b \in H$. Da $+$ eine Verknüpfung auf H ist, gilt $a - b \in H$.

$\Leftarrow$ Sei $H \neq \emptyset$, und sei $a - b \in H$ für alle $a, b \in H$. Da $H \neq \emptyset$, gibt es ein $a \in H$. Nach Voraussetzung liegt $a - a = 0$ in H, somit hat H ein neutrales Element.

Nach Voraussetzung liegt mit $a \in H$ auch $0 - a = -a$ in H. Es folgt, dass jedes Element in H ein inverses Element in H besitzt.

Das Assoziativgesetz gilt für alle Elemente in H, denn $H \subseteq G$, und es gilt für alle Elemente in G.

Da mit $b \in H$ auch $-b \in H$, gilt nach Voraussetzung $a-(-b) = a+b \in H$, und dies zeigt, dass $+$ eine Verknüpfung auf H ist. Somit ist $(H, +)$ eine Gruppe.

□

(2) Sei G eine Gruppe, und seien K, H Untergruppen von G.

Behauptung $K \cap H$ ist eine Untergruppe von G.

Beweis: Die Untergruppen K und H enthalten beide das neutrale Element e von G. Somit ist $K \cap H$ nicht die leere Menge.

Seien $a, b \in K \cap H$. Dann gilt $a, b \in K$, und $ab^{-1} \in K$, denn K ist eine Untergruppe von G. Analog gilt $ab^{-1} \in H$. Es folgt $ab^{-1} \in K \cap H$, und mit dem Untergruppenkriterium ist $K \cap H$ eine Untergruppe von G. □

Aufgabe 4.2.8

(1) Sei $G = \mathbb{Z}$ mit der Addition. Sei $m \in \mathbb{Z}$.

Gesucht sind alle Elemente in $\langle m \rangle$ und die Ordnung von m.

Nach Definition ist $\langle m \rangle = \{im \mid i \in \mathbb{Z}\}$, wobei wir die additive Schreibweise in $\langle m \rangle$ verwenden. Die Gruppen $\langle m \rangle$ enthalten für $m \neq 0$ unendlich viele Elemente, also gilt $\text{ord}(m) = \infty$ für alle $m \neq 0$. Die Ordnung von 0 ist 1. □

(2) Sei $G = S_3$, also

$$G = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}.$$

Seien $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ und $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

Gesucht sind $\langle \sigma \rangle$, $\langle \tau \rangle$, $\text{ord}(\sigma)$ und $\text{ord}(\tau)$.

Es gilt $\sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{id}$. Somit ist $\sigma \circ \sigma$ das neutrale Element in S_3. Es folgt $\sigma^n = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ für alle geraden ganzen Zahlen n und $\sigma^n = \sigma$ für alle ungeraden ganzen Zahlen. Somit gelten $\langle \sigma \rangle = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$ und $\text{ord}(\sigma) = 2$.

Es gilt $\tau \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \tau^2$ und $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \tau^3$. Es folgt $\tau^n = \text{id}$ für alle ganzen Zahlen n, die durch 3 teilbar sind.

Ist $n = 3x + 1$ für eine ganze Zahl x, so gilt $\tau^n = (\tau^3)^x \circ \tau = \text{id} \circ \tau = \tau$.

Ist $n = 3x + 2$ für eine ganzen Zahl x, so gilt $\tau^n = (\tau^3)^x \circ \tau^2 = \text{id} \circ \tau^2 = \tau^2$.
Es folgt $\langle \tau \rangle = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$ und $\text{ord}(\tau) = 3$. □

Aufgabe 4.3.4

(1) Sei $G = S_3$, und sei $H = A_3$ die Untergruppe der Permutationen σ mit $\operatorname{sgn}(\sigma) = 1$. Gesucht sind die verschiedenen Linksnebenklassen modulo H.

Es sind

$$G = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$$

und

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}.$$

Für alle $\sigma \in H$ gilt $\sigma H = H$.

Sei $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Dann gilt

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Es folgt $\sigma H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$.

Sei $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Dann gilt

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Es folgt $\sigma H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$.

Sei $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Dann gilt

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Es folgt $\sigma H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$.

(2) Sei $G = \mathbb{Z}$, und sei $H = n\mathbb{Z}$ für ein $n \in \mathbb{Z}$.

Behauptung Die verschiedenen Linksnebenklassen von $n\mathbb{Z}$ sind

$$0 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}.$$

Beweis: Sei $a \in \mathbb{Z}$. Wir dividieren a durch n mit Rest und erhalten $a = xn + r$ mit $0 \leq r < n$. Dann gilt $a + n\mathbb{Z} = r + n\mathbb{Z}$. Es folgt, dass $0 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}$ alle Linksnebenklassen von $\mathbb{Z}$ sind. Es bleibt zu zeigen, dass diese Nebenklassen verschieden sind. Dazu sei $x \in (m + n\mathbb{Z}) \cap (m' + n\mathbb{Z})$ für $0 \leq m, m' < n$. Dann gibt es $z, z' \in \mathbb{Z}$ mit $x = m + nz = m' + nz'$. Es folgt $0 = (m - m') + n(z - z') \in n\mathbb{Z}$. Somit gilt $m - m' = 0$, denn $-(n-1) \leq m - m' < n - 1$, also $m = m'$. □

Aufgabe 4.3.7 Sei $(G, +)$ eine Gruppe, und sei H eine endliche Untergruppe von G.

Behauptung Alle Rechtsnebenklassen modulo H haben die Mächtigkeit $|H|$.

Beweis: Sei $a \in G$. Wir definieren eine Abbildung

$$f : H + a \to H \text{ durch } f(h + a) = h + a - a = h \text{ für alle } h + a \in H + a.$$

Die Abbildung f ist injektiv und surjektiv, also bijektiv. Da H und $H + a$ endliche Mengen sind, folgt $|H + a| = |H|$. □

Aufgabe 4.4.10

Es gilt $200 = 2^3 \cdot 5^2$. Mit der Formel in Korollar 4.4.9 folgt $\varphi(200) = 2^2 \cdot 1 \cdot 5 \cdot 4 = 80$. Somit ist 80 die Anzahl der zu 200 teilerfremden Zahlen x mit $0 < x \leq 200$.

Aufgabe 4.5.3

(1) Wir definieren $\phi' : G \to H$ durch $\phi'(0) = 1$, $\phi'(1) = -i$, $\phi'(2) = -1$ und $\phi'(3) = i$.

Offenbar ist ϕ' bijektiv. Wir zeigen, dass ϕ' strukturverträglich ist. Es gilt:

$$\begin{array}{lllllll} \phi'(0+0) & = & \phi'(0) & = & 1 & = & \phi'(0) \cdot \phi'(0) \\ \phi'(0+1) & = & \phi'(1) & = & -i & = & \phi'(0) \cdot \phi'(1) \\ \phi'(0+2) & = & \phi'(2) & = & -1 & = & \phi'(0) \cdot \phi'(2) \\ \phi'(0+3) & = & \phi'(3) & = & i & = & \phi'(0) \cdot \phi'(3). \end{array}$$

Da G und H abelsch sind, folgt $\phi'(0+z) = \phi'(z+0) = \phi'(0) \cdot \phi'(z) = \phi'(z) \cdot \phi'(0)$ für alle $z \in \mathbb{Z}/4\mathbb{Z}$.

$$\begin{array}{lllllll} \phi'(1+1) & = & \phi'(2) & = & -1 & = & \phi'(1) \cdot \phi'(1) \\ \phi'(1+2) & = & \phi'(3) & = & i & = & \phi'(1) \cdot \phi'(2) \\ \phi'(1+3) & = & \phi'(0) & = & 1 & = & \phi'(1) \cdot \phi'(3). \end{array}$$

Es folgt $\phi'(1+z) = \phi'(z+1) = \phi'(1) \cdot \phi'(z) = \phi'(z) \cdot \phi'(1)$ für alle $z \in \mathbb{Z}/4\mathbb{Z}$.

$$\begin{array}{lllllll} \phi'(2+2) & = & \phi'(0) & = & 1 & = & \phi'(2) \cdot \phi'(2) \\ \phi'(2+3) & = & \phi'(1) & = & -i & = & \phi'(2) \cdot \phi'(3). \end{array}$$

Es folgt $\phi'(2+z) = \phi'(z+2) = \phi'(2) \cdot \phi'(z) = \phi'(z) \cdot \phi'(2)$ für alle $z \in \mathbb{Z}/4\mathbb{Z}$.

$$\phi'(3+3) = \phi'(2) = -1 = \phi'(3) \cdot \phi'(3).$$

Also gilt $\phi(z+z') = \phi(z) \cdot \phi(z')$ für alle $z, z' \in \mathbb{Z}/4\mathbb{Z}$. Somit ist ϕ' ein Gruppenhomomorphismus.

(2) Wir definieren $h : G \to H$ durch $h(0) = i$, $h(1) = -i$, $h(2) = 1$ und $h(3) = -1$. Offenbar ist h bijektiv. Da beispielsweise $h(0+1) = h(1) = -i \neq h(0) \cdot h(1) = i(-i) = 1$, folgt, dass h kein Gruppenisomorphismus ist.

Aufgabe 4.6.8

(1) Ohne Lösung

(2) In Beispiel 4.5.6 wurde gezeigt, dass $\mathrm{Kern}(\phi) = n\mathbb{Z}$ ist. Es folgt $\mathbb{Z}/\mathrm{Kern}(\phi) = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$, die Menge der Nebenklassen modulo $n\mathbb{Z}$. In Aufgabe 4.3.4 haben wir gesehen, dass $0+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}$ die verschiedenen Nebenklassen sind. Es folgt $\mathbb{Z}/\mathrm{Kern}(\phi) = \{0 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$.

(3) Sei S ein Normalteiler von G, und sei G endlich. Dann ist $G/S = \{gS \mid g \in G\}$ ebenfalls eine endliche Menge.

Die Menge G/S war definiert als die Menge der Linksnebenklassen von G modulo S. In Definition 4.3.5 hatten wir die Anzahl $[G : S]$ dieser Nebenklassen als den Index von S in G bezeichnet. Mit dem Satz 4.3.8 von Lagrange folgt $[G : S] = \dfrac{|G|}{|S|}$.

Aufgabe 4.6.9

Sei S ein Normalteiler von G, und sei $\pi : G \to G/S$, definiert durch $\pi(g) = gS$ für alle $g \in G$, der kanonische Epimorphismus von G auf G/S.

Behauptung Es ist $\mathrm{Kern}(\pi) = S$.

Beweis: Sei $g \in G$. Es gilt

$$\begin{array}{rcl} g \in \mathrm{Kern}(\pi) & \Leftrightarrow & gS = e_G S \\ & \Leftrightarrow & e_G^{-1} g = g \in S, \end{array}$$

wobei das letzte Äquivalenzzeichen aus dem Kriterium 4.6.2 für die Gleichheit von Nebenklassen folgt. Es folgt die Behauptung. □

Aufgabe 4.7.2

Seien $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ und $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Die Permutation σ ist eine Transposition, und es folgt, dass $\sigma^{-1} = \sigma$ ist. Es folgt

$$\begin{array}{rcl} \sigma \circ \tau \circ \sigma^{-1} & = & \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \\ & = & \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\ & \neq & \tau. \end{array}$$

Aufgabe 4.7.4

Sei $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Wir haben in Aufgabe 4.7.2 gesehen, dass $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \notin N(\{\tau\})$ gilt. Analog gilt für die anderen Transpositionen in S_3

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq \tau$$

und

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\circ\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\circ\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\neq\tau.$$

Es folgt, dass $N(\{\tau\})$ keine Transpositionen enthält.

Die identische Permutation und τ selbst liegen in $N(\{\tau\})$. Auch $\tau^{-1}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ liegt in $N(\{\tau\})$, denn $\tau^{-1}\circ\tau\circ\tau=\tau$. Somit gilt

$$N(\{\tau\})=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}.$$

Aufgabe 4.7.8

Behauptung Wenn G eine Gruppe ist, so ist $C(G)$ ein Normalteiler von G.

Beweis: Nach Definition gilt $C(G)g=gC(G)$ für alle $g\in G$. Es ist also nur zu zeigen, dass das Zentrum von G eine Untergruppe von G ist.

Dazu eine Vorbemerkung: Wenn $b\in C(G)$ und $x\in G$, so gilt $bx=xb$, also $x=b^{-1}xb$, und, indem wir von rechts mit b^{-1} multiplizieren, folgt $xb^{-1}=b^{-1}x$. Dies zeigt, dass auch b^{-1} in $C(G)$ liegt.

Um zu beweisen, dass $C(G)$ eine Untergruppe von G ist, benutzen wir das Untergruppenkriterium 4.2.4.

$C(G)$ ist nicht leer, denn $e_G\in C(G)$. Seien $a,b\in C(G)$. Dann gilt für alle $g\in G$:

$$(ab^{-1})g=a(b^{-1}g)=(b^{-1}g)a=b^{-1}(ga)=(ga)b^{-1}=g(ab^{-1}).$$

Es folgt $ab^{-1}\in C(G)$, und mit dem Untergruppenkriterium folgt die Behauptung. □

Aufgabe 4.8.3

(1) **Behauptung** 1 und -1 sind die einzigen erzeugenden Elemente von $\mathbb{Z}$.

Beweis: In Beispiel 4.8.2 haben wir gesehen, dass 1 und -1 erzeugende Elemente von $\mathbb{Z}$ sind. Wir müssen also nur zeigen, dass es keine weiteren erzeugenden Elemente gibt. Sei $a\in\mathbb{Z}$, $a\notin\{-1,1\}$. Angenommen, a wäre ein erzeugendes Element von $\mathbb{Z}$. Dann gibt es ein $n\in\mathbb{Z}$ mit $na=1$. Das ist ein Widerspruch, denn in $\mathbb{Z}$ sind 1 und -1 die einzigen invertierbaren Elemente. □

(2) **Behauptung** S_3 ist nicht zyklisch.

Beweis: Wir zeigen, dass keines der Elemente in S_3 die Ordnung $6 = |S_3|$ hat.

Die identische Permutation id hat die Ordnung 1, ist also kein erzeugendes Element.

Die Transpositionen in S_3 haben die Ordnung 2, sind also auch keine erzeugenden Elemente.

Es bleiben die Permutationen $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ und $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ zu überprüfen. Es ist $\sigma^2 = \tau$ und $\sigma^3 = \mathrm{id}$. Somit ist 3 die Ordnung von σ, das heißt, σ ist kein erzeugendes Element von S_3. Analog hat τ die Ordung 3, ist also auch kein erzeugendes Element. □

(3) **Behauptung** A_3 ist zyklisch.

Beweis: Es ist $A_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$. Die Permutationen $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ und $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ haben die Ordnung 3, sie sind also erzeugende Elemente von A_3. □

(4) **Behauptung** Zyklische Gruppen sind abelsch.

Beweis: Sei G eine zyklische Gruppe mit erzeugendem Element x. Seien $a = x^n$ und $b = x^m$ Elemente in G. Dann gilt

$$ab = x^n x^m = x^{n+m} = x^{m+n} = x^m x^n = ba,$$

und es folgt, dass G abelsch ist. □

Aufgabe 4.8.14

(1) Sei $n = 12$. Die Einheitengruppe von $\mathbb{Z}/12\mathbb{Z}$ ist $(\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$. In $\mathbb{Z}/12\mathbb{Z}$ gilt

$$\begin{array}{lllll} 1^2 & = & 1 & & \\ 5^2 & = & 25 & = & 1 \\ 7^2 & = & 49 & = & 1 \\ 11^2 & = & 121 & = & 1. \end{array}$$

Es folgt, dass $(\mathbb{Z}/12\mathbb{Z})^\times$ nicht zyklisch ist.

(2) Es ist $81 = 3^4$. In $\mathbb{Z}/3\mathbb{Z}$ ist 2 ein erzeugendes Element von $(\mathbb{Z}/3\mathbb{Z})^\times$. Es ist $2^2 \bmod 9 = 4 \bmod 9 \neq 1$. Im Beweis von 4.8.13 wurde gezeigt, dass 2 ein erzeugendes Element von $(\mathbb{Z}/81\mathbb{Z})^\times$ ist.

Aufgabe 4.9.3

Seien G und H Gruppen.

(1) **Behauptung** $G \times H$ ist genau dann abelsch ist, wenn G und H abelsch sind.

Beweis: Sei $G \times H$ abelsch. Seien $g, g' \in G$ und $h, h' \in H$. Dann gilt $(gg', hh') = (g, h)(g', h') = (g', h')(g, h) = (g'g, h'h)$. Es folgt $gg' = g'g$ und $hh' = h'h$ für alle $g, g' \in G$ und alle $h, h' \in H$. Somit sind G und H abelsch.

Seien umgekehrt G und H abelsch. Seien $(g, h), (g', h') \in G \times H$. Dann gilt $(g, h)(g', h') = (gg', hh') = (g'g, h'h) = (g'h')(g, h)$. Somit ist $G \times H$ abelsch. □

(2) Sei $G \simeq G'$, und sei $H \simeq H'$.

Behauptung $G \times H$ und $G' \times H'$ sind isomorph.

Beweis: Seien $\phi : G \to G'$ und $\psi : H \to H'$ Isomorphismen. Wir definieren $f : G \times H \to G' \times H'$ durch $f((g, h)) = (\phi(g), \psi(h))$ für alle $(g, h) \in G \times H$. Es ist $f^{-1} : G' \times H' \to G \times H$, definiert durch $f^{-1}((g', h')) = (\phi^{-1}(g'), \psi^{-1}(h'))$ für alle $(g', h') \in G' \times H'$, invers zu f. Somit ist f bijektiv. Ein Routinebeweis zeigt, dass f strukturverträglich ist. □

Aufgabe 4.9.5

Es ist $\langle (1, 2) \rangle = \{(1, 2), (0, 1), (1, 0), (0, 2), (1, 1), (0, 0)\}$.

Kurseinheit 3

Ringe

Studierhinweise

In dieser Kurseinheit werden wir grundlegende Definitionen und Eigenschaften von Ringen untersuchen und ein erstes Public-Key-Kryptosystem vorstellen.

Nachdem wir in Abschnitt 5.1 einige grundlegende Begriffe und Beispiele behandelt haben, wird in Abschnitt 5.2 eine ganz wichtige Konstruktion vorgestellt, wie wir aus Ringen neue Ringe herstellen können. Es geht um so genannte Faktorringe modulo einem Ideal. Diese Konstruktion ist analog zu Konstruktionen, die Sie im Laufe des Studiums schon kennen gelernt haben: In der Linearen Algebra haben Sie Faktorräume modulo einem Unterraum und in Kurseinheit 2 Faktorgruppen modulo einem Normalteiler gesehen. Die Konstruktion eines Faktorringes modulo einem Ideal ist ganz ähnlich, nur dass eben auf die besondere Situation, dass wir mit Ringen arbeiten, eingegangen wird. Sie kennen schon Beispiele für Faktorringe. Die Ringe $\mathbb{Z}/n\mathbb{Z}$ sind Faktorringe, mit denen Sie schon seit dem ersten Semester arbeiten. Die wichtigsten Faktorringe in der Kryptografie sind die Ringe $\mathbb{Z}/n\mathbb{Z}$ und gewisse Faktorringe von Polynomringen $\mathbb{F}_p[T]$, wobei p eine Primzahl ist. Letztere werden benötigt, um die endlichen Körper zu konstruieren, die nicht von der Form $\mathbb{F}_p$, p eine Primzahl sind. Diesen Körpern wird sich die Kurseinheit 5 widmen.

In Abschnitt 5.3 geht es um Ringhomomorphismen. Das sind Abbildungen zwischen Ringen, die die Ringstrukturen respektieren. Nichts in diesem Abschnitt ist wirklich überraschend. Sie werden viele Analogien zwischen Vektorraumhomomorphismen (linearen Abbildungen) und Gruppenhomomorphismen feststellen.

Abschnitt 5.4 widmet sich einem klassischen Satz der elementaren Zahlentheorie, dem so genannten Chinesischen Restsatz. Dieser Satz gibt Antwort auf die Frage, wie gewisse Kongruenzen simultan gelöst werden können. Dieser Satz ist schon seit etwa 2000 Jahren bekannt, ist aber alles andere als ein alter Hut. Er hat wichtige Anwendungen in der Computeralgebra und der Kryptografie.

In Abschnitt 5.5 werden wir spezielle Unterringe von Ringen untersuchen, die so genannten Primringe. Diese sind in gewisser Weise die „kleinsten Unterringe“ von Ringen. Primringe werden bei der Konstruktion der endlichen Körper in Kursein-

heit 5 wieder eine Rolle spielen.

Besonders wichtige Ringe in der Kryptografie sind der Ring $\mathbb{Z}$ und Polynomringe über endlichen Körpern sowie Faktorringe dieser Ringe. Diese Ringe sind kommutativ. Wir werden daher in Abschnitt 5.6 auf diese spezielle Situation eingehen und Ideale und Faktorringe kommutativer Ringe näher betrachten.

Abschnitt 5.6 widmet sich Polynomringen. Hier werden wir unter anderem einige Fakten aus der Linearen Algebra II wiederholen, wo Polynome im Zusammenhang mit dem charakteristischen Polynom einer Matrix oder eines Endomorphismus studiert werden. Dieser Abschnitt ist im gewissen Sinne schon der Auftakt zu Kurseinheit 5.

Nach all der Mathematik geht es in Abschnitt 5.8 dann endlich wieder zum zentralen Thema dieses Kurses: der Kryptografie. Dieser Abschnitt behandelt das RSA-Kryptosystem. Dieses System wurde schon 1978 entdeckt, spielt aber immer noch eine zentrale Rolle in der Public-Key-Kryptografie. Wir werden in Abschnitt 5.8 nur sagen wie und warum es funktioniert. Warum es wirklich „gut“, das heißt „schnell“ ist, wird in Kurseinheit 4 präzisiert und erklärt.

Kapitel 5

Ringe

5.1 Notation und Beispiele

Obgleich Sie Ringe schon kennen, wiederholen wir noch einmal die Definition:

5.1.1 Definition Ein **Ring** $(R, +, \cdot)$ ist eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$, so dass folgende Bedingungen erfüllt sind:

(i) $(R, +)$ ist eine abelsche Gruppe.

(ii) $\cdot$ ist assoziativ, und es gibt ein **neutrales Element** der Multiplikation $e \in R$, so dass $a \cdot e = e \cdot a = a$ für alle $a \in R$ gilt.

(iii) Es gelten die **Distributivgesetze**, das heißt, für alle $a, b, c \in R$ gilt

(a) $a(b + c) = ab + ac$

(b) $(a + b)c = ac + bc$.

Wenn R zusätzlich noch die Bedingung

(iv) Für alle $a, b \in R$ gilt $a \cdot b = b \cdot a$

erfüllt, so wird R ein **kommutativer Ring** genannt.

Hier gleich eine **Warnung**: Es gibt konkurrierende Definitionen von Ringen. Oft wird die Bedingung (ii) dahingehend abgeschwächt, dass die Existenz eines neutralen Elementes der Multiplikation nicht gefordert wird. Wenn Sie zusätzliche Literatur lesen, müssen Sie also immer nachsehen, welche Definition für einen Ring benutzt wird.

5.1.2 Beispiele (a) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring.

(b) Für alle $n \in \mathbb{N}$, $n > 1$, ist $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ein kommutativer Ring.

(c) Sei $R = \{0\}$. Dann ist R ein Ring. Das neutrale Element der Addition und der Multiplikation ist in beiden Fällen das Element 0.

(d) Sei R ein Ring. Der Polynomring $R[T]$ ist ein Ring, und $R[T]$ ist genau dann kommutativ, wenn R kommutativ ist. Dies haben wir in der Linearen Algebra I, Kurseinheit 2, gezeigt.

(e) Sei R ein kommutativer Ring, und seien $\mathrm{M}_{nn}(R)$ die $n \times n$-Matrizen über R. Mit der Addition und der Multiplikation von Matrizen ist $\mathrm{M}_{nn}(R)$ ein Ring. Für $n > 1$ ist dieser Ring nicht kommutativ.

(f) Sei R die Menge der Funktionen von $\mathbb{R}$ nach $\mathbb{R}$. Für alle $f, g \in R$ definieren wir $f + g : \mathbb{R} \to \mathbb{R}$ durch $(f + g)(x) = f(x) + g(x)$ und $f \cdot g : \mathbb{R} \to \mathbb{R}$ durch $(f \cdot g)(x) = f(x) \cdot g(x)$ für alle $x \in \mathbb{R}$. Mit diesen Verknüpfungen ist $(R, +, \cdot)$ ein kommutativer Ring.

5.1.3 Notationen Wir behalten die Notationen bei, die wir in 4.1.4 bei den Gruppen bereits eingeführt haben. Sei $(R, +, \cdot)$ ein Ring.

(a) Das neutrale Element in $(R, +)$ wird mit 0 bezeichnet. Ist $a \in R$, so bezeichnen wir das inverse Element zu a in $(R, +)$ mit $-a$. An Stelle von $b+(-a)$ schreiben wir $b - a$. Ist $n \in \mathbb{N}$, so schreiben wir na für die Summe $a + \cdots + a$ mit n Summanden a und $(-n)a = n(-a)$. Ferner ist $0a = 0$.

(b) Das neutrale Element der Multiplikation wird mit 1 bezeichnet. An Stelle von $a \cdot b$ schreiben wir nur ab. Ist $a \in R$ bezüglich der Multiplikation invertierbar, so bezeichnen wir das inverse Element mit a^{-1}. Ist $n \in \mathbb{N}$, so schreiben wir a^n für das Produkt $a \cdot \cdots \cdot a$ von n Faktoren a. Ist a invertierbar, so wird a^0 als 1 und a^{-m} als $(a^{-1})^m$ definiert.

Analog zu Produkten von Gruppen (vergleichen Sie Abschnitt 4.9) können wir Produkte von Ringen definieren.

Dazu seien $(R_1, +_1, \cdot_1), \ldots, (R_n, +_n, \cdot_n)$ Ringe. Wir betrachten das cartesische Produkt

$$\prod_{i=1}^{n} R_i = R_1 \times \cdots \times R_n = \{(r_1, \ldots, r_n) \mid r_i \in R_i, 1 \leq i \leq n\}.$$

Auf $\prod_{i=1}^{n} R_i$ definieren wir zwei Verknüpfungen

$$\begin{array}{rccccc} + : & (R_1 \times \cdots \times R_n) & \times & (R_1 \times \cdots \times R_n) & \to & (R_1 \times \cdots \times R_n) \\ & ((r_1, \ldots, r_n), & & (r'_1, \ldots, r'_n)) & \mapsto & (r_1 +_1 r'_1, \ldots, r_n +_n r'_n) \end{array}$$

und

$$\begin{array}{rccccc} \cdot : & (R_1 \times \cdots \times R_n) & \times & (R_1 \times \cdots \times R_n) & \to & (R_1 \times \cdots \times R_n) \\ & ((r_1, \ldots, r_n), & & (r'_1, \ldots, r'_n)) & \mapsto & (r_1 \cdot_1 r'_1, \ldots, r_n \cdot_n r'_n). \end{array}$$

Mit diesen Verknüpfungen ist $\prod_{i=1}^{n} R_i$ ein Ring mit neutralem Element $(0, \ldots, 0)$ der Addition und neutralem Element $(1, \ldots, 1)$ der Multiplikation.

5.1.4 Definition Der Ring $\prod_{i=1}^{n} R_i$ wird das **direkte Produkt** der Ringe $R_1, \ldots, R_n$ genannt.

Je nachdem, welche zusätzlichen Eigenschaften Ringe besitzen, werden weitere Definitionen eingeführt.

5.1.5 Definitionen (a) Ein kommutativer Ring $(R, +, \cdot)$ mit $1 \neq 0$ heißt **Integritätsbereich**, wenn aus $ab = 0$ folgt, dass $a = 0$ oder $b = 0$ ist.

(b) Ein Ring $(R, +, \cdot)$ heißt **Schiefkörper**, wenn $(R \setminus \{0\}, \cdot)$ eine Gruppe ist.

(c) Ein kommutativer Schiefkörper wird ein **Körper** genannt.

5.1.6 Aufgabe Beweisen Sie, dass in jedem Schiefkörper aus $ab = 0$ folgt, dass $a = 0$ oder $b = 0$ gilt.

5.1.7 Beispiele (a) Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein Integritätsbereich.

(b) Jeder Körper ist ein Integritätsbereich.

(c) Sei $\mathbb{K}$ ein Körper. Dann ist der Polynomring $\mathbb{K}[T]$ ein Integritätsbereich.

(d) Sei $n \in \mathbb{N}$, und sei $n = ab$ für Elemente $a \neq 1$ und $b \neq 1$ in $\mathbb{N}$. Dann ist $\mathbb{Z}/n\mathbb{Z}$ kein Integritätsbereich, denn $ab = 0$ in $\mathbb{Z}/n\mathbb{Z}$, aber $a \neq 0$ und $b \neq 0$.

(e) Sie haben in Kurseinheit 7 der Linearen Algebra I mit den Quaternionen $\mathbb{H}$ einen Schiefkörper kennen gelernt, der kein Körper ist.

5.1.8 Aufgabe Seien $R_1, \ldots, R_n$ Ringe. Beweisen oder widerlegen Sie folgende Aussagen.

(a) $\prod_{i=1}^{n} R_i$ ist genau dann ein Integritätsbereich, wenn alle R_i, $1 \leq i \leq n$ Integritätsbereiche sind.

(b) $\prod_{i=1}^{n} R_i$ ist genau dann ein Körper, wenn alle R_i, $1 \leq i \leq n$ Körper sind.

(c) $\prod_{i=1}^{n} R_i$ ist genau dann kommutativ, wenn alle R_i, $1 \leq i \leq n$ kommutativ sind.

Jeder Körper ist ein Schiefkörper, und er ist, wie wir oben in Aufgabe 5.1.6 bereits festgestellt haben, ein Integritätsbereich. Die Umkehrung gilt nicht. Beispielsweise ist $\mathbb{Z}$ ein Integritätsbereich, der kein Körper ist. Ist R ein endlicher Integritätsbereich, so gilt die Umkehrung allerdings schon:

5.1.9 Proposition Jeder Integritätsbereich, der nur endlich viele Elemente enthält, ist ein Körper.

Beweis: Sei $R = \{a_1, \ldots, a_n\}$ ein Integritätsbereich. Sei $a \in R$, $a \neq 0$. Wir bilden $aa_1, \ldots, aa_n$. Diese Elemente sind verschieden, denn aus $aa_i = aa_j$ folgt $aa_i - aa_j = a(a_i - a_j) = 0$. Da R ein Integritätsbereich ist, folgt dann $a = 0$ oder $a_i - a_j = 0$. Die Annahme $a \neq 0$ impliziert $a_i - a_j = 0$, also $a_i = a_j$. Die n Elemente $aa_1, \ldots, aa_n$ sind damit alle Elemente aus R, das heißt, jedes Element in R ist von der Form aa_i. Dies trifft insbesondere für das Element 1 zu. Zu $a \in R$, $a \neq 0$ gibt es also ein $a_i \in R$ mit $aa_i = 1$. Da R kommutativ ist, folgt auch $a_i a = 1$. Somit hat jedes Element in $R \setminus \{0\}$ ein inverses Element, und es folgt, dass $(R \setminus \{0\}, \cdot)$ eine abelsche Gruppe, also $(R, +, \cdot)$ ein Körper ist. □

5.2 Ideale und Faktorringe

5.2.1 Definition Sei $(R, +, \cdot)$ ein Ring. Eine Teilmenge R' von R heißt **Unterring** von R, wenn R' mit den Verknüpfungen $+$ und $\cdot$ in R ein Ring ist, und wenn $1 \in R'$ ist.

Wenn R' ein Unterring von R ist, dann ist $(R', +)$ eine Untergruppe von $(R, +)$.

5.2.2 Beispiele (a) Sei $\mathbb{Q}$ der Körper der rationalen Zahlen. Dann ist $\mathbb{Z}$ ein Unterring von $\mathbb{Q}$.

(b) Sei $\mathbb{K}$ ein Körper. Dann ist $\mathbb{K}$ ein Unterring des Polynomringes $\mathbb{K}[T]$.

(c) Sei $\mathrm{M}_{nn}(\mathbb{K})$ die Menge der $n \times n$-Matrizen über einem Körper $\mathbb{K}$. Sei $\mathrm{B}_{nn}(\mathbb{K})$ die Teilmenge der oberen Dreiecksmatrizen. Da das Produkt von zwei oberen Dreiecksmatrizen eine obere Dreiecksmatrix ist, ist $\mathrm{B}_{nn}(\mathbb{K})$ ein Unterring von $\mathrm{M}_{nn}(\mathbb{K})$.

(d) Sei $n \in \mathbb{N}$, $n > 1$. Dann ist $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ **kein** Unterring von $\mathbb{Z}$. Zwar ist $(n\mathbb{Z}, +)$ eine Untergruppe von $(\mathbb{Z}, +)$, und es gilt auch $(nz)(nz') = n(nzz') \in n\mathbb{Z}$, aber $1 \notin n\mathbb{Z}$. Somit ist $n\mathbb{Z}$ kein Ring.

5.2.3 Definition Sei $(R, +, \cdot)$ ein Ring. Ein **Ideal** I in R ist eine Untergruppe von $(R, +)$, so dass für alle $a \in I$ und alle $b \in R$ die Elemente ab und ba in I liegen. Ist I ein Ideal in R, so schreiben wir $I \lhd R$.

5.2.4 Beispiele (a) Sei $n \in \mathbb{N}$, $n > 1$. Dann ist $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ ein Ideal in $\mathbb{Z}$.

(b) Sei R ein kommutativer Ring, und sei $x \in R$. Dann ist $(x) = \{xr \mid r \in R\}$ ein Ideal in R.

Beachten Sie, dass das Beispiel (a) ein Spezialfall dieses Beispiels ist. In (a) ist $R = \mathbb{Z}$ und $x = n$. Ein weiterer wichtiger Spezialfall ist der, wenn $R = \mathbb{K}[T]$, $\mathbb{K}$ ein Körper, und $f = \sum_{i=0}^{n} a_i T^i$ ein Polynom in $\mathbb{K}[T]$ ist. Dann ist $(f) = \{fg \mid g \in \mathbb{K}[T]\}$ ein Ideal in $\mathbb{K}[T]$.

(c) Sei $R = \mathbb{Q}$. Zwar ist $\mathbb{Z}$ ein Unterring von $\mathbb{Q}$, allerdings kein Ideal. Es ist beispielsweise $1 \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$, aber $1 \cdot \frac{1}{2} \notin \mathbb{Z}$.

5.2.5 Aufgaben

1. Sei $(R, +, \cdot)$ ein Ring, und sei I ein Ideal in R. Beweisen Sie, dass $I = R$ ist, falls $1 \in I$ gilt.
2. Sei R ein Ring, und seien I_1, I_2 Ideale in R. Beweisen Sie, dass $I_1 \cap I_2$ ein Ideal in R ist.
3. Sei R ein kommutativer Ring, und sei I ein Ideal in R. Sei $\mathrm{M}_{nn}(I)$ die Menge der $n \times n$-Matrizen, deren Einträge in I liegen. Beweisen Sie, dass $\mathrm{M}_{nn}(I)$ ein Ideal in $\mathrm{M}_{nn}(R)$ ist.

Mit Hilfe von Idealen in kommutativen Ringen können wir eine Charakterisierung von Körpern geben:

5.2.6 Proposition (Charakterisierung von Körpern)

Ein kommutativer Ring $R \neq \{0\}$ ist genau dann ein Körper, wenn $\{0\}$ und R die einzigen Ideale in R sind.

Beweis: Sei R ein Körper, und sei $I \neq \{0\}$ ein Ideal in R. Sei $a \in I$, $a \neq 0$. Da R ein Körper ist, ist a invertierbar. Da I ein Ideal ist, folgt $aa^{-1} = 1 \in I$. Dann gilt $r \cdot 1 = r \in I$ für alle $r \in R$, also $R \subseteq I$. Da auch $I \subseteq R$, folgt $R = I$. Dies zeigt, dass $\{0\}$ und R die einzigen Ideale in R sind.

Sei umgekehrt $R \neq \{0\}$ ein kommutativer Ring, dessen einzige Ideale $\{0\}$ und R sind. Sei $a \in R$, $a \neq 0$. Dann ist $(a) \neq \{0\}$, denn $a \in (a)$. Es folgt $(a) = R$. Somit ist jedes Element $r \in R$ von der Form $r = ax$ mit $x \in R$. Insbesondere gibt es $x \in R$ mit $ax = 1$. Es gilt auch $xa = 1$, denn R ist kommutativ. Somit ist jedes $a \neq 0$ in R invertierbar, und es folgt, dass R ein Körper ist. □

Sei $(R, +, \cdot)$ ein Ring, und sei I ein Ideal in R. Da Ideale Normalteiler (vergleichen Sie bitte mit Definition 4.6.3 und Proposition 4.6.4) von $(R, +)$ sind, erhalten wir eine Klasseneinteilung auf R mit Nebenklassen $r + I = \{r + s \mid s \in I\}$ modulo I. Wir bezeichnen eine solche Nebenklasse mit $[r]$, also

$$[r] = \{r + s \mid s \in I\}.$$

5.2.7 Definition Sei R ein Ring, und sei I ein Ideal in R. Zwei Elemente $a, b \in R$ heißen **kongruent modulo** I, wenn sie in derselben Nebenklasse modulo I liegen. Sind a und b kongruent modulo I, so schreiben wir $a \equiv b (\mathrm{mod} I)$.

5.2.8 Aufgabe Sei R ein Ring, und sei I ein Ideal in R.

1. Seien $a, b \in R$. Beweisen Sie, dass $a \equiv b (\mathrm{mod} I)$ genau dann, wenn $a - b \in I$ gilt.
2. Sei $U \subseteq R^\times$ die Menge der Einheiten $a \in R^\times$ mit $a \equiv 1 (\mathrm{mod} I)$. Beweisen Sie, dass U ein Normalteiler von $R^\times$ ist.

5.2.9 Proposition (Rechenregeln für Kongruenzen)

Sei R ein Ring, und sei I ein Ideal in R. Seien $a, b, r, s \in R$. Dann gilt:

(a) Die folgenden Aussagen sind äquivalent:

(1) $[a] = [b]$.

(2) $a \equiv b (\mathrm{mod} I)$.

(3) $a - b \in I$.

(b) Wenn $a \equiv b(\mathrm{mod} I)$, so gilt

(1) $a + r \equiv b + r(\mathrm{mod} I)$.

(2) $ar \equiv br(\mathrm{mod} I)$.

(3) $na \equiv nb(\mathrm{mod} I)$ für alle $n \in \mathbb{Z}$.

(c) Wenn $a \equiv b(\mathrm{mod} I)$ und $r \equiv s(\mathrm{mod} I)$, so gilt

(1) $a + r \equiv b + s(\mathrm{mod} I)$.

(2) $ar \equiv bs(\mathrm{mod} I)$.

Beweis:

(a) Sei $[a] = [b]$. Da $a \in [a]$ und $b \in [b]$, folgt $a, b \in [a]$. Somit liegen a und b in derselben Nebenklasse modulo I, und es folgt $a \equiv b(\mathrm{mod} I)$, also (1)⇒(2).

Es gilt

$$\begin{array}{rcl} a \equiv b(\mathrm{mod} I) & \Leftrightarrow & \text{es gibt ein } x \in R \text{ mit } a, b \in [x] \\ & \Leftrightarrow & a = x + s \text{ und } b = x + s' \text{ für } s, s' \in I \\ & \Leftrightarrow & a - b = s - s' \in I. \end{array}$$

Insbesondere gilt (2)⇒(3).

Sei $a - b \in I$. Dann gilt $a = b + s$ für ein $s \in I$. Es folgt $a \in [b]$. Es gilt auch $a \in [a]$, und da Nebenklassen gleich oder disjunkt sind, folgt $[a] = [b]$, also (3)⇒(1).

(b) Sei $a \equiv b(\mathrm{mod} I)$, also $a - b \in I$ mit (a).

(1) Es ist $(a + r) - (b + r) = a - b \in I$. Mit (a) folgt $a + r \equiv b + r(\mathrm{mod} I)$.

(2) Es ist $ar - br = (a - b)r \in I$, denn $(a - b) \in I$ und I ist ein Ideal. Mit (a) folgt die Behauptung.

(3) Es ist $na - nb = n(a - b)$ und $a - b \in I$. Da $(I, +)$ eine Gruppe ist, folgt $n(a - b) \in I$. Wieder folgt mit (a) die Behauptung.

(c) Seien $a \equiv b(\mathrm{mod} I)$ und $r \equiv s(\mathrm{mod} I)$, also $a - b, r - s \in I$.

(1) Es gilt $(a+r)-(b+s) = (a-b)+(r-s) \in I$, denn $(I, +)$ ist eine Gruppe.

(2) Es gilt

$$\begin{array}{rcl} ar - bs & = & ar - bs - as + as \\ & = & a(r - s) + (a - b)s. \end{array}$$

Da I ein Ideal ist, folgt $a(r-s) \in I$ und $(a-b)s \in I$. Da $(I,+)$ eine Gruppe ist, gilt $a(r-s)+(a-b)s \in I$. Mit (a) folgt die Behauptung.

□

Sei R ein Ring, und sei $I \lhd R$. Sei R/I die Menge der Nebenklassen modulo I, also

$$R/I = \{[r] \mid r \in R\}.$$

Für zwei Nebenklassen $[a], [b] \in R/I$ definieren wir

$$[a]+[b] = [a+b] \text{ und } [a] \cdot [b] = [ab].$$

Wir zeigen, dass $+$ und $\cdot$ wohldefiniert sind. Dazu seien $[a] = [a']$ und $[b] = [b']$. Mit Proposition 5.2.9 (a) folgt $a \equiv a' (\mathrm{mod} I)$ und $b \equiv b' (\mathrm{mod} I)$. Mit Proposition 5.2.9 (c) gilt $a+b \equiv a'+b' (\mathrm{mod} I)$ und $ab \equiv a'b' (\mathrm{mod} I)$, also $[a+b] = [a'+b']$ und $[ab] = [a'b']$. Somit sind $+$ und $\cdot$ Verknüpfungen auf R/I. Ein Standardbeweis zeigt, dass R/I mit diesen Verknüpfungen ein Ring ist.

5.2.10 Definition Sei R ein Ring, und sei $I \lhd R$. Der Ring R/I wird **Faktorring von R modulo I** oder **Restklassenring von R modulo I** genannt.

In dem folgenden Beispiel werden wir den Ring $\mathbb{Z}/n\mathbb{Z}$ neu entdecken.

5.2.11 Beispiel Sei $R = \mathbb{Z}$, und sei $I = n\mathbb{Z}$ für ein $n \in \mathbb{N}$, $n > 1$. Wir haben in 5.2.4 gesehen, dass I ein Ideal in $\mathbb{Z}$ ist. Somit ist $\mathbb{Z}/n\mathbb{Z} = \{[a] \mid a \in \mathbb{Z}\}$. Weiter gilt $[a] = [a']$ genau dann, wenn $a - a' \in n\mathbb{Z}$, wenn also n ein Teiler von $a - a'$ ist.

Sei $[a] \in \mathbb{Z}/n\mathbb{Z}$. Wir dividieren a durch n mit Rest und erhalten

$$a = xn + a \,\mathrm{mod} n \text{ für ein } x \in \mathbb{Z},$$

also $a - a \,\mathrm{mod} n = xn \in n\mathbb{Z}$, und damit $[a] = [a \,\mathrm{mod} n]$. Es folgt

$$\mathbb{Z}/n\mathbb{Z} = \{[0], \ldots, [n-1]\}.$$

Seien $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$. Mit der Definition der Verknüpfungen in $\mathbb{Z}/n\mathbb{Z}$ folgt

$$[a]+[b] = [a+b] = [(a+b)\mathrm{mod} n] \text{ und } [a] \cdot [b] = [ab] = [(ab)\mathrm{mod} n].$$

Bis auf die Klammerschreibweise der Elemente in $\mathbb{Z}/n\mathbb{Z}$, die wir in den bisherigen Kapiteln nicht benutzt haben, liefert die Konstruktion der Bildung des Restklassenringes modulo einem Ideal also gerade den Ring $\mathbb{Z}/n\mathbb{Z}$, mit dem wir in den vorigen Kapiteln und in der Linearen Algebra I bereits gearbeitet haben.

5.3 Ringhomomorphismen

Wie bei Vektorräumen und Gruppen interessieren wir uns bei Ringen für strukturerhaltende Abbildungen zwischen Ringen.

5.3.1 Definition Seien R und R' Ringe. Eine Abbildung $\phi : R \to R'$ heißt ein **Ringhomomorphismus** oder kurz ein **Homomorphismus**, wenn für alle $r_1, r_2 \in R$ gilt:

(i) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$, und

(ii) $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$, und

(iii) $\phi(1) = 1$.

Injektive Ringhomomorphismen werden **Monomorphismen** und surjektive **Epimorphismen** genannt. Ist $\phi : R \to R'$ ein bijektiver Ringhomomorphismus, so wird ϕ ein **Isomorphismus** genannt, und wir sagen, dass R und R' **isomorph** sind. Sind R und R' isomorph, so schreiben wir $R \simeq R'$. Ist ϕ ein Isomorphismus, und ist $R = R'$, so wird ϕ ein **Automorphismus** genannt.

5.3.2 Aufgabe Sei $\phi : R \to R'$ ein Ringhomomorphismus. Sei $\phi|_{R^\times} : R^\times \to R'$ definiert durch $\phi|_{R^\times}(r) = \phi(r)$ für alle $r \in R^\times$.

(a) Beweisen Sie, dass $\phi|_{R^\times}(r) \in R'^\times$ für alle $r \in R^\times$ ist.

(b) Beweisen Sie, dass $\phi|_{R^\times} : R^\times \to R'^\times$ ein Gruppenhomomorphismus ist.

Wenn $\phi : R \to R'$ ein Ringhomomorphismus ist, dann ist ϕ ein Gruppenhomomorphismus von $(R, +)$ nach $(R', +)$. Analog zu Kern und Bild von Gruppenhomomorphismen definieren wir Kern und Bild von Ringhomomorphismen:

5.3.3 Definition Sei $\phi : R \to R'$ ein Ringhomomorphismus. Das **Bild** und der **Kern** von ϕ sind folgende Teilmengen von R beziehungsweise R':

$$\text{Bild}(\phi) = \{r' \in R' \mid \text{ es gibt ein } r \in R \text{ mit } \phi(r) = r'\} \subseteq R'$$

$$\text{Kern}(\phi) = \{r \in R \mid \phi(r) = 0\} \subseteq R.$$

Völlig analog zu 4.5.7 gilt:

5.3.4 Proposition Sei $\phi : R \to R'$ ein Ringhomomorphismus. Dann gilt:

(a) Bild(ϕ) ist ein Unterring von R'.

(b) Kern(ϕ) ist ein Ideal in R.

(c) Der Homomorphismus ϕ ist genau dann injektiv, wenn Kern(ϕ) = $\{0\}$ ist.

Beweis:

(a) Da ϕ ein Gruppenhomomorphismus ist, ist (Bild(ϕ), +) mit 4.5.7 eine Untergruppe von $(R', +)$. Diese Gruppe ist auch abelsch, denn $(R', +)$ ist abelsch.

Seien $a', b' \in$ Bild(ϕ). Dann gibt es $a, b \in R$ mit $a' = \phi(a)$ und $b' = \phi(b)$. Es folgt

$$a'b' = \phi(a)\phi(b) = \phi(ab) \in \text{Bild}(\phi),$$

und dies zeigt, dass die Multiplikation eine Verknüpfung in Bild(ϕ) ist. Das Assoziativgesetz der Multiplikation gilt für alle Elemente in R', also gilt es insbesondere in Bild(ϕ). Da $\phi(1) = 1$, liegt das neutrale Element der Multiplikation in Bild(ϕ).

Die Distributivgesetze gelten in R', also insbesondere in Bild(ϕ).

Es folgt, dass Bild(ϕ) ein Unterring von R' ist.

(b) Mit Proposition 4.5.7 ist (Kern(ϕ), +) eine Untergruppe von $(R, +)$. Sei $a \in$ Kern(ϕ), und sei $r \in R$. Dann gilt $\phi(ar) = \phi(a)\phi(r) = 0 \cdot \phi(r) = 0$, also $ar \in$ Kern(ϕ). Analog folgt $ra \in$ Kern(ϕ). Somit ist Kern(ϕ) ein Ideal in R.

(c) Diese Behauptung ist gerade Proposition 4.5.7 (c).

□

Sei $\phi : R \to R'$ ein Ringhomomorphismus. Da Kern(ϕ) ein Ideal in R ist, können wir den Restklassenring $R/$Kern(ϕ) bilden.

Völlig analog zum Homomorphiesatz von Gruppen 4.6.7 gilt:

5.3.5 Satz (Homomorphiesatz für Ringe)

Sei $\phi : R \to R'$ ein Ringhomomorphismus. Dann ist $R/$Kern(ϕ) isomorph zu Bild(ϕ). Genauer, es ist

$$\begin{array}{rccc} \Phi: & R/\text{Kern}(\phi) & \to & \text{Bild}(\phi) \\ & [r] & \mapsto & \phi(r) \end{array}$$

ein Isomorphismus von Ringen.

Beweis:

1. Wir zeigen zunächst, dass Φ wohldefiniert ist. Dazu sei $[r] = [s]$. Mit den Rechenregeln für Kongruenzen, 5.2.9 (a), gilt $r - s \in \text{Kern}(\phi)$. Es folgt $\phi(r) - \phi(s) = \phi(r - s) = 0$, also $\phi(r) = \phi(s)$. Dies zeigt $\Phi(r) = \Phi(s)$.

2. Wir zeigen nun, dass Φ ein Ringhomomorphismus ist. Dazu seien $[r], [s] \in R/\text{Kern}(\phi)$. Dann gilt

$$\Phi([r] + [s]) = \Phi([r + s]) = \phi(r + s) = \phi(r) + \phi(s) = \Phi([r]) + \Phi([s])$$

und

$$\Phi([r][s]) = \Phi([rs]) = \phi(rs) = \phi(r)\phi(s) = \Phi([r])\Phi([s])$$

und

$$\Phi([1]) = \phi(1) = 1.$$

Es folgt, dass Φ ein Homomorphismus ist.

3. Nun zeigen wir, dass Φ injektiv ist. Sei $[r] \in \text{Kern}(\Phi)$. Dann gilt $\phi(r) = 0$, also $r \in \text{Kern}(\phi)$. Somit gilt $r - 0 \in \text{Kern}(\phi)$, also $[r] = [0]$ mit den Rechenregeln für Kongruenzen 5.2.9 (a). Mit Proposition 5.3.4 folgt, dass Φ injektiv ist.

4. Sei $\phi(r) \in \text{Bild}(\phi)$. Dann ist $[r]$ ein Urbild von $\phi(r)$ unter Φ. Dies zeigt, dass Φ surjektiv ist.

□

Jedes Ideal ist der Kern eines Ringhomomorphismus, wie das folgende Ergebnis zeigt.

5.3.6 Proposition Sei R ein Ring und sei I ein Ideal in R. Sei

$$\pi : R \to R/I \text{ definiert durch } \pi(r) = [r] \text{ für alle } r \in R.$$

Dann ist π ein Epimorphismus, und $\text{Kern}(\pi) = I$.

Beweis: Dass π ein Homomorphismus ist, folgt unmittelbar aus der Definition der Addition und der Multiplikation von Elementen in R/I. Ebenfalls ist klar, dass π surjektiv, also ein Epimorphismus ist.

Sei $s \in I$. Dann gilt $\pi(s) = [s]$, und mit den Rechenregeln für Kongruenzen 5.2.9 (a) folgt $[s] = [0]$, denn $s - 0 \in I$. Es folgt $I \subseteq \text{Kern}(\pi)$. Sei umgekehrt $r \in \text{Kern}(\pi)$. Dann gilt $[r] = [0]$, also $r - 0 = r \in I$ mit den Rechenregeln für Kongruenzen 5.2.9 (a). Es folgt $\text{Kern}(\pi) \subseteq I$, und damit $\text{Kern}(\pi) = I$. □

5.3.7 Definition Sei R ein Ring und sei I ein Ideal in R. Sei

$$\pi : R \to R/I \text{ definiert durch } \pi(r) = [r] \text{ für alle } r \in R.$$

Dann wird π der **kanonische Epimorphismus** von R nach R/I genannt.

Wir werden in Proposition 5.3.9 das Ergebnis folgender Aufgabe benötigen:

5.3.8 Aufgabe Sei $\phi : R \to R'$ ein Epimorphismus, und sei $I \lhd R$ ein Ideal in R. Sei

$$\phi(I) = \{s' \in R' \mid \text{ es gibt ein } s \in I \text{ mit } \phi(s) = s'\}.$$

Beweisen Sie, dass $\phi(I)$ ein Ideal in R' ist.

5.3.9 Proposition Sei $\phi : R \to R'$ ein Epimorphismus, und sei $I \lhd R$ ein Ideal in R, das Kern(ϕ) enthält. Sei $I' = \phi(I)$. Dann ist

$$f : R/I \to R'/I', \text{ definiert durch } f([r]) = [\phi(r)] \text{ für alle } [r] \in R/I,$$

ein Isomorphismus von Ringen.

Beweis: Mit Aufgabe 5.3.8 ist I' ein Ideal in R', und wir können R'/I' bilden.

1. Wir zeigen, dass f wohldefiniert ist.

   Sei $[r] = [s]$, also $r - s \in I$. Es folgt $\phi(r - s) = \phi(r) - \phi(s) \in I'$, also $[\phi(r)] = [\phi(s)]$ mit den Rechenregeln für Kongruenzen 5.2.9 (a).

2. Wir zeigen nun, dass f ein Homomorphismus ist.

   Seien $r, s \in R$. Dann gilt

   $$\begin{aligned} f([r] + [s]) &= f([r + s]) \\ &= [\phi(r + s)] \\ &= [\phi(r) + \phi(s)] \\ &= [\phi(r)] + [\phi(s)] \\ &= f([r]) + f([s]). \end{aligned}$$

   Analog folgt $f([r][s]) = f([r])f([s])$. Es gilt $f([1]) = [\phi(1)] = [1]$, und dies zeigt, dass f ein Homomorphismus ist.

3. In diesem Schritt zeigen wir, dass f injektiv ist.

   Sei $[r] \in$ Kern(f), also $[\phi(r)] = [0]$. Dann gilt $\phi(r) = 0 + \phi(s)$ für ein $s \in I$. Es folgt

   $$\phi(r) - \phi(s) = \phi(r - s) = 0,$$

also $r - s \in \text{Kern}(\phi)$. Da $\text{Kern}(\phi) \subseteq I$, gilt damit $r - s \in I$. Mit den Rechenregeln für Kongruenzen 5.2.9 (a) folgt $[r] = [s] = [0]$, also $\text{Kern}(f) = \{[0]\}$. Proposition 5.3.4 impliziert, dass f injektiv ist.

4. Sei $[r'] \in R'/I'$. Da ϕ surjektiv ist, gibt es ein $r \in R$ mit $\phi(r) = r'$. Es folgt $[r'] = [\phi(r)]$, und $[r]$ ist ein Urbild von $[r']$ unter f.

□

Diese Proposition wird manchmal der „Erste Isomorphiesatz für Ringe“ genannt.

5.3.10 Aufgabe Sei R ein kommutativer Ring, und sei I ein Ideal in R. Sei $\mathrm{M}_{nn}(I)$ die Menge der $n \times n$-Matrizen, deren Einträge in I liegen. Sie haben in Aufgabe 5.2.5 gezeigt, dass $\mathrm{M}_{nn}(I)$ ein Ideal in $\mathrm{M}_{nn}(R)$ ist. Verwenden Sie den Homomorphiesatz für Ringe um zu zeigen, dass $\mathrm{M}_{nn}(R)/\mathrm{M}_{nn}(I)$ isomorph zu $\mathrm{M}_{nn}(R/I)$ ist.

5.4 Der Chinesische Restsatz

In diesem Abschnitt werden wir einen speziellen Isomorphismus für ganz spezielle Ringe konstruieren. Die Konstruktion ist etwa 2000 Jahre alt (bevor bekannt war, was ein Ring ist) und hat wichtige Anwendungen in der Computer Algebra. Wir werden am Ende des Abschnitts näher auf diesen Sachverhalt eingehen.

Wir haben im Abschnitt 4.9 in Satz 4.9.7 beziehungsweise in Korollar 4.9.8 gesehen, dass die Gruppe $\mathbb{Z}/n\mathbb{Z}$ isomorph zu $\prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ ist, sofern $n = \prod_{i=1}^{r} p_i^{s_i}$, $p_i \neq p_j$ für $i \neq j$, die Primfaktorzerlegung von n ist. Allerdings war der Beweis des Satzes nicht konstruktiv, das heißt, wir haben keinen expliziten Isomorphismus von $\mathbb{Z}/n\mathbb{Z}$ nach $\prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ angegeben. Wir werden das in diesem Kapitel nachholen, und darüberhinaus zeigen, dass $\mathbb{Z}/n\mathbb{Z}$ und $\prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ als Ringe isomorph sind.

Dieses Ergebnis ist unter dem Namen „Chinesischer Restsatz“ bekannt.

Wenn Sie es vielleicht selbst einmal probieren wollen? Unser Ziel ist es, eine bijektive, strukturverträgliche Abbildung

$$\phi : \mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/p_1^{s_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{s_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_{r-1}^{s_{r-1}}\mathbb{Z}) \times (\mathbb{Z}/p_r^{s_r}\mathbb{Z})$$

zu definieren. Dazu müssen wir also jedem $x \in \{0, \ldots, n-1\}$ ein r-Tupel von Elementen in $\mathbb{Z}/p_1^{s_1}\mathbb{Z}, \ldots, \mathbb{Z}/p_r^{s_r}\mathbb{Z}$ zuordnen. Mit der Einstellung „Das Bild muss was mit x und den individuellen $\mathbb{Z}/p_i^{s_i}\mathbb{Z}$ zu tun haben“, werden Sie vermutlich

$$\phi(x) = (x \bmod p_1^{s_1}, x \bmod p_2^{s_2}, \ldots, x \bmod p_{r-1}^{s_{r-1}}, x \bmod p_r^{s_r})$$

vorschlagen. Und das ist auch richtig. Wir werden zunächst nur zeigen, dass ϕ surjektiv ist. Da $\mathbb{Z}/n\mathbb{Z}$ und $\prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ gleich viele Elemente enthalten, folgt aus der Surjektivität schon die Bijektivität.

Wir beginnen mit einigen Vorbemerkungen. Stehende Annahme in diesem Abschnitt ist, dass $n = \prod_{i=1}^{r} p_i^{s_i}$, $p_i \neq p_j$ für $i \neq j$, die Primfaktorzerlegung von n ist. Für alle $1 \leq i \leq r$ sei $q_i = \prod_{\substack{j=1 \\ j \neq i}}^{r} p_j^{s_j}$.

5.4.1 Bemerkung Für alle $1 \leq i \leq r$ gilt $\mathrm{ggT}(q_i \bmod p_i^{s_i}, p_i^{s_i}) = 1$, insbesondere ist $q_i \bmod p_i^{s_i}$ in $\mathbb{Z}/p_i^{s_i}\mathbb{Z}$ invertierbar.

Beweis: Angenommen, $\mathrm{ggT}(q_i \bmod p_i^{s_i}, p_i^{s_i}) = d > 1$. Da $d | p_i^{s_i}$, folgt $p_i | d$. Sei

$$q_i = \prod_{\substack{j=1 \\ j \neq i}}^{r} p_j^{s_j} = x p_i^{s_i} + q_i \bmod p_i^{s_i}$$

mit $x \in \mathbb{Z}$. Da $p_i | q_i \bmod p_i^{s_i}$ und $p_i | p_i^{s_i}$, folgt $p_i | \prod_{\substack{j=1 \\ j \neq i}}^{r} p_j^{s_j}$, ein Widerspruch. Es folgt $d = 1$. Mit Korollar 2.4.12 folgt, dass $q_i \bmod p_i^{s_i}$ in $\mathbb{Z}/p_i^{s_i}\mathbb{Z}$ invertierbar ist. □

5.4.2 Notation Für alle $1 \leq i \leq r$ bezeichnen wir das zu $q_i \bmod p_i^{s_i}$ in $\mathbb{Z}/p_i^{s_i}\mathbb{Z}$ inverse Element mit r_i.

5.4.3 Bemerkung Für alle $i \neq j$ gilt $q_i \bmod p_j^{s_j} = 0$.

Beweis: Offenbar, denn q_i ist für alle $i \neq j$ ein Vielfaches von $p_j^{s_j}$. □

5.4.4 Satz (Chinesischer Restsatz)

Die Abbildung

$$\begin{array}{rccccccc} \phi: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/p_1^{s_1} & \times & \ldots & \times & \mathbb{Z}/p_r^{s_r} \\ & x & \mapsto & (x \bmod p_1^{s_1} & , & \ldots & , & x \bmod p_r^{s_r}) \end{array}$$

ist bijektiv. Das Urbild eines Elementes $(x_1, \ldots, x_r) \in \prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ unter ϕ ist $\left(\sum_{i=1}^{r} x_i q_i r_i\right) \bmod n$.

Beweis: Sei $(x_1, \ldots, x_r) \in \prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$, und sei $x = \left(\sum_{i=1}^{r} x_i r_i q_i\right) \bmod n$.

Wir untersuchen den k-ten Eintrag $x \bmod p_k^{s_k}$ von $\phi(x)$.

$$\begin{aligned} x \bmod p_k^{s_k} &= \left(\left(\sum_{i=1}^{r} x_i q_i r_i\right) \bmod n\right) \bmod p_k^{s_k} \\ &= \left(\left(\sum_{i=1}^{r} x_i q_i r_i\right) - tn\right) \bmod p_k^{s_k} \text{ für ein } t \in \mathbb{Z} \\ &= \left(\sum_{i=1}^{r} x_i q_i r_i\right) \bmod p_k^{s_k}, \text{ denn } p_k^{s_k} | n \\ &= \sum_{i=1}^{r} (x_i q_i r_i) \bmod p_k^{s_k} \\ &= x_k q_k r_k \bmod p_k^{s_k}, \text{ denn } q_i \bmod p_k^{s_k} = 0 \text{ für } i \neq k \\ &= x_k, \text{ denn } q_k r_k \bmod p_k^{s_k} = 1. \end{aligned}$$

Es folgt $\phi(x) = (x_1, \ldots, x_r)$, das heißt, ϕ ist surjektiv. Wie wir oben bereits überlegt haben, folgt, dass ϕ bijektiv ist. □

Wieso heißt der Chinesische Restsatz Chinesischer Restsatz? Erklären wir zunächst einmal den Begriff „Restsatz“. Nehmen wir an, wir hätten r verschiedene Primzahlen $p_1, \ldots p_r$ und r Reste $x_1 \bmod p_1^{s_1}, \ldots, x_r \bmod p_r^{s_r}$ gegeben. Wir können uns die

Frage stellen, ob es eine ganze Zahl x gibt, die beim Teilen durch $p_1^{s_1}, \ldots, p_r^{s_r}$ mit Rest die vorgegebenen Reste

$$x \mathrm{mod} p_1^{s_1} = x_1 \mathrm{mod} p_1^{s_1}, \ldots, x \mathrm{mod} p_r^{s_r} = x_r \mathrm{mod} p_r^{s_r}$$

besitzt. Der Chinesische Restsatz gibt eine Antwort auf diese Frage. Ja, genauer, es gibt genau ein $x \in \{0, \ldots, \prod_{i=1}^{r} p_i^{s_i} - 1\}$ mit dieser Eigenschaft. Und mit der in der Formulierung des Satzes genannten Formel für das Urbild von $(x_1, \ldots, x_r)$ unter ϕ können wir das x berechnen. Da das Verfahren, wie man ein solches x finden kann, bereits im ersten Jahrhundert unserer Zeitrechnung dem chinesischen Mathematiker Sun-Tsu bekannt war, wurde der Satz eben Chinesischer Restsatz genannt.

5.4.5 Aufgabe Bestimmen Sie die kleinste ganze Zahl x für die gilt:

$$\begin{aligned} x &\equiv 2 (\bmod 3) \\ x &\equiv 1 (\bmod 5) \\ x &\equiv 6 (\bmod 7). \end{aligned}$$

Woran Sun-Tsu sicher nicht im Traum gedacht hat, ist, dass der Chinesische Restsatz etwa 2000 Jahre später hoch aktuell in der Computeralgebra und Kryptografie werden würde. Und das liegt an Folgendem: Die im Chinesischen Restsatz angegebene Abbildung ist weit mehr als irgendeine Bijektion. Es gilt nämlich:

5.4.6 Proposition Sei $\phi : \mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ die Abbildung wie im Chinesischen Restsatz. Dann gilt für alle $x, y \in \mathbb{Z}/n\mathbb{Z}$

$$\begin{aligned} \phi(x+y) &= \phi(x) + \phi(y) \text{ und} \\ \phi(xy) &= \phi(x)\phi(y) \text{ und} \\ \phi(1) &= 1, \end{aligned}$$

das heißt, ϕ ist ein Isomorphismus von Ringen.

Bevor wir dieses Ergebnis beweisen, wollen wir zunächst einmal klären, wieso dies so wichtige Folgerungen in der Computeralgebra hat.

Wenn wir mit dem Rechner $x + y$ oder xy mit $x, y \in \mathbb{Z}$ berechnen wollen, dann ist es völlig egal, ob wir diese Rechnung in $\mathbb{Z}$ durchführen oder in $\mathbb{Z}/n\mathbb{Z}$, so lange das Ergebnis kleiner als n ist. Wenn x und y, und damit n nun riesig groß sind, so kann es Zeit und Speicher sparender sein, die Rechnung auszulagern und viele kleinere

Rechnungen zu machen. Mit anderen Worten, wir können ein großes n, dessen Primfaktorzerlegung $n = \prod_{i=1}^{r} p_i^{s_i}$ wir kennen, wählen, und an Stelle von $x+y$ oder xy berechnen wir einfach $((x+y) \bmod p_1^{s_1}, \ldots, (x+y) \bmod p_r^{s_r})$ beziehungsweise $(xy \bmod p_1^{s_1}, \ldots, xy \bmod p_r^{s_r})$. Die einzelnen Einträge können sogar parallel berechnet werden. Der Chinesische Restsatz garantiert, dass wir das Ergebnis mit der im Satz angegebenen Formel wieder zusammensetzen können und das Ergebnis in $\mathbb{Z}/n\mathbb{Z}$ erhalten.

Beweis: (**Proposition 5.4.6)** Seien $x, y \in \mathbb{Z}/n\mathbb{Z}$. Dann gilt

$$\begin{aligned} \phi(x+y) &= ((x+y) \bmod p_1^{s_1}, \ldots, (x+y) \bmod p_r^{s_r}) \\ &= ((x \bmod p_1^{s_1} + y \bmod p_1^{s_1}) \bmod p_1^{s_1}, \ldots, (x \bmod p_r^{s_r} + y \bmod p_r^{s_r}) \bmod p_r^{s_r}) \end{aligned}$$

und

$$\begin{aligned} \phi(x) + \phi(y) &= (x \bmod p_1^{s_1}, \ldots, x \bmod p_r^{s_r}) + (y \bmod p_1^{s_1}, \ldots, y \bmod p_r^{s_r}) \\ &= ((x \bmod p_1^{s_1} + y \bmod p_1^{s_1}) \bmod p_1^{s_1}, \ldots, (x \bmod p_r^{s_r} + y \bmod p_r^{s_r}) \bmod p_r^{s_r}), \end{aligned}$$

also $\phi(x+y) = \phi(x) + \phi(y)$.

Analog wird gezeigt, dass auch $\phi(xy) = \phi(x)\phi(y)$ gilt.

Da $1 \bmod p_i^{s_i} = 1 \in \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ für alle $1 \leq i \leq r$, folgt $\phi(1) = (1, \cdots, 1) = 1 \in \prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$. □

5.5 Der Primring eines Ringes

Wir werden den Homomorphiesatz für Ringe, Satz 5.3.5, dazu benutzen, den „kleinsten“ Unterring $P(R)$ eines Ringes R zu bestimmen. Dabei soll der kleinste Unterring bedeuten, dass $P(R)$ ein Ring ist, der in allen Unterringen von R enthalten ist. Zunächst einmal ist gar nicht klar, dass es immer einen Unterring von R gibt, der in allen Unterringen von R enthalten ist. Klar ist hingegen, dass ein Unterring mit dieser Eigenschaft eindeutig ist, falls er denn existiert. Denn seien S und S' Unterringe von R, die in allen Unterringen von R enthalten sind. Dann gilt $S \subseteq S'$ und $S' \subseteq S$, also $S = S'$.

Sei nun also $(R, +, \cdot)$ ein Ring. Um Verwirrungen zu vermeiden, bezeichnen wir das neutrale Element der Multiplikation in R mit e.

Wir definieren eine Abbildung $\phi : \mathbb{Z} \to R$ durch $\phi(n) = ne$ für alle $n \in \mathbb{Z}$. Hierbei benutzen wir die in 5.1.3 festgelegte Notation. Für alle $m, n \in \mathbb{Z}$ gilt dann

$$\phi(m+n) = (m+n)e = me + ne = \phi(m) + \phi(n)$$

und

$$\phi(mn) = (mn)e = (mn)e^2 = (me)(ne) = \phi(m)\phi(n).$$

Weiter gilt $\phi(1) = 1e = e$, und es folgt

5.5.1 Bemerkung Die Abbildung $\phi : \mathbb{Z} \to R$, definiert durch $\phi(n) = ne$ für alle $n \in \mathbb{Z}$, ist ein Homomorphismus von Ringen mit $\text{Bild}(\phi) = \mathbb{Z}e = \{ne \mid n \in \mathbb{Z}\}$. □

Mit Proposition 5.3.4 ist $\text{Bild}(\phi)$ ein Unterring von R. Sei S ein weiterer Unterring von R. Dann gilt $e \in S$, denn S enthält das neutrale Element der Multiplikation. Da $+$ eine Verknüpfung auf S ist, gilt $ne \in S$ für alle $n \in \mathbb{Z}$. Es folgt $\text{Bild}(\phi) = \mathbb{Z}e \subseteq S$. Wir haben also gezeigt:

5.5.2 Bemerkung Es ist $\mathbb{Z}e$ ein Unterring von R, und für alle Unterringe S von R gilt $\mathbb{Z}e \subseteq S$. □

Damit haben wir den kleinsten Unterring von R gefunden, und wir definieren:

5.5.3 Definition Sei R ein Ring, und sei e das neutrale Element der Multiplikation in R. Der Unterring $\mathbb{Z}e$ von R wird der **Primring** von R genannt und mit $P(R)$ bezeichnet.

Mit dem Homomorphiesatz für Ringe, Satz 5.3.5, gilt $\text{Bild}(\phi) = \mathbb{Z}e \simeq \mathbb{Z}/\text{Kern}(\phi)$. Weiter wissen wir mit Proposition 5.3.4, dass $\text{Kern}(\phi)$ ein Ideal in $\mathbb{Z}$ ist. Dies zeigt

5.5.4 Bemerkung Sei R ein Ring, und sei $P(R)$ der Primring von R. Dann gilt $P(R) \simeq \mathbb{Z}/I$, und I ist ein Ideal in $\mathbb{Z}$. □

Wie sehen nun die Ideale I in $\mathbb{Z}$ aus? Zunächst einmal haben wir die Ideale $\{0\}$ und $\mathbb{Z}$ in $\mathbb{Z}$. Weiter wissen wir, dass $(I, +)$ eine Untergruppe von $(\mathbb{Z}, +)$ ist. Da $\mathbb{Z}$ zyklisch ist, folgt mit Proposition 4.8.5, dass $(I, +)$ zyklisch ist. Sei I ein Ideal in $\mathbb{Z}$ mit $I \neq \{0\}$. Sei $k \in I$, $k \neq 0$. Mit k liegt auch $-k$ in I, und es folgt, dass I eine positive Zahl enthält. Sei m die kleinste positive Zahl in I. Dann gilt

$$(m) = \{mn \mid n \in \mathbb{Z}\} = m\mathbb{Z} \subseteq I.$$

Sei umgekehrt $z \in I$. Wir teilen z durch m mit Rest und erhalten $z = xm + r$ mit $x, r \in \mathbb{Z}$ und $0 \leq r < m$. Ist $r \neq 0$, so gilt $z - xm = r \in I$, ein Widerspruch, denn m war die kleinste positive Zahl in I. Somit gilt $z \in m\mathbb{Z}$, also $I = m\mathbb{Z}$. Ist $m = 1$, so ist $m\mathbb{Z} = \mathbb{Z}$. Wir haben hiermit gezeigt:

5.5.5 Bemerkung Die Ideale in $\mathbb{Z}$ sind $m\mathbb{Z}$ mit $m \geq 0$. □

Ist $I = \{0\}$, so ist $\mathbb{Z}/I$ isomorph zu $\mathbb{Z}$. Kombinieren wir nun die Bemerkungen 5.5.4 und 5.5.5, so erhalten wir:

5.5.6 Bemerkung Sei R ein Ring, und sei $P(R)$ der Primring von R. Dann gilt $P(R) \simeq \mathbb{Z}$ oder $P(R) \simeq \mathbb{Z}/m\mathbb{Z}$ für ein $m > 0$. □

Wie können wir entscheiden, welcher der beiden Fälle vorliegt? Hierzu betrachten wir den Isomorphismus

$$\begin{array}{rccc} \Phi: & \mathbb{Z}/\mathrm{Kern}(\phi) & \to & \mathrm{Bild}(\phi) = P(R) \\ & [n] & \mapsto & \phi(n) = ne \end{array}$$

aus dem Homomorphiesatz 5.3.5 für Ringe.

Ist $\mathrm{Kern}(\phi) = \{0\}$, also $\mathbb{Z}/\mathrm{Kern}(\phi) \simeq \mathbb{Z}$, so ist $\Phi([n]) = ne \neq 0$ für alle $n \in \mathbb{Z}$, $n \neq 0$, denn Φ ist injektiv.

Ist $\mathrm{Kern}(\phi) = m\mathbb{Z}$ für ein $m > 0$, so sind

$$\Phi([1]) = e \neq 0, \ldots, \Phi([m-1]) = (m-1)e \neq 0,$$

und es ist $\Phi([m]) = \Phi([0]) = 0$. Somit ist m die kleinste positive Zahl mit $me = 0$.

Fassen wir unsere Überlegungen zusammen, so erhalten wir:

5.5.7 Proposition (Klassifikation der Primringe)

Sei R ein Ring mit Primring $P(R)$, und sei e das neutrale Element der Multiplikation in R. Dann gilt $P(R) \simeq \mathbb{Z}$ oder $P(R) \simeq \mathbb{Z}/m\mathbb{Z}$ für ein $m > 0$.

(a) Ist $P(R) \simeq \mathbb{Z}$, so gilt $ne \neq 0$ für alle $n \neq 0$.

(b) Ist $P(R) \simeq \mathbb{Z}/m\mathbb{Z}$ für ein $m > 0$, so ist m die kleinste positive Zahl mit $me = 0$. □

5.5.8 Aufgabe Geben Sie ein Beispiel für einen Ring R, der unendlich viele Elemente enthält und dessen Primring endlich ist.

5.5.9 Korollar Sei R ein Ring mit Primring $P(R) \simeq \mathbb{Z}/m\mathbb{Z}$ für ein $m > 0$. Dann gilt $na = 0$ für alle $a \in R$ und alle Vielfachen n von m.

Beweis: Sei $n = xm$ für ein $x \in \mathbb{Z}$. Es ist $na = xma = x(me)a = x(0a) = x0 = 0$ für alle $a \in R$. □

5.5.10 Definition Sei R ein Ring mit Primring $P(R)$.

(i) Wenn $P(R) \simeq \mathbb{Z}$ ist, dann sagen wir, dass R die **Charakteristik** 0 hat und schreiben $\text{char}(R) = 0$.

(ii) Wenn $P(R) \simeq \mathbb{Z}/m\mathbb{Z}$ für ein $m > 1$ ist, dann sagen wir, dass R die **Charakteristik** m hat, beziehungsweise, dass R **positive Charakteristik** hat, und schreiben $\text{char}(R) = m$.

Für den Ring $R = \{0\}$ ist keine Charakteristik definiert.

5.5.11 Proposition Sei R ein Integritätsbereich mit $\text{char}(R) = m > 0$. Dann ist m eine Primzahl.

Beweis: Da Integritätsbereiche Elemente $\neq 0$ enthalten (vergleichen Sie mit Definition 5.1.5), ist $m \geq 2$. Angenommen, m ist keine Primzahl. Dann gibt es $s > 1$ und $t > 1$ in $\mathbb{N}$ mit $m = st$, und es sind $s < m$ und $t < m$. Sei e das neutrale Element der Multiplikation in R. Dann gilt

$$0 = me = (st)e = (se)(te).$$

Da R ein Integritätsbereich ist, folgt $se = 0$ oder $te = 0$. Dies ist ein Widerspruch, denn m ist die kleinste positive Zahl mit $me = 0$. □

Da Körper Integritätsbereiche sind, folgt

5.5.12 Korollar Sei $\mathbb{K}$ ein Körper mit $\text{char}(\mathbb{K}) = m > 0$. Dann ist m eine Primzahl. □

5.5.13 Korollar Die Charakteristik eines endlichen Körpers $\mathbb{K}$ ist eine Primzahl.

Beweis: Mit Korollar 5.5.12 reicht es zu zeigen, dass endliche Körper eine positive Charakteristik haben. Wir betrachten die Elemente $e, 2e, \ldots$. Da $\mathbb{K}$ nur endlich viele Elemente enthält, gibt es positive Zahlen k und m mit $k < m$ und $ke = me$. Es folgt $me - ke = (m - k)e = 0$ und $m - k \neq 0$. Mit Proposition 5.5.7 folgt $\text{char}(\mathbb{K}) \neq 0$. □

Nicht jeder Ring hat Primzahl-Charakteristik. Beispielsweise ist 6 die Charakteristik von $\mathbb{Z}/6\mathbb{Z}$.

5.5.14 Aufgabe Ein Ring R heißt **einfach**, falls $R \neq \{0\}$, und falls $\{0\}$ und R die einzigen Ideale in R sind. Beweisen Sie, dass einfache kommutative Ringe die Charakteristik 0 oder p haben, wobei p eine Primzahl ist.

Sei $\mathbb{K}$ ein endlicher Körper. Der Primring $P(\mathbb{K})$ ist mit Korollar 5.5.13 ein Körper mit p Elementen, p eine Primzahl. Damit ist $\mathbb{K}$ ein Vektorraum über $P(\mathbb{K})$. Da $\mathbb{K}$ nur endlich viele Elemente enthält, ist die Dimension von $\mathbb{K}$ über $P(\mathbb{K})$ endlich, etwa $\dim_{P(\mathbb{K})}(\mathbb{K}) = n$. Es gibt also $b_1, \ldots, b_n \in \mathbb{K}$, so dass jedes Element $b \in \mathbb{K}$ eindeutig in der Form $b = a_1 b_1 + \cdots + a_n b_n$ mit $a_1, \ldots, a_n \in P(\mathbb{K})$ geschrieben werden kann. Für jedes a_i haben wir p Möglichkeiten, und es folgt

5.5.15 Satz (Ordnung endlicher Körper)

Ein endlicher Körper hat p^n Elemente, wobei p eine Primzahl und $n \in \mathbb{N}$ ist. □

Insbesondere gibt es keine Körper mit 15 Elementen, denn 15 ist keine Primzahlpotenz. Bisher kennen Sie nur endliche Körper mit p Elementen, nämlich die Körper $\mathbb{Z}/p\mathbb{Z}$, p eine Primzahl. Wir werden in Kurseinheit 5 zeigen, dass es zu jeder Primzahl p und jeder natürlichen Zahl n einen Körper mit p^n Elementen gibt.

In kommutativen Ringen R mit $\mathrm{char}(R) = p$, p eine Primzahl, kann man die binomische Formel so einfach ausrechnen – jedenfalls für p-Potenzen – wie man es sich immer wünscht. Zunächst aber eine Erinnerung an die Lineare Algebra. Sie haben in der Linearen Algebra II, Kurseinheit 3, folgendes Ergebnis kennengelernt:

5.5.16 Satz (Binomische Formel)

Sei R ein Ring, und seien $a, b \in R$ zwei Ringelemente, für die $ab = ba$ gilt. Sei $n \in \mathbb{N}_0$. Dann gilt

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

□

Dabei bezeichnet $\binom{n}{k}$ den so genannten Binomialkoeffizienten, also $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ für alle $0 \leq k \leq n$ und $\binom{n}{k} = 0$ für alle $k > n$. Es sind $0! = 1$ und $n! = n(n-1)\cdots 2 \cdot 1$ für alle $n \in \mathbb{N}$. Mit der binomischen Formel, Satz 5.5.16, folgt

5.5.17 Proposition Sei R ein kommutativer Ring der Charakteristik $p > 0$, und sei p eine Primzahl. Dann gilt

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

für alle $a, b \in R$ und alle $n \in \mathbb{N}$.

Beweis: Wir beweisen die Behauptung mit Induktion nach n. Sei $n = 1$. Da $ab = ba$ für alle $a, b \in R$, können wir die binomische Formel anwenden, und es gilt

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} + b^p.$$

Es ist $\binom{p}{k} k!(p-k)! = p!$, und für $1 \leq k \leq p-1$ sind weder $k!$ noch $(p-k)!$ durch p teilbar. Da $p!$ durch p teilbar ist, folgt, dass $\binom{p}{k}$ durch p teilbar ist. Mit Korollar 5.5.9 gilt $\binom{p}{k} a^k b^{p-k} = 0$ für alle $1 \leq k \leq p-1$, und es folgt die Behauptung. Sei nun $n \geq 1$. Dann gilt

$$(a+b)^{p^{n+1}} = \left((a+b)^{p^n}\right)^p = (a^{p^n} + b^{p^n})^p = a^{p^{n+1}} + b^{p^{n+1}}.$$

□

5.5.18 Aufgabe Sei R ein kommutativer Ring der Charakteristik $p > 0$. Seien $a_1, \ldots, a_m \in R$. Beweisen Sie, dass

$$(a_1 + \cdots + a_m)^{p^n} = a_1^{p^n} + \cdots + a_m^{p^n}$$

für alle $m, n \in \mathbb{N}$ gilt.

5.5.19 Korollar Wenn $\mathbb{K}$ ein endlicher Körper der Charakteristik $p > 0$ ist, dann ist die Abbildung $\sigma : \mathbb{K} \to \mathbb{K}$, definiert durch $\sigma(a) = a^p$ für alle $a \in \mathbb{K}$, ein Automorphismus.

Beweis: Mit Proposition 5.5.17 gilt $\sigma(a+b) = (a+b)^p = a^p + b^p = \sigma(a) + \sigma(b)$ für alle $a, b \in \mathbb{K}$. Es gilt auch $\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\sigma(b)$ und $\sigma(1) = 1^p = 1$. Somit ist σ ein Homomorphismus. Es ist $\text{Kern}(\sigma) = \{0\}$, und es folgt, dass σ injektiv ist. Da $\mathbb{K}$ endlich ist, folgt, dass σ auch surjektiv, also ein Automorphismus ist. □

Der Automorphismus σ aus Korollar 5.5.19 wird zu Ehren des Mathematikers Ferdinand Georg Frobenius (1849 - 1917) auch **Frobenius Automorphismus** genannt.

5.6 Ideale in kommutativen Ringen

In diesem Abschnitt sei R ein kommutativer Ring. Wir werden spezielle Ideale in R betrachten, die wir in Kurseinheit 5 für die Konstruktion der endlichen Körper benötigen werden.

5.6.1 Definition Sei R ein kommutativer Ring. Ein Element $a \in R$ heißt **Teiler** eines Elementes $b \in R$, wenn es ein $c \in R$ gibt, so dass $ac = b$ ist. Zwei Elemente $a, b \in R$ heißen **assoziiert**, wenn es eine Einheit $\epsilon \in R^\times$ gibt, so dass $a = b\epsilon$ ist. Ein Element $c \in R$ heißt **Primelement**, wenn c keine Einheit ist, und wenn c nur die Einheiten und die zu c assoziierten Elemente als Teiler besitzt.

5.6.2 Beispiel Sei $R = \mathbb{Z}$. Die Einheiten in $\mathbb{Z}$ sind 1 und -1. Somit sind a und b in $\mathbb{Z}$ genau dann assoziiert, wenn sie gleich sind oder sich nur durch das Vorzeichen unterscheiden. Die Primelemente in $\mathbb{Z}$ sind die Primzahlen und die Negativen der Primzahlen.

5.6.3 Definition Ein Ideal $P \neq R$ in R heißt **Primideal**, wenn für alle $a, b \in R$ mit $ab \in P$ folgt, dass a oder b in P liegen.

5.6.4 Beispiele (a) Sei $R = \mathbb{Z}$. Dann ist $\{0\}$ ein Primideal in $\mathbb{Z}$, denn $\mathbb{Z}$ ist ein Integritätsbereich.

(b) Sei $R = \mathbb{Z}$, und sei $p \in \mathbb{Z}$ eine Primzahl. Sei $P = p\mathbb{Z} = \{pz \mid z \in \mathbb{Z}\}$. Dann ist P ein Primideal, denn wenn $a, b \in \mathbb{Z}$ und $ab \in P$, so gilt $p|ab$, und es folgt $p|a$ oder $p|b$. Im ersten Fall liegt a in P, im zweiten Fall gilt $b \in P$.

(c) Sei $R = \mathbb{Z}$, und seien $a \neq 0$ und $b \neq 0$ Elemente in $\mathbb{Z}$, die beide keine Einheiten sind. Sei $n = ab$. Dann ist $I = n\mathbb{Z}$ kein Primideal, denn $ab \in I$, aber $a \notin I$ und $b \notin I$.

5.6.5 Definition Ein Ideal $M \neq R$ in R heißt, **maximales** Ideal, wenn für jedes Ideal I in R mit $M \subseteq I$ folgt, dass $M = I$ oder $I = R$ ist.

5.6.6 Aufgabe Sei $R = \mathbb{Z}$, und seien $m\mathbb{Z}$ und $n\mathbb{Z}$ Ideale in $\mathbb{Z}$. Beweisen Sie:

1. Genau dann gilt $m\mathbb{Z} \subseteq n\mathbb{Z}$, wenn n ein Teiler von m ist.
2. Genau dann gilt $m\mathbb{Z} = n\mathbb{Z}$, wenn m und n assoziiert sind.
3. Genau dann ist $n\mathbb{Z}$ ein maximales Ideal, wenn n ein Primelement in $\mathbb{Z}$ ist.

5.6.7 Aufgabe Geben Sie ein Beispiel für ein Primideal, das nicht maximal ist.

5.6.8 Definition Ein Ideal I in R heißt **Hauptideal**, wenn es ein $a \in I$ gibt, so dass $I = (a) = \{ar \mid r \in R\}$ ist. Ein Ring R heißt **Hauptidealring**, wenn R ein Integritätsbereich ist, und wenn alle Ideale in R Hauptideale sind.

5.6.9 Beispiel Mit Bemerkung 5.5.5 sind die Ideale in $\mathbb{Z}$ von der Form $n\mathbb{Z}$, $n > 0$ und $\{0\} = 0\mathbb{Z}$. Somit ist $\mathbb{Z}$ ein Hauptidealring.

5.6.10 Satz (Faktorringe von kommutativen Ringen)

Sei R ein kommutativer Ring. Dann gilt:

(a) Ein Ideal M in R ist genau dann maximal, wenn R/M ein Körper ist.

(b) Ein Ideal P in R ist genau dann ein Primideal, wenn R/P ein Integritätsbereich ist.

(c) Jedes maximale Ideal in R ist ein Primideal.

(d) Wenn R ein Hauptidealring ist, so ist $R/(c)$ genau dann ein Körper, wenn c ein Primelement in R ist.

Beweis:

(a) Sei M ein maximales Ideal in R. Wir müssen zeigen, dass jedes Element $[a] \neq [0]$ in R/M invertierbar ist. Mit den Rechenregeln für Kongruenzen, 5.2.9 (a), ist $[a] \neq [0]$ genau dann, wenn $a \notin M$. Da $M \neq R$ gibt es Elemente $a \notin M$. Sei also $a \notin M$. Sei

$$I = \{ar + m \mid r \in R \text{ und } m \in M\}.$$

Das Ideal M ist in I enthalten. Wir zeigen, dass I ein Ideal in R ist. Mit dem Untergruppenkriterium, 4.2.4, ist $(I, +)$ eine Untergruppe von $(R, +)$. Seien $ar + m \in I$ und $b \in R$. Dann gilt $(ar + m)b = a(br) + mb$, denn R ist kommutativ. Da M ein Ideal ist, gilt $mb \in M$. Es folgt, dass $(ar + m)b \in I$, und analog $b(ar + m) \in I$. Somit ist I ein Ideal. Das Ideal I enthält a. Da $a \notin M$, ist M in I echt enthalten. Da M maximal ist, folgt $I = R$. Jedes Element in R, also auch das Element 1, hat damit eine Darstellung der Form $ar + m$ mit $r \in R$ und $m \in M$. Sei also $ar + m = 1$ für gewisse $r \in R$ und $m \in M$. Dann gilt

$$[a][r] = (a+M)(r+M) = ar+M = (1-m)+M = (1+M)-(m+M) = 1+M = [1],$$

und es folgt, dass $[a]$ invertierbar ist. Somit ist R/M ein Körper.

Sei umgekehrt R/M ein Körper. Sei I ein Ideal in R, welches M echt enthält. Sei $a \in I$, $a \notin M$. Dann ist $[a] \neq [0]$, und es folgt, dass es ein $r \in R$ mit

$[a][r] = ar + M = 1 + M$ gibt. Es folgt $ar + m = 1$ für ein $m \in M$. Da $a \in I$ und $m \in I$, gilt $ar + m \in I$, also $1 \in I$. Es folgt $(1) = R \subseteq I$, also $I = R$. Somit ist M ein maximales Ideal in R.

(b) Sei P ein Primideal in R. Da $P \neq R$, gilt $1 \notin P$, also mit den Rechenregeln für Kongruenzen, 5.2.9 (a), $[1] \neq [0] \in R/P$. Seien $[a][b] = [0]$ in R/P, also $ab \in P$. Dann gilt $a \in P$ oder $b \in P$, und damit $[a] = [0]$ oder $[b] = [0]$ in R/P. Somit ist R/P ein Integritätsbereich.

Sei umgekehrt R/P ein Integritätsbereich. Sei $ab \in P$. Dann gilt $[0] = [ab] = [a][b]$, und es folgt $a \in P$ oder $b \in P$. Somit ist P ein Primideal.

(c) Diese Behauptung folgt aus (a) und (b), denn jeder Körper ist ein Integritätsbereich.

(d) Sei R ein Hauptidealring, sei (c) ein Ideal in R, und sei $R/(c)$ ein Körper.

Wenn c eine Einheit in R ist, so gilt $1 \in (c)$, also $(c) = R$, ein Widerspruch. Somit ist c keine Einheit in R.

Wenn c weder eine Einheit noch ein Primelement in R ist, so gibt es einen Teiler a von c, der weder eine Einheit noch assoziiert zu c ist. Es ist $a \neq 0$, denn anderenfalls wäre $c = 0$, und a und c wären assoziiert. Wir schreiben $c = ab$ mit $b \in R$. Angenommen, $a \in (c)$. Dann gibt es ein $d \in R$ mit $a = cd = abd$, also $a(1 - bd) = 0$. Da Hauptidealringe Integritätsbereiche sind, folgt $1 - bd = 0$, also $bd = 1$. Es folgt, dass d eine Einheit ist, ein Widerspruch, denn dann sind $a = cd$ und c assoziiert. Dieser Widerspruch zeigt $a \notin (c)$. Es folgt $(c) \subsetneq (a)$. Da a keine Einheit in R ist, gilt auch $(a) \subsetneq R$. Somit ist (c) nicht maximal. Dies ist ein Widerspruch, denn mit (a) ist $R/(c)$ kein Körper. Der Widerspruch zeigt, dass c ein Primelement ist.

Sei umgekehrt c ein Primelement in R. Da c keine Einheit ist, gilt $(c) \neq R$. Sei I ein Ideal, das (c) enthält. Da R ein Hauptidealring ist, folgt $I = (a)$ für ein $a \in R$. Es folgt $c \in (a)$, das heißt, a ist ein Teiler von c. Somit ist a eine Einheit, und damit $(a) = R$, oder a ist assoziiert zu c, also $I = (c)$. Dies zeigt, dass (c) ein maximales Ideal ist, und mit (a) folgt die Behauptung.

□

Als Folgerung etwas, das wir seit grauer Vorzeit schon wissen:

5.6.11 Korollar Sei $n \in \mathbb{Z}$. Genau dann ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper, wenn n assoziiert zu einer Primzahl ist.

Beweis: Die Primelemente in $\mathbb{Z}$ sind die Assoziierten der Primzahlen. Die Behauptung folgt nun mit 5.6.10 (d). □

5.7 Der Ring $\mathbb{K}[T]$

In Kurseinheit 2 der Linearen Algebra II haben Sie bereits Polynomringe über Ringen kennen gelernt. Wir werden in der Kryptologie vornehmlich an Polynomringen über Körpern interessiert sein. Faktorringe von Polynomringen über endlichen Körpern $\mathbb{Z}/p\mathbb{Z}$, p eine Primzahl, spielen eine zentrale Rolle bei der Konstruktion der endlichen Körper, die nicht von der Form $\mathbb{Z}/p\mathbb{Z}$ sind. In Kurseinheit 1 der Linearen Algebra II haben wir Polynomringe über Körpern im Zusammenhang mit dem charakteristischen Polynom studiert. Viele der dort hergeleiteten Ergebnisse werden wir auch hier benötigen, und wir werden, ohne Beweis, einige der Resultate wiederholen.

Zunächst erinnern wir an einige Begriffe.

5.7.1 Definition Sei R ein Ring, und sei $f = \sum_{i=0}^{n} a_i T^i \in R[T]$ ein Polynom, das nicht das Nullpolynom ist. Wir können annehmen, dass $a_n \neq 0$ ist. Dann wird a_n der **Leitkoeffizient** von f und a_0 der **konstante Term** von f genannt. Die Zahl n heißt der **Grad** von f, abgekürzt $\mathrm{Grad}(f) = n$. Den Grad des Nullpolynoms definieren wir als $-\infty$. Polynome vom Grad ≤ 0 werden **konstante** Polynome genannt. Ist $a_n = 1$, so sagen wir, dass das Polynom f **normiert** ist.

Sei $\mathbb{K}$ ein Körper. Dann ist $\mathbb{K}[T]$ ein Integritätsbereich, und $\mathbb{K}[T]^\times = \mathbb{K}^\times$. Die invertierbaren Elemente in $\mathbb{K}[T]$ sind also die Polynome vom Grad 0.

Wir erinnern an die Division mit Rest in $\mathbb{K}[T]$:

5.7.2 Proposition (Division mit Rest in $\mathbb{K}[T]$)

Zu Polynomen $f, g \in \mathbb{K}[T]$ mit $f \neq 0$ gibt es eindeutig bestimmte Polynome $q, r \in \mathbb{K}[T]$ mit

$$g = qf + r \quad \text{und} \quad \mathrm{Grad}(r) < \mathrm{Grad}(f).$$

Beweis: Lineare Algebra II, Kurseinheit 1. □

Diese Proposition impliziert, dass jedes Ideal in $\mathbb{K}[T]$ ein Hauptideal ist:

5.7.3 Proposition Der Ring $\mathbb{K}[T]$ ist ein Hauptidealring. Genauer, ist $I \neq (0)$ ein Ideal in $\mathbb{K}[T]$, so gibt es ein eindeutig bestimmtes, normiertes Polynom $g \in \mathbb{K}[T]$ mit $I = (g)$.

Beweis: Wir wissen bereits, dass $\mathbb{K}[T]$ ein Integritätsbereich ist. Sei $I \neq (0)$ ein Ideal in $\mathbb{K}[T]$. Sei $h \neq 0$ ein Polynom vom kleinsten Grad in I, und sei b der Leitkoeffizient von h. Dann ist $b^{-1}h = g$ ein normiertes Polynom in I und $\mathrm{Grad}(h) = \mathrm{Grad}(g)$. Sei f ein beliebiges Polynom in I. Wir teilen f durch g mit Rest und erhalten $f = qg + r$ mit $\mathrm{Grad}(r) < \mathrm{Grad}(g)$. Da I ein Ideal ist, gilt $f - qg = r \in I$. Da $h \neq 0$ ein Polynom vom kleinsten Grad in I ist, folgt $r = 0$, also $I = (g)$. Sei $g' \in I$ ein weiteres normiertes Polynom mit $I = (g')$. Dann gilt $g' = c_1 g$ und $g = c_2 g'$. Es folgt $g' = c_1 c_2 g'$, also $c_1 c_2 = 1$, und c_1, c_2 sind konstant. Da g' und g normiert sind, folgt $g = g'$. □

5.7.4 Satz Seien $f_1, \ldots, f_n$ Polynome in $\mathbb{K}[T]$, die nicht alle 0 sind. Dann gibt es ein eindeutig bestimmtes, normiertes Polynom $d \in \mathbb{K}[T]$ mit folgenden Eigenschaften:

(i) d teilt f_i für alle $1 \leq i \leq n$, und

(ii) jedes Polynom $c \in \mathbb{K}[T]$, das alle f_i, $1 \leq i \leq n$, teilt, ist auch ein Teiler von d.

Das Polynom d kann in der Form

$$d = b_1 f_1 + \cdots + b_n f_n \text{ mit } b_1, \ldots, b_n \in \mathbb{K}[T]$$

geschrieben werden.

Beweis: Sei $I = \{c_1 f_1 + \cdots + c_n f_n \mid c_1, \ldots, c_n \in \mathbb{K}[T]\}$. Dann ist I ein Ideal in $\mathbb{K}[T]$. Da nicht alle f_i das Nullpolynom sind, ist $I \neq (0)$. Mit Proposition 5.7.3 folgt, dass es ein eindeutig bestimmtes normiertes Polynom $d \in \mathbb{K}[T]$ gibt, so dass $I = (d)$ ist. Dieses Polynom d hat die Eigenschaft (i) der Behauptung, und es gilt $d = b_1 f_1 + \cdots + b_n f_n$ für gewisse $b_1, \ldots, b_n \in \mathbb{K}[T]$. Wenn c jedes Polynom f_i, $1 \leq i \leq n$ teilt, so teilt c auch $d = b_1 f_1 + \cdots + b_n f_n$. Es bleibt zu zeigen, dass d eindeutig ist. Sei d_1 ein weiteres normiertes Polynom mit den Eigenschaften (i) und (ii). Es folgt $d | d_1$ und $d_1 | d$, also $(d) = (d_1) = I$. Mit Proposition 5.7.3 folgt $d = d_1$. □

5.7.5 Definition Seien $f_1, \ldots, f_n$ und d in $\mathbb{K}[T]$ wie in Satz 5.7.4. Dann wird d **größter gemeinsamer Teiler** von $f_1, \ldots, f_n$ genannt und mit $\mathrm{ggT}(f_1, \ldots, f_n)$ bezeichnet. Ist $\mathrm{ggT}(f_1, \ldots, f_n) = 1$, so sagt man, dass $f_1, \ldots, f_n$ **teilerfremd** sind. Sie werden **paarweise teilerfremd** genannt, wenn $\mathrm{ggT}(f_i, f_j) = 1$ ist für alle $1 \leq i, j \leq n$ und $i \neq j$.

Sie haben in der Linearen Algebra II, Kurseinheit 1, gesehen, dass der größte gemeinsame Teiler von zwei Polynomen $f, g \in \mathbb{K}[T]$ mit Hilfe des Euklidischen Algorithmus berechnet werden kann.

Dazu seien $f, g \in \mathbb{K}[T]$. Wir können voraussetzen, dass $g \neq 0$, und dass g kein Teiler von f ist. Wir benutzen wiederholte Division mit Rest und erhalten

$$\begin{array}{lcll} f & = & q_1 g + r_1 & 0 \leq \mathrm{Grad}(r_1) < \mathrm{Grad}(g) \\ g & = & q_2 r_1 + r_2 & 0 \leq \mathrm{Grad}(r_2) < \mathrm{Grad}(r_1) \\ r_1 & = & q_3 r_2 + r_3 & 0 \leq \mathrm{Grad}(r_3) < \mathrm{Grad}(r_2) \\ & \vdots & & \\ r_{s-2} & = & q_s r_{s-1} + r_s & 0 \leq \mathrm{Grad}(r_s) < \mathrm{Grad}(r_{s-1}) \\ r_{s-1} & = & q_{s+1} r_s. & \end{array}$$

Dabei sind $q_1, \ldots, q_{s+1}$ und $r_1, \ldots, r_s$ Polynome in $\mathbb{K}[T]$. Da der Grad von g endlich ist, muss der Prozess des wiederholten Teilens mit Rest abbrechen. Wenn r_s, der kleinste Rest $\neq 0$, den Leitkoeffizienten b hat, so ist $\mathrm{ggT}(f, g) = b^{-1} r_s$. Um den größten gemeinsamen Teiler von $f_1, \ldots, f_n$ mit $n > 2$ zu bestimmen, berechnet man zunächst $\mathrm{ggT}(f_1, f_2)$, dann $\mathrm{ggT}(\mathrm{ggT}(f_1, f_2), f_3)$, und so weiter.

5.7.6 Aufgabe Berechnen Sie den größten gemeinsamen Teiler von $f = 2T^6 + T^3 + T^2 + 2 \in \mathbb{F}_3[T]$ und $g = T^4 + T^2 + 2T \in \mathbb{F}_3[T]$.

Den Gegenpart zum größten gemeinsamen Teiler von Polynomen $f_1, \ldots, f_n$ in $\mathbb{K}[T]$ spielt das kleinste gemeinsame Vielfache von $f_1, \ldots, f_n$.

5.7.7 Proposition Seien $f_1, \ldots, f_n$ Polynome $\neq 0$ in $\mathbb{K}[T]$. Dann gibt es ein eindeutig bestimmtes normiertes Polynom $h \in \mathbb{K}[T]$, so dass gilt:

(i) h ist Vielfaches von jedem f_i, $1 \leq$i$\leq n$, und

(ii) wenn $b \in \mathbb{K}[T]$ ein Vielfaches von allen f_i, $1 \leq i \leq n$, ist, dann ist b Vielfaches von h.

Beweis: Sei $I = (f_1) \cap \cdots \cap (f_n)$. Mit Aufgabe 5.2.5 ist der Durchschnitt von Idealen ein Ideal, und es folgt, dass I ein Ideal in $\mathbb{K}[T]$ ist. Es gibt also ein eindeutig

bestimmtes normiertes Polynom h mit $(f_1) \cap \cdots \cap (f_n) = (h)$. Da $h \in (f_i)$ für alle $1 \leq i \leq n$, ist h ein Vielfaches aller f_i. Jedes weitere gemeinsame Vielfache h' aller f_i liegt in $I = (h)$, ist also ein Vielfaches von h. □

5.7.8 Definition Seien $f_1, \ldots, f_n$ und h wie in Proposition 5.7.7. Dann wird h das **kleinste gemeinsame Vielfache** von $f_1, \ldots, f_n$ genannt und mit $\mathrm{kgV}(f_1 \ldots, f_n)$ bezeichnet.

Die Primelemente in $\mathbb{K}[T]$ werden irreduzible Elemente genannt. Weil dieser Begriff so wichtig ist, wiederholen wir die Definition.

5.7.9 Definition Ein Polynom $p \in \mathbb{K}[T]$ heißt **irreduzibel über** $\mathbb{K}$ oder **irreduzibel in** $\mathbb{K}[T]$ oder **Primelement in** $\mathbb{K}[T]$, wenn $\mathrm{Grad}(p) > 0$, und wenn $p = ab$ mit $a, b \in \mathbb{K}[T]$ impliziert, dass a oder b konstant sind. Ein Polynom von positivem Grad, das nicht irreduzibel ist, wird reduzibel genannt.

Ob ein Polynom irreduzibel ist oder nicht hängt ganz entscheidend von dem Körper $\mathbb{K}$ ab. Beispielsweise ist T^2-2 irreduzibel in $\mathbb{Q}[T]$, aber $T^2-2 = (T+\sqrt{2})(T-\sqrt{2})$ ist reduzibel in $\mathbb{R}[T]$.

Normierte irreduzible Polynome spielen in $\mathbb{K}[T]$ in etwa die Rolle, die Primzahlen in $\mathbb{Z}$ spielen. In Analogie zu 4.4.6 gilt etwa

5.7.10 Lemma Sei $p \in \mathbb{K}[T]$ irreduzibel und seien $f_1, \ldots, f_n \in \mathbb{K}[T]$. Wenn p das Produkt $\prod_{i=1}^{n} f_i$ teilt, dann teilt p einen der Faktoren f_i.

Beweis: Sei p ein Teiler von $\prod_{i=1}^{n} f_i$. Dann gilt

$$(f_1 + (p)) \cdots (f_n + (p)) = \prod_{i=1}^{n} f_i + (p) = 0 + (p)$$

im Faktorring $\mathbb{K}[T]/(p)$. Da $\mathbb{K}[T]/(p)$ mit Satz 5.6.10 ein Körper ist, folgt $f_i + (p) = 0 + (p)$ für ein $1 \leq i \leq n$. Dies bedeutet $f_i \in (p)$, und somit ist p ein Teiler von f_i. □

Weiter gilt in $\mathbb{K}[T]$ ein Analogon zur eindeutigen Primfaktorzerlegung in $\mathbb{Z}$:

5.7.11 Satz (Eindeutige Zerlegung von Polynomen in irreduzible Faktoren)

Jedes Polynom $f \in \mathbb{K}[T]$ mit $\mathrm{Grad}(f) \geq 1$ lässt sich als Produkt $f = ep_1^{s_1} \cdots p_n^{s_n}$ schreiben, wobei $e \in \mathbb{K}^\times$, $s_1, \ldots, s_n \in \mathbb{N}$ und $p_1, \ldots, p_n$ verschiedene normierte und irreduzible Polynome sind. Die Einheit e, die Zahlen $s_1, \ldots, s_n$ und die Polynome $p_1, \ldots, p_n$ sind (bis auf die Reihenfolge) eindeutig bestimmt. □

Eine Beweis dieses Satzes wurde in der Linearen Algebra II, Kurseinheit 1, erbracht.

5.7.12 Notation Wir nennen eine Zerlegung von f wie in 5.7.11 eine **kanonische Zerlegung von** f.

Es ist eine wichtige Frage über Polynome in $\mathbb{K}[T]$, zu entscheiden, ob sie irreduzibel sind oder nicht. In der Kryptografie ist insbesondere der Fall interessant, in dem der Körper $\mathbb{K}$ ein endlicher Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ist, wobei p eine Primzahl ist. In einer solchen Situation können wir im Prinzip alle irreduziblen Polynome von einem vorgegebenen Grad n bestimmen. Man macht eine Liste aller Polynome vom Grad n (es gibt nur endlich viele), dann berechnet man alle Produkte von Polynomen kleineren Grades und erstellt auf diese Weise eine Liste der reduziblen Polynome vom Grad n. Nun eliminiert man die reduziblen Polynome vom Grad n von der Liste aller Polynome vom Grad n. Übrig bleiben die irreduziblen vom Grad n. Wenn n oder p groß sind, eine zugegebenermaßen mühsame Arbeit.

5.7.13 Aufgabe Bestimmen Sie alle irreduziblen Polynome vom Grad 4 in $\mathbb{F}_2[T]$.

Wir haben in der Linearen Algebra II bereits Körperelemente in Polynome eingesetzt, indem wir die Unbestimmte T durch ein Körperelement x ersetzt haben. Genauer, wenn $f = \sum_{i=0}^{n} a_i T^i$ ein Polynom in $\mathbb{K}[T]$ und $x \in \mathbb{K}$ ist, so bezeichnen wir mit $f(x)$ das Element $\sum_{i=0}^{n} a_i x^i$ in $\mathbb{K}$.

Eine wichtige Rolle spielen die so genannten Nullstellen eines Polynoms $f \in \mathbb{K}[T]$.

5.7.14 Definition Ein Element $\lambda \in \mathbb{K}$ heißt **Nullstelle** oder **Wurzel** eines Polynoms $f \in \mathbb{K}[T]$, wenn $f(\lambda) = 0$ ist.

Wir hatten in der Linearen Algebra II gesehen:

5.7.15 Proposition (Nullstellen und irreduzible Faktoren)

Ein Element $\lambda \in \mathbb{K}$ ist genau dann Nullstelle von $f \in \mathbb{K}[T]$, wenn $f = (T - \lambda)q$ für ein Polynom $q \in \mathbb{K}[T]$ ist. □

5.7.16 Definition Sei λ eine Nullstelle von $f \in \mathbb{K}[T]$. Die größte natürliche Zahl v, so dass $(T - \lambda)^v$ ein Teiler von f ist, wird die **Vielfachheit** von λ genannt und mit $\alpha(\lambda)$ bezeichnet. Wenn $\alpha(\lambda) > 1$ ist, dann sagen wir, dass λ eine **mehrfache Nullstelle** von f ist.

Die folgenden Korollare aus Proposition 5.7.15 wurden in der Linearen Algebra II, Kurseinheit 1, bewiesen:

5.7.17 Korollar Seien $\lambda_1, \ldots, \lambda_s$ verschiedene Nullstellen von $f \in K[T]$ mit Vielfachheiten $\alpha(\lambda_1), \ldots, \alpha(\lambda_s)$. Dann gibt es ein Polynom $q \in K[T]$, so dass

$$f = (T - \lambda_1)^{\alpha(\lambda_1)} \cdots (T - \lambda_s)^{\alpha(\lambda_s)} q$$

ist. □

5.7.18 Korollar (Anzahl der Nullstellen von Polynomen)

Ein Polynom $f \in \mathbb{K}[T]$, $f \neq 0$, vom Grad n hat höchstens n verschiedene Nullstellen. □

Unmittelbar aus Korollar 5.7.17 folgt

5.7.19 Korollar Sei f ein Polynom in $\mathbb{K}[T]$ vom Grad n. Seien $\lambda_1, \ldots, \lambda_s$ verschiedene Nullstellen von $f \in \mathbb{K}[T]$ mit Vielfachheiten $\alpha(\lambda_1), \ldots, \alpha(\lambda_s)$. Dann gilt $\sum_{i=1}^{s} \alpha(\lambda_i) \leq n$. □

Ob ein Polynom $f \in \mathbb{K}[T]$ mehrfache Nullstellen hat, können wir an der Ableitung von f ablesen.

5.7.20 Definition Sei $f = \sum_{i=0}^{n} a_i T^i$ ein Polynom in $\mathbb{K}[T]$. Die **Ableitung** f' von f ist das Polynom $f' = \sum_{i=1}^{n} i a_i T^{i-1}$.

Es gelten die üblichen Rechenregeln

$$\begin{aligned} (af + bg)' &= af' + bg' \\ (fg)' &= f'g + fg' \end{aligned}$$

für alle $a, b \in \mathbb{K}$ und alle $f, g \in \mathbb{K}[T]$.

5.7.21 Proposition Genau dann ist $\lambda \in \mathbb{K}$ eine mehrfache Nullstelle eines Polynoms $f \in \mathbb{K}[T]$, wenn λ eine Nullstelle von f und von f' ist.

Beweis: Sei λ eine Nullstelle von f mit $\alpha(\lambda) \geq 2$. Mit Korollar 5.7.17 ist f von der Form

$$f = (T - \lambda)^{\alpha(\lambda)} q,$$

wobei q ein Polynom in $\mathbb{K}[T]$ ist. Es folgt

$$f' = \alpha(\lambda)(T - \lambda)^{\alpha(\lambda)-1} q + (T - \lambda)^{\alpha(\lambda)} q'.$$

Somit ist λ auch eine Nullstelle von f'.

Sei umgekehrt λ eine Nullstelle von f und von f'. Mit Proposition 5.7.15 folgt $f = (T-\lambda)g$ für ein $g \in \mathbb{K}[T]$. Somit gilt $f' = g+(T-\lambda)g'$, also $g = f'-(T-\lambda)g'$. Da λ eine Nullstelle von f' ist, teilt $T - \lambda$ die rechte Seite dieser Gleichung, also auch die linke. Es folgt $g = (T - \lambda)h$ für ein $h \in \mathbb{K}[T]$. Somit gilt

$$f = (T - \lambda)g = (T - \lambda)^2 h,$$

und es folgt, dass λ eine mehrfache Nullstelle von f ist. □

Es gibt einen Zusammenhang zwischen der Nicht-Existenz von Nullstellen und Irreduzibilität. Wenn f ein irreduzibles Polynom vom Grad ≥ 2 ist, dann besagt 5.7.15, dass f keine Wurzel in $\mathbb{K}$ besitzt. Die Umkehrung gilt für Polynome vom Grad 2 oder 3, aber nicht notwendigerweise für Polynome höheren Grades.

5.7.22 Proposition Ein Polynom f in $\mathbb{K}[T]$ vom Grad 2 oder 3 ist genau dann irreduzibel, wenn es keine Nullstelle in $\mathbb{K}$ hat.

Beweis: Sei $f \in \mathbb{K}[T]$ ein Polynom vom Grad 2 oder 3. Wenn f reduzibel ist, so hat f einen Teiler g vom Grad 1. Dieser hat die Form $aT - b = a(T - \frac{b}{a})$ für $a, b \in \mathbb{K}$, $a \neq 0$. Es folgt, dass $\frac{b}{a}$ eine Nullstelle von f ist. Umgekehrt, wenn f eine Nullstelle besitzt, so besagt 5.7.15 gerade, dass f reduzibel ist. □

Diese Beobachtung ermöglicht uns, irreduzible Polynome vom Grad ≤ 3 über Körpern $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, p eine Primzahl, zu bestimmen. Wir setzen die endlich vielen Elemente ein; bekommen wir 0 raus, so ist das Polynom reduzibel, ist das Ergebnis immer $\neq 0$, so ist das Polynom irreduzibel. Folgendes Beispiel mag das veranschaulichen.

5.7.23 Beispiel Wir bestimmen alle irreduziblen Polynome vom Grad ≤ 3 in $\mathbb{F}_2[T]$.

Zunächst einmal sind alle Polynome vom Grad 1 irreduzibel. Diese sind $f_1 = T$ und $f_2 = T + 1$.

Es gibt folgende Polynome vom Grad 2: $g_1 = T^2$, $g_2 = T^2 + 1$, $g_3 = T^2 + T$, und $g_4 = T^2 + T + 1$. Es ist $g_1(0) = 0$, also ist g_1 reduzibel (wofür wir natürlich keine Theorie brauchen, um das zu sehen). Es ist $g_2(1) = 1 + 1 = 0$, also ist auch g_2 reduzibel. Es ist $g_3(0) = 0$, also ist g_3 ebenfalls reduzibel. Es ist $g_4(0) = 1$ und $g_4(1) = 1 + 1 + 1 = 1$. Somit ist g_4 irreduzibel in $\mathbb{F}_2[T]$.

Es gibt folgende Polynome vom Grad 3 in $\mathbb{F}_2[T]$: $h_1 = T^3$, und h_1 ist reduzibel. $h_2 = T^3 + 1$, und $h_2(1) = 0$, das heißt, h_2 ist reduzibel. $h_3 = T^3 + T$, offenbar reduzibel. $h_4 = T^3 + T^2$, ebenfalls reduzibel. $h_5 = T^3 + T + 1$; es sind $h_5(0) = 1$ und $h_5(1) = 1$. Somit ist h_5 irreduzibel. Analog ist $h_6 = T^3 + T^2 + 1$ irreduzibel. Das Polynom $h_7 = T^3 + T^2 + T$ ist offenbar durch T teilbar. Auch $h_8 = T^3 + T^2 + T + 1$ ist reduzibel, denn $h_8(1) = 0$.

Wir erhalten also folgende irreduzible Polynome vom Grad ≤ 3: $T, T + 1, T^2 + T + 1, T^3 + T + 1$ und $T^3 + T^2 + 1$.

5.8 Das RSA-Kryptosystem

Das RSA-Kryptosystem ist ein Beispiel für ein Public-Key-Kryptosystem, wie wir sie in Kapitel 1 allgemein eingeführt haben. Zur Erinnerung, in einem Public-Key-Kryptosystem werden die Schlüssel K und die Chiffrierungsregeln e_K nicht geheim gehalten. Es ist ausreichend, Zusatzinformation – so genannte geheime Schlüssel – zu verbergen.

Das RSA-Kryptosystem ist nach seinen Entdeckern Ronald Rivest, Adi Shamir und Leonard Adleman [RSA] benannt, und ist, obwohl es schon 1978 publiziert wurde, das wohl bekannteste und heute noch am häufigsten eingesetzte Public-Key-Verfahren.

Die mathematischen Grundlagen dieses Systems sind spezielle Eigenschaften der Restklassenringe $\mathbb{Z}/n\mathbb{Z}$, die in dieser und der letzten Kurseinheit hergeleitet wurden.

Beschreiben wir zunächst, wie Alice in die Liste der befugten Teilnehmerinnen und Teilnehmer des RSA-Verfahrens aufgenommen wird.

Alice wählt zwei große, verschiedene Primzahlen p und q und bildet $m = pq$. Die Primzahlen p und q hält sie geheim. Weiter berechnet sie $\varphi(m) = (p-1)(q-1)$ und wählt eine Zahl e mit $\mathrm{ggT}(e, \varphi(m)) = 1$. Dabei bezeichnet φ die Eulersche φ-Funktion. Da $\mathrm{ggT}(e, \varphi(m)) = 1$, ist e in $\mathbb{Z}/\varphi(m)\mathbb{Z}$ invertierbar. Alice berechnet $d \in \mathbb{Z}/\varphi(m)\mathbb{Z}$, so dass $e \cdot d = 1$ in $\mathbb{Z}/\varphi(m)\mathbb{Z}$ ist. Dann gilt $ed = r\varphi(m) + 1$ für ein $r \in \mathbb{Z}$.

So weit die Vorbereitungen.

Das Paar (m, e) ist der öffentliche Schlüssel von Alice.

Die Primzahlen p, q und die Zahl d bilden den geheimen Schlüssel von Alice.

Die Klartextmenge und die Geheimtextmenge in Alice' Kryptosystem ist die Menge $\mathbb{Z}/m\mathbb{Z}$.

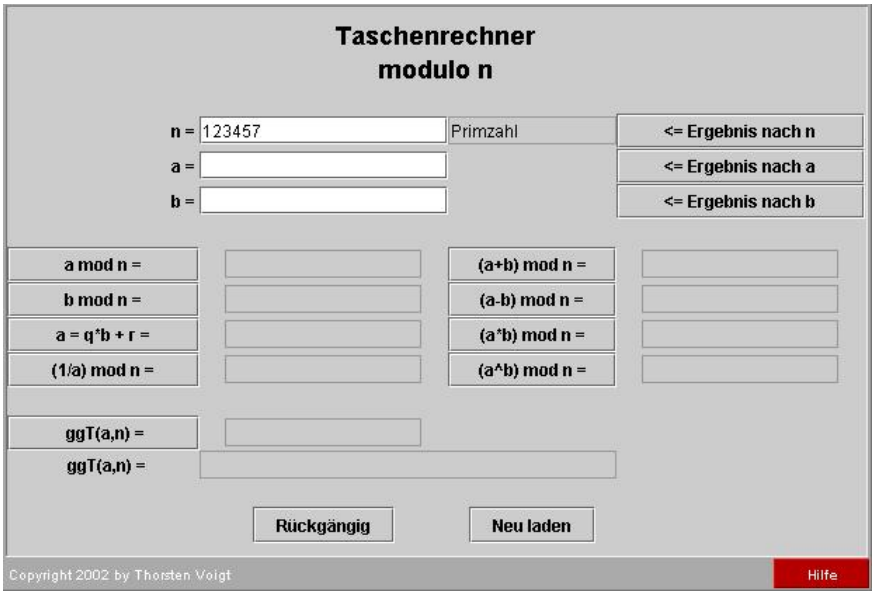
Chiffrierung im RSA-Verfahren: Will Bob an Alice die Nachricht $x \in \mathbb{Z}/m\mathbb{Z}$ schicken, so bildet er $y = x^e$ in $\mathbb{Z}/m\mathbb{Z}$ und schickt y an Alice.

Dechiffrierung im RSA-Verfahren: Alice hat eine Nachricht $y \in \mathbb{Z}/m\mathbb{Z}$ empfangen. Diese ist von der Form $y = x^e$ in $\mathbb{Z}/m\mathbb{Z}$, wobei x der Klartext ist. Sie bildet $y^d = (x^e)^d = x^{ed}$ in $\mathbb{Z}/m\mathbb{Z}$. Da $ed = r\varphi(m) + 1$, folgt mit der Folgerung 4.4.13 aus dem Kleinen Satz von Fermat, dass $y^d = x$ ist, und sie erhält Bobs Klartext.

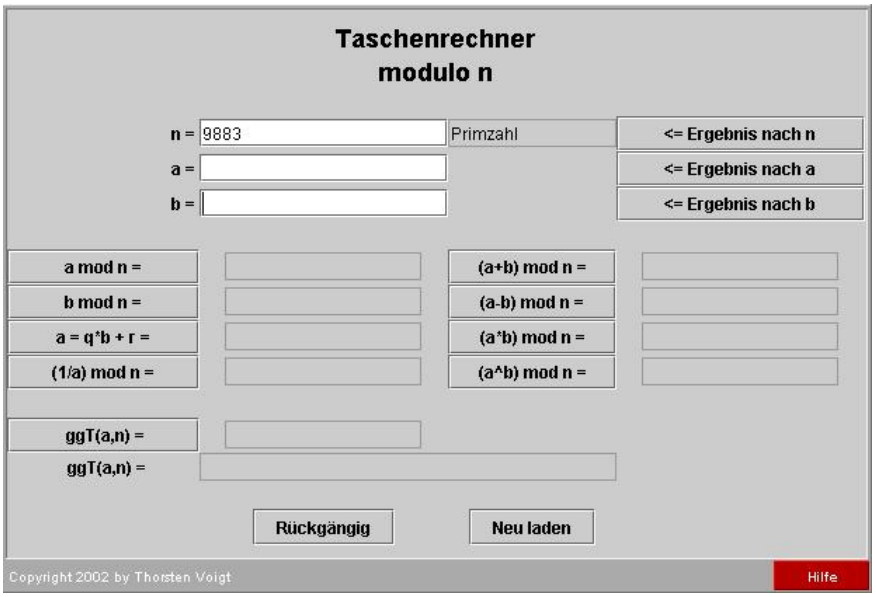
Warum das RSA-Verfahren schnell und sicher ist, werden wir später sehen. Wenden wir uns zunächst einem Beispiel zu. Dabei benutzen wir für die Rechnungen den Taschenrechner für modulare Arithmetik, der in der virtuellen Universität bereit steht. Hier wird er in Form von Screenshots eingebunden.

5.8.1 Ein Beispiel

Als Primzahl p wählen wir $p = 123457$.



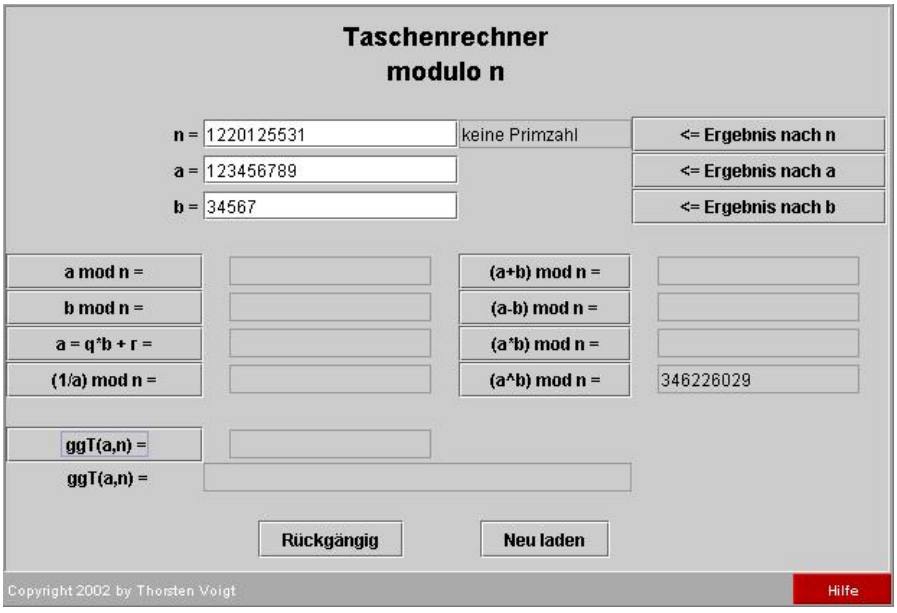
Als Primzahl q wählen wir $q = 9883$.



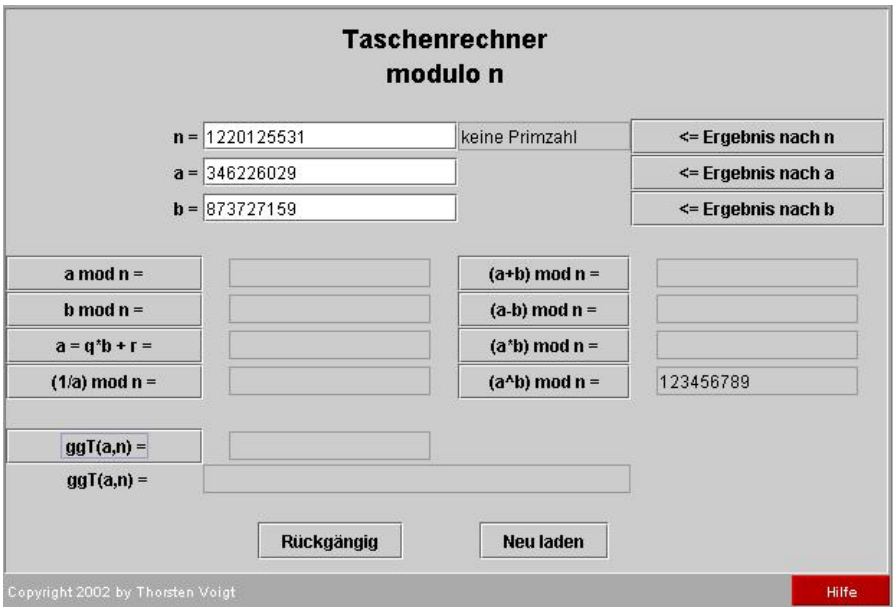
Weiter berechnen wir, etwa mit dem Taschenrechner des Computers, $m = pq = 1220125531$ und $\varphi(m) = (p-1)(q-1) = 1219992192$. Wir wählen $e = 34567$. Um zu überprüfen, ob wirklich $\mathrm{ggT}(e, \varphi(m)) = 1$ gilt, tragen wir $\varphi(m)$ als n und e als a in den Taschenrechner ein und berechnen $\mathrm{ggT}(a, n)$. Jetzt berechnen wir das zu

e inverse Element in $\mathbb{Z}/\varphi(m)\mathbb{Z}$. Wir erhalten $d = 873727159$.

Jetzt haben wir alle Bestandteile des Schlüssels zusammen: der öffentliche Schlüssel ist $m = pq = 1220125531$ und $e = 34567$, und der geheime Schlüssel ist $p = 123457$, $q = 9883$ und $d = 873727159$. Nun können wir chiffrieren und dechiffrieren. Wir tragen $m = pq = 1220125531$ als n in den Taschenrechner ein. Die Zahl 123456789 wird dann als $123456789^{34567} = 346226029$ in $\mathbb{Z}/m\mathbb{Z}$ chiffriert.



Um zu überprüfen, ob das Verfahren in diesem Beispiel geklappt hat, müssen wir das Ergebnis in die 873727159-te Potenz erheben:



Wir erhalten die Ausgangsnachricht 123456789.

5.8.2 Analyse des RSA-Verfahrens, oder, wo ist der Trick?

Wir hatten in Kapitel 1 gewisse Forderungen an ein Public-Key-Kryptosystem gestellt. Wir werden in diesem Abschnitt erklären, warum das RSA-Verfahren diesen Anforderungen genügt.

Wiederholen wir aber zunächst noch einmal die Forderungen:

1. Für alle Klartexte $x \in \mathcal{P}$ muss sich $e_K(x)$ sehr schnell berechnen lassen.
2. **Ohne** den geheimen Schlüssel lässt sich das Urbild eines Geheimtextes $y \in \mathcal{C}$ unter e_K praktisch – das heißt, in angemessener Zeit – nicht berechnen, selbst dann nicht, wenn K und e_K bekannt sind.
3. Dazu Befugte können aus dem öffentlichen Schlüssel K den geheimen Schlüssel schnell herleiten.
4. **Mit** dem geheimen Schlüssel lässt sich $d_K(y)$ für alle Geheimtexte y sehr schnell berechnen.

Wenden wir uns zunächst Punkt 3. zu, also der Konstruktion des öffentlichen und des geheimen Schlüssels. Diese Konstruktion darf nur wenig Speicherplatz und

Rechenzeit beanspruchen.

Alice, die befugte Teilnehmerin des RSA-Kommunikationsnetzes muss zwei verschiedene große Primzahlen wählen.

Dies geschieht in der Regel so, dass ein Zufallszahlengenerator zwei große ungerade Zahlen p und q vorschlägt, von denen aber nicht klar ist, ob diese wirklich Primzahlen sind oder nicht. Alice unterwirft diese Zahlen einem so genannten „probabilistischen Primzahltest“, dazu sagen wir in der folgenden Kurseinheit mehr. Wenn das Ergebnis dieses Testes lautet: „p ist keine Primzahl“, dann setzt Alice p auf $p+2$ und unterzieht diese Zahl erneut einem probabilistischen Primzahltest. Dies setzt sie so lange fort, bis das Ergebnis des Testes lautet: „p ist eine Primzahl“. Analog verfährt sie mit der Zahl q. Die Zahlen p und q, beziehungsweise die Zahlen $p-1$ und $q-1$ miteinander zu multiplizieren, ist kein Problem.

Ein probabilistischer Primzahltest ist ein schnell durchführbarer Algorithmus, in den eine ungerade Zahl n eingesetzt wird, und der als Ergebnis die Antworten „n ist keine Primzahl“ oder „n ist eine Primzahl“ liefert. Dabei ist das Ergebnis „n ist keine Primzahl“ immer richtig. Lautet die Antwort „n ist eine Primzahl“, so können wir allerdings nicht völlig sicher sein, dass die Antwort richtig ist.

Kommen wir zurück zur Schlüsselkonstruktion im RSA-Kryptosystem. Sie haben bisher gesehen, wie die Wahl von zwei großen Primzahlen erfolgt. Als nächsten Schritt muss Alice eine Zahl e so wählen, dass $\mathrm{ggT}(e, \varphi(m)) = 1$ ist. Wieder schlägt ein Zufallszahlengenerator eine Zahl e vor. Mit Hilfe des euklidischen Algorithmus, der ein wirklich schnell durchführbarer Algorithmus ist, berechnet Alice $\mathrm{ggT}(e, \varphi(m))$. Ist das Ergebnis $\neq 1$, so setzt sie e auf $e+1$ und versucht es erneut. Nach wenigen Schritten wird sie eine Zahl e gefunden haben, die $\mathrm{ggT}(e, \varphi(m)) = 1$ erfüllt.

Die Berechnung des zu e in $\mathbb{Z}/\varphi(m)\mathbb{Z}$ inversen Elements d erfolgt wieder mit dem Euklidischen Algorithmus.

So weit zur Schlüsselerzeugung. Wenden wir uns den Punkten 1. und 4. zu, also der Chiffrierung und Dechiffrierung. Beide erfolgen mit Hilfe des so genannten „wiederholten Quadrierungsalgorithmus“, den wir in der folgenden Kurseinheit vorstellen werden. Dieser Algorithmus ist schnell durchführbar.

Es bleibt zu klären, warum Oscar, der Lauscher an der unsicheren Leitung, ein ernst zu nehmendes Problem hat.

Das Problem besteht darin, dass Oscar nur $m = pq$ kennt, nicht aber die Faktoren p und q von m, die er zur Berechnung von d (bzw. $\varphi(m)$) benötigt. Oscar sieht sich also mit dem Problem konfrontiert, die Zahl m in Primfaktoren zu zerlegen.

Dieses Problem wird in der Zahlentheorie schon seit Jahrhunderten untersucht, und es gilt als ein sehr schweres Problem. Bis heute sind keine schnellen Algorithmen bekannt, mit deren Hilfe Zahlen als Produkte von Primfaktoren geschrieben werden können. Zwar können probabilistische Primzahltests dazu eingesetzt werden, zu entscheiden, ob eine gegebene Zahl n eine Primzahl ist oder nicht, aber keiner dieser Tests liefert einen Faktor von n.

Die Sicherheit des RSA-Verfahrens beruht also darauf, dass keine schnellen Algorithmen bekannt sind, eine Zahl m als Produkt ihrer Faktoren zu schreiben.

Es ist ein offenes mathematisches Problem, ob es schnelle (dieser Begriff ist natürlich zu präzisieren) Faktorisierungsalgorithmen gibt oder nicht. Es wird vermutete, dass dies nicht der Fall ist. Außerdem ist auch nicht bekannt, ob wirklich die Zahl m faktorisiert werden muss, um das RSA-Kryptosystem zu brechen.

5.8.3 Realistische Größen bei der Nutzung des RSA-Verfahrens

Die Sicherheit des RSA-Verfahrens beruhte auf dem Problem, eine große natürliche Zahl in ihre Primfaktoren zu zerlegen. Daher darf die Schlüssellänge nicht zu klein gewählt werden. Die Länge eines Schlüssels wird gemessen in der Anzahl der Speicherbits, die benötigt werden, um diesen Wert im Computer darzustellen.

Mit welchen Schlüssellängen das RSA-Verfahren im Herbst 2004 als sicher galt, wird hier aus den Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik `http://www.bsi.de/` zitiert:

„Werden bei asymmetrischer Verschlüsselungs- und Signaturverfahren Algorithmen eingesetzt, deren Sicherheit auf dem Problem des Faktorisierens großer Zahlen basiert, so wird heute angenommen, daß Schlüssellängen von weniger als 1024 Bit als unsicher zu betrachten sind. Dies begründet sich in den Fortschritten bei der Entwicklung effizienter Faktorisierungsalgorithmen, die heute unter massivem Rechnereinsatz Faktorisierungen von Zahlen mit rund 500 Bit erlauben. Daneben ist die mögliche Entwicklung von opto-elektronischen Beschleunigern für einen wesentlichen Teil- Rechenschritt bei diesen Verfahren in Betracht zu ziehen, was diese wesentlich beschleunigen würde.

...

Betroffen ist der RSA-Algorithmus, der als asymmetrisches Verfahren auf dem Faktorisierungsproblem basiert. Wird dieser mit einer Schlüssellänge unter 768 Bit betrieben, kann von potentiellen Unsicherheiten ausgegangen werden. Für die nächsten Jahre wird eine Schlüssellänge von mehr als 1024 Bit als ausreichend sicher angesehen.“

Eine Zahl mit 1024 Bit Länge hat etwa 300 Stellen.

In den USA ist nur eine Schlüssellänge von 512 Bit erlaubt.

5.8.4 Neuere und neuste Geschichte des RSA-Kryptosystems

In den USA war das RSA-Verfahren patentiert. Das Patent hatte die Firma RSA Security vom Massachusetts Institute of Technology (MIT) erworben, bei dem die Entdecker Rivest, Shamir und Adleman angestellt waren. Kommerzielle RSA-Nutzer in den USA mussten Lizenzgebühren zahlen, auch wenn keine Implementierung durch RSA Security erfolgte. Europäische Software kostete deutlich mehr oder konnte gar nicht erst vertrieben werden. Am 20. September 2000 lief das Patent aus, und das RSA-Verfahren wurde Allgemeingut.

Es wird immer wieder davon berichtet, dass das RSA-Kryptosystem gebrochen worden wäre. So wird etwa über Angriffe auf RSA durch Einsatz spezieller Hardware oder durch Anwendung cleverer mathematischer Verfahren berichtet.

Es gibt spezielle RSA-Challanges, in denen wissenschaftliche Institutionen aber auch Individuen aufgefordert werden, speziell vorgegebene Zahlen zu faktorisieren. Dies dient unter anderem auch dazu, herauszufinden, wie groß die Schlüssellängen gewählt werden müssen, damit das RSA-Verfahren noch als sicher angesehen werden kann. Wenn Sie sich daran beteiligen wollen, finden Sie weitere Information unter `http://www.rsasecurity.com/rsalabs/challenges/factoring/`.

Es gibt heute Public-Key-Verfahren, die als genauso sicher wie RSA gelten, die aber mit deutlich geringerer Schlüssellänge auskommen. Diese Verfahren beruhen auf der mathematischen Theorie elliptischer Kurven, die wir in Kurseinheit 6 vorstellen werden. Mehr zur Kryptografie auf elliptischen Kurven finden Sie unter `http://www.cryptovision.com/Kurvenfabrik/kfindex2.html`.

5.8.5 Aufgaben

5.8.1 Aufgabe Übernehmen Sie die Rolle von Alice. Sie möchten in die Liste derer aufgenommen werden, die mit Hilfe des RSA-Verfahrens miteinander kommunizieren. Der Zufallszahlengenerator hat Ihnen als Primzahlen p und q die Zahlen $p = 2345$ und $q = 76543$ vorgeschlagen, und als zu $(p-1)(q-1)$ teilerfremde Zahl e die Zahl $e = 97251$.

Nehmen Sie die vorgeschlagenen Zahlen als Basis zur Konstruktion des geheimen und des öffentlichen Schlüssels im RSA-Kryptosystem.

Wie lautet Ihr geheimer, wie Ihr öffentlicher Schlüssel? Wie wird dechiffriert?

In den beiden folgenden Aufgaben werden wir Buchstaben wie folgt mit Zahlen identifizieren:

$a \leftrightarrow 01$	$b \leftrightarrow 02$	$c \leftrightarrow 03$	$d \leftrightarrow 04$	$e \leftrightarrow 05$	$f \leftrightarrow 06$	$g \leftrightarrow 07$	$h \leftrightarrow 08$
$i \leftrightarrow 09$	$j \leftrightarrow 10$	$k \leftrightarrow 11$	$l \leftrightarrow 12$	$m \leftrightarrow 13$	$n \leftrightarrow 14$	$o \leftrightarrow 15$	$p \leftrightarrow 16$
$q \leftrightarrow 17$	$r \leftrightarrow 18$	$s \leftrightarrow 19$	$t \leftrightarrow 20$	$u \leftrightarrow 21$	$v \leftrightarrow 22$	$w \leftrightarrow 23$	$x \leftrightarrow 24$
$y \leftrightarrow 25$	$z \leftrightarrow 26$						

Eine Leerstelle werden wir mit 00 identifizieren. Wir fassen dann den Text in Blöcke der Länge 2 zusammen, und erhalten Ziffernfolgen der Länge 4 (möglicherweise mit führender Null). Diese Ziffernfolgen werden wir chiffrieren beziehungsweise dechiffrieren. Ein Beispiel: „Es geht los“ wird zu 0519 0007 0508 2000 1215 1924. Dabei haben wir, da der Text aus einer ungeraden Anzahl von Buchstaben/Leerstellen bestand, den Text am Ende um ein x verlängert.

5.8.2 Aufgabe Übernehmen Sie die Rolle von Bob. Sie möchten Alice die Botschaft „wie immer um Mitternacht“ übermitteln. Alice' öffentlicher Schlüssel ist $(2923, 725)$.

Chiffrieren Sie die Nachricht mit Alice' öffentlichem Schlüssel.

5.8.3 Aufgabe Sie sind Oscar, und Sie haben folgende Nachricht von Bob an Alice abgefangen:

2201	2352	1458	0207	2417
1951	0717	0795	1442	0876
2730	1205	0795.		

Der öffentliche Schlüssel von Alice ist $(2881, 137)$. Wie lautet der Klartext?

Lösungen der Aufgaben

Aufgabe 5.1.6

Behauptung In jedem Schiefkörper R folgt aus $ab = 0$, dass $a = 0$ oder $b = 0$ gilt.

Beweis: Sei R ein Schiefkörper. Wir zeigen zunächst, dass $r \cdot 0 = 0$ ist, für alle $r \in R$.

Es gilt $r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0$. Wir subtrahieren auf beiden Seiten der Gleichung $r \cdot 0$ und erhalten $0 = r \cdot 0$.

Seien nun $a, b \in R$ mit $ab = 0$. Wenn $a = 0$, so sind wir fertig. Sei also $a \neq 0$. Wir müssen zeigen, dass $b = 0$ ist. Wir multiplizieren die Gleichung $ab = 0$ auf beiden Seiten mit a^{-1}. Dann folgt $a^{-1}ab = b = 0$, und wir sind fertig. □

Aufgabe 5.1.8 Seien $R_1, \ldots, R_n$ Ringe.

(a) **Behauptung** $\prod_{i=1}^{n} R_i$ ist in der Regel kein Integritätsbereich, wenn $R_1, \ldots, R_n$ Integritätsbereiche sind.

Beweis: Sei etwa $R_1 = R_2 = \mathbb{Z}$. Dann sind R_1 und R_2 Integritätsbereiche. Der Ring $\mathbb{Z} \times \mathbb{Z}$ ist kein Integritätsbereich, denn $(1, 0)$ und $(0, 1)$ sind $\neq 0$, aber $(1, 0)(0, 1) = (0, 0)$. □

(b) **Behauptung** $\prod_{i=1}^{n} R_i$ ist in der Regel kein Körper, wenn alle R_i, $1 \leq i \leq n$ Körper sind.

Beweis: Sei etwa $R_1 = R_2 = \mathbb{R}$. Dann liegen $(1, 0)$ und $(0, 1)$ in $\mathbb{R} \times \mathbb{R}$, und es gilt $(1, 0)(0, 1) = (0, 0)$. Somit ist $\mathbb{R} \times \mathbb{R}$ kein Integritätsbereich. Mit Aufgabe 5.1.6 folgt, dass $\mathbb{R} \times \mathbb{R}$ kein Körper ist. □

(c) **Behauptung** $\prod_{i=1}^{n} R_i$ ist genau dann kommutativ, wenn alle R_i, $1 \leq i \leq n$ kommutativ sind.

Beweis: Seien $R_1, \ldots, R_n$ kommutativ. Dann gilt für alle $a_i, b_i \in R_i, 1 \leq i \leq n$:

$$\begin{aligned} & a_i b_i = b_i a_i \\ \Leftrightarrow \quad & (a_1 b_1, \ldots, a_n b_n) = (b_1 a_1, \ldots, b_n a_n) \\ \Leftrightarrow \quad & (a_1, \ldots, a_n)(b_1, \ldots, b_n) = (b_1, \ldots, b_n)(a_1, \ldots, a_n) \\ \Leftrightarrow \quad & \prod_{i=1}^{n} R_i \text{ ist kommutativ.} \end{aligned}$$

□

Aufgabe 5.2.5

1. Sei $(R, +, \cdot)$ ein Ring, und sei I ein Ideal in R.

   Behauptung Falls $1 \in I$, so gilt $I = R$.

   Beweis: Sei $1 \in I$. Nach Definition gilt $r \cdot 1 = 1 \cdot r = r \in I$ für alle $r \in R$. Es folgt $R \subseteq I$, also $R = I$. □

2. Sei R ein Ring, und seien I_1, I_2 Ideale in R.

   Behauptung $I_1 \cap I_2$ ist ein Ideal in R.

   Beweis: Mit dem Untergruppenkriterium folgt, dass $(I_1 \cap I_2, +)$ eine abelsche Gruppe ist. Sei $x \in I_1 \cap I_2$. Sei $r \in R$. Dann gilt $rx, xr \in I_1$, denn I_1 ist ein Ideal in R. Analog gilt $xr, rx \in I_2$. Es folgt $rx, xr \in I_1 \cap I_2$, das heißt, $I_1 \cap I_2$ ist ein Ideal in R. □

3. Sei R ein kommutativer Ring, und sei I ein Ideal in R. Sei $\mathrm{M}_{nn}(I)$ die Menge der $n \times n$-Matrizen, deren Einträge in I liegen.

   Behauptung Es ist $\mathrm{M}_{nn}(I)$ ein Ideal in $\mathrm{M}_{nn}(R)$.

   Beweis: Mit dem Untergruppenkriterium folgt, dass $(\mathrm{M}_{nn}(I), +)$ eine abelsche Gruppe ist. Sei $A = (a_{ij}) \in \mathrm{M}_{nn}(I)$, und sei $B = (b_{ij}) \in \mathrm{M}_{nn}(R)$. Seien $C = (c_{ij}) = AB$ und $D = (d_{ij}) = BA$. Dann gelten $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \in I$ und $d_{ij} = \sum_{k=1}^{n} b_{ik} a_{kj} \in I$ für alle $1 \leq i, j \leq n$, denn I ist ein Ideal in R. Es folgt $AB, BA \in \mathrm{M}_{nn}(I)$. Somit ist $\mathrm{M}_{nn}(I)$ ein Ideal in $\mathrm{M}_{nn}(R)$. □

Aufgabe 5.2.8 Sei R ein Ring, und sei I ein Ideal in R.

1. Seien $a, b \in R$.

   Behauptung Es ist $a \equiv b(\mathrm{mod} I)$ genau dann, wenn $a - b \in I$ gilt.

   Beweis: Es gilt

   $$\begin{aligned} a \equiv b(\mathrm{mod} I) &\Leftrightarrow a = b + c \text{ für ein } c \in I \\ &\Leftrightarrow a - b = c \text{ für ein } c \in I \\ &\Leftrightarrow a - b \in I. \end{aligned}$$

   □

2. Sei $U \subseteq R^\times$ die Menge der Einheiten $a \in R^\times$ mit $a \equiv 1(\mathrm{mod} I)$.

   Behauptung U ist ein Normalteiler von $R^\times$.

   Beweis: Wir zeigen zunächst mit dem Untergruppenkriterium, dass U eine Untergruppe von $R^\times$ ist.

   Die Menge U ist nicht leer, denn $1 \in U$.

   Seien $a, b \in U$. Dann ist ab^{-1} eine Einheit in R. Seien $a = 1 + c$ und $b = 1 + c'$ für Elemente $c, c' \in I$. Indem wir die zweite Gleichung mit b^{-1} multiplizieren, erhalten wir $1 = b^{-1} + b^{-1}c'$, wobei $d = b^{-1}c' \in I$ gilt. Es folgt $ab^{-1} = (1 + c)(1 - d) = 1 + (c - d - cd)$, und $c - d - cd \in I$. Somit gilt $ab^{-1} \in U$, und mit dem Untergruppenkriterium folgt, dass U eine Untergruppe von $R^\times$ ist.

   Zum Beweis, dass U ein Normalteiler von $R^\times$ ist, benutzen wir die zweite Bedingung von Proposition 4.6.4. Dazu seien $r \in R^\times$ und $x = 1 + c \in U$ mit $c \in I$. Dann gilt $rxr^{-1} = r(1 + c)r^{-1} = 1 + rcr^{-1} \in U$, denn $rxr^{-1} \in R^\times$ und $rcr^{-1} \in I$. Es folgt $rUr^{-1} \subseteq U$, und dies impliziert die Behauptung. □

Aufgabe 5.3.2 Sei $\phi : R \to R'$ ein Ringhomomorphismus. Sei $\phi|_{R^\times} : R^\times \to R'$ definiert durch $\phi|_{R^\times}(r) = \phi(r)$ für alle $r \in R^\times$.

(a) **Behauptung** Es gilt $\phi|_{R^\times}(r) \in R'^\times$ für alle $r \in R^\times$.

Beweis: Sei r eine Einheit in R. Dann gilt $rr^{-1} = 1$ und $1 = \phi(1) = \phi(rr^{-1}) = \phi(r)\phi(r^{-1})$. Analog folgt, dass $\phi(r^{-1})\phi(r) = 1$ gilt. Somit ist $\phi(r)$ invertierbar. Es folgt, dass $\phi|_{R^\times}$ invertierbare Elemente in R auf invertierbare Elemente in R' abbildet. □

(b) **Behauptung** Es ist $\phi|_{R^\times} : R^\times \to R'^\times$ ein Gruppenhomomorphismus.

Beweis: Wir haben im ersten Teil der Aufgabe gesehen, dass $\phi|_R$ eine Abbildung von $R^\times$ nach $R'^\times$ ist. Da $\phi|_R(rs) = \phi|_R(r)\phi|_R(s)$ für alle $r, s \in R$, folgt, dass $\phi|_{R^\times}$ ein Gruppenhomomophismus ist. □

Aufgabe 5.3.8 Sei $\phi : R \to R'$ ein Epimorphismus, und sei $I \lhd R$ ein Ideal in R. Sei

$$\phi(I) = \{s' \in R' \mid \text{ es gibt ein } s \in I \text{ mit } \phi(s) = s'\}.$$

Behauptung Es ist $\phi(I)$ ein Ideal in R'.

Beweis: Da ϕ ein Ringhomomorphismus ist, folgt mit dem Untergruppenkriterium, dass $(\phi(I), +)$ eine abelsche Untergruppe von $(R', +)$ ist. Sei $\phi(c) \in \phi(I)$, und sei $r' \in R'$. Da ϕ surjektiv ist, gibt es ein $r \in R$ mit $\phi(r) = r'$. Dann gilt

$$\phi(c)r' = \phi(c)\phi(r) = \phi(cr) \in \phi(I),$$

denn $cr \in I$. Analog folgt, dass $r'\phi(c)$ in $\phi(I)$ liegt. Somit ist $\phi(I)$ ein Ideal in R'. □

Aufgabe 5.3.10 Sei R ein kommutativer Ring, und sei I ein Ideal in R. Sei $\mathrm{M}_{nn}(I)$ die Menge der $n \times n$-Matrizen, deren Einträge in I liegen.

Behauptung $\mathrm{M}_{nn}(R)/\mathrm{M}_{nn}(I)$ ist isomorph zu $\mathrm{M}_{nn}(R/I)$.

Beweis: Wir definieren $\phi : \mathrm{M}_{nn}(R) \to \mathrm{M}_{nn}(R/I)$ durch $\phi((a_{ij})) = ([a_{ij}])$ für alle $A = (a_{ij}) \in \mathrm{M}_{nn}(R)$.

Die Abbildung ϕ ist ein Epimorphismus, und

$$\mathrm{Kern}(\phi) = \{A = (a_{ij}) \in \mathrm{M}_{nn}(R) \mid a_{ij} \in I \text{ für alle } 1 \leq i, j \leq n\} = \mathrm{M}_{nn}(I).$$

Mit dem Homomorphiesatz folgt die Behauptung. □

Aufgabe 5.4.5

Gesucht ist die kleinste ganze Zahl x für die gilt:

$$\begin{aligned} x &\equiv 2 (\bmod 3) \\ x &\equiv 1 (\bmod 5) \\ x &\equiv 6 (\bmod 7). \end{aligned}$$

Wir berechnen das Urbild von $(2 \bmod 3, 1 \bmod 5, 6 \bmod 7)$ unter der Abbildung ϕ des chinesischen Restsatzes.

Es ist $n = 3 \cdot 5 \cdot 7 = 105$. Weiter sind $q_1 = 35$, $q_2 = 21$ und $q_3 = 15$. Die r_i berechnen wir mir dem Euklidischen Algorithmus oder durch scharfes Hinsehen (hier entscheiden wir uns für die letztere Variante): $r_1 = 2$, $r_2 = 1$ und $r_3 = 1$.

Es folgt

$$x = (2 \cdot 35 \cdot 2 + 1 \cdot 21 \cdot 1 + 6 \cdot 15 \cdot 1) \bmod 105 = 251 \bmod 105 = 41.$$

Das gesuchte x ist somit $x = 41$. □

Aufgabe 5.5.8 Sei $R = \mathbb{F}_2[T]$. Der Ring R hat unendlich viele Elemente, und sein Primring $\mathbb{F}_2$ hat 2 Elemente. □

Aufgabe 5.5.14

Behauptung Einfache, kommutative Ringe haben die Charakteristik 0 oder p, wobei p eine Primzahl ist.

Beweis: Sei R ein kommutativer Ring. Angenommen, $\mathrm{char}(R) = m$, und $m = st$, mit $s, t \neq 1$. Dann gilt $0 = me = (se)(te)$ mit $se \neq 0$ und $te \neq 0$. Sei $I = (se)$ das von se erzeugte Ideal. Dann gilt $I \neq \{0\}$, denn $se \in I$. Angenommen, $I = R$. Dann gilt $1 \in I$, also $1 = ser$ für ein $r \in R$. Dann folgt $0 = (te)(se)r = te$, ein Widerspruch. Somit ist I ein Ideal, dass $\{0\}$ echt enthält, und das in R echt enthalten ist. Es folgt, dass R nicht einfach ist. □

Aufgabe 5.5.18 Sei R ein kommutativer Ring der Charakteristik $p > 0$. Seien $a_1, \ldots, a_m \in R$.

Behauptung Es gilt $(a_1 + \cdots + a_m)^{p^n} = a_1^{p^n} + \cdots + a_m^{p^n}$ für alle $m, n \in \mathbb{N}$.

Beweis: Wir beweisen die Behauptung mit Induktion nach m. Ist $m = 1$, so ist die Behauptung offenbar richtig. Sei $m > 1$. Dann gilt

$$\begin{aligned}(a_1 + \cdots + a_m)^{p^n} &= ((a_1 + \cdots + a_{m-1}) + a_m)^{p^n} \\ &= (a_1 + \cdots + a_{m-1})^{p^n} + a_m^{p^n} \text{ mit der Binomischen Formel} \\ &= a_1^{p^n} + \cdots + a_m^{p^n} \text{ mit der Induktionsvoraussetzung.}\end{aligned}$$

□

Aufgabe 5.6.6 Sei $R = \mathbb{Z}$, und seien $m\mathbb{Z}$ und $n\mathbb{Z}$ Ideale in $\mathbb{Z}$.

1. **Behauptung** Genau dann gilt $m\mathbb{Z} \subseteq n\mathbb{Z}$, wenn n ein Teiler von m ist.

   Beweis: Sei $m\mathbb{Z} \subseteq n\mathbb{Z}$. Da $m \in m\mathbb{Z}$, folgt $m \in n\mathbb{Z}$, also $m = xn$ für ein $x \in \mathbb{Z}$. Somit ist n ein Teiler von m.

   Sei umgekehrt n ein Teiler von m, also $m = xn$, $x \in \mathbb{Z}$. Dann gilt $my = nxy \in n\mathbb{Z}$ für alle $my \in m\mathbb{Z}$. Es folgt $m\mathbb{Z} \subseteq n\mathbb{Z}$. □

2. **Behauptung** Genau dann gilt $m\mathbb{Z} = n\mathbb{Z}$, wenn m und n assoziiert sind.

   Beweis: Seien m und n assoziiert. Dann gilt $m = \pm n$, und es folgt $m\mathbb{Z} = n\mathbb{Z}$.

   Sei umgekehrt $m\mathbb{Z} = n\mathbb{Z}$. Mit dem ersten Teil der Aufgabe gilt $m|n$ und $n|m$. Es folgt, dass m und n assoziiert sind. □

3. **Behauptung** Genau dann ist $n\mathbb{Z}$ ein maximales Ideal, wenn n ein Primelement in $\mathbb{Z}$ ist.

   Beweis: Sei n kein Primelement. Dann gibt es $s \neq 1$ und $t \neq 1$ mit $n = st$. Dann ist $n\mathbb{Z}$ echt in $s\mathbb{Z}$ enthalten, und es folgt, dass $n\mathbb{Z}$ nicht maximal ist.

   Sei umgekehrt n ein Primelement. Sei $I \neq \mathbb{Z}$ ein Ideal in $\mathbb{Z}$, das $n\mathbb{Z}$ enthält. Dann ist I von der Form $m\mathbb{Z}$, und mit dem ersten Teil der Aufgabe folgt $n\mathbb{Z} = m\mathbb{Z}$. □

Aufgabe 5.6.7

Sei $R = \mathbb{Z}$, und sei $I = \{0\}$. Dann ist I ein Primideal, denn wenn $ab \in I$ für $a, b \in R$, so folgt $a = 0$ oder $b = 0$. Das Nullideal ist aber nicht maximal. □

Aufgabe 5.7.6

$$\begin{aligned} 2T^6 + T^3 + T^2 + 2 &= (2T^2 + 1)(T^4 + T^2 + 2T) + T + 2 \\ T^4 + T^2 + 2T &= (T^3 + T^2 + 2T + 1)(T + 2) + 1 \\ T + 2 &= (T + 2) \cdot 1. \end{aligned}$$

Die Polynome f und g sind somit teilerfremd. □

Aufgabe 5.7.13 Die Polynome vom Grad 4 über $\mathbb{F}_2$ sind:

T^4, $T^4 + 1$, $T^4 + T$, $T^4 + T^2$, $T^4 + T^3$, $T^4 + T + 1$, $T^4 + T^2 + 1$, $T^4 + T^3 + 1$, $T^4 + T^2 + T$, $T^4 + T^3 + T$, $T^4 + T^3 + T^2$, $T^4 + T^2 + T + 1$, $T^4 + T^3 + T + 1$, $T^4 + T^3 + T^2 + 1$, $T^4 + T^3 + T^2 + T$, $T^4 + T^3 + T^2 + T + 1$.

Die meisten der Polynome können wir durch Überlegen schon als reduzibel aussortieren. Wenn ein Polynom 2 oder 4 Summanden besitzt, dann ist es reduzibel, denn dann sind 0 oder 1 Nullstellen. Auch jedes Polynom ohne konstanten Term 1 ist reduzibel, denn dann ist T ein Faktor. Somit bleiben uns noch folgende Polynome:

$T^4 + T + 1$, $T^4 + T^2 + 1$, $T^4 + T^3 + 1$, $T^4 + T^3 + T^2 + T + 1$.

Ein reduzibles Polynom vom Grad 4 ist Produkt von zwei Polynomen vom Grad 2 oder Produkt eines Polynomes vom Grad 1 mit einem vom Grad 3. Die Polynome vom Grad 2 sind T^2, $T^2 + 1$, $T^2 + T$, $T^2 + T + 1$. Keiner der vier Kandidaten oben

ist durch T^2 oder T^2+T teilbar. Die verbleibenden Produkte von Polynomem vom Grad 2 sind:

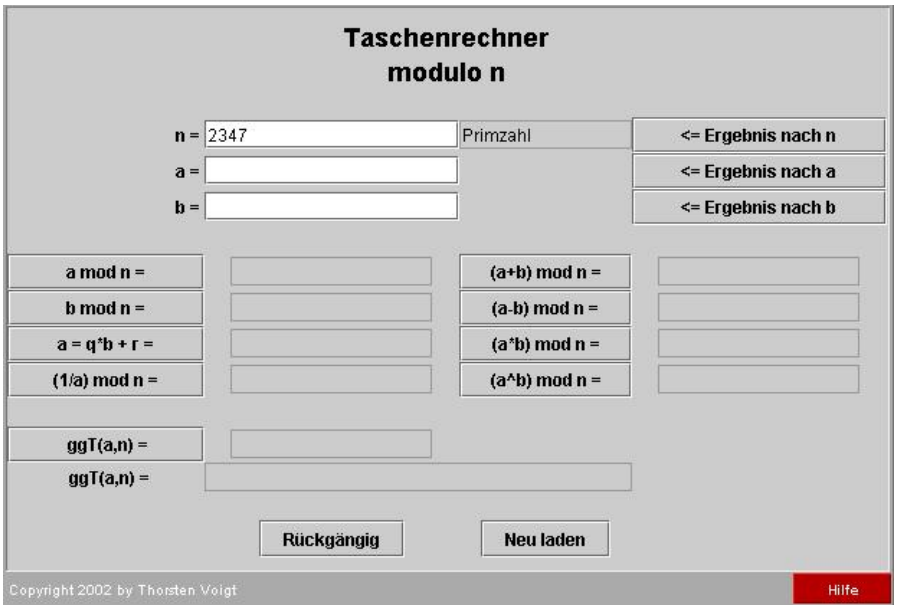
$(T^2+1)^2 = T^4+1$, $(T^2+1)(T^2+T+1) = T^4+T^3+T+1$ und $(T^2+T+1)^2 = T^4+T^2+1$.

Damit verkürzt sich unsere Liste auf

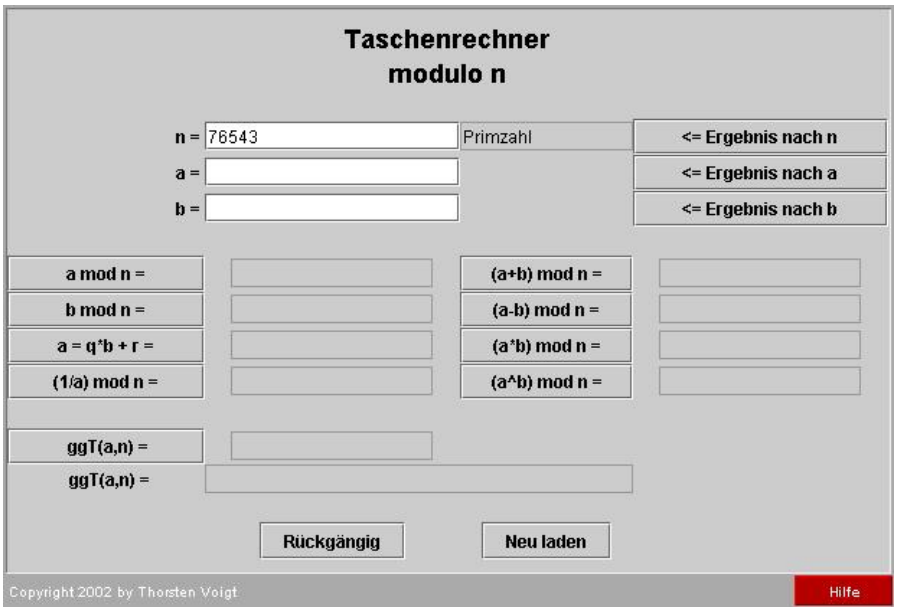
T^4+T+1, T^4+T^3+1, $T^4+T^3+T^2+T+1$.

Diese Polynome sind irreduzibel oder das Produkt eines Polynoms vom Grad 3 mit einem Polynom $\neq T$ vom Grad 1. Im letzteren Fall hätten die Polynome Nullstellen. Wir setzen die Elemente von $\mathbb{F}_2$ ein und stellen fest, dass sie keine Nullstellen haben. Somit sind sie irreduzibel. Die irreduziblen Polynome vom Grad 4 sind damit T^4+T+1, T^4+T^3+1, $T^4+T^3+T^2+T+1$. □

Aufgabe 5.8.1 Die Zahl 2345 ist natürlich keine Primzahl. Wir erhöhen um 2 und setzen die Zahl 2347 als n in den Taschenrechner zum Rechnen in $\mathbb{Z}/n\mathbb{Z}$ ein. Glück gehabt, 2347 ist eine Primzahl, und wir setzen $p = 2347$.



Wir setzen 76543 als n in den Taschenrechner ein.



Es zeigt sich, dass 76543 eine Primzahl ist, und wir setzen $q = 76543$.

Wir berechnen $\varphi(m) = (p-1)(q-1) = 179567532$ und setzen diese Zahl als n in den Taschenrechner ein. Es ist $\mathrm{ggT}(97251, 179567532) = 3$. Wir erhöhen die vorgeschlagene Zahl $e = 97251$ um 2 und erhalten $\mathrm{ggT}(97253, 179567532) = 1$.

Das zu e in $\mathbb{Z}/179567532\mathbb{Z}$ inverse Element ist $d = 83169053$.

Wir berechnen $m = pq = 2347 \cdot 76543 = 179646421$.

Der öffentliche Schlüssel ist $(179646421, 97253)$.

Der geheime Schlüssel ist $(2347, 76543)$ beziehungsweise 83169053.

Zum Dechiffrieren werden die Geheimtextzahlen in $\mathbb{Z}/179646421\mathbb{Z}$ in die 83169053-te Potenz erhoben.

Aufgabe 5.8.2 Wir übersetzen zunächst den Text in Zahlen:

$$\begin{array}{cccccc} 2309 & 0500 & 0913 & 1305 & 1800 & 2113 \\ 0013 & 0920 & 2005 & 1814 & 0103 & 0820. \end{array}$$

Wir geben 2923 als n und 725 als b in den Taschenrechner ein. Dann setzen wir die vierstelligen Zahlen, die unserem Klartext entsprechen jeweils als a in den Taschenrechner ein und bilden a^b. Wir erhalten die Ziffernfolge:

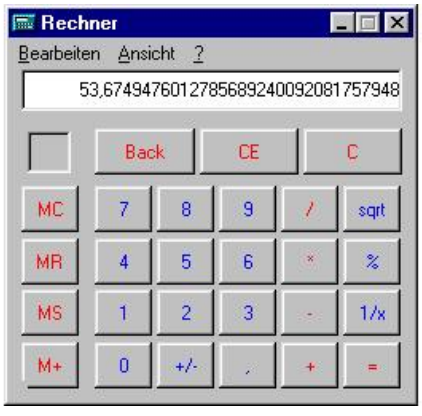
$$\begin{array}{cccccc} 1800 & 1280 & 1362 & 1987 & 0890 & 1135 \\ 1589 & 1685 & 1785 & 1111 & 2900 & 1153. \end{array}$$

Dies ist der Geheimtext, und den schicken wir an Alice.

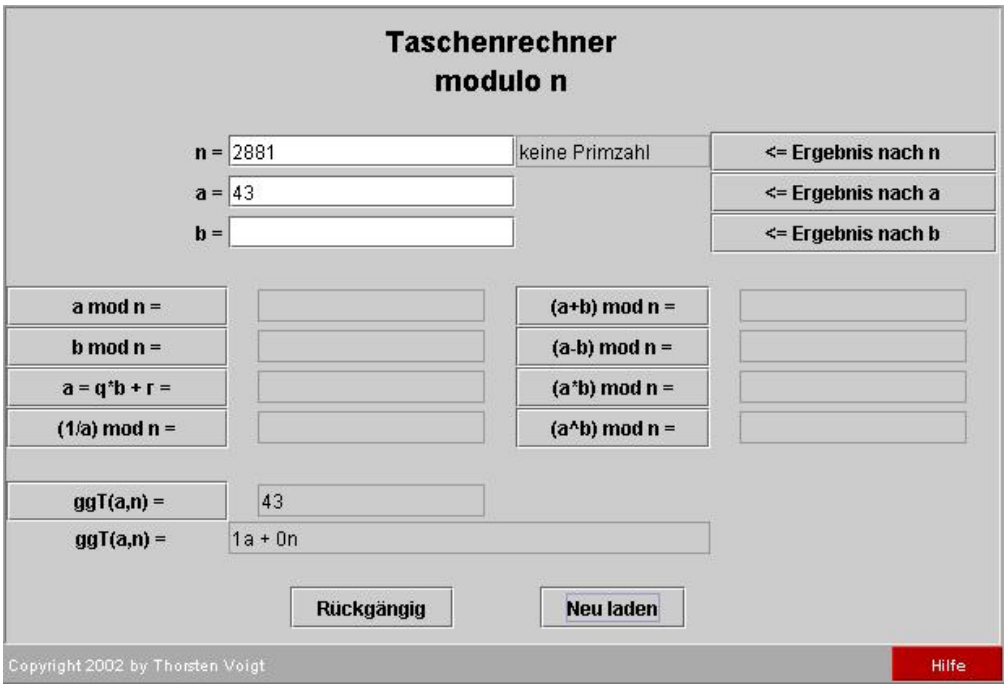
Aufgabe 5.8.3 Wir müssen versuchen, Alice' geheimen Schlüssel herzuleiten.

Wir wissen, dass $m = pq$ ist, wobei p und q verschiedene Primzahlen sind. Wie groß können diese Teiler von m maximal werden? Mit Hilfe des Taschenrechners (zum Beispiel dem des Computers) berechnen wir

$\sqrt{2881} =$



Einer der beiden Teiler von m muss daher eine Primzahl sein, die kleiner als 54 ist. Um einen solchen Teiler zu bestimmen, können wir den Taschenrechner benutzen. Wir geben 2881 als n ein. Als a geben wir Primzahlen ein, die kleiner als 54 sind und berechnen $\mathrm{ggT}(a, n)$. Nach einigen Versuchen finden wir:



Somit ist 43 ein Teiler von m, und es gilt $m = 43 \cdot 67$.

Als nächstes berechnen wir $(p-1)(q-1) = 42 \cdot 66 = 2772$. Diese Zahl tragen wir als n in den Taschenrechner ein. Weiter tragen wir die Zahl $e = 137$ als a in den Taschenrechner ein und berechnen das zu a inverse Element in $\mathbb{Z}/2772\mathbb{Z}$.

Es ist also $d = 2165$, und wir dechiffrieren, indem wir die abgefangenen Zahlen in $\mathbb{Z}/2881\mathbb{Z}$ in die 2165-te Potenz erheben. Wir erhalten

$$\begin{array}{lllll} 0409 & 0519 & 0500 & 2601 & 0812 \\ 0514 & 0019 & 0914 & 0400 & 2621 \\ 0011 & 1205 & 0914. & & \end{array}$$

Die führenden Nullen müssen wir natürlich selbst einfügen.

In Buchstaben übersetzt erhalten wir den Klartext: „Diese Zahlen sind zu klein“.

Kurseinheit 4

Effiziente Algorithmen

Studierhinweise

Kurseinheit 4 ist in zwei Kapitel aufgeteilt. Im ersten dieser Kapitel geht es um Grundsätzliches zu Algorithmen. Da wir in diesem Kurs etliche Algorithmen behandeln, gibt es eine kurze Einführung darüber, was ein Algorithmus überhaupt ist. Wir führen eine vereinfachte Programmiersprache ein, in der die Algorithmen formuliert werden. Diese Programmiersprache hat nur wenige Elemente und ist sehr intuitiv. Sie soll aber auch nur dazu dienen, Algorithmen kurz und präzise darzustellen. - Und schließlich liegt der Schwerpunkt dieses Kurses ja auch auf der Mathematik.

Es wird auch dargestellt, wann ein Algorithmus effizient ist. Die effizienten Algorithmen sind die, die als praktikabel gelten. Für grundlegende Algorithmen, die im Kurstext immer wieder benötigt werden, wie zum Beispiel die Division mit Rest und der Euklidische Algorithmus, wird gezeigt, dass sie effizient sind. Dabei haben wir allerdings nicht den Ehrgeiz, den jeweils schnellsten bekannten Algorithmus vorzustellen. Meistens halten wir uns an das, was Ihnen schon aus der Schule bekannt ist.

Im zweiten Kapitel dieser Kurseinheit werden drei sogenannte „probabilistische“ Algorithmen vorgestellt. Dies sind Algorithmen, bei denen der Zufall Einfluss auf die Laufzeit und das Ergebnis des Algorithmus' hat. Um diese Algorithmen zu verstehen, ist eine kleine Einführung in die Wahrscheinlichkeitstheorie nötig, ebenfalls sehr kurz und knapp. Diese Einführung befindet sich am Ende des ersten Kapitels, bevor dann im zweiten Kapitel die drei Primzahltests vorgestellt werden. Dies sind probabilistische Algorithmen, die eine natürliche Zahl n als Eingabe haben und als Ausgabe entweder „n ist zusammengesetzt“ oder „n ist wahrscheinlich prim“. Das ist natürlich nicht restlos befriedigend. Lieber wäre uns, wenn wir mit Bestimmtheit wüssten, dass n entweder prim oder zusammengesetzt ist. Während dieser Kurstext geschrieben wurde, wurde ein Test [AKS] veröffentlicht (zumindest als Preprint - also Vorabdruck), der alle Anforderungen erfüllt. Er **entscheidet**, ob n eine Primzahl ist, und er ist effizient. Allerdings kommt er nicht an die Geschwindigkeit der probabilistischen Primzahltests heran. Vielleicht werden wir diesen Test

in eine der Folgeversionen einarbeiten.

Sie fragen sich jetzt vielleicht, was Primzahltests mit Kryptografie zu tun haben. Aber bei näherem Hinsehen stellen wir fest, dass in der Kryptografie dauernd Primzahlen benötigt werden. Beim RSA-Verfahren zum Beispiel werden zwei Primzahlen benötigt. Bei vielen anderen Verfahren braucht man einen endlichen Körper, also zum Beispiel eine Primzahl p, um dann $\mathbb{Z}/p\mathbb{Z}$ zu bilden. Diese Primzahlen werden per Zufall ermittelt. Es wird zufällig eine ungerade Zahl ermittelt, und dann wird ein Primzahltest auf diese Zahl losgelassen. Entweder besteht die Zahl den Test und ist selbst eine Primzahl oder der Test wird für $n+2$ wiederholt. Das wird so lange fortgesetzt bis eine Primzahl gefunden ist.

Von den drei Tests, die wir behandeln, ist der erste, der Fermat-Test, der offensichtlichste. Leider gibt es aber natürliche Zahlen, für die dieser Test nicht funktioniert. Diese sogenannten Carmichael-Zahlen muss man sich entweder merken oder einen anderen Test benutzen, zum Beispiel den Rabin-Miller-Test, der einer der am häufigsten benutzten Tests ist. Der dritte Test, den wir vorstellen, der Solovay-Strassen-Test, ist einer ersten probabilistischen Algorithmen überhaupt. Um zu zeigen, dass dieser Test effizient ist, wird unter anderem das quadratische Reziprozitätsgesetz bewiesen. Dieses wichtige Gesetz, das schon von Euler und Legendre formuliert wurde, wurde zuerst von Gauß bewiesen.

Kapitel 6

Effiziente Algorithmen und Wahrscheinlichkeit

6.1 Was ist ein Algorithmus?

Im Text werden an zahlreichen Stellen Algorithmen vorgestellt, um gewisse Probleme zu lösen (zum Beispiel der Euklidische Algorithmus, RSA, Primzahltests (in Kapitel 7), Quadratwurzeln in $\mathbb{F}_p$ finden (in Kapitel 10) und andere). Es stellt sich natürlich dann zuerst einmal die Frage, was ein Algorithmus überhaupt ist. Das ist einfach zu beschreiben: Ein **Algorithmus** ist eine Anleitung, wie eine Aufgabe oder ein Problem in endlicher Zeit zu lösen ist. Es kann also sowohl eine Anleitung für einen Computer sein, wie zwei n-Bit Zahlen zu addieren sind, als auch eine Strickanleitung für einen Pullover – wobei wir uns hier natürlich eher für die Computeralgorithmen interessieren. Die **Laufzeit**, die ein Algorithmus benötigt, um eine Aufgabe zu bewältigen, ist die Anzahl der Schritte, die ausgeführt werden müssen. Dabei wird die Anzahl der Schritte meistens abhängig von der Eingabegröße angegeben.

Sei $n \in \mathbb{N}$ und sei $n = (\alpha_{k-1} \dots \alpha_1 \alpha_0)_2$ die Binärdarstellung von n. Die α_i aus einer Binärdarstellung, die also entweder 0 oder 1 sind, heißen **Bits**. Ist $\alpha_{k-1} = 1$, also die Länge der Binärdarstellung von n minimal, dann gilt

$$\begin{aligned} 2^{k-1} &= 1 \cdot 2^{k-1} + 0 \cdot 2^{k-2} + \ldots + 0 \cdot 2^0 \leq \alpha_{k-1} 2^{k-1} + \alpha_{k-2} 2^{k-2} + \ldots + \alpha_0 2^0 \\ &\leq 1 \cdot 2^{k-1} + 1 \cdot 2^{k-2} + \ldots + 1 \cdot 2^0 = 2^k - 1, \end{aligned}$$

also $2^{k-1} \leq n < 2^k$, oder $k - 1 \leq \log_2 n < k$.

6.1.1 Aufgabe Wieviele Bits haben die Binärdarstellungen von 9, 99 und 999?

6.1.2 Definition Für $\alpha \in \mathbb{R}$ sei $[\alpha]$ die größte ganze Zahl kleiner oder gleich α. Die Zahl $[\alpha]$ wird die „**Gaußklammer** von α“ genannt.

6.1.3 Beispiel Ist $\alpha = \sqrt{2}$, dann ist $[\alpha] = 1$. Ist $\alpha = -\sqrt{2}$, dann ist $[\alpha] = -2$.

Mit den Überlegungen oben folgt, dass die Länge der Binärdarstellung von $n \in \mathbb{N}$ gerade $[\log_2 n]+1$ ist. In der Regel werden wir natürliche Zahlen in Binärdarstellung betrachten. Die Binärdarstellung für eine ganze Zahle n ist so aufgebaut, dass das führende, also erste Bit, Null ist, wenn $n \geq 0$ ist und 1, wenn $n < 0$ ist. Es schließt sich die Binärdarstellung von $|n|$ an.

In der Kryptologie wird nun als Eingabegröße für einen Algorithmus meistens die Anzahl der Bits in der Eingabe benutzt. Als Schritte in einem Algorithmus werden Bitoperationen gezählt, das heißt Berechnungen mit einzelnen Bits (zum Beispiel die Addition zweier Bits). Dabei werden in der Regel nur echte Berechnungen wie zum Beispiel die Addition von zwei Bits gezählt und keine Vergleiche, weil die sehr schnell ausgeführt werden können.

Wir werden im Laufe des Kurses einige Algorithmen vorstellen, häufig in einer vereinfachten Programmiersprache. In dieser Programmiersprache bedeutet $\leftarrow$ eine Zuweisung, das heißt, $i \leftarrow 3$ bedeutet zum Beispiel, dass i von nun an den Wert 3 hat. Die Zuweisung $i \leftarrow i + 1$ bedeutet, dass i von nun an um eins größer ist. Weiterhin gibt es in dieser Programmiersprache **for**-Schleifen und **while**-Schleifen. Betrachten wir zum Beispiel

1. $F \leftarrow 1$

2. **for** $i = 1 \ldots n$ **do**

3. $\quad F \leftarrow iF$

4. **übergebe** F.

Hier wird $n!$ ausgerechnet: Im ersten Schritt wird $F = 1$ gesetzt. Anschließend wird nacheinander für jedes i von 1 bis n die Anweisung der **for**-Schleife ausgeführt. Diese Anweisung (es können natürlich auch mehrere sein) wird durch Einrücken gekennzeichnet. In unserem Fall wird zuerst $F = 1$ gesetzt, dann ist $F = 1 \cdot 1 = 1$, dann $F = 2 \cdot 1 = 2$, und für $i = n$ schließlich $F = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n = n!$. Hinter **übergebe** steht immer das Ergebnis, das der Algorithmus liefert. Das Ganze hätten wir auch mit einer **while**-Schleife machen können:

1. $F \leftarrow 1$ und $i \leftarrow 1$

2. **while** $i \leq n$ **do**

3. $\quad F \leftarrow iF$

4. $i \leftarrow i + 1$

5. übergebe F.

Hier werden zuerst F und i auf 1 gesetzt, und in jedem Durchlauf der **while**-Schleife wird zuerst i mit F multipliziert und dann i um eins erhöht. Der letzte Durchlauf der **while**-Schleife ist der, in dem zuerst F mit n multipliziert wird und dann $i = n + 1$ gesetzt wird. Also wird auch hier $n!$ berechnet.

Desweiteren gibt es noch die **if**-Anweisung, die wir auch ganz kurz vorstellen möchten:

1. $j \leftarrow 1$

2. for $i = 1 \dots 10$ **do**

3. **if** i ist gerade **then** $j \leftarrow j + i$

4. **else** $j \leftarrow j - i$

5. übergebe j.

Was wird hier gemacht? Nun ja, eigentlich ist es ja klar: Wenn i gerade ist, wird i addiert und wenn i ungerade ist, wird i subtrahiert. Das Ergebnis ist also $1 - 1 + 2 - 3 + 4 - 5 + 6 - 7 + 8 - 9 + 10 = 6$. Auch bei den Anweisungen, die dem **then** beziehungsweise **else** folgen, wird durch Einrücken deutlich gemacht, welche Anweisungen dazu gehören.

6.1.4 Beispiel Seien $a, b \in \mathbb{N}$ Zahlen in Binärdarstellung, die addiert werden sollen. Wir nehmen an, dass beide Binärdarstellungen die Länge n haben. Hat eine von beiden weniger Stellen in der Binärdarstellung, wird links mit Nullen aufgefüllt. Mit der Schulmethode funktioniert die Addition so:

$$\begin{array}{cccccccc} & & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ + & & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & & & & \\ \hline & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}$$

Nun werden wir die Schulmethode als Algorithmus formulieren. Dabei werden viele Fallunterscheidungen gemacht. Das wäre in den meisten Programmiersprachen eleganter zu machen als in unserer.

6.1.5 Algorithmus (Addition zweier Binärzahlen)

Eingabe Zwei natürliche Zahlen in Binärdarstellung $a = (\alpha_{n-1} \dots \alpha_0)_2$ und $b = (\beta_{n-1} \dots \beta_0)_2$.

Ausgabe Die Binärdarstellung $(\gamma_n \dots \gamma_0)_2$ von $a + b$.

1. if $\alpha_0 = \beta_0 = 0$ **then** $\gamma_0 \leftarrow 0$ und $a_1 \leftarrow 0$

2. **else if** $\alpha_0 = \beta_0 = 1$ **then** $\gamma_0 \leftarrow 0$ und $a_1 \leftarrow 1$

3. **else** $\gamma_0 \leftarrow 1$ und $a_1 \leftarrow 0$

4. for $i = 1 \ldots n-1$ **do**

5. **if** $\alpha_i = \beta_i = a_i = 0$ **then** $\gamma_i \leftarrow 0$ und $a_{i+1} \leftarrow 0$

6. **else if** ($\alpha_i = \beta_i = 1$ und $a_i = 0$) oder ($\alpha_i = a_i = 1$ und $\beta_i = 0$) oder ($\alpha_i = 0$ und $\beta_i = a_i = 1$)

7. **then** $\gamma_i \leftarrow 0$ und $a_{i+1} \leftarrow 1$

8. **else if** ($\alpha_i = \beta_i = 0$ und $a_i = 1$) oder ($\alpha_i = a_i = 0$ und $\beta_i = 1$) oder ($\alpha_i = 1$ und $\beta_i = a_i = 0$)

9. **then** $\gamma_i \leftarrow 1$ und $a_{i+1} \leftarrow 0$

10. **else** $\gamma_i \leftarrow 1$ und $a_{i+1} \leftarrow 1$

11. if $a_n = 0$ **then** $\gamma_n \leftarrow 0$

12. **else** $\gamma_n \leftarrow 1$.

13. übergebe $(\gamma_n \ldots \gamma_0)_2$.

Zunächst wird die erste Ziffer, also γ_0, im Ergebnis berechnet. Hier kommt noch kein Übertrag ins Spiel, und es werden zwei Zuweisungen gemacht. Nun wird die **for**-Schleife $n-1$ Mal durchlaufen, in der aus α_i, β_i und dem Übertrag a_i die Ziffer γ_i und der Übertrag a_{i+1} berechnet werden. In jeder Schleife wird einer der Schritte 5, 7, 9 oder 10 ausgeführt (Vergleiche werden ja nicht gezählt), und in jedem dieser Schritte werden zwei Zuweisungen gemacht. Außerdem gibt es noch einen Schritt nach der **for**-Schleife. Insgesamt benötigt der Algorithmus also $2 + 2(n-1) + 1 = 2n + 1$ Schritte, um zwei n-Bit Zahlen zu addieren.

6.1.6 Beispiel Seien $a, b \in \mathbb{N}$ Zahlen mit n beziehungsweise m Binärstellen, und sei $n \geq m$. Die Zahlen a und b sollen multipliziert werden. Wieder halten wir uns an das Schulschema:

$$
\begin{array}{cccccccccc}
1 & 1 & 1 & 0 & 1 & \cdot & 1 & 1 & 0 & 1 \\
\hline
 & & & & & & 1 & 1 & 0 & 1 \\
 & & & 1 & 1 & 1 & 0 & 1 & & \\
 & & 1 & 1 & 1 & 0 & 1 & & & \\
 & & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & & & \\
\hline
 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1
\end{array}
$$

Die Multiplikationen mit einem einzelnen Bit spielen hier keine Rolle, denn es wird nur geschaut, ob mit 0 oder 1 multipliziert wird. Bei einer 0 tut man gar nichts, bei einer 1 wird die linke der beiden zu multiplizierenden Zahlen ins Schema geschrieben. Es müssen also nur am Ende höchstens m Zahlen mit höchstens $n+m$ Bits aufaddiert werden. Das erfordert, wie wir in Beispiel 6.1.4 gesehen haben, höchstens $m(2(n+m)+1)$ Schritte, und da $n \geq m$ ist, sind das höchstens $m(4n+1)$ Schritte.

6.1.7 Aufgabe Wieviele Schritte benötigt die Subtraktion einer m-Bit Zahl von einer n-Bit Zahl, wobei $1 \leq m < n$ gilt?

6.2 Die $\mathcal{O}$-Notation

Oft ist die genaue Anzahl der Schritte, die ein Algorithmus benötigt, gar nicht so wichtig, sondern eher die Größenordnung dieser Zahl, abhängig von der Eingabegröße. Deswegen ist die $\mathcal{O}$-Notation sehr nützlich, die hilft, Größenordnungen zu beschreiben.

6.2.1 Definition Seien $f, g : \mathbb{N}_0^r \longrightarrow \mathbb{R}$. Gibt es $B, C \in \mathbb{N}_0$, so dass für alle $(n_1, \ldots, n_r) \in \mathbb{N}_0^r$ mit $n_i \geq B$ für alle $1 \leq i \leq r$ gilt:

1. $f(n_1, \ldots, n_r) > 0$ und $g(n_1, \ldots, n_r) > 0$, und
2. $f(n_1, \ldots, n_r) < C \cdot g(n_1, \ldots, n_r)$,

dann sagen wir, dass f durch g beschränkt ist und schreiben $f = \mathcal{O}(g)$. (Man sagt: „f ist gleich Groß-O von g“.)

6.2.2 Beispiele

1. Sei $f : \mathbb{N}_0 \longrightarrow \mathbb{R}$. Dann bedeutet $f = \mathcal{O}(1)$, dass f – jedenfalls für große $n \in \mathbb{N}_0$ – durch eine Konstante beschränkt ist, denn es gibt $B, C \in \mathbb{N}_0$, so dass für alle $n \geq B$ gilt: $f(n) > 0$ und $f(n) < C \cdot 1$.
2. Sei $f : \mathbb{N}_0 \longrightarrow \mathbb{N}$ definiert durch

   $f(n)$ = Anzahl der Bit-Operationen im Algorithmus aus Beispiel 6.1.4 zur Addition von zwei n-Bit Zahlen.

   Dann gilt $f = \mathcal{O}(n)$ (mit $B = 2$ und $C = 3$ beispielsweise).
3. Sei $f : \mathbb{N}_0^2 \longrightarrow \mathbb{N}$ definiert durch

   $f(n, m)$ = Anzahl der Bit-Operationen im Algorithmus aus Beispiel 6.1.6 zur Multiplikation einer n-Bit Zahl mit einer m-Bit Zahl.

Dann gilt $f(n,m) = \mathcal{O}(nm)$.

6.2.3 Aufgabe Welches sind bei (3) die zugehörigen Konstanten B und C?

Die $\mathcal{O}$-Notation ist sehr hilfreich, um das Verhalten von Algorithmen für große Eingaben abzuschätzen. Je nachdem, wie groß die Konstanten B und C aus Definition 6.2.1 gewählt sind, kann es sein, dass zwei Algorithmen zwar für kleine Eingabewerte ähnliche Laufzeiten haben, sich aber asymptotisch, das heißt für sehr große Eingaben, deutlich unterscheiden.

So gibt es zum Beispiel für die Multiplikation von zwei n-Bit Zahlen asymptotisch schnellere Verfahren als die Schulmethode, die ja die Größenordnung $\mathcal{O}(n^2)$ hat. Die Methode von Schönhage und Strassen aus dem Jahr 1971 benötigt nur $\mathcal{O}(n \log n \log(\log n))$ Operationen. Das macht asymptotisch einen ganz schönen Unterschied, aber für kleine Eingaben (der genaue Wert hängt vom Computer und vom Programmierer ab) ist trotzdem die Schulmethode vorzuziehen.

Normalerweise werden solche Algorithmen als effizient bezeichnet, bei denen die Anzahl der Bitoperationen auch bei großen Eingaben durch ein Polynom beschränkt ist:

6.2.4 Definition

1. Ein Algorithmus zur Durchführung einer Rechnung mit Binärzahlen $n_1, \ldots, n_r$, deren Bitlänge $k_1, \ldots, k_r$ ist, heißt **polynomial**, falls es $d_1, \ldots, d_r \in \mathbb{N}_0$ gibt, so dass die Anzahl der Bitoperationen, die zur Durchführung benötigt werden, $\mathcal{O}(k_1^{d_1} \cdots k_r^{d_r})$ ist.
2. Ein Algorithmus heißt **effizient**, wenn er polynomial ist.

Polynomiale Algorithmen gibt es zum Beispiel für die Grundrechenarten über $\mathbb{Z}$ und auch über endlichen Körpern, für die Division mit Rest in $\mathbb{Z}$ und für die Reduktion modulo m für jedes $m \in \mathbb{N}$. Andererseits gibt es Probleme, bei denen es entweder bewiesen ist, dass es keine effizienten Algorithmen gibt, um sie zu lösen, oder bei denen vermutet wird, dass es keine effizienten Algorithmen gibt, um sie zu lösen. Ein Beispiel für die letzte Kategorie ist das Faktorisieren von Zahlen in Primfaktoren.

6.2.5 Aufgabe Sei $p \in \mathbb{R}[T]$ mit $p = \sum_{i=0}^{d} a_i T^i$ und $a_d > 0$. Zeigen Sie: $p = \mathcal{O}(T^d)$.

6.3 Division mit Rest

Beim Rechnen in Restklassenringen und endlichen Körpern und auch bei vielen anderen Anwendungen, wie zum Beispiel beim Euklidischen Algorithmus, wird die Division mit Rest (über $\mathbb{Z}$) benötigt. Mit der Schulmethode funktioniert die Division mit Rest folgendermaßen:

$$
\begin{array}{cccccccccccccc}
 & 1 & 0 & 0 & 1 & 1 & 0 & : & 1 & 0 & 1 & = & 1 & 1 & 1 \\
- & & 1 & 0 & 1 & & & & & & & & & & \\
\cline{2-5}
 & & 1 & 0 & 0 & 1 & & & & & & & & & \\
- & & & 1 & 0 & 1 & & & & & & & & & \\
\cline{3-6}
 & & & 1 & 0 & 0 & 0 & & & & & & & & \\
- & & & & 1 & 0 & 1 & & & & & & & & \\
\cline{4-6}
 & & & & & 1 & 1 & & & & & & & &
\end{array}
$$

Als Algorithmus sieht das so aus:

6.3.1 Algorithmus (Division mit Rest)

Eingabe $a = (\alpha_{n-1} \dots \alpha_0)_2$ und $b = (\beta_{m-1} \dots \beta_0)_2$ mit $m < n$.

Ausgabe Die Binärdarstellungen von $q, r \in \mathbb{N}$ mit $a = qb + r$ und $r < b$.

1. **for** $i = n - 1 \dots 0$ **do**

2. **if** $(\alpha_{n-1} \dots \alpha_i)_2 \geq (\beta_{m-1} \dots \beta_0)_2$

3. **then** $\gamma_i \leftarrow 1$

4. $(\alpha_{n-1} \dots \alpha_i)_2 \leftarrow (\alpha_{n-1} \dots \alpha_i)_2 - (\beta_{m-1} \dots \beta_0)_2$

5. **else** $\gamma_i \leftarrow 0$

6. **übergebe** $q = (\gamma_{n-1} \dots \gamma_0)_2$ und $r = (\alpha_{n-1} \dots \alpha_0)_2$.

Machen wir zunächst ein kleines Beispiel:

6.3.2 Beispiel **Eingabe** $a = (1101)_2$ und $b = (10)_2$.

1. $i = 3$.

2. $(1)_2 < (10)_2$, also

5. $\gamma_3 \leftarrow 0$.

1. $i = 2$.

2. $(11)_2 \geq (10)_2$, also

3. $\gamma_2 \leftarrow 1$

4. $(\alpha_3\alpha_2) \leftarrow (11)_2 - (10)_2 = (01)_2$.

1. $i = 1$.

2. $(010)_2 \geq (10)_2$, also

3. $\gamma_1 \leftarrow 1$

4. $(\alpha_3\alpha_2\alpha_1)_2 \leftarrow (010)_2 - (10)_2 = (000)_2$.

1. $i = 0$.

2. $(0001)_2 < (10)_2$, also

3. $\gamma_0 \leftarrow 0$.

6. Das Ergebnis ist $q = (0110)_2 = (110)_2$ und $r = (0001)_2 = (1)_2$.

Jedes Bit von a wird genau einmal angesehen. Entweder wird in Schritt 3 eine Zuweisung gemacht, oder es werden die Schritte 4 und 5 ausgeführt, also eine Zuweisung und eine Subtraktion einer m-Bit Zahl von einer höchstens n-Bit Zahl. Wie Sie in Aufgabe 6.1.7 gezeigt haben, lässt sich jede einzelne Subtraktion in der Zeit $\mathcal{O}(n)$ durchführen. Da höchstens n Subtraktionen durchgeführt werden, benötigt die Division mit Rest also $\mathcal{O}(n^2)$ Schritte und ist damit effizient.

6.3.3 Aufgabe Bis jetzt haben wir die Division mit Rest nur für natürliche Zahlen betrachtet. Was ist für ganze Zahlen zu beachten? Oder mit anderen Worten, wie kann man für $a, b \in \mathbb{Z}$ das Ergebnis der Division von a mit Rest durch b beschreiben, wenn man das der Division von $|a|$ mit Rest durch $|b|$ kennt?

6.4 Wiederholtes Quadrieren

In einigen Kryptosystemen, zum Beispiel RSA, ist es nötig, $b^n \bmod m$ für große $n, m \in \mathbb{N}$ auszurechnen. Geht man naiv vor, dann berechnet man zuerst $b^2 \bmod m, b^3 \bmod m, \ldots, b^{n-1} \bmod m, b^n \bmod m$. Man benötigt also $(n-1)$ Multiplikationen. Die Eingaben b, n und m haben die Bitlängen $[\log_2 b] + 1$, $[\log_2 n] + 1$ und $[\log_2 m] + 1$, die $(n-1)$-fache Multiplikation liefert also keinen effizienten Algorithmus mehr, denn $(n-1)$ ist in der Größenordnung von $2^{[\log n]+1}$.

Also muss man geschickter vorgehen. Der Algorithmus, der nun beschrieben wird, heißt „Wiederholter Quadrierungsalgorithmus“ oder „Wiederholtes Quadrieren“.

Die Idee ist, dass man nicht alle Potenzen von b berechnet, sondern im Wesentlichen die Potenzen $b \bmod m, b^2 \bmod m, b^4 \bmod m, b^8 \bmod m$ und so weiter.

Zunächst erinnern wir daran, dass es geschickt ist, in jedem Multiplikationsschritt sofort modulo m zu reduzieren (2.2.6). Auf diese Weise kommen immer nur Zahlen vor, die kleiner als m^2 sind.

Um nun also $b^n \bmod m$ für $b, n, m \in \mathbb{N}$ und $b < m$ zu berechnen, wird $n = (\alpha_k \dots \alpha_0)_2$ als Binärzahl geschrieben. Dann ist

$$\begin{aligned} b^n \bmod m &= b^{\alpha_0 2^0 + \alpha_1 2^1 + \dots + \alpha_k 2^k} \bmod m \\ &= b^{\alpha_0 2^0} \cdot b^{\alpha_1 2^1} \cdot \dots \cdot b^{\alpha_k 2^k} \bmod m. \end{aligned}$$

6.4.1 Algorithmus (Wiederholtes Quadrieren)

Eingabe $b, n, m \in \mathbb{N}$ mit $b < m$, wobei $n = (\alpha_k \dots \alpha_0)_2$ in Binärdarstellung ist.

Ausgabe $b^n \bmod m$.

1. $a_0 \leftarrow 1$, $b_0 \leftarrow b$.

2. **for** $i = 0 \dots k$ **do**

3. **if** $\alpha_i = 1$ **then** $a_{i+1} \leftarrow a_i b_i \bmod m$

4. **else** $a_{i+1} \leftarrow a_i \bmod m$.

5. $b_{i+1} \leftarrow b_i^2 \bmod m$.

6. **übergebe** a_{k+1}.

6.4.2 Lemma In Algorithmus 6.4.1 gilt für alle $0 \le i \le k$:

$$a_{i+1} = b^{\alpha_0 2^0 + \dots + \alpha_i 2^i} \bmod m \text{ und } b_{i+1} = b^{2^{i+1}} \bmod m.$$

Beweis: Mit Induktion nach i: Sei $i = 0$. Es gilt

$$b_1 \equiv b_0^2 \equiv b^2 \equiv b^{2^1} (\mathrm{mod} m)$$

und

$$\begin{aligned} a_1 &\equiv \left\{ \begin{array}{ll} b, & \text{falls } \alpha_0 = 1 \\ 1, & \text{falls } \alpha_0 = 0 \end{array} \right\} \\ &\equiv b^{\alpha_0 2^0} (\mathrm{mod} m). \end{aligned}$$

Sei nun $0 \le i \le k-1$, und es gelte

$$a_{i+1} = b^{\alpha_0 2^0 + \dots + \alpha_i 2^i} \bmod m \text{ und } b_{i+1} = b^{2^{i+1}} \bmod m.$$

Dann folgt:

$$\begin{aligned} a_{i+2} &\equiv \left\{ \begin{array}{ll} a_{i+1}b_{i+1}, & \text{falls } \alpha_{i+1}=1 \\ a_{i+1}, & \text{falls } \alpha_{i+1}=0 \end{array} \right\} \\ &\equiv \left\{ \begin{array}{ll} b^{\alpha_0 2^0+\ldots+\alpha_i 2^i}\cdot b^{2^{i+1}}, & \text{falls } \alpha_{i+1}=1 \\ b^{\alpha_0 2^0+\ldots+\alpha_i 2^i}\cdot b^{0}, & \text{falls } \alpha_{i+1}=0 \end{array} \right\} \\ &\equiv \left\{ \begin{array}{ll} b^{\alpha_0 2^0+\ldots+\alpha_i 2^i+1\cdot 2^{i+1}}, & \text{falls } \alpha_{i+1}=1 \\ b^{\alpha_0 2^0+\ldots+\alpha_i 2^i+0\cdot 2^{i+1}}, & \text{falls } \alpha_{i+1}=0 \end{array} \right\} \\ &\equiv b^{\alpha_0 2^0+\ldots+\alpha_{i+1}2^{i+1}} (\mathrm{mod} m). \end{aligned}$$

Außerdem folgt:

$$b_{i+2} \equiv b_{i+1}^2 \equiv (b^{2^{i+1}})^2 \equiv b^{2^{i+2}} (\mathrm{mod} m).$$

□

Mit dem Lemma gilt also

$$a_{k+1} \equiv b^{\alpha_0 2^0+\ldots+\alpha_k 2^k} \equiv b^n (\mathrm{mod} m).$$

Das heißt, b^n mod m lässt sich in $k+1$ Schritten berechnen, wobei $k+1$ die Bitlänge von n ist. In jedem Schritt werden zwei Zahlen der Größe höchstens m (also mit einer Bitlänge höchstens so groß wie die von m) multipliziert. Anschließend muss das Ergebnis noch modulo m reduziert werden. Für die Multiplikation und die Reduktion modulo m, die ja nichts anderes als eine Division mit Rest durch m ist, gibt es effiziente Algorithmen, also ist das Wiederholte Quadrieren ebenfalls ein effizienter Algorithmus.

6.4.3 Aufgabe Berechnen Sie 2^{14} mod 7 durch Wiederholtes Quadrieren.

6.5 Der Euklidische Algorithmus

In diesem Abschnitt soll plausibel gemacht werden, dass der Euklidische Algorithmus effizient ist. Erinnern wir uns also an Abschnitt 2.4:

Gegeben sind $a, b \in \mathbb{Z}$. Ohne Einschränkung können wir annehmen, dass $b \geq a > 0$ gilt, denn $\mathrm{ggT}(a,b) = \mathrm{ggT}(b,a) = \mathrm{ggT}(|a|,|b|)$. Beim Euklidischen Algorithmus

werden nun eine Reihe von Divisionen mit Rest durchgeführt:

$$\begin{aligned} b &= q_1 a + r_2 \\ a &= q_2 r_2 + r_3 \\ r_2 &= q_3 r_3 + r_4 \\ &\vdots \\ r_{n-1} &= q_n r_n. \end{aligned}$$

Setzen wir $b = r_0$ und $a = r_1$, dann gelten folgende Bedingungen für die r_i und q_i: Für $1 \leq i < n$ ist $0 < r_{i+1} < r_i$. Außerdem ist $q_i \geq 1$ für $1 \leq i \leq n$. Wir wollen nun die Länge n der Folge von Resten und damit die Anzahl der Divisionen mit Rest im Euklidischen Algorithmus abschätzen. Dazu setzen wir noch $r_{n+1} = 0$. Dann gilt für $1 \leq i < n$:

$$\begin{aligned} r_i &= q_{i+1} r_{i+1} + r_{i+2} \geq r_{i+1} + r_{i+2}, \text{ denn } q_{i+1} \geq 1 \\ &> 2r_{i+2}, \text{ denn } r_{i+1} > r_{i+2}. \end{aligned}$$

Also gilt $r_i > 2r_{i+2}$ für $1 \leq i < n$ und damit auch

$$\prod_{i=1}^{n-2} r_i > 2^{n-2} \prod_{i=1}^{n-2} r_{i+2} = 2^{n-2} \prod_{i=3}^{n} r_i.$$

Wir teilen durch $\prod_{i=3}^{n-2} r_i$ und erhalten

$$r_1 r_2 > 2^{n-2} r_{n-1} r_n > 2^{n-2},$$

denn $r_{n-1} > r_n \geq 1$. Da $r_1 > r_2$ und $r_1 = a$ gilt, folgt $r_1^2 = a^2 > 2^{n-2}$. Es folgt $2 \log_2 a > n - 2$, oder $n < 2(\log_2 a + 1)$. Wir sehen also, dass die Länge n der Folge von Resten im Euklidischen Algorithmus zu a und b (und damit die Anzahl der Divisionen mit Rest) beschränkt ist durch $2(\log_2 a + 1)$, das Doppelte der Bitlänge von a. Bei jeder einzelnen Division mit Rest haben die vorkommenden Zahlen höchstens die Größe von b. Also haben wir gezeigt:

6.5.1 Proposition Der Euklidische Algorithmus aus 2.4.7 ist ein effizienter Algorithmus.

Die Schranke für n kann übrigens noch verbessert werden. Außerdem kann man zeigen, dass auch der erweiterte Euklidische Algorithmus effizient ist.

6.6 Grundlagen der Wahrscheinlichkeitsrechnung

Die Beispiele für Algorithmen, die bisher vorkamen, sind alle von der Form, dass für dieselbe Eingabe immer dieselben Schritte ausgeführt werden. Solche Algorithmen werden „deterministisch“ genannt. Im Gegensatz dazu stehen die „probabilistischen“ Algorithmen. Bei der Ausführung eines solchen Algorithmus' werden zufällig Primzahlen oder ganze Zahlen oder Ähnliches ausgewählt, so dass die Schritte, die ausgeführt werden, sich bei zwei Durchläufen mit derselben Eingabe unterscheiden können. Manchmal unterscheiden sich sogar die Ergebnisse, denn bei den Algorithmen, die wir in dieser Kurseinheit kennenlernen werden, ist es erlaubt, dass „... hat wahrscheinlich diese Eigenschaft“ als Ergebnis herauskommt. Ebenso können sich die Laufzeiten unterscheiden.

Bevor wir aber probabilistische Algorithmen kennenlernen werden, führen wir ganz kurz und nur auf das Notwendigste beschränkt in die Grundlagen der Wahrscheinlichkeitstheorie ein. Dabei halten wir uns in der Darstellung an [Bu].

Sei S eine endliche, nicht-leere Menge. Sie wird **Ergebnismenge** genannt. Ihre Elemente – oder besser gesagt die einelementigen Teilmengen von S – heißen **Elementarereignisse**. Die Ergebnismenge braucht man, um die möglichen Ergebnisse von Experimenten zu modellieren.

6.6.1 Beispiel Beim Würfeln ist $S = \{1, 2, 3, 4, 5, 6\}$, die Elementarereignisse sind $\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}$.

Ein **Ereignis** ist eine Teilmenge von S. Das **sichere Ereignis** ist S selbst, und das **leere Ereignis** ist die leere Menge. Die Menge aller Ereignisse ist $\mathcal{P}(S)$, die Potenzmenge von S.

6.6.2 Beispiel Das Ereignis, eine gerade Zahl zu würfeln, ist $\{2, 4, 6\}$.

6.6.3 Definition Eine **Wahrscheinlichkeitsverteilung** auf S ist eine Abbildung P, die jedem Ereignis eine reelle Zahl zuordnet, also $P : \mathcal{P}(S) \longrightarrow \mathbb{R}$, und die folgenden Eigenschaften erfüllt:

(i) $P(A) \geq 0$ für alle $A \subseteq S$.

(ii) $P(S) = 1$.

(iii) $P(A \cup B) = P(A) + P(B)$, falls $A \cap B = \emptyset$ ist.

6.6.4 Bemerkungen 1. $P(\emptyset) = 0$, denn angenommen, $P(\emptyset) > 0$, dann wäre $P(S) = P(S) + P(\emptyset) > 1$ nach Definition 6.6.3 (iii), denn $S \cap \emptyset = \emptyset$. Dies ist jedoch ein Widerspruch zu Definition 6.6.3 (ii).

2. Ist $A \subseteq B \subseteq S$, dann ist $P(A) \leq P(B)$, denn sei $B = A \cup C$ mit $A \cap C = \emptyset$, dann ist $P(B) = P(A) + P(C)$ nach Definition 6.6.3 (iii), und $P(C) \geq 0$ nach Definition 6.6.3 (i). Also folgt $P(B) \geq P(A)$.

3. Es gilt $0 \leq P(A) \leq 1$ für alle $A \subseteq S$, denn $0 \leq P(A)$ gilt nach Definition 6.6.3 (i), und $P(A) \leq P(S) = 1$ gilt nach (ii) und 2.

4. $P(S \setminus A) = 1 - P(A)$ für alle $A \subseteq S$, denn $1 = P(S) = P(S \setminus A) + P(A)$ nach Definition 6.6.3 (iii), also $P(S \setminus A) = 1 - P(A)$.

5. $P(A) = \sum_{a \in A} P(\{a\})$ für alle $A \subseteq S$, denn da A die disjunkte Vereinigung der Mengen $\{a\}$ mit $a \in A$ ist, folgt die Behauptung aus Definition 6.6.3 (iii) mit Induktion.

6. Aus 5. folgt, dass es reicht, die Wahrscheinlichkeitsverteilung auf den Elementarereignissen zu definieren.

6.6.5 Beispiel Die zum Würfeln gehörende Wahrscheinlichkeitsverteilung ordnet jedem Elementarereignis die Wahrscheinlichkeit $\frac{1}{6}$ zu. Die Wahrscheinlichkeit, eine gerade Zahl zu würfeln, ist dann $P(\{2,4,6\}) = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2}$.

6.6.6 Aufgabe Es wird zufällig eine Zahl zwischen 1 und 1000 gezogen. Jede Zahl ist gleich wahrscheinlich. Wie groß ist die Wahrscheinlichkeit, eine Quadratzahl zu ziehen?

6.6.7 Definition Sei S eine Ergebnismenge und P eine Wahrscheinlichkeitsverteilung auf S. Seien $A, B \subseteq S$ Ereignisse und sei $P(B) \neq 0$. Dann ist die **bedingte Wahrscheinlichkeit** $P(A|B)$, also die Wahrscheinlichkeit von A unter der Bedingung B, definiert als:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}.$$

Man kann sich das so vorstellen: Man weiß schon, dass B eingetreten ist und möchte unter dieser Bedingung die Wahrscheinlichkeit ausrechnen, dass A eintritt.

Nehmen wir beispielsweise an, dass die Wahrscheinlichkeit, beim Münzwurf Kopf oder Zahl zu werfen, jeweils genau $\frac{1}{2}$ ist. Wenn man nun eine Münze zweimal wirft, dann ist die zugehörige Egebnismenge $\{KK, ZZ, KZ, ZK\}$, wobei KK für zweimal Kopf, ZZ für zweimal Zahl, KZ für erst Kopf und dann Zahl und ZK für erst Zahl und dann Kopf steht. Die Wahrscheinlichkeit für jedes Elementarereignis ist $\frac{1}{4}$. Also ist insbesondere die Wahrscheinlichkeit, dass man zweimal hintereinander Zahl wirft, $\frac{1}{4}$. Das Ereignis, im zweiten Wurf Zahl zu werfen, ist $A = \{ZZ, KZ\}$. Wenn man aber schon weiß, dass der erste Wurf Zahl ist, dann ist die bedingte

Wahrscheinlichkeit, dass auch der zweite Wurf Zahl ist:

$$P(\{ZZ, KZ\}|\{ZK, ZZ\}) = \frac{P(\{ZZ\})}{P(\{ZK, ZZ\})} = \frac{\frac{1}{4}}{\frac{1}{2}} = \frac{1}{2}.$$

Man sieht also, dass die Wahrscheinlichkeit, Zahl zu werfen, nicht davon abhängt, ob man vorher auch schon Zahl geworfen hat.

6.6.8 Definition Zwei Ereignisse $A, B \subseteq S$ heißen **unabhängig**, wenn $P(A \cap B) = P(A)P(B)$ ist.

6.6.9 Beispiel Im Beispiel oben sind die Ereignisse $A = \{ZZ, KZ\}$, dass der zweite Wurf Zahl ist, und $B = \{ZZ, ZK\}$, dass der erste Wurf Zahl ist, unabhängig, denn es gilt:

$$\frac{1}{4} = P(A \cap B) = P(\{ZZ\}) = P(A)P(B) = \frac{1}{2} \cdot \frac{1}{2}.$$

6.6.10 Lemma Zwei Ereignisse $A, B \subseteq S$, wobei $P(B) \neq 0$ gilt, sind genau dann unabhängig, wenn $P(A|B) = P(A)$ gilt.

Beweis: Seien zunächst A und B unabhängig. Dann ist

$$\begin{aligned} P(A|B) &= \frac{P(A \cap B)}{P(B)} = \frac{P(A)P(B)}{P(B)}, \text{ denn } A \text{ und } B \text{ sind unabhängig} \\ &= P(A). \end{aligned}$$

Nun gelte $P(A|B) = P(A)$. Dann ist $P(A \cap B) = P(A|B)P(B) = P(A)P(B)$. □

Diese Grundlagen der Wahrscheinlichkeitstheorie sollten ausreichen, um die probabilistischen Algorithmen und deren Analyse zu verstehen. Was ein probabilistischer Algorithmus genau ist, schauen wir uns einfach in den konkreten Beispielen an.

6.6.11 Aufgabe Es wird mit zwei Würfeln gewürfelt. Wie groß ist die Wahrscheinlichkeit dafür, dass beide Würfel ein verschiedenes Ergebnis zeigen unter der Bedingung, dass die Summe der Ergebnisse gerade ist?

Lösungen der Aufgaben

Lösungen der Aufgaben in Kapitel 6

Aufgabe 6.1.1 Gesucht sind die Längen der Binärdarstellungen von 9, 99 und 999.

Es gilt

$$9 = 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0,$$

also $9 = (1001)_2$, und die Länge der Binärdarstellung ist 4. Das hätten wir natürlich auch direkt ausrechnen können: Sei k die Länge der Binärdarstellung von 9, dann gilt $k - 1 \leq \log_2 9 < k$, also $k = 4$.

Weiter ist für $n = 99$ dann $k - 1 \leq \log_2 99 < k$, also ist die Länge k der Binärdarstellung von 99 gleich 7. Zur Sicherheit rechnen wir nach:

$$99 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0,$$

also $99 = (1100011)_2$.

Nun zu $n = 999$. Es gilt $k - 1 \leq \log_2 999 < k$, also ist die Länge k der Binärdarstellung von 999 gleich 10. Die Probe:

$$999 = 1 \cdot 2^9 + 1 \cdot 2^8 + 1 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0,$$

also $999 = (1111100111)_2$. □

Aufgabe 6.1.7 Gefragt ist nach der Anzahl der Schritte, die benötigt werden, um eine m-Bit Zahl von einer n-Bit Zahl zu subtrahieren, wobei $1 \leq m < n$ gilt.

Wir gehen wieder nach dem Schulverfahren vor:

$$\begin{array}{cccccc} & 1 & 1 & 1 & 0 & 1 \\ - & & 1 & 0 & 1 & 1 \\ & & & {\scriptstyle 1} & & \\ \hline & 1 & 0 & 0 & 1 & 0 \end{array}$$

Wie bei der Addition wird jedes Bit der oberen Zahl einmal angesehen, und dann wird eine Fallunterscheidung gemacht, je nachdem, wie die einzelnen Bits aussehen und ob es Überträge gibt. Außer beim ersten Bit werden immer das Ergebnisbit und der Übertrag betrachtet. Insgesamt werden also $2n-1$ Schritte gemacht. □

Aufgabe 6.2.3 Sei $f : \mathbb{N}_0^2 \longrightarrow \mathbb{N}$ definiert durch

$$f(n,m) \;=\; \text{Anzahl der Bit-Operationen im Algorithmus aus Beispiel 6.1.6 zur Multiplikation einer } n\text{-Bit Zahl mit einer } m\text{-Bit Zahl.}$$

Dann gilt $f(n,m) = \mathcal{O}(nm)$. Gefragt ist nun nach den Konstanten B und C.

Für alle $n, m \in \mathbb{N}$ gilt $f(n,m) > 0$ und $nm > 0$. Wir können also $B = 1$ setzen. Außerdem gilt für alle $n, m \in \mathbb{N}$

$$f(n,m) \leq m(4n+1) = 4mn + m \leq 4mn + mn = 5mn.$$

Setze also $C = 5$. □

Aufgabe 6.2.5 Sei $p \in \mathbb{R}[T]$ mit $p = \sum_{i=0}^{d} a_i T^i$ und $a_d > 0$.

Behauptung $p = \mathcal{O}(T^d)$.

Beweis: Jetzt brauchen wir ein kleines bisschen Analysis: Da $a_d > 0$ gilt, folgt $\lim_{n\to\infty} p(n) = \infty$. Also gibt es ein $B_1 \in \mathbb{N}$ mit $p(n) > 0$ für alle $n \geq B_1$. Außerdem gilt $n^d > 0$ für $n \geq B_1$. Es gilt

$$\lim_{n\to\infty} \frac{p(n)}{n^d} = \lim_{n\to\infty} \frac{\sum_{i=0}^{d} a_i n^i}{n^d} = \lim_{n\to\infty} \sum_{i=0}^{d} a_i \frac{n^i}{n^d} = a_d + \sum_{i=0}^{d-1} \lim_{n\to\infty} a_i \frac{1}{n^{d-i}} = a_d.$$

Da also $\lim_{n\to\infty} \frac{p(n)}{n^d} = a_d$ gilt, gibt es ein $B_2 \in \mathbb{N}$ mit

$$\begin{aligned}
&\left|\frac{p(n)}{n^d} - a_d\right| < 1 \text{ für alle } n \geq B_2 \\
\Rightarrow\;& -1 < \frac{p(n)}{n^d} - a_d < 1 \text{ für alle } n \geq B_2 \\
\Rightarrow\;& -1 + a_d < \frac{p(n)}{n^d} < 1 + a_d \text{ für alle } n \geq B_2 \\
\Rightarrow\;& p(n) < (1+a_d)n^d \text{ für alle } n \geq B_2.
\end{aligned}$$

Die Behauptung folgt also mit $B = \max\{B_1, B_2\}$ und $C = (1 + a_d)$. □

Aufgabe 6.3.3 Wie kann man das Ergebnis der Division von a mit Rest durch b beschreiben, wenn man das der Division von $|a|$ mit Rest durch $|b|$ kennt?

Es gelte $|a| = q|b| + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < |b|$. Wir machen eine Fallunterscheidung.

Gilt $a, b \geq 0$, dann ändert sich nichts bei der Division mit Rest.

Gilt $a, b < 0$, dann ist also $-a = q(-b) + r$ und damit $a = qb - r$. Ist $r = 0$, dann ist dies schon die Division mit Rest. Ist $r > 0$, dann folgt $a = (q+1)b + (-b - r)$, und $-b - r = |b| - r$, also $0 < |b| - r < |b|$.

Gilt $a \geq 0$ und $b < 0$, dann ist $a = q(-b) + r$, also $a = (-q)b + r$, und dies ist die Division mit Rest.

Gilt $a < 0$ und $b \geq 0$, dann ist $-a = qb + r$, also $a = (-q)b - r$. Ist $r = 0$, dann ist dies die Division mit Rest. Ist $r > 0$, dann ist $a = (-q-1)b + (b - r)$ und $0 < b - r < b$. □

Aufgabe 6.4.3 Es soll $2^{14} \bmod 7$ mit Wiederholtem Quadrieren berechnet werden.

Eingabe $b = 2$, $m = 7$ und $n = 14 = (1110)_2$.

1. $a_0 \leftarrow 1$ und $b_0 \leftarrow b = 2$.

2. $i = 0$.

3. $\alpha_0 = 0$, also

4. $a_1 \leftarrow a_0 = 1$.

5. $b_1 \leftarrow b_0^2 \bmod 7 = 4$.

2. $i = 1$.

3. $\alpha_1 = 1$, also $a_2 \leftarrow a_1 b_1 \bmod 7 = 4$.

5. $b_2 \leftarrow b_1^2 \bmod 7 = 2$.

2. $i = 2$.

3. $\alpha_2 = 1$, also $a_3 \leftarrow a_2 b_2 \bmod 7 = 1$.

5. $b_3 \leftarrow b_2^2 \bmod 7 = 4$.

2. $i = 3$.

3. $\alpha_3 = 1$, also $a_4 \leftarrow a_3 b_3 \bmod 7 = 4$.

5. $b_4 \leftarrow b_3^2 \bmod 7 = 2$.

6. Das Ergebnis ist $a_4 = 4$.

(Natürlich hätte man das in diesem Fall mit dem kleinen Fermat schneller berechnen können: $2^6 \equiv 1(\text{mod}7)$, also auch $2^{12} \equiv 1(\text{mod}7)$. Es folgt $2^{14} \equiv 2^2 \equiv 4(\text{mod}7)$.) □

Aufgabe 6.6.6 Es wird zufällig eine Zahl zwischen 1 und 1000 gezogen. Jede Zahl ist gleich wahrscheinlich. Wie groß ist die Wahrscheinlichkeit, eine Quadratzahl zu ziehen?

Behauptung Die Wahrscheinlichkeit ist $\frac{31}{1000}$.

Beweis: Die Ergebnismenge ist $S = \{1, \ldots, 1000\}$. Es gilt $P(\{i\}) = \frac{1}{1000}$ für alle $i \in S$. Die gesuchte Menge ist $\{1, 4, 9, 16, \ldots\}$. Wieviele Quadratzahlen ≤ 1000 gibt es? Es gilt $[\sqrt{1000}] = 31$, also gibt es 31 Quadratzahlen ≤ 1000, und $P(\{1, 4, 9, 16, \ldots, 961\}) = \frac{31}{1000}$. □

Aufgabe 6.6.11 Es wird mit zwei Würfeln gewürfelt. Wie groß ist die Wahrscheinlichkeit dafür, dass beide Würfel ein verschiedenes Ergebnis zeigen unter der Bedingung, dass die Summe der Ergebnisse gerade ist?

Behauptung Die Wahrscheinlichkeit ist $\frac{2}{3}$.

Beweis: Die Ergebnismenge ist $S = \{11, 12, 13, \ldots, 16, 21, 22, \ldots, 66\}$, wobei zum Beispiel 23 bedeutet, dass erst mit dem ersten Würfel eine 2 und dann mit dem zweiten eine 3 gewürfelt wird. Die Menge S hat 36 Elemente, und jedes Elementarereignis hat die Wahrscheinlichkeit $\frac{1}{36}$. Sei

$$\begin{aligned} A &= \{\text{alle Ereignisse, so dass beide Würfel ein verschiedenes Ergebnis zeigen}\} \\ B &= \{\text{alle Ereignisse, so dass die Summe der Ergebnisse gerade ist}\}. \end{aligned}$$

Zunächst berechnen wir $P(B)$. Es gibt folgende Möglichkeiten dafür, dass die Summe gerade ist:

$$\begin{aligned} \text{Summe} = 2 &: 11 \\ 4 &: 13, 22, 31 \\ 6 &: 15, 24, 33, 42, 51 \\ 8 &: 26, 35, 44, 53, 62 \\ 10 &: 46, 55, 64 \\ 12 &: 66. \end{aligned}$$

Also liegen 18 Ereignisse in B, und es gilt $P(B) = \frac{18}{36} = \frac{1}{2}$. Bei $A \cap B$ fallen alle Ereignisse weg, bei denen beide Würfel das Gleiche zeigen. Dies sind 6 Ereignisse.

Also $P(A \cap B) = \frac{12}{36} = \frac{1}{3}$. Damit gilt

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{\frac{1}{3}}{\frac{1}{2}} = \frac{2}{3}.$$

Übrigens gilt $P(A) = \frac{30}{36} = \frac{5}{6}$, also sind A und B nicht unabhängig. □

Kapitel 7

Drei Primzahltests

7.1 Der Fermat-Test

Bei vielen Kryptosystemen werden eine - oder sogar mehrere - Primzahlen benötigt, die zufällig gewählt sein sollen. Dafür wird in der Praxis zunächst zufällig eine ungerade Zahl n_0 gewählt. Das soll so geschehen, dass jede Zahl in der Ergebnismenge gleich wahrscheinlich ist, und die Wahl einer Zufallszahl soll unabhängig von der Wahl der vorherigen Zufallszahl sein. In der Praxis stellen diese Forderungen ein Riesenproblem dar, weil man „echten“ Zufall mit dem Rechner nicht simulieren kann. Meistens reichen jedoch sogenannte Pseudozufallszahlen aus.

Hat man nun also n_0, testet man, ob $n_0, n_0 + 2, n_0 + 4, \ldots$ eine Primzahl ist und nimmt die kleinste Primzahl, die größer oder gleich n_0 ist. Benötigt wird also ein Primzahltest. Das ist ein Test, dem eine Zahl $n \in \mathbb{N}$ unterworfen wird. Fällt n bei diesem Test durch, dann ist n zusammengesetzt (das heißt keine Primzahl), die Faktoren von n sind damit allerdings noch nicht bekannt. Besteht n den Test, dann ist zwar noch nicht bewiesen, dass n eine Primzahl ist, aber die Wahrscheinlichkeit, dass n keine ist, ist äußerst gering, wenn n viele Primzahltests besteht. Ganz aktuell ist ein effizienter Test, der **beweist**, dass n prim oder zusammengesetzt ist (siehe [AKS]). Diesen Test werden wir hier aber nicht vorstellen. Dafür werden wir sehen, dass die probabilistischen Tests, die hier behandelt werden, für die Praxis vollkommen ausreichen.

Der erste Test, der behandelt werden soll, ist der Fermat-Test. Zur Erinnerung wiederholen wir Fermats kleinen Satz 4.4.12:

7.1.1 Satz Sei n eine Primzahl und $b \in \mathbb{N}$ mit $\mathrm{ggT}(b, n) = 1$. Dann gilt $b^{n-1} \bmod n = 1$.

Am schönsten wäre es, wenn auch die Umkehrung des kleinen Satzes von Fermat gelten würde, wenn also $b^{n-1} \bmod n = 1$ für ein $b \in \mathbb{N}$ mit $\mathrm{ggT}(b, n) = 1$ schon implizieren würde, dass n eine Primzahl ist. Ganz so einfach ist es jedoch nicht, wie das folgende Beispiel zeigt:

7.1.2 Beispiel Wähle $n = 91 = 7 \cdot 13$ und $b = 3$. Dann ist $3^{90} \bmod 91 = 1$, obwohl 91 keine Primzahl ist.

7.1.3 Definition Sei $n \in \mathbb{N}$ eine zusammengesetzte Zahl, und sei $b \in (\mathbb{Z}/n\mathbb{Z})^\times$. Wir nennen n eine **Pseudoprimzahl** zur Basis b, falls $b^{n-1} \bmod n = 1$ gilt.

7.1.4 Beispiel Beispiel 7.1.2 zeigt, dass 91 eine Pseudoprimzahl zur Basis 3 ist. Es gilt jedoch $2^{90} \bmod 91 = 64$, das heißt, 91 ist keine Pseudoprimzahl zur Basis 2.

7.1.5 Aufgabe Sei $n \in \mathbb{N}$ zusammengesetzt. Zeigen Sie, dass die Menge

$$P = \{b \in (\mathbb{Z}/n\mathbb{Z})^\times \mid n \text{ ist Pseudoprimzahl zur Basis } b\}$$

eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$ ist.

7.1.6 Proposition Sei n eine zusammengesetzte Zahl. Entweder n ist eine Pseudoprimzahl für alle Basen $b \in (\mathbb{Z}/n\mathbb{Z})^\times$, oder n ist keine Pseudoprimzahl zur Basis b für mindestens die Hälfte aller $b \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Beweis: In Aufgabe 7.1.5 haben Sie gezeigt, dass die Menge

$$P = \{b \in (\mathbb{Z}/n\mathbb{Z})^\times \mid n \text{ ist eine Pseudoprimzahl zur Basis } b\}$$

eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$ ist. Da nach dem Satz von Lagrange die Ordnung einer Untergruppe die Gruppenordnung teilt, ist also entweder $P = (\mathbb{Z}/n\mathbb{Z})^\times$, oder die Ordnung von P ist ein echter Teiler der Ordnung von $(\mathbb{Z}/n\mathbb{Z})^\times$, und dann gehören höchstens die Hälfte der Elemente von $(\mathbb{Z}/n\mathbb{Z})^\times$ zu P. Oder, anders ausgedrückt, mindestens die Hälfte der Elemente von $(\mathbb{Z}/n\mathbb{Z})^\times$ gehört nicht zu P. □

Es gibt tatsächlich zusammengesetzte Zahlen $n \in \mathbb{N}$, für die $P = (\mathbb{Z}/n\mathbb{Z})^\times$ gilt. Zum Beispiel ist 561 eine solche Zahl, was wir später beweisen werden, ohne alle $b \in (\mathbb{Z}/561\mathbb{Z})^\times$ durch zu probieren.

7.1.7 Definition Eine zusammengesetzte Zahl $n \in \mathbb{N}$ heißt **Carmichael-Zahl**, falls $b^{n-1} \bmod n = 1$ für alle $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ gilt.

R.D. Carmichael berechnete im Jahr 1910 erstmals 15 Beispiele für solche Zahlen.

Wenn man jetzt wüsste, dass es nur sehr wenige Carmichael-Zahlen gibt, könnte man folgenden Test als Primzahltest vorschlagen:

Fermat-Test
Sei $n \in \mathbb{N}$. Wähle zufällig $b \in \mathbb{N}$ mit $0 < b < n$. Ist $\mathrm{ggT}(b, n) \neq 1$, dann ist dies ein Teiler von n, und n ist zusammengesetzt. Ist $\mathrm{ggT}(b, n) = 1$, dann berechne $b^{n-1} \bmod n$. Gilt $b^{n-1} \bmod n \neq 1$, dann ist n zusammengesetzt. Gilt $b^{n-1} \bmod n = 1$, dann ist n entweder prim oder eine Carmichael-Zahl, oder n ist zusammengesetzt, und die Wahrscheinlichkeit ein solches b zu wählen, war höchstens $\frac{1}{2}$.

7.1.8 Aufgabe Welches ist die Ergebnismenge beim Fermat-Test, was ist die Wahrscheinlichkeitsverteilung, und was genau ist das Ereignis, dessen Wahrscheinlichkeit höchstens $\frac{1}{2}$ ist?

Gäbe es die Carmichael-Zahlen nicht, hätten wir schon einen schönen Primzahltest gefunden. Wenn n nämlich zusammengesetzt und keine Carmichael-Zahl ist, dann ist die Wahrscheinlichkeit höchstens $\frac{1}{2}$, dass der Fermat-Test ausgibt: „Die Zahl n ist wahrscheinlich prim.“. Andererseits, wenn der Fermat-Test ausgibt: „Die Zahl n ist zusammengesetzt“, dann ist das Ergebnis korrekt. Ist n eine Primzahl, dann wird immer ausgegeben, dass n wahrscheinlich eine Primzahl ist. Wiederholt man den Fermat-Test k Mal für dasselbe zusammengesetzte n, und zwar so, dass die Wahl von b jeweils unabhängig von der vorhergehenden ist, dann ist die Wahrscheinlichkeit, dass der Test k Mal ausgibt: „Die Zahl n ist wahrscheinlich prim“ schon nur noch höchstens $\frac{1}{2^k}$. Das heißt, man kann die Irrtumswahrscheinlichkeit beliebig klein machen.

Außerdem ist der Fermat-Test effizient, denn es werden ein größter gemeinsamer Teiler und eine Potenz in $(\mathbb{Z}/n\mathbb{Z})^\times$ berechnet. Dass sich der größte gemeinsame Teiler effizient berechnen lässt, haben wir in 6.5 gesehen, und die Potenz lässt sich mit dem Wiederholten Quadrieren aus 6.4 effizient berechnen.

Abgesehen vom Problem mit den Carmichael-Zahlen haben wir es hier mit unserem ersten probabilistischen Algorithmus zu tun. Die Laufzeit und zum Teil auch das Ergebnis hängen von der Wahl von b ab. Außerdem gibt es eine Irrtumswahrscheinlichkeit, mit der der Fermat-Test ein falsches Ergebnis ausgibt. Diese Wahrscheinlichkeit ist jedoch höchstens $\frac{1}{2}$, und möchte man sie auf höchstens $\frac{1}{2^k}$ für ein $k \in \mathbb{N}$ drücken, muss man den Test einfach k Mal ausführen. In der Regel

wählt man k dabei irgendwo zwischen 20 und 50, und dann ist die Irrtumswahrscheinlichkeit schon sehr klein - wohl kleiner als die Wahrscheinlichkeit, dass bei der Berechnung ein Hardwarefehler, ein Blitzeinschlag oder Ähnliches auftritt.

Es bleibt also noch das Problem mit den Carmichael-Zahlen. Pommerance, ein bekannter Mathematiker, der wichtige Arbeiten zur Computeralgebra geschrieben hat, sagte dazu: „Using the Fermat-congruence is so simple, that it seems a shame to give up on it just because there are a few counterexamples."

Leider sind es jedoch nicht nur einige wenige Gegenbeispiele, sondern es gibt unendlich viele Carmichael-Zahlen, wie Alford, Granville und Pommerance 1994 in [AGP] gezeigt haben. Wir werden im Folgenden die Carmichael-Zahlen genauer untersuchen, um dann eine Verbesserung des Fermat-Tests aufzuzeigen, bei der es keine Gegenstücke zu den Carmichael-Zahlen mehr gibt. Leider ist der Beweis, dass es unendlich viele Carmichael-Zahlen gibt, zu aufwändig und zu schwierig für diesen Kurs.

Die folgende äquivalente Charakterisierung von Carmichael-Zahlen stammt von Korselt aus dem Jahr 1899. Er konnte zwar diese äquivalente Beschreibung finden, aber kein Beispiel für eine solche Zahl.

7.1.9 Satz (Korselt 1899) Sei $n \in \mathbb{N}$ eine ungerade, zusammengesetzte Zahl.

1. Wenn n durch p^2 teilbar ist, wobei p eine Primzahl ist, dann ist n keine Carmichael-Zahl.
2. Sei n nicht durch eine Quadratzahl teilbar. Genau dann ist n eine Carmichael-Zahl, wenn $p-1 \mid n-1$ für jede Primzahl p gilt, die n teilt.

Beweis:

1. Angenommen, es gibt eine Primzahl p, so dass $p^2 \mid n$ gilt. In 4.8.13 wurde gezeigt, dass $(\mathbb{Z}/p^2\mathbb{Z})^\times$ zyklisch ist, sei also g ein Erzeuger von $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Sei $n = p^k n'$ mit $\mathrm{ggT}(p, n') = 1$. Mit dem Chinesischen Restsatz gibt es ein $b \in \mathbb{Z}$ mit $b \equiv g(\mathrm{mod} p^2)$ und $b \equiv 1(\mathrm{mod} n')$. Mit diesen Bedingungen ist $\mathrm{ggT}(b, n') = \mathrm{ggT}(b, p) = \mathrm{ggT}(b, n) = 1$ (mit Lemma 4.4.4). Wir zeigen nun, dass n keine Pseudoprimzahl zur Basis b mod n ist.

   Angenommen, n ist eine Pseudoprimzahl zur Basis b mod n, also b^{n-1} mod $n = 1$. Da p^2 ein Teiler von n ist, folgt b^{n-1} mod $p^2 = 1$. Da b mod $p^2 = g$ ein Erzeuger von $(\mathbb{Z}/p^2\mathbb{Z})^\times$ ist, gilt also $\varphi(p^2) = p(p-1) | n-1$, das heißt, $n-1$ mod $p = 0$. Es gilt jedoch $n-1$ mod $p = p-1$, denn p teilt n. Dieser Widerspruch zeigt, dass n keine Pseudoprimzahl zur Basis b mod n und damit keine Carmichael-Zahl ist.

2. Zuerst nehmen wir an, dass $p-1 \mid n-1$ für jede Primzahl p gilt, die n teilt. Sei $b \in (\mathbb{Z}/n\mathbb{Z})^\times$. Da $p-1 \mid n-1$, ist b^{p-1} ein Teiler von b^{n-1} für alle Primzahlen p, die n teilen. Mit Fermats kleinem Satz gilt $b^{p-1} \bmod p = 1$ und damit $b^{n-1} \bmod p = 1$ für alle Primzahlen p, die n teilen. Also ist $b^{n-1}-1$ durch alle Primzahlen p teilbar, die n teilen. Das heißt n teilt $b^{n-1}-1$, denn n wird von keiner Quadratzahl geteilt, und $b^{n-1} \bmod n = 1$. Also ist n eine Carmichael-Zahl.

   Wir nehmen nun an, dass n eine Carmichael-Zahl ist. Angenommen, es gibt eine Primzahl p, die n teilt, so dass $p-1$ nicht $n-1$ teilt. Sei g ein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$. Mit dem Chinesischen Restsatz gibt es eine ganze Zahl $b \in \mathbb{Z}$ mit $b \equiv g (\mathrm{mod} p)$ und $b \equiv 1 (\mathrm{mod} \frac{n}{p})$. Da $\mathrm{ggT}(b,p) = \mathrm{ggT}(b,\frac{n}{p}) = 1$ gilt, ist auch $\mathrm{ggT}(b,n) = 1$ (siehe Lemma 4.4.4). Da $p-1$ nicht $n-1$ teilt, ist $b^{n-1} \bmod p = g^{n-1} \bmod p \neq 1$, denn g ist ein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$, und die Ordnung dieser Gruppe ist $p-1$. Doch aus $b^{n-1} \bmod p \neq 1$ folgt auch $b^{n-1} \bmod n \neq 1$, also ist n keine Carmichael-Zahl, ein Widerspruch.

□

7.1.10 Beispiel Die Zahl $561 = 3 \cdot 11 \cdot 17$ ist eine Carmichael-Zahl, denn $3-1 = 2 \mid 560$, $11-1 = 10 \mid 560$ und $17-1 = 16 \mid 560$. Diese Zahl ist sogar die kleinste Carmichael-Zahl, die es gibt.

7.1.11 Proposition Eine Carmichael-Zahl ist Produkt von mindestens drei verschiedenen Primzahlen.

Beweis: Satz 7.1.9 besagt, dass eine Carmichael-Zahl Produkt von mindestens zwei verschiedenen Primzahlen ist. Nehmen wir also an, dass $n = pq$ für zwei verschiedene Primzahlen p und q mit $p < q$ gilt. Nach Satz 7.1.9 gilt $q-1 \mid n-1$, also $n-1 \bmod (q-1) = 0$. Andererseits gilt aber $n-1 = pq-1 = p(q-1+1)-1 = p(q-1)+p-1$, also

$$\begin{aligned} n-1 \bmod (q-1) &= p-1, \text{ denn } 0 < p-1 < q-1 \\ &\neq 0, \text{ ein Widerspruch.} \end{aligned}$$

□

7.1.12 Aufgabe Für $k \geq 1$ ist die k-te Fermat-Zahl definiert als $2^{2^k}+1$. Zeigen Sie, dass für alle $k \in \mathbb{N}$ gilt: Ist die k-te Fermat-Zahl zusammengesetzt, dann ist sie eine Pseudoprimzahl zur Basis 2.

7.2 Der Rabin-Miller-Test

Um das Problem beim Fermat-Test mit den Carmichael-Zahlen in den Griff zu bekommen, gibt es zwei Möglichkeiten: Entweder man macht sich eine Tabelle mit allen Carmichael-Zahlen bis zu einer gewissen Schranke (es gibt zum Beispiel 646 Carmichael-Zahlen kleiner als 10^9), oder man muss den Fermat-Test verbessern. Das ergibt dann den Rabin-Miller-Test, den wir in diesem Abschnitt beschreiben wollen.

Beim Fermat-Test wird überprüft, ob $b^{n-1} \equiv 1 (\mathrm{mod} n)$ für ein $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ gilt. Ist $n-1$ eine gerade Zahl, kann man aber auch $b^{\frac{n-1}{2}} \bmod n$ bilden. Ist n eine Primzahl, dann ist $b^{n-1} \equiv 1 (\mathrm{mod} n)$, und es muss $b^{\frac{n-1}{2}} \equiv \pm 1 (\mathrm{mod} n)$ gelten, denn $(b^{\frac{n-1}{2}})^2 - 1 \bmod n = 0$, und das Polynom $T^2 - 1$ hat über dem Körper $\mathbb{F}_n$ nur die beiden Nullstellen 1 und -1. Ist n jedoch zusammengesetzt, dann kann es auch noch mehr Lösungen geben:

7.2.1 Beispiel Für $n = 8$ hat das Polynom $T^2 - 1$ in $(\mathbb{Z}/8\mathbb{Z})$ die Nullstellen $1, 3, 5, 7$.

Ist $b^{\frac{n-1}{2}} \equiv 1 (\mathrm{mod} n)$, und ist $\frac{n-1}{2}$ gerade, dann kann man $b^{\frac{n-1}{4}} \bmod n$ bilden und testen, ob $b^{\frac{n-1}{4}} \equiv \pm 1 (\mathrm{mod} n)$ gilt. Ist eine andere Zahl als ± 1 das Ergebnis, dann ist sicher, dass n zusammengesetzt ist. Kommt 1 heraus und ist $\frac{n-1}{4}$ wieder gerade, kann man $b^{\frac{n-1}{8}} \bmod n$ bilden und so weiter.

Da man in $\mathbb{Z}/n\mathbb{Z}$ leichter quadrieren als Quadratwurzeln ziehen kann, fängt man andersherum an: Man berechnet $r, s \in \mathbb{N}$, so dass $n-1 = 2^r s$ gilt, wobei s ungerade ist. Das kann man effizient mit höchstens r Divisionen durch 2 tun, und $r \leq \log_2 n$. Nun berechnet man nacheinander

$$x_0 = b^s \bmod n, x_1 = b^{2^1 s} \bmod n = x_0^2 \bmod n, \ldots, x_r = b^{2^r s} \bmod n = b^{n-1} \bmod n.$$

Die Folge $(x_0, x_1, \ldots, x_r)$ kann folgende Gestalt haben:

- $(x_0, \ldots, x_r) = (1, \ldots, 1)$ oder $(x_0, \ldots, x_r) = (*, \ldots, *, n-1, 1 \ldots, 1)$, wobei die Elemente $*$ nicht 1 oder $n-1$ sind. Dann ist n „wahrscheinlich prim“.
- $(x_0, \ldots, x_r) = (*, \ldots, *, 1, \ldots, 1)$, $(x_0, \ldots, x_r) = (*, \ldots, *)$ oder $(x_0, \ldots, x_r) = (*, \ldots, *, n-1)$, wobei die Elemente $*$ nicht 1 oder $n-1$ sind. Dann ist n zusammengesetzt.

7.2.2 Beispiel Sei $n = 341 = 31 \cdot 11$. Dann ist $340 = 2^2 \cdot 85$, also $r = 2$ und $s = 85$. Setze $b = 2$. Dann ist $x_0 = 2^{85} \bmod 341 = 32$, $x_1 = x_0^2 \bmod 341 = 1$ und $x_2 = x_1^2 \bmod 341 = 1$. Die Folge ist also $(x_0, x_1, x_2) = (32, 1, 1)$, das heißt 341 ist zusammengesetzt.

Die erste Frage, die sich stellt, ist, ob es zusammengesetzte Zahlen gibt, bei denen der erste der beiden Fälle auftritt, und wir müssen diese Frage leider mit „ja“ beantworten.

7.2.3 Beispiel Sei $n = 2047 = 23 \cdot 89$. Dann ist $n - 1 = 2046 = 2 \cdot 1023$, also $r = 1$ und $s = 1023$. Setze $b = 2$. Dann ist $x_0 = 2^{1023} \bmod 2047 = 1$ und $x_1 = x_0^2 \bmod 2047 = 1$. Die Folge ist also $(x_0, x_1) = (1, 1)$.

Das obige Beispiel führt zu folgender Definition:

7.2.4 Definition Eine zusammengesetzte, ungerade Zahl n heißt **starke Pseudoprimzahl** zur Basis $b \in (\mathbb{Z}/n\mathbb{Z})^\times$, falls $n - 1 = 2^r s$ ist mit s ungerade, und falls entweder $b^s \bmod n = 1$ gilt, oder falls es ein i mit $0 \leq i < r$ gibt, so dass $b^{2^i s} \equiv -1 (\mathrm{mod} n)$ beziehungsweise $b^{2^i s} \bmod n = n - 1$ gilt.

7.2.5 Bemerkungen

1. Gilt $b^s \bmod n = 1$, dann ist natürlich auch $b^{2^i s} \bmod n = 1$ für alle $1 \leq i \leq r$, das heißt, die Folge ist $(x_0, \ldots, x_r) = (1, \ldots, 1)$.
2. Gilt $b^{2^i s} \bmod n = n - 1$, dann ist $b^{2^j s} \bmod n = 1$ für $j > i$, das heißt, die Folge ist $(x_0, \ldots, x_r) = (*, \ldots, *, n - 1, 1, \ldots, 1)$.
3. Ist n eine starke Pseudoprimzahl zur Basis b, dann ist n auch eine Pseudoprimzahl zur Basis b, denn in beiden Fällen ist $b^{n-1} \bmod n = 1$.
4. Es gibt 14884 Pseudoprimzahlen zur Basis 2, die kleiner als 10^{10} sind, aber nur 3291 starke Pseudoprimzahlen zur Basis 2 (siehe [KR]).

Die wichtige Frage ist die, ob es bei den starken Pseudoprimzahlen ein Analogon zu den Carmichael-Zahlen gibt. Das ist nicht der Fall, und das werden wir auch beweisen. Es gibt ein Ergebnis von Rabin, siehe [Ra], dass eine zusammengesetzte Zahl n für höchstens $\frac{1}{4}$ aller Elemente $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ eine starke Pseudoprimzahl zur Basis b ist. Der Beweis dieses Satzes ist jedoch zu lang und kompliziert, um ihn hier zu präsentieren. Wir werden stattdessen ein schwächeres Ergebnis zeigen.

7.2.6 Satz Sei n eine zusammengesetzte, ungerade Zahl. Dann gilt für höchstens die Hälfte aller $b \in (\mathbb{Z}/n\mathbb{Z})^\times$, dass n eine starke Pseudoprimzahl zur Basis b ist.

Beweis: Ist n keine Carmichael-Zahl, dann gilt für mindestens die Hälfte aller $b \in (\mathbb{Z}/n\mathbb{Z})^\times$, dass n keine Pseudoprimzahl und damit auch keine starke Pseudoprimzahl zur Basis b ist.

Sei also nun n eine Carmichael-Zahl. Dann ist n Produkt von mindestens drei verschiedenen Primzahlen, also $n = \prod_{i=1}^{k} p_i$, wobei $k \geq 3$ gilt und die p_i alle

verschieden sind. Sei $n-1 = 2^r s$ mit $r, s \in \mathbb{N}$ und s ungerade. Betrachte

$$I = \{i \in \mathbb{N}_0 \mid 0 \leq i \leq r \text{ und für alle } b \in (\mathbb{Z}/n\mathbb{Z})^\times \text{ gilt } b^{2^i s} \bmod n = 1\}.$$

Da n eine Carmichael-Zahl ist, gilt $r \in I$ (denn $b^{2^r s} \bmod n = b^{n-1} \bmod n = 1$ für alle $b \in (\mathbb{Z}/n\mathbb{Z})^\times$). Außerdem folgt aus $i \in I$, $0 \leq i < r$, auch $i+1 \in I$, denn aus $b^{2^i s} \bmod n = 1$ folgt $b^{2^{i+1} s} \bmod n = (b^{2^i s})^2 \bmod n = 1$ für alle $b \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Sei jetzt $g \in \mathbb{N}$ so, dass $g \bmod p_1$ ein Erzeuger von $(\mathbb{Z}/p_1\mathbb{Z})^\times$ ist. Dann gilt $\operatorname{ord}(g \bmod p_1) = p_1 - 1$, also ist die Ordnung gerade. Nun ist s aber ungerade, das heißt, $p_1 - 1 \nmid s$, und $g^s \bmod p_1 \neq 1$. Mit dem Chinesischen Restsatz folgt, dass es ein $b \in \mathbb{Z}$ gibt mit $b^s \bmod n \neq 1$. Also gilt $0 \notin I$. Es gibt also ein $l \in \mathbb{N}$ mit $0 \leq l < r$ und $l \notin I$, aber $l+1 \in I$. Sei dann

$$G = \{b \in (\mathbb{Z}/n\mathbb{Z})^\times \mid b^{2^l s} \bmod n \equiv \pm 1 (\bmod n)\}.$$

Dies ist eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$, denn $1 \in G$ und sind $a, b \in G$, dann ist

$$(ab^{-1})^{2^l s} \equiv a^{2^l s}(b^{-1})^{2^l s} \equiv \pm 1 \cdot (b^{2^l s})^{-1} \equiv \pm 1 \cdot (\pm 1)^{-1} \equiv \pm 1 \cdot \pm 1 \equiv \pm 1 (\bmod n),$$

also $ab^{-1} \in G$. Mit dem Untergruppenkriterium folgt, dass G eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$ ist.

Wir zeigen nun, dass $G \neq (\mathbb{Z}/n\mathbb{Z})^\times$ gilt. Da $l \notin I$ gilt, gibt es ein $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, so dass $a^{2^l s} \bmod n \neq 1$ gilt. Das heißt, es gibt ein $i \in \mathbb{N}$ mit $1 \leq i \leq k$, so dass $a^{2^l s} \bmod p_i \neq 1$ gilt. Mit dem Chinesischen Restsatz existiert ein $b \in \mathbb{Z}$ mit $b \equiv a (\bmod p_i)$ und $b \equiv 1 (\bmod p_j)$ für $j \neq i$. Dann ist $b \bmod n \notin G$, denn $b^{2^l s} \bmod p_i \neq 1$ und $b^{2^l s} \not\equiv -1 (\bmod p_j)$ für $j \neq i$. Also gilt $b^{2^l s} \not\equiv \pm 1 (\bmod n)$. Es folgt $G \neq (\mathbb{Z}/n\mathbb{Z})^\times$.

Andererseits sind die Elemente $b \in (\mathbb{Z}/n\mathbb{Z})^\times \setminus G$ gerade so, dass n keine starke Pseudoprimzahl zur Basis b ist, denn $b^{2^l s} \not\equiv \pm 1 (\bmod n)$ (weil $b \notin G$) und $b^{2^{l+1} s} \equiv 1 (\bmod n)$ (weil $l+1 \in I$ gilt). Da G eine Untergruppe ist, die nicht ganz $(\mathbb{Z}/n\mathbb{Z})^\times$ ist, ist also mindestens die Hälfte der Elemente aus $(\mathbb{Z}/n\mathbb{Z})^\times$ nicht in G, und damit ist n für mindestens die Hälfte der Elemente $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ keine Pseudoprimzahl zur Basis b. □

Nun sind alle Zutaten für den Rabin-Miller-Test vollständig:

Rabin-Miller-Test
Sei $n \in \mathbb{N}$ ungerade. Wähle zufällig $b \in \mathbb{N}$ mit $0 < b < n$. Ist $\mathrm{ggT}(b, n) \neq 1$, dann ist ein Teiler von n gefunden, und n ist zusammengesetzt. Ist $\mathrm{ggT}(b, n) = 1$, berechne $r, s \in \mathbb{N}$, so dass $n - 1 = 2^r s$ gilt, wobei s ungerade ist. Berechne die Folge

$$(x_0 = b^s \bmod n, x_1 = b^{2^1 s} \bmod n, \ldots, x_r = b^{2^r s} \bmod n = b^{n-1} \bmod n).$$

Gilt $(x_0, \ldots, x_r) = (*, \ldots, *)$, $(x_0, \ldots, x_r) = (*, \ldots, *, 1, \ldots, 1)$ oder $(x_0, \ldots, x_r) = (*, \ldots, *, n-1)$, wobei $* \neq 1$ und $* \neq n-1$ gilt, dann ist n zusammengesetzt. Gilt $(x_0, \ldots, x_r) = (1, \ldots, 1)$ oder $(x_0, \ldots, x_r) = (*, \ldots, *, n-1, 1, \ldots, 1)$, dann ist n entweder prim, oder n ist zusammengesetzt, und die Wahrscheinlichkeit eine solche Zahl b zu wählen, war höchstens $\frac{1}{2}$.

Wie beim Fermat-Test kann man den Rabin-Miller-Test k Mal hintereinander für verschiedene, unabhängig gewählte b ausführen. Die Wahrscheinlichkeit, dass n zusammengesetzt ist und dies nicht erkannt wird, ist dann höchstens $\frac{1}{2^k}$.

Auch der Rabin-Miller-Test ist effizient, denn es werden $r + 1$ Werte $x_0, \ldots, x_r$ berechnet, und r ist höchstens so groß wie $\log_2 n$. Die Berechnung eines einzelnen x_i ist ebenfalls effizient mit Wiederholtem Quadrieren zu machen. Der Wert r selbst wird durch Dividieren durch 2 berechnet bis das Ergebnis ungerade ist. Das erfordert r Divisionen durch 2, das heißt, r lässt sich effizient berechnen.

7.2.7 Aufgabe Zeigen Sie mit dem Rabin-Miller-Test, dass 561 zusammengesetzt ist.

Der Rabin-Miller-Test (aus dem Jahr 1980) ist der Primzahltest, der in der Praxis am häufigsten verwendet wird. So verwendet zum Beispiel das Computeralgebra-System MuPAD den Rabin-Miller-Test (mit $k = 10$). Das Computeralgebra-System Maple verwendet den Rabin-Miller-Test in Kombination mit einem anderen Primzahltest.

7.3 Der Solovay-Strassen-Test

Im Folgenden wird ein weiterer probabilistischer Primzahltest behandelt, der Test von Solovay und Strassen (1977). Dies hat eher historische als praktische Gründe.

Der Solovay-Strassen-Test war nämlich der erste effiziente probabilistische Primzahltest und einer der ersten probabilistischen Algorithmen überhaupt. Um den Solovay-Strassen-Test zu verstehen, werden das Legendre- und das Jacobi-Symbol eingeführt. Sei $p > 2$ eine Primzahl.

Frage: Wieviele $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ sind Quadratzahlen, also von der Form $a = b^2 \bmod p$ für ein $b \in (\mathbb{Z}/p\mathbb{Z})^\times$?

Diese Frage lässt sich leicht beantworten: Sei g ein primitives Element von $(\mathbb{Z}/p\mathbb{Z})^\times$. Dann ist $a = g^j \bmod p$ eine Quadratzahl genau dann, wenn $j \in \mathbb{Z}$ gerade ist. Ist nämlich j gerade, also $j = 2k$ für ein $k \in \mathbb{Z}$, dann ist $a \equiv g^j \equiv (g^k)^2 (\mathrm{mod} p)$, also eine Quadratzahl. Ist andererseits a eine Quadratzahl, also $a = b^2 \bmod p$ mit $b \in (\mathbb{Z}/p\mathbb{Z})^\times$, dann gilt $b = g^k \bmod p$ für ein $k \in \mathbb{Z}$, und $a \equiv b^2 \equiv (g^k)^2 \equiv g^{2k} (\mathrm{mod} p)$, also ist $a = g^j \bmod p$ für ein gerades j.

7.3.1 Aufgabe Sei $p > 2$ eine Primzahl, und sei g ein primitives Element von $(\mathbb{Z}/p\mathbb{Z})^\times$. Es gelte $g^i \equiv g^j (\mathrm{mod} p)$ für $i, j \in \mathbb{Z}$. Zeigen Sie, dass i genau dann gerade ist, wenn j gerade ist.

7.3.2 Definition Sei $p > 2$ eine Primzahl. Eine Quadratzahl in $(\mathbb{Z}/p\mathbb{Z})^\times$ wird **quadratischer Rest** modulo p genannt. Eine Zahl, die keine Quadratzahl ist, wird **quadratischer Nichtrest** modulo p genannt.

Wir haben oben also Folgendes gezeigt:

7.3.3 Lemma Sei $p > 2$ eine Primzahl. Dann sind die Hälfte der Elemente in $(\mathbb{Z}/p\mathbb{Z})^\times$ quadratische Reste, und die andere Hälfte sind quadratische Nichtreste modulo p. □

7.3.4 Definition Sei $a \in \mathbb{Z}$ und $p > 2$ eine Primzahl. Das **Legendre-Symbol** $(\frac{a}{p})$ ist definiert als

$$(\frac{a}{p}) \quad = \quad \begin{cases} 0, & \text{falls } p \mid a \text{ gilt.} \\ 1, & \text{falls } a \bmod p \text{ quadratischer Rest modulo } p \text{ ist.} \\ -1, & \text{falls } a \bmod p \text{ quadratischer Nichtrest modulo } p \text{ ist.} \end{cases}$$

Das Legendre-Symbol wird ausgesprochen $(\frac{a}{p})$ =„das Legendre-Symbol von a über p“ und ist benannt nach Adrien-Marie Legendre (1752-1833) .

7.3.5 Beispiel Sei $p = 7$. Dann ist $(\mathbb{Z}/7\mathbb{Z})^\times = \{1, 2, 3, 4, 5, 6\}$, und es gilt $1^2 \equiv 1 \equiv 6^2 (\mathrm{mod} 7)$, $2^2 \equiv 4 \equiv 5^2 (\mathrm{mod} 7)$ und $3^2 \equiv 2 \equiv 4^2 (\mathrm{mod} 7)$, also ist $(\frac{0}{7}) = 0$, $(\frac{1}{7}) = (\frac{4}{7}) = (\frac{2}{7}) = 1$ und $(\frac{3}{7}) = (\frac{5}{7}) = (\frac{6}{7}) = -1$.

Die folgende Proposition geht auf Leonhard Euler (1707-1783) zurück.

7.3.6 Proposition Sei $a \in \mathbb{Z}$ und $p > 2$ eine Primzahl. Dann gilt:

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} (\mathrm{mod} p).$$

Beweis: Gilt $p \mid a$, dann ist $a \bmod p = 0$, also auch $a^{\frac{p-1}{2}} \equiv 0 \equiv (\frac{a}{p})(\mathrm{mod} p)$. Es gelte nun also $p \nmid a$. Dann ist $a \bmod p \in (\mathbb{Z}/p\mathbb{Z})^\times$. Sei g ein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$. Ist $a \bmod p$ ein quadratischer Rest modulo p, dann gilt $a \equiv g^{2k} (\mathrm{mod} p)$ für ein $k \in \mathbb{N}_0$. Also folgt

$$a^{\frac{p-1}{2}} \equiv (g^{2k})^{\frac{p-1}{2}} \equiv (g^{p-1})^k \equiv 1^k \equiv 1 (\mathrm{mod} p).$$

Ist $a \bmod p$ ein quadratischer Nichtrest modulo p, dann gilt $a \equiv g^{2k+1} (\mathrm{mod} p)$ für ein $k \in \mathbb{N}_0$. Also folgt

$$a^{\frac{p-1}{2}} \equiv (g^{2k+1})^{\frac{p-1}{2}} \equiv g^{k(p-1)+\frac{p-1}{2}} \equiv (g^{p-1})^k \cdot g^{\frac{p-1}{2}} \equiv 1^k \cdot g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} (\mathrm{mod} p).$$

Nun ist aber $g^{\frac{p-1}{2}} \not\equiv 1 (\mathrm{mod} p)$, denn die Ordnung von g in $(\mathbb{Z}/p\mathbb{Z})^\times$ ist $p-1$. Andererseits ist $(g^{\frac{p-1}{2}})^2 \equiv g^{p-1} \equiv 1 (\mathrm{mod} p)$, also ist $g^{\frac{p-1}{2}} \equiv \pm 1 (\mathrm{mod} p)$. Insgesamt folgt $g^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod} p)$, also $a^{\frac{p-1}{2}} \equiv -1 \equiv (\frac{a}{p})(\mathrm{mod} p)$. □

7.3.7 Lemma Sei $p > 2$ eine Primzahl, und seien $a, b \in \mathbb{Z}$.

1. Gilt $a \equiv b (\mathrm{mod} p)$, dann ist $(\frac{a}{p}) = (\frac{b}{p})$.
2. $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.
3. $(\frac{-1}{p}) = \begin{cases} 1, & \text{falls } p \bmod 4 = 1. \\ -1, & \text{falls } p \bmod 4 = 3. \end{cases}$

Beweis:

1. Sei $a \equiv b (\mathrm{mod} p)$. Dann ist $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} (\mathrm{mod} p)$, also $(\frac{a}{p}) = (\frac{b}{p})$.
2. Es gilt
$$(\frac{ab}{p}) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (\frac{a}{p})(\frac{b}{p}) (\mathrm{mod} p).$$
Es folgt die Behauptung.

3. Es gilt $(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}} (\mathrm{mod} p)$. Also ist

$$\begin{aligned}(\frac{-1}{p}) = 1 &\Leftrightarrow \frac{p-1}{2} \text{ ist gerade} \Leftrightarrow \frac{p-1}{2} = 2k \text{ für ein } k \in \mathbb{N}_0 \\ &\Leftrightarrow p - 1 = 4k \text{ für ein } k \in \mathbb{N}_0 \Leftrightarrow p = 4k + 1 \text{ für ein } k \in \mathbb{N}_0 \\ &\Leftrightarrow p \bmod 4 = 1.\end{aligned}$$

Da p ungerade ist, gilt entweder $p \bmod 4 = 1$ oder $p \bmod 4 = 3$. Also folgt die Behauptung.

□

7.3.8 Aufgabe Berechnen Sie $(\frac{40}{31})$ und $(\frac{-4}{31})$.

Die Definition des Legendre-Symbols wird nun erweitert auf beliebige ungerade Zahlen.

7.3.9 Definition Sei $n > 2$ eine ungerade Zahl und sei $a \in \mathbb{Z}$. Sei $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ die Primzahlzerlegung von n, wobei $p_i \neq p_j$ für $i \neq j$ und $1 \leq i, j \leq r$ gilt. Das **Jacobi-Symbol** $(\frac{a}{n})$ ist definiert als

$$(\frac{a}{n}) = (\frac{a}{p_1})^{\alpha_1} \cdot \ldots \cdot (\frac{a}{p_r})^{\alpha_r}.$$

Das Jacobi-Symbol ist nach Gustav Carl Jacob Jacobi (1804-1851) benannt. Sie sehen sofort, dass für eine Primzahl n das Jacobi- und das Legendre-Symbol übereinstimmen. Ist n jedoch zusammengesetzt, dann macht das Jacobi-Symbol keine Aussage mehr darüber, ob $a \bmod n$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ ein quadratischer Rest ist oder nicht, obwohl man ja auch in $(\mathbb{Z}/n\mathbb{Z})^\times$ quadratische Reste definieren könnte. Ist zum Beispiel $n = 15$ und $a = 2$, dann ist

$$(\frac{2}{15}) = (\frac{2}{3})(\frac{2}{5}) = (-1) \cdot (-1) = 1,$$

denn 2 ist ein quadratischer Nichtrest in $(\mathbb{Z}/3\mathbb{Z})^\times$ und in $(\mathbb{Z}/5\mathbb{Z})^\times$. Jedoch gibt es kein $b \in (\mathbb{Z}/15\mathbb{Z})^\times$, so dass $b^2 \bmod 15 = 2$ gilt.

7.3.10 Aufgabe Sei $n > 2$ ungerade und zusammengesetzt, und sei $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Zeigen Sie: Ist a ein quadratischer Rest in $(\mathbb{Z}/n\mathbb{Z})^\times$, das heißt, es gibt ein $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ mit $b^2 \bmod n = a$, dann gilt $(\frac{a}{n}) = 1$.

Für das Jacobi-Symbol gelten ähnliche Eigenschaften wie für das Legendre-Symbol in Lemma 7.3.7.

7.3.11 Lemma Sei $n > 2$ eine ungerade Zahl und seien $a, b \in \mathbb{Z}$.

1. Gilt $a \equiv b(\mathrm{mod} n)$, dann folgt $(\frac{a}{n}) = (\frac{b}{n})$.
2. $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$.
3. $(\frac{1}{n}) = 1$.

Beweis: Sei $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ die Primfaktorzerlegung von n.

1. Es gelte $a \equiv b(\mathrm{mod} n)$. Dann ist $a \equiv b(\mathrm{mod} p_i)$ für $1 \leq i \leq r$ und
$$(\frac{a}{n}) = (\frac{a}{p_1})^{\alpha_1} \dots (\frac{a}{p_r})^{\alpha_r} = (\frac{b}{p_1})^{\alpha_1} \dots (\frac{b}{p_r})^{\alpha_r} = (\frac{b}{n})$$
mit Lemma 7.3.7.
2. Es gilt
$$(\frac{ab}{n}) = (\frac{ab}{p_1})^{\alpha_1} \dots (\frac{ab}{p_r})^{\alpha_r} = (\frac{a}{p_1})^{\alpha_1} \dots (\frac{a}{p_r})^{\alpha_r} (\frac{b}{p_1})^{\alpha_1} \dots (\frac{b}{p_r})^{\alpha_r} = (\frac{a}{n})(\frac{b}{n})$$
mit Lemma 7.3.7.
3. Es gilt $(\frac{1}{n}) = (\frac{1}{p_1})^{\alpha_1} \dots (\frac{1}{p_r})^{\alpha_r} = 1$, denn 1 ist immer ein quadratischer Rest.

□

Beim Solovay-Strassen-Test wird nun einfach für ein ungerades $n > 2$ ein $b \in \mathbb{N}$ mit $0 < b < n$ und $\mathrm{ggT}(b, n) = 1$ gewählt und getestet, ob

$$b^{\frac{n-1}{2}} \equiv (\frac{b}{n})(\mathrm{mod} n) \tag{7.1}$$

gilt. Ist n prim, dann gilt Bedingung (7.1) mit Proposition 7.3.6. Es gibt jedoch auch zusammengesetzte Zahlen n und Zahlen $b \in \mathbb{N}$ mit $0 < b < n$ und $\mathrm{ggT}(b, n) = 1$, so dass Bedingung (7.1) gilt. Dies führt zu folgender Definition:

7.3.12 Definition Sei $n > 2$ ungerade und zusammengesetzt. Sei $b \in (\mathbb{Z}/n\mathbb{Z})^\times$. Die Zahl n heißt **Eulersche Pseudoprimzahl** zur Basis b, wenn $b^{\frac{n-1}{2}} \equiv (\frac{b}{n})(\mathrm{mod}\ n)$ gilt.

7.3.13 Beispiel Die Zahl $2047 = 23 \cdot 89$ ist Eulersche Pseudoprimzahl zur Basis 2, denn $(\frac{2}{2047}) = 1 \equiv 2^{1023}(\mathrm{mod} 2047)$.

7.3.14 Lemma Ist n eine Eulersche Pseudoprimzahl zur Basis b, dann ist n auch eine Pseudoprimzahl zur Basis b.

Beweis: Ist n eine Eulersche Pseudoprimzahl zur Basis b, dann gilt $b^{\frac{n-1}{2}} \equiv (\frac{b}{n}) \equiv \pm 1 (\mathrm{mod} n)$. Also

$$(b^{\frac{n-1}{2}})^2 \equiv b^{n-1} \equiv (\frac{b}{n})^2 \equiv 1 (\mathrm{mod} n),$$

das heißt, n ist Pseudoprimzahl zur Basis b. □

Die Umkehrung von Lemma 7.3.14 gilt nicht, wie das folgende Beispiel zeigt:

7.3.15 Beispiel Es gilt $91 = 7 \cdot 13$, und $3^{90} \bmod 91 = 1$. Also ist 91 Pseudoprimzahl zur Basis 3. Es ist jedoch $3^{45} \bmod 91 = 27$, das heißt, 91 ist nicht Eulersche Pseudoprimzahl zur Basis 3.

Die folgende Proposition zeigt, dass es - wie bei den starken Pseudoprimzahlen - kein Analogon zu den Carmichael-Zahlen gibt.

7.3.16 Proposition Sei $n > 2$ eine ungerade, zusammengesetzte Zahl. Dann gilt für mindestens die Hälfte aller $b \in (\mathbb{Z}/n\mathbb{Z})^\times$, dass n keine Eulersche Pseudoprimzahl zur Basis b ist.

Beweis: Sei $G = \{b \in (\mathbb{Z}/n\mathbb{Z})^\times \mid n \text{ ist Eulersche Pseudoprimzahl zur Basis } b\}$. Dann ist G eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$, denn $1 \in G$, und für $a \in G$ gilt

$$(a^{-1})^{\frac{n-1}{2}} \equiv (a^{\frac{n-1}{2}})^{-1} \equiv (\frac{a}{n})^{-1} (\mathrm{mod} n).$$

Außerdem gilt

$$(\frac{a}{n})(\frac{a^{-1} \bmod n}{n}) = (\frac{aa^{-1} \bmod n}{n}) = (\frac{1}{n}) = 1,$$

mit Lemma 7.3.11, also $(\frac{a}{n})^{-1} = (\frac{a^{-1} \bmod n}{n})$, das heißt, $a^{-1} \bmod n \in G$. Seien nun $a, b \in G$. Dann ist

$$(ab^{-1})^{\frac{n-1}{2}} \equiv a^{\frac{n-1}{2}} (b^{-1})^{\frac{n-1}{2}} \equiv (\frac{a}{n})(\frac{b^{-1}}{n}) \equiv (\frac{ab^{-1}}{n}) (\mathrm{mod} n)$$

mit Lemma 7.3.11. Also gilt $ab^{-1} \bmod n \in G$. Mit dem Untergruppenkriterium gilt nun, dass G eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$ ist. Da die Ordnung von G die Gruppenordnung teilt, wissen wir schon, dass entweder alle Elemente von $(\mathbb{Z}/n\mathbb{Z})^\times$ in G liegen oder höchstens die Hälfte. Wir müssen also noch zeigen, dass $G \neq (\mathbb{Z}/n\mathbb{Z})^\times$ gilt, dass es also immer ein $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ mit $b^{\frac{n-1}{2}} \not\equiv (\frac{b}{n}) (\mathrm{mod} n)$ gibt. Dazu unterscheiden wir zwei Fälle.

1. Fall $n = p^2 n'$, wobei p eine Primzahl ist und $n' \in \mathbb{N}$ gilt (das heißt, es gibt ein Primzahlquadrat, das n teilt). Sei $n = p^\alpha p_1^{\alpha_1} \dots p_r^{\alpha_r}$ die Primfaktorzerlegung von n, wobei p und die p_i für $1 \leq i \leq r$ alle verschieden seien. Setze $b = 1 + \frac{n}{p} = 1 + pn'$. Dann ist

$$(\frac{b}{n}) = (\frac{1+pn'}{n}) = (\frac{1+pn'}{p})^\alpha (\frac{1+pn'}{p_1})^{\alpha_1} \dots (\frac{1+pn'}{p_r})^{\alpha_r}.$$

Es gilt $1 + pn' \bmod p_i = 1$ für $1 \leq i \leq r$ und $1 + pn' \bmod p = 1$. Also ist $(\frac{b}{n}) = 1$ mit Lemma 7.3.11. Andererseits ist für $j \in \mathbb{N}$

$$(1+pn')^j = 1^j + \binom{j}{1} pn' + \binom{j}{2} (pn')^2 + \dots + \binom{j}{j} (pn')^j.$$

Die Summanden $\binom{j}{2}(pn')^2, \dots, \binom{j}{j}(pn')^j$ werden alle von n geteilt. Also ist $(1+pn')^j \bmod n = 1 + jpn' \bmod n$.

Setze nun $j = \frac{n-1}{2}$. Dann ist

$$b^{\frac{n-1}{2}} \equiv (1+pn')^{\frac{n-1}{2}} \equiv 1 + \frac{n-1}{2} pn' (\mathrm{mod} n).$$

Angenommen, $\frac{n-1}{2} pn' \bmod n = 0$. Dann folgt $p \mid \frac{n-1}{2}$, das heißt, es gibt ein $k \in \mathbb{N}$ mit $pk = \frac{n-1}{2}$. Also ist $p(2k) = n - 1$ und $n - p(2k) = 1$. Dies ist ein Widerspruch, denn p teilt $n - p(2k)$, aber p teilt nicht 1. Also gilt $b^{\frac{n-1}{2}} \not\equiv 1 (\mathrm{mod} n)$.

2. Fall $n = p_1 \cdot \ldots \cdot p_r$, und die p_i sind verschiedene Primzahlen für $1 \leq i \leq r$. Da p_1 eine Primzahl ist, gibt es ein $a \in (\mathbb{Z}/p_1\mathbb{Z})^\times$ mit $(\frac{a}{p_1}) = -1$. Mit dem Chinesischen Restsatz gibt es ein $b \in \mathbb{Z}$ mit $b \bmod p_1 = a$ und $b \bmod \frac{n}{p_1} = 1$. Dann gilt

$$(\frac{b}{n}) = (\frac{b}{p_1}) \dots (\frac{b}{p_r}) = (-1) \cdot 1 \cdot \ldots \cdot 1 = -1.$$

Angenommen, $b^{\frac{n-1}{2}} \equiv -1 (\mathrm{mod} n)$. Da $\frac{n}{p_1} \mid n$ gilt, folgt dann auch $b^{\frac{n-1}{2}} \equiv -1 (\mathrm{mod} \frac{n}{p_1})$. Andererseits ist aber $b \bmod \frac{n}{p_1} = 1$, das heißt $b^{\frac{n-1}{2}} \equiv 1 (\mathrm{mod}\ \frac{n}{p_1})$. Also ist $1 \equiv -1 (\mathrm{mod} \frac{n}{p_1})$ und damit $\frac{n}{p_1} = 2$ und n gerade. Dies ist ein Widerspruch zu der Voraussetzung, dass n ungerade ist.

□

Nun kann der Primzahltest von Solovay-Strassen formuliert werden.

Solovay-Strassen-Test
Sei $n \in \mathbb{N}$, $n > 2$, ungerade. Wähle zufällig $b \in \mathbb{N}$ mit $0 < b < n$. Gilt $\mathrm{ggT}(b, n) \neq 1$, dann ist n zusammengesetzt. Ist $\mathrm{ggT}(b, n) = 1$, dann berechne $b^{\frac{n-1}{2}} \bmod n$ und $(\frac{b}{n})$. Gilt $b^{\frac{n-1}{2}} \not\equiv (\frac{b}{n})(\mathrm{mod} n)$, dann ist n zusammengesetzt. Gilt $b^{\frac{n-1}{2}} \equiv (\frac{b}{n})(\mathrm{mod} n)$, dann ist entweder n eine Primzahl, oder n ist zusammengesetzt, und die Wahrscheinlichkeit, ein solches b zu wählen, ist höchstens $\frac{1}{2}$.

7.3.17 Aufgabe Benutzen Sie den Solovay-Strassen-Test, um zu zeigen, dass 15 zusammengesetzt ist.

Klar ist, dass $b^{\frac{n-1}{2}} \bmod n$ mit Wiederholtem Quadrieren effizient berechnet werden kann. Um den Solovay-Strassen-Test effizient anwenden zu können, muss jedoch auch $(\frac{b}{n})$ effizient berechnet werden, und der Rest der Kurseinheit wird sich genau damit befassen.

7.3.18 Lemma (Gauß-Lemma) Sei p eine ungerade Primzahl, und sei $a \in \mathbb{Z}$ mit $p \nmid a$. Sei

$$S = \{a \bmod p, 2a \bmod p, \ldots, \frac{p-1}{2} a \bmod p\}.$$

Sei k die Anzahl der Elemente in S, die größer sind als $\frac{p}{2}$. Dann gilt $(\frac{a}{p}) = (-1)^k$.

Beweis: Die $\frac{p-1}{2}$ Elemente $ia \bmod p$ mit $1 \leq i \leq \frac{p-1}{2}$ sind alle verschieden, denn angenommen, $ia \bmod p = ja \bmod p$ für $1 \leq i, j \leq \frac{p-1}{2}$, dann folgt $(i-j)a \bmod p = 0$, also $i - j \bmod p = 0$ oder $a \bmod p = 0$. Da $p \nmid a$ nach Voraussetzung gilt, muss also $i - j \bmod p = 0$ gelten. Nun ist aber $1 \leq i, j \leq \frac{p-1}{2}$, also folgt aus $i - j \bmod p = 0$ schon $i - j = 0$, also $i = j$.

Seien also $s_1, \ldots, s_k$ die Elemente in S, die größer als $\frac{p}{2}$ sind, und seien $t_1, \ldots, t_l$ die Elemente in S, die kleiner als $\frac{p}{2}$ sind. (Beachten Sie, dass $\frac{p}{2}$ selbst keine natürliche Zahl ist!) Dann gilt $k + l = \frac{p-1}{2}$. Betrachtet man nun $p - s_i$ für $1 \leq i \leq k$, dann sind dies k verschiedene Elemente kleiner oder gleich $\frac{p-1}{2}$. Angenommen, es gilt $p - s_i = t_j$ für ein $1 \leq i \leq k$ und ein $1 \leq j \leq l$. Dann gibt es $x, y \in \mathbb{N}$ mit $1 \leq x, y \leq \frac{p-1}{2}$ und $p - xa \equiv ya(\mathrm{mod} p)$, und damit $-xa \equiv ya(\mathrm{mod} p)$, also $(x + y)a \bmod p = 0$. Da $p \nmid a$ gilt, ist $a \bmod p \neq 0$. Also folgt $(x + y) \bmod p = 0$. Es ist aber $1 \leq x, y \leq \frac{p-1}{2}$, das heißt $1 \leq x + y \leq p - 1$, ein Widerspruch.

Wir haben also jetzt gezeigt, dass $p - s_1, \ldots, p - s_k, t_1, \ldots, t_l$ zusammen $\frac{p-1}{2}$ verschiedene Zahlen zwischen 1 und $\frac{p-1}{2}$ sind, oder, mit anderen Worten,

$$\{p - s_1, \ldots, p - s_k, t_1, \ldots, t_l\} = \{1, \ldots, \frac{p-1}{2}\}$$

Also gilt

$$\left(\frac{p-1}{2}\right)! \equiv \prod_{i=1}^{k}(p-s_i)\prod_{j=1}^{l}t_j \equiv (-1)^k\prod_{i=1}^{k}s_i\prod_{j=1}^{l}t_j(\mathrm{mod}p).$$

Jedes s_i beziehungsweise t_j ist von der Form $xa \bmod p$ für ein $1 \leq x \leq \frac{p-1}{2}$. Also

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^k\prod_{x=1}^{\frac{p-1}{2}}xa \equiv (-1)^k a^{\frac{p-1}{2}}\prod_{x=1}^{\frac{p-1}{2}}x \equiv (-1)^k a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!(\mathrm{mod}p).$$

Nun ist $(\frac{p-1}{2})! \bmod p \neq 0$, es darf also gekürzt werden:

$$\begin{aligned} 1 &\equiv (-1)^k a^{\frac{p-1}{2}}(\mathrm{mod}p), \text{ oder} \\ (-1)^k &\equiv a^{\frac{p-1}{2}} \equiv (\frac{a}{p})(\mathrm{mod}p) \end{aligned}$$

mit Proposition 7.3.6. □

7.3.19 Beispiel Seien $p = 13$ und $a = 3$. Dann ist $S = \{3, 6, 9, 12, 2, 5\}$. Da $\frac{p}{2} = 6,5$ gilt, ist $k = 2$, und $(\frac{3}{13}) = (-1)^2 = 1$ (und in der Tat ist $4^2 \bmod 13 = 3$).

7.3.20 Aufgabe Sei $p > 2$ eine Primzahl. Berechnen Sie $(\frac{-1}{p})$ mit dem Gauß-Lemma.

Der Wert des Legendre-Symbols $(\frac{a}{p})$ hängt also davon ab, ob k aus dem Gauß-Lemma gerade oder ungerade ist, oder, anders ausgedrückt, ob $k \bmod 2 = 0$ oder $k \bmod 2 = 1$ gilt. Das folgende Lemma beschreibt eine Methode, wie $k \bmod 2$ berechnet werden kann. Zuvor jedoch noch eine Bemerkung zur Gaußklammer:

Seien $b \in \mathbb{Z}$ und $a \in \mathbb{N}$, und sei $b = qa + r$ die Division von b mit Rest durch a, das heißt, es gelte $0 \leq r < a$. Dann folgt $\frac{b}{a} = q + \frac{r}{a}$, und $0 \leq \frac{r}{a} < 1$. Also ist q die größte ganze Zahl kleiner oder gleich $\frac{b}{a}$, und $q = [\frac{b}{a}]$. Insbesondere gilt

$$b = [\frac{b}{a}]a + r = [\frac{b}{a}]a + b \bmod a.$$

7.3.21 Lemma Sei p eine ungerade Primzahl, sei $a \in \mathbb{Z}$, und es gelte $p \nmid a$. Sei k definiert wie im Gauß-Lemma, und sei

$$T = \sum_{i=1}^{\frac{p-1}{2}}[\frac{ia}{p}].$$

Dann gilt $k \equiv T + (a-1)\frac{p^2-1}{8}(\mathrm{mod}2)$.

Beweis: Seien $s_1, \ldots, s_k, t_1, \ldots, t_l$ definiert wie im Beweis des Gauß-Lemmas. Dann gilt - wie dort gezeigt -

$$\{p - s_1, \ldots, p - s_k, t_1, \ldots, t_l\} = \{1, \ldots, \frac{p-1}{2}\}.$$

Also gilt

$$\begin{aligned} \sum_{i=1}^{\frac{p-1}{2}} i &= \frac{(\frac{p-1}{2})(\frac{p-1}{2}+1)}{2} = \frac{(\frac{p-1}{2})(\frac{p+1}{2})}{2} = \frac{p^2-1}{8} \\ &= \sum_{i=1}^{k}(p - s_i) + \sum_{j=1}^{l} t_j = kp - \sum_{i=1}^{k} s_i + \sum_{j=1}^{l} t_j. \end{aligned}$$

Nun ist aber

$$\begin{aligned} a\frac{p^2-1}{8} &= \sum_{i=1}^{\frac{p-1}{2}} ia = \sum_{i=1}^{\frac{p-1}{2}}([\frac{ia}{p}]p + ia \bmod p) \\ &= \sum_{i=1}^{\frac{p-1}{2}}[\frac{ia}{p}]p + \sum_{i=1}^{k} s_i + \sum_{j=1}^{l} t_j = pT + \sum_{i=1}^{k} s_i + \sum_{j=1}^{l} t_j. \end{aligned}$$

Es folgt

$$\begin{aligned} (a-1)\frac{p^2-1}{8} &= pT + \sum_{i=1}^{k} s_i + \sum_{j=1}^{l} t_j - kp + \sum_{i=1}^{k} s_i - \sum_{j=1}^{l} t_j \\ &= p(T-k) + 2\sum_{i=1}^{k} s_i. \end{aligned}$$

Da $p \bmod 2 = 1$ gilt, folgt $(a-1)^{\frac{p^2-1}{8}} \equiv T - k(\text{mod}2)$ oder $k \equiv T + (a-1)^{\frac{p^2-1}{8}}(\text{mod}2)$. □

Nun sind wir in der Lage, schnell zu entscheiden, ob 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$ ein quadratischer Rest ist oder nicht.

7.3.22 Proposition Sei p eine ungerade Primzahl. Dann gilt

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{falls } p \bmod 8 \in \{1,7\}. \\ -1, & \text{falls } p \bmod 8 \in \{3,5\}. \end{cases}$$

Beweis: Wir berechnen T aus Lemma 7.3.21:

$$T = \sum_{i=1}^{\frac{p-1}{2}} [\frac{2i}{p}] = [\frac{2}{p}] + [\frac{4}{p}] + \ldots + [\frac{p-1}{p}] = 0,$$

denn $0 \leq \frac{2i}{p} < 1$ für $1 \leq i \leq \frac{p-1}{2}$. Mit $a = 2$ folgt also aus Lemma 7.3.21, dass $k \equiv \frac{p^2-1}{8} (\mathrm{mod} 2)$ gilt.

Jede ungerade Primzahl p ist von der Form $p = 8n + 1$ oder $p = 8n + 3$ oder $p = 8n + 5$ oder $p = 8n + 7$ für ein $n \in \mathbb{N}_0$. Berechnen wir also $\frac{p^2-1}{8}$ für die verschiedenen Fälle:

p	$\frac{p^2-1}{8}$	$\frac{p^2-1}{8} \bmod 2$
$8n+1$	$\frac{(8n+1)^2-1}{8} = \frac{64n^2+16n}{8} = 8n^2+2n$	0
$8n+3$	$\frac{(8n+3)^2-1}{8} = \frac{64n^2+48n+8}{8} = 8n^2+6n+1$	1
$8n+5$	$\frac{(8n+5)^2-1}{8} = \frac{64n^2+80n+24}{8} = 8n^2+10n+3$	1
$8n+7$	$\frac{(8n+7)^2-1}{8} = \frac{64n^2+112n+48}{8} = 8n^2+14n+6$	0

□

7.3.23 Korollar Sei $n \in \mathbb{N}$ ungerade. Dann gilt $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$.

Beweis: In Proposition 7.3.22 haben wir ja bereits gesehen, dass

$$(-1)^{\frac{n^2-1}{8}} = \begin{cases} 1, & \text{wenn } n \bmod 8 \in \{1,7\} \\ -1, & \text{wenn } n \bmod 8 \in \{3,5\} \end{cases}$$

gilt. Sei nun $n = \prod_{i=1}^{r} p_i \prod_{j=1}^{r'} q_j \prod_{k=1}^{s} x_k \prod_{l=1}^{s'} y_l$, wobei $p_i \bmod 8 = 1$ für $1 \leq i \leq r$, $q_j \bmod 8 = 7$ für $1 \leq j \leq r'$, $x_k \bmod 8 = 3$ für $1 \leq k \leq s$ und $y_l \bmod 8 = 5$ für $1 \leq l \leq s'$ gilt, und alle p_i, q_j, x_k und y_l sind (nicht notwendigerweise verschiedene) Primzahlen. Dann ist

$$\begin{aligned} (\frac{2}{n}) &= \prod_{i=1}^{r} (\frac{2}{p_i}) \prod_{j=1}^{r'} (\frac{2}{q_j}) \prod_{k=1}^{s} (\frac{2}{x_k}) \prod_{l=1}^{s'} (\frac{2}{y_l}) \\ &= 1^r \cdot 1^{r'} \cdot (-1)^s \cdot (-1)^{s'} = (-1)^{s+s'} = \begin{cases} 1 & s+s' \text{ ist gerade} \\ -1 & s+s' \text{ ist ungerade.} \end{cases} \end{aligned}$$

Außerdem ist

$$\begin{aligned} n \bmod 8 &= \prod_{i=1}^{r} (p_i \bmod 8) \prod_{j=1}^{r'} (q_j \bmod 8) \prod_{k=1}^{s} (x_k \bmod 8) \prod_{l=1}^{s'} (y_l \bmod 8) \bmod 8 \\ &= 1^r \cdot 7^{r'} \cdot 3^s \cdot 5^{s'} \bmod 8. \end{aligned}$$

Dabei gilt $1^r \cdot 7^{r'} \bmod 8 \in \{1,7\}$ und $3^s \cdot 5^{s'} \in \{1,7\}$, wenn $s+s'$ gerade ist, und $3^s \cdot 5^{s'} \in \{3,5\}$, wenn $s+s'$ ungerade ist. Insgesamt ist also

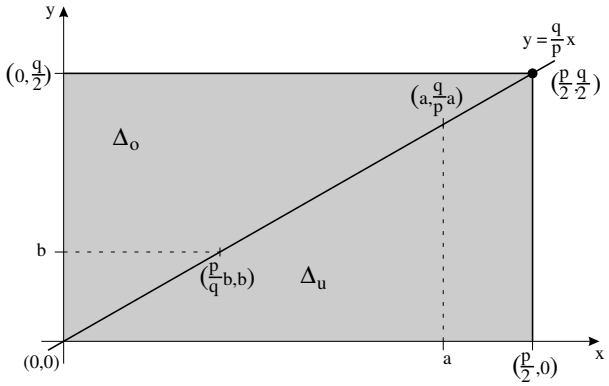
$$n \bmod 8 \in \begin{cases} \{1,7\}, & \text{wenn } s+s' \text{ gerade ist} \\ \{3,5\}, & \text{wenn } s+s' \text{ ungerade ist.} \end{cases}$$

Damit ergibt sich die Behauptung. □

7.3.24 Lemma Seien p und q verschiedene, ungerade Primzahlen. Dann gilt

$$\sum_{i=1}^{\frac{p-1}{2}} [\frac{qi}{p}] + \sum_{i=1}^{\frac{q-1}{2}} [\frac{pi}{q}] = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Beweis: Wir betrachten folgendes Rechteck:



Zählen wir die Punkte (a,b) in diesem Rechteck mit $1 \le a \le \frac{p-1}{2}$ und $1 \le b \le \frac{q-1}{2}$, das heißt, die ganzzahligen Punkte, die innerhalb des Rechtecks liegen, dann sind das $(\frac{p-1}{2})(\frac{q-1}{2})$.

Nun benutzen wir eine andere Methode, um diese Punkte zu zählen. Wir zählen nämlich die Punkte unter- und oberhalb der Geraden $y = \frac{q}{p}x$. Auf der Geraden selbst liegen keine ganzzahligen Punkte. Wenn wir nämlich annehmen, dass es $a, b \in \mathbb{N}$ gibt mit $b = \frac{q}{p}a$ und $1 \le a \le \frac{p-1}{2}$ und $1 \le b \le \frac{q-1}{2}$, dann folgt $pb = qa$, das heißt, $p \mid a$ und $q \mid b$. Da aber $1 \le a \le \frac{p-1}{2}$ und $1 \le b \le \frac{q-1}{2}$ gilt, ist dies ein Widerspruch.

Für jedes a mit $1 \le a \le \frac{p-1}{2}$ zählen wir nun die ganzzahligen Punkte $(a,b) \in \Delta_u$, also die ganzzahligen Punkte (a,b) mit $1 \le b < \frac{q}{p}a$. Dies sind gerade $[\frac{qa}{p}]$ viele. Das heißt, es gibt $\sum_{i=1}^{\frac{p-1}{2}} [\frac{qi}{p}]$ viele ganzzahlige Punkte innerhalb von Δ_u.

Nun zählen wir die ganzzahligen Punkte innerhalb von Δ_o: Ist $1 \leq b \leq \frac{q-1}{2}$, dann suchen wir ganzzahlige Punkte mit $1 \leq a \leq \frac{p}{q}b$ (denn die Gerade hat die Gleichung $y = \frac{q}{p}x$ oder $x = \frac{p}{q}y$). Dies sind $[\frac{p}{q}b]$ viele. Insgesamt gibt es also $\sum_{i=1}^{\frac{q-1}{2}}[\frac{pi}{q}]$ Punkte innerhalb von Δ_o. Zusammen erhalten wir die Behauptung. □

Das quadratische Reziprozitätsgesetz, das wir im Folgenden beweisen werden, wurde schon von Leonhard Euler (1707-1783) und Adrien-Marie Legendre (1752-1833) formuliert. Der erste richtige Beweis stammt von Carl Friedrich Gauß (1777-1855). Er veröffentlichte ihn im Jahr 1796, mit 18 Jahren. Gauß war sehr stolz auf sein Ergebnis und nannte das Reziprozitätsgesetz „Theorema Aureum“, den goldenen Satz. Im Laufe seines Lebens publizierte er acht Beweise für diesen Satz. Aber auch andere Mathematiker, wie zum Beispiel Augustin Louis Cauchy (1789-1857), Gotthold Eisenstein (1823-1852), Lejeune Dirichlet (1805-1859), Richard Dedekind (1831-1916) und Leopold Kronecker (1823-1891), haben Beweise für das quadratische Reziprozitätsgesetz gefunden. Bis 1921 waren 56 Beweise bekannt. Mittlerweile gibt es über 100 mehr oder weniger unterschiedliche Beweise für dieses wichtige Gesetz.

7.3.25 Satz (Quadratisches Reziprozitätsgesetz) Seien p und q verschiedene, ungerade Primzahlen. Dann gilt

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} 1, & \text{falls } p \bmod 4 = 1 \text{ oder } q \bmod 4 = 1. \\ -1, & \text{falls } p \bmod 4 = 3 \text{ und } q \bmod 4 = 3. \end{cases}$$

Beweis: In Lemma 7.3.21 setze $a = q$. Da $(q-1)$ gerade ist, folgt $k \bmod 2 = T \bmod 2$. Mit dem Gauß-Lemma gilt also $(\frac{q}{p}) = (-1)^k = (-1)^T$, wobei $T = \sum_{i=1}^{\frac{p-1}{2}}[\frac{qi}{p}]$ gilt. Nun setzen wir $p = q$ und $a = p$ in Lemma 7.3.21. Auch $(p-1)$ ist gerade, also ist $(\frac{p}{q}) = (-1)^{k'} = (-1)^{T'}$, wobei $T' = \sum_{i=1}^{\frac{q-1}{2}}[\frac{pi}{q}]$ gilt. Es folgt

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}}[\frac{pi}{q}]+\sum_{i=1}^{\frac{q-1}{2}}[\frac{pi}{q}]} = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$$

mit Lemma 7.3.24.

Im Beweis von Lemma 7.3.7 wurde gezeigt, dass $\frac{p-1}{2}$ und $\frac{q-1}{2}$ genau dann ungerade sind, wenn $p \bmod 4 = 3$ und $q \bmod 4 = 3$ gilt. Es folgt der zweite Teil der Behauptung des Satzes. □

7.3.26 Korollar Seien p und q verschiedene ungerade Primzahlen. Dann gilt

$$(\frac{p}{q}) = \begin{cases} -(\frac{q}{p}), & \text{falls } p \equiv q \equiv 3(\text{mod}4) \text{ gilt.} \\ (\frac{q}{p}), & \text{sonst.} \end{cases}$$

7.3.27 Aufgabe Beschreiben Sie die Primzahlen $p > 2$, für die 5 mod p ein quadratischer Rest ist.

Bis jetzt ging es nur um das Legendre-Symbol, doch auch für das Jacobi-Symbol gilt die äquivalente Aussage zum quadratischen Reziprozitätsgesetz. Zunächst noch eine Überlegung vorweg:

7.3.28 Lemma Sei $a \in \mathbb{N}$ ungerade, und sei $a = \prod_{i=1}^{n} p_i$, wobei die p_i Primzahlen seien, die nicht unbedingt alle verschieden sein müssen. Weiter sei $1 \leq r \leq n$, und es gelte $p_i \bmod 4 = 3$ für $1 \leq i \leq r$ und $p_i \bmod 4 = 1$ für $r+1 \leq i \leq n$. Dann gilt $a \bmod 4 = 3$ genau dann, wenn r ungerade ist.

Beweis: Es gilt

$$a \equiv (\prod_{i=1}^{n} p_i) \equiv (\prod_{i=1}^{r} p_i)(\prod_{i=r+1}^{n} p_i) \equiv (\prod_{i=1}^{r} 3)(\prod_{i=r+1}^{n} 1) \equiv 3^r(\text{mod}4).$$

Sei r ungerade, das heißt $r = 2l+1$ für ein $l \in \mathbb{N}_0$. Dann ist

$$3^r \equiv 3^{2l+1} \equiv (3^2)^l \cdot 3 \equiv 9^l \cdot 3 \equiv 1^l \cdot 3 \equiv 3(\text{mod}4).$$

Ist r gerade, also $r = 2l$ für ein $l \in \mathbb{N}_0$, dann ist

$$3^r \equiv 3^{2l} \equiv (3^2)^l \equiv 9^l \equiv 1^l \equiv 1(\text{mod}4).$$

□

7.3.29 Satz (Reziprozitätsgesetz für das Jacobi-Symbol) Seien $a, b > 2$ ungerade Zahlen mit $\text{ggT}(a,b) = 1$. Dann gilt:

$$(\frac{a}{b})(\frac{b}{a}) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}.$$

Beweis: Sei $a = \prod_{i=1}^{n} p_i$, wobei die p_i Primzahlen und $p_i \bmod 4 = 3$ für $1 \leq i \leq r$ und $p_i \bmod 4 = 1$ für $r+1 \leq i \leq n$ seien. Analog sei $b = \prod_{j=1}^{m} q_j$, wobei die q_j

Primzahlen und $q_j \bmod 4 = 3$ für $1 \leq j \leq s$ und $q_j \bmod 4 = 1$ für $s+1 \leq j \leq m$ seien. Es gilt

$$\begin{aligned}
(\frac{a}{b})(\frac{b}{a}) &= \prod_{j=1}^{m}(\frac{a}{q_j})\prod_{i=1}^{n}(\frac{b}{p_i}) \text{ nach Definition} \\
&= \prod_{j=1}^{m}\prod_{i=1}^{n}(\frac{p_i}{q_j})\prod_{i=1}^{n}\prod_{j=1}^{m}(\frac{q_j}{p_i}) \text{ nach Lemma 7.3.11} \\
&= \prod_{j=1}^{m}\prod_{i=1}^{n}(\frac{p_i}{q_j})(\frac{q_j}{p_i}) \\
&= \prod_{j=1}^{m}\prod_{i=1}^{n}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} \text{ mit dem Quadratischen Reziprozitätsgesetz.}
\end{aligned}$$

Nun ist $\frac{p_i-1}{2}$ ungerade für $1 \leq i \leq r$ und gerade für $r+1 \leq i \leq n$. Weiter ist $\frac{q_j-1}{2}$ ungerade für $1 \leq j \leq s$ und gerade für $s+1 \leq j \leq m$. Also folgt

$$\begin{aligned}
\prod_{i=1}^{n}\prod_{j=1}^{m}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} = -1 &\Leftrightarrow rs \text{ ist ungerade} \\
&\Leftrightarrow r \text{ ist ungerade und } s \text{ ist ungerade} \\
&\Leftrightarrow a \bmod 4 = 3 \text{ und } b \bmod 4 = 3 \text{ (mit Lemma 7.3.28)} \\
&\Leftrightarrow (-1)^{\frac{a-1}{2}\frac{b-1}{2}} = -1.
\end{aligned}$$

□

Wie würde man jetzt also vorgehen, um $(\frac{a}{b})$ für natürliche, teilerfremde Zahlen $b > a \geq 2$ mit b ungerade zu berechnen? Zuerst schreiben wir $a = 2^k a'$, wobei a' ungerade ist. Dann ist $(\frac{a}{b}) = (\frac{2}{b})^k(\frac{a'}{b})$, und $(\frac{2}{b})^k = 1$, wenn k gerade ist und $(-1)^{\frac{b^2-1}{8}}$, wenn k ungerade ist. Wir haben also das Problem der Berechnung von $(\frac{a}{b})$ auf die Berechnung von $(\frac{a'}{b})$ reduziert. Mit dem quadratischen Reziprozitätsgesetz ist $(\frac{a'}{b}) = (-1)^{\frac{a'-1}{2}\frac{b-1}{2}}(\frac{b}{a'})$. Nun gilt $(\frac{b}{a'}) = (\frac{r}{a'})$, wobei $r \equiv b(\mathrm{mod} a')$ und $0 \leq r < a'$ gilt. Nun muss also nur noch $(\frac{r}{a'})$ berechnet werden, wobei $r < a'$ gilt, a' ungerade ist und $\mathrm{ggT}(a', r) = 1$ gilt. Wir haben unser Anfangsproblem also auf dasselbe Problem mit kleineren Eingabewerten reduziert.

Dies können wir nun wiederholen bis irgendwann nur noch ein Jacobi-Symbol der Form $(\frac{1}{n}) = 1$ berechnet wird. Genau wie hier beschrieben, geht nun der Algorithmus vor:

7.3.30 Algorithmus (Berechnung des Jacobi-Symbols)

Eingabe Natürliche Zahlen $a, b \in \mathbb{N}$ mit $b > a \geq 2$, b ungerade und $\mathrm{ggT}(a, b) = 1$.

Ausgabe Das Jacobi-Symbol $(\frac{a}{b})$.

1. $x \leftarrow a$, $y \leftarrow b$ und $J \leftarrow 1$.

2. **while** $x \neq 1$ **do**

3. Berechne $k, x' \in \mathbb{N}_0$, wobei $x = 2^k x'$ gilt und x' ungerade ist.

4. **if** k ist ungerade **then** $J \leftarrow (-1)^{\frac{y^2-1}{8}} J$.

5. **if** $x' \neq 1$ **then**

6. $J \leftarrow (-1)^{\frac{x'-1}{2}\frac{y-1}{2}} J$.

7. dividiere y mit Rest durch x', das heißt, berechne $0 \leq r < x'$ mit

$$y = qx' + r.$$

8. $y \leftarrow x'$ und $x \leftarrow r$.

9. **else** $x \leftarrow 1$.

10. **übergebe** J.

Um den Algorithmus besser zu verstehen, sehen wir uns zunächst ein Beispiel an.

7.3.31 Beispiel Wir wollen mit dem Algorithmus $(\frac{7405}{54323})$ berechnen.

Eingabe $a = 7405$ und $b = 54323$.

1. $x \leftarrow 7405$, $y \leftarrow 54323$ und $J \leftarrow 1$.

2. Es gilt $7405 \neq 1$, also

3. $7405 = 2^0 \cdot 7405$, also $k = 0$ und $x' = 7405$.

4. k ist gerade, also ist nichts zu tun.

5. $x' \neq 1$, also

6. $J \leftarrow (-1)^{\frac{7405-1}{2}\frac{54323-1}{2}} \cdot 1 = 1$.

7. $54323 = 7 \cdot 7405 + 2488$, also $r = 2488$.

8. $y \leftarrow 7405$ und $x \leftarrow 2488$.

Bis jetzt haben wir also berechnet: $(\frac{7405}{54323}) = (\frac{2488}{7405})$. Nun kommt der zweite Durchlauf der **while**-Schleife:

2. Es gilt $2488 \neq 1$, also

3. $2488 = 2^3 \cdot 311$, also $k = 3$ und $x' = 311$.

4. $J \leftarrow (-1)^{\frac{7405^2-1}{8}} \cdot 1 = -1$.

5. $x' \neq 1$, also

6. $J \leftarrow (-1)^{\frac{311-1}{2}\frac{7405-1}{2}}(-1) = -1$.

7. $7405 = 23 \cdot 311 + 252$, also $r = 252$.

8. $y \leftarrow 311$ und $x \leftarrow 252$.

Neues Zwischenergebnis ist $(\frac{7405}{54323}) = -(\frac{252}{311})$. Es folgt der dritte Durchlauf der **while**-Schleife:

2. $252 \neq 1$, also

3. $252 = 2^2 \cdot 63$, also $k = 2$ und $x' = 63$.

4. k ist gerade, also ist nichts zu tun.

5. $x' \neq 1$, also

6. $J \leftarrow (-1)^{\frac{63-1}{2}\frac{311-1}{2}}(-1) = 1$.

7. $311 = 4 \cdot 63 + 59$, also $r = 59$.

8. $y \leftarrow 63$ und $x \leftarrow 59$.

Nun haben wir als Zwischenergebnis $(\frac{7405}{54323}) = (\frac{59}{63})$. Wir benötigen noch einen vierten Durchlauf:

2. $59 \neq 1$, also

3. $59 = 2^0 \cdot 59$, also $k = 0$ und $x' = 59$.

4. k ist gerade, also ist nicht zu tun.

5. $x' \neq 1$, also

6. $J \leftarrow (-1)^{\frac{59-1}{2}\frac{63-1}{2}} \cdot 1 = -1$.

7. $63 = 59 + 4$, also $r = 4$.

8. $y \leftarrow 59$ und $x \leftarrow 4$.

Nun ist das Zwischenergebnis $(\frac{7405}{54323}) = -(\frac{4}{59})$. Der nächste Durchlauf der **while**-Schleife liefert:

2. $4 \neq 1$, also

3. $4 = 2^2 \cdot 1$, also $k = 2$ und $x' = 1$.

4. k ist gerade, also ist nichts zu tun.

5. $x' = 1$, also weiter mit Schritt 9.

9. $x \leftarrow 1$.

Die **while**-Schleife wird nun beendet:

2. $x = 1$, also wird die **while**-Schleife beendet.

10. Das Ergebnis ist $J = -1$.

Nun wollen wir uns davon überzeugen, dass Algorithmus 7.3.30 immer das Richtige tut.

7.3.32 Lemma In Algorithmus 7.3.30 gilt nach jedem Durchlauf der **while**-Schleife

$$(\frac{a}{b}) = J(\frac{x}{y}),$$

und es gilt $y > x$, y ist ungerade und $\mathrm{ggT}(x, y) = 1$.

Beweis: Wir beweisen die Behauptung durch Induktion über die Anzahl n der Durchläufe der **while**-Schleife. Für $n = 0$, also vor der ersten **while**-Schleife, gilt $x = a$, $y = b$ und $J = 1$, also $(\frac{a}{b}) = 1 \cdot (\frac{x}{y})$ und x, y sind natürliche Zahlen mit $y > x$, $\mathrm{ggT}(x, y) = 1$ und y ist ungerade. Sei nun $n \geq 0$, und es gelte nach n Durchläufen $(\frac{a}{b}) = J(\frac{x}{y})$ mit $y > x$ und y ist ungerade mit $\mathrm{ggT}(x, y) = 1$. Ist $x = 1$, dann ist $(\frac{1}{y}) = 1$, und die **while**-Schleife bricht mit J als dem richtigen Ergebnis ab. Geht der Algorithmus in die nächste Schleife, ist also $x > 1$, dann gilt $(\frac{x}{y}) = (\frac{2^k x'}{y}) = (\frac{2}{y})^k (\frac{x'}{y})$, wobei $(\frac{2}{y})^k = 1$ gilt, wenn k gerade ist und $(\frac{2}{y})^k = (-1)^{\frac{y^2-1}{8}}$, wenn k ungerade ist. Das heißt, nach der Zuweisung $J \leftarrow (-1)^{\frac{y^2-1}{8}} J$ gilt $(\frac{a}{b}) = J(\frac{x'}{y})$. Ist $x' = 1$, dann ist $(\frac{x'}{y}) = (\frac{1}{y}) = 1$, und es gilt $(\frac{a}{b}) = J$. Der Algorithmus endet für $x' = 1$ also mit dem richtigen Ergebnis. Ist $x' \neq 1$, dann ist $(\frac{x'}{y}) = (-1)^{\frac{x'-1}{2}\frac{y-1}{2}} (\frac{y}{x'})$ und $(\frac{y}{x'}) = (\frac{r}{x'})$, wobei r der Rest der Division von y durch x' ist. Da $\mathrm{ggT}(x', y) = 1$ ist, folgt $r \neq 0$ und $\mathrm{ggT}(r, x') = 1$ (denn jeder gemeinsame Teiler von r und x' ist auch ein Teiler von y). Außerdem ist x' nach Voraussetzung ungerade. Das heißt, nach Durchlaufen der **while**-Schleife und den Zuweisungen $x \leftarrow r$ und $y \leftarrow x'$ gilt weiterhin $(\frac{a}{b}) = J(\frac{x}{y})$, $y > x$, y ist ungerade und $\mathrm{ggT}(x, y) = 1$. □

Schauen wir uns nun zunächst an, welche Schritte innerhalb einer **while**-Schleife durchgeführt werden: In Schritt 3 werden Zweierpotenzen aus x gezogen. Dieses ist mit k Divisionen von x durch 2 möglich, wobei $k \leq \log_2 x \leq \log_2 a$ ist. In

Schritt 4 muss nun noch $(-1)^{\frac{y^2-1}{8}}$ berechnet werden, wenn k gerade ist. Wie wir in Lemma 7.3.22 gesehen haben, muss dazu $y \bmod 8$ berechnet werden, dies ist also eine Division mit Rest durch 8. In Schritt 6 wird $(-1)^{\frac{x'-1}{2}\frac{y-1}{2}}$ gebildet. Dazu müssen, wie wir in 7.3.25 gesehen haben, $x' \bmod 4$ und $y \bmod 4$ berechnet werden. Das ist als eine Division mit Rest durch 4 effizient möglich. Schritt 7 ist ebenfalls eine Division mit Rest, also effizient durchführbar. Schritt 8 besteht schließlich aus Zuweisungen, so dass wir sehen, dass sich alle Schritte innerhalb einer **while**-Schleife effizient ausführen lassen.

Um die Anzahl der Durchläufe der **while**-Schleife bei der Berechnung von $(\frac{a}{b})$ abzuschätzen, nehmen wir zunächst an, dass in keinem der Schritte bei der Division mit Rest ein gerader Rest herauskommt, dass also in Schritt 3 immer $k = 0$ gilt . Schauen wir uns ein Beispiel an:

Eingabe $a = 51$ und $b = 127$.

1. $x \leftarrow 51$, $y \leftarrow 127$ und $J \leftarrow 1$.

2. $51 \neq 1$, also

3. $51 = 2^0 \cdot 51$, also $k = 0$ und $x' = 51$.

4. Hier ist nichts zu tun.

5. $51 \neq 1$, also

6. $J \leftarrow (-1)^{\frac{51-1}{2}\frac{127-1}{2}} \cdot 1 = -1$.

7. $127 = 2 \cdot 51 + 25$, also $r = 25$.

8. $x \leftarrow 25$ und $y \leftarrow 57$.

2. $25 \neq 1$, also

3. $25 = 2^0 \cdot 25$, also $k = 0$ und $x' = 25$.

4. Hier ist nichts zu tun.

5. $25 \neq 1$, also

6. $J \leftarrow (-1)^{\frac{25-1}{2}\frac{51-1}{2}}(-1) = -1$.

7. $51 = 2 \cdot 25 + 1$, also $r = 1$.

8. $x \leftarrow 1$ und $y \leftarrow 25$.

2. $x = 1$, also wird die **while**-Schleife beendet.

10. Das Ergebnis ist $J = -1$.

Schaut man genau hin, sieht man, dass im Schritt 7 genau dieselben Divisionen mit Rest ausgeführt werden wie beim Euklidischen Algorithmus:

$$\begin{aligned} 127 &= 2 \cdot 51 + 25 \\ 51 &= 2 \cdot 25 + 1. \end{aligned}$$

Wenn Zweierpotenzen auftreten, werden die Divisionen mit Rest etwas modifiziert. Wir berechnen:

$$\begin{aligned} b &= q_1 a + 2^{k_2} r_2 \\ a &= q_2 r_2 + 2^{k_3} r_3 \\ r_2 &= q_3 r_3 + 2^{k_4} r_4 \\ &\vdots \\ r_{n-1} &= q_n r_n. \end{aligned}$$

Wenn wir nun wieder $b = r_0$ und $a = r_1$ setzen, dann ist $q_i \geq 1$ für $1 \leq i \leq n$ und $k_i \geq 0$ für $2 \leq i \leq n$. Außerdem ist r_i ungerade für $0 \leq i \leq n$, und es gilt $0 < 2^{k_i} r_i < r_{i-1}$ für $2 \leq i \leq n$. Nun können wir die Länge n der modifizierten Folge von Resten analog zu 6.5 abschätzen: Für $1 \leq i \leq n-2$ gilt:

$$r_i = q_{i+1} r_{i+1} + 2^{k_{i+2}} r_{i+2} \geq r_{i+1} + 2^{k_{i+2}} r_{i+2} \geq r_{i+1} + r_{i+2} > 2 r_{i+2}.$$

Genauso wie in 6.5 folgt jetzt $n < 2(\log_2 a + 1)$. Wir haben also gezeigt:

7.3.33 Proposition In Algorithmus 7.3.30 ist die Anzahl der Durchläufe der **while**-Schleife zur Berechnung des Jacobi-Symbols $(\frac{a}{b})$ beschränkt durch $2(\log_2 a + 1)$. □

Die Anzahl der Durchläufe der **while**-Schleife in Algorithmus 7.3.30 zur Berechnung von $(\frac{a}{b})$ ist also beschränkt durch das Doppelte der Bitlänge von a, und damit ist Algorithmus 7.3.30 effizient.

7.3.34 Aufgabe Ist die Anzahl der Divisionen mit Rest zur Berechnung des Jacobi-Symbols immer kleiner als die Anzahl der Divisionen mit Rest beim Euklidischen Algorithmus?

Lösungen der Aufgaben

Lösungen der Aufgaben in Kapitel 7

Aufgabe 7.1.5 Sei $n \in \mathbb{N}$ zusammengesetzt.

Behauptung Die Menge

$$P = \{b \in (\mathbb{Z}/n\mathbb{Z})^\times \mid n \text{ ist Pseudoprimzahl zur Basis } b\}$$

ist eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$.

Beweis: Seien $a, b \in P$. Dann gilt $a^{n-1} \equiv 1(\mathrm{mod} n)$ und $b^{n-1} \equiv 1(\mathrm{mod} n)$. Es folgt

$$(ab^{-1})^{n-1} \equiv a^{n-1}(b^{-1})^{n-1} \equiv 1 \cdot (b^{n-1})^{-1} \equiv 1^{-1} \equiv 1(\mathrm{mod} n),$$

also $ab^{-1} \in P$. Mit dem Untergruppenkriterium gilt, dass P eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$ ist. □

Aufgabe 7.1.8 Welches ist die Ergebnismenge beim Fermat-Test, was ist die Wahrscheinlichkeitsverteilung, und was genau ist das Ereignis, dessen Wahrscheinlichkeit höchstens $\frac{1}{2}$ ist?

Die Ergebnismenge beim Fermat-Test ist $S = \{1, \ldots, n-1\}$. Es gilt $P(\{i\}) = \frac{1}{n-1}$ für alle $i \in S$. Sei $A = \{i \in S \mid \mathrm{ggT}(i, n) = 1\}$ und sei $B = \{i \in A \mid n \text{ ist Pseudoprimzahl zur Basis } i\}$. Es ist $A \subseteq S$, also $P(A) \leq P(S) = 1$. Außerdem folgt mit Proposition 7.1.6, dass $|B| \leq \frac{1}{2}|A|$ gilt – wenn n zusammengesetzt und keine Carmichael-Zahl ist. Es folgt $P(B) \leq \frac{1}{2}P(A) \leq \frac{1}{2}$. □

Aufgabe 7.1.12 Für $k \geq 1$ ist die k-te Fermat-Zahl definiert als $2^{2^k} + 1$.

Behauptung Für alle $k \in \mathbb{N}$ gilt: Ist die k-te Fermat-Zahl zusammengesetzt, dann ist sie eine Pseudoprimzahl zur Basis 2.

Beweis: Sei $k \geq 1$. Dann gilt:

$$2^{2^{2^k}} \equiv (2^{2^k})^{2^{2^k-k}} \equiv (-1)^{2^{2^k-k}} \equiv 1 (\mathrm{mod} 2^{2^k}+1),$$

also ist $2^{2^k}+1$ eine Pseudoprimzahl zur Basis 2, wenn diese Zahl zusammengesetzt ist. □

Aufgabe 7.2.7 Zeigen Sie mit dem Rabin-Miller-Test, dass 561 zusammengesetzt ist.

Es gilt $560 = 2^4 \cdot 5 \cdot 7$, setze also $r = 4$ und $s = 35$. Setze außerdem $b = 2$. Dann gilt:

$$\begin{aligned} x_0 &= 2^{35} \bmod 561 = 263 \\ x_1 &= 263^2 \bmod 561 = 166 \\ x_2 &= 166^2 \bmod 561 = 67 \\ x_3 &= 67^2 \bmod 561 = 1 \\ x_4 &= 1. \end{aligned}$$

Also ist 561 zusammengesetzt. □

Aufgabe 7.3.1 Sei $p > 2$ eine Primzahl, und sei g ein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$. Es gelte $g^i \equiv g^j (\mathrm{mod} p)$ für $i, j \in \mathbb{Z}$.

Behauptung i ist genau dann gerade, wenn j gerade ist.

Beweis: Es gelte $g^i \equiv g^j (\mathrm{mod} p)$ und i sei gerade. Dann folgt $g^{i-j} \equiv 1 (\mathrm{mod} p)$, also $p-1 \mid i-j$. Es gibt also ein $k \in \mathbb{Z}$ mit $j = i - k(p-1)$. Da i und $p-1$ gerade sind, ist auch j gerade.

Die andere Richtung wird analog bewiesen. □

Aufgabe 7.3.8 Zu berechnen sind $(\frac{40}{31})$ und $(\frac{-4}{31})$.

Es gilt

$$\begin{aligned} (\frac{40}{31}) &= (\frac{9}{31}) = (\frac{3}{31})^2 = 1 \text{ und} \\ (\frac{-4}{31}) &= (\frac{-1}{31})(\frac{4}{31}) = (\frac{-1}{31}) = -1, \text{ denn } 31 \bmod 4 = 3. \end{aligned}$$

□

Aufgabe 7.3.10 Sei $n > 2$ ungerade und zusammengesetzt, und sei $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Behauptung Ist a ein quadratischer Rest in $(\mathbb{Z}/n\mathbb{Z})^\times$, das heißt, es gibt ein $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ mit $b^2 \bmod n = a$, dann gilt $(\frac{a}{n}) = 1$.

Beweis: Sei $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ die Primzahlzerlegung von n. Für $1 \leq i \leq k$ gilt dann $b^2 \equiv a (\mathrm{mod} p_i)$, also ist a ein quadratischer Rest $\mathrm{mod} p_i$. Es folgt

$$(\frac{a}{n}) = (\frac{a}{p_1})^{\alpha_1} \dots (\frac{a}{p_k})^{\alpha_k} = 1^{\alpha_1} \dots 1^{\alpha_k} = 1.$$

□

Aufgabe 7.3.17 Benutzen Sie den Solovay-Strassen-Test, um zu zeigen, dass 15 zusammengesetzt ist.

Wähle $b = 2$, dann ist $\mathrm{ggT}(2, 15) = 1$, und es gilt $2^7 \equiv 2^3 \cdot 2^4 \equiv 2^3 \equiv 8 (\mathrm{mod}\ 15)$. Da $(\frac{2}{15}) = \pm 1$ ist, gilt auf jeden Fall $b^{\frac{n-1}{2}} \not\equiv (\frac{b}{n}) (\mathrm{mod} n)$, also ist $n = 15$ zusammengesetzt. □

Aufgabe 7.3.20 Sei $p > 2$ eine Primzahl. Berechnen Sie $(\frac{-1}{p})$ mit dem Gauß-Lemma.

Wir wollen $(\frac{-1}{p})$ berechnen und berechnen dazu

$$S = \{-1 \bmod p, -2 \bmod p, \dots, -\frac{p-1}{2} \bmod p\} = \{p-1, p-2, \dots, \frac{p+1}{2}\}.$$

k ist die Anzahl der Elemente in S, die größer als $\frac{p}{2}$ sind, also $k = \frac{p-1}{2}$. Es folgt mit dem Gauß-Lemma:

$$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{falls } \frac{p-1}{2} \text{ gerade ist, also falls } p \bmod 4 = 1 \text{ gilt,} \\ -1, & \text{falls } \frac{p-1}{2} \text{ ungerade ist, also falls } p \bmod 4 = 3 \text{ gilt.} \end{cases}$$

□

Aufgabe 7.3.27 Beschreiben Sie die Primzahlen $p > 2$, für die $5 \bmod p$ ein quadratischer Rest ist.

Sei $p > 2$ eine Primzahl mit $(\frac{5}{p}) = 1$. Da $5 \bmod 4 = 1$ gilt, ist

$$1 = (\frac{5}{p}) = (\frac{p}{5}) = (\frac{p \bmod 5}{5}).$$

Es gilt $(\frac{1}{5}) = (\frac{4}{5}) = 1$ und $(\frac{2}{5}) = (\frac{3}{5}) = -1$. Also folgt, dass $(\frac{5}{p}) = 1$ genau dann gilt, wenn $p \bmod 5 = 1$ oder $p \bmod 5 = 4$ gilt.

Die Zahl $p = 11$ ist ein Beispiel für die erste Bedingung und die Zahl $p = 19$ ist ein Beispiel für die zweite Bedingung. □

Aufgabe 7.3.34 Ist die Anzahl der Divisionen mit Rest zur Berechnung des Jacobi-Symbols immer kleiner als die Anzahl der Divisionen mit Rest beim Euklidischen Algorithmus?

Nein, für $a = 189$ und $b = 347$ werden im Euklidischen Algorithmus folgende Divisionen mit Rest gemacht:

$$\begin{aligned} 347 &= 1 \cdot 189 + 158 \\ 189 &= 1 \cdot 158 + 31 \\ 158 &= 5 \cdot 31 + 3 \\ 31 &= 10 \cdot 3 + 1. \end{aligned}$$

Zur Berechnung des Jacobi-Symbols werden folgende Divisionen mit Rest durchgeführt:

$$\begin{aligned} 347 &= 1 \cdot 189 + 158 && r' \text{ ist also } 79 \\ 189 &= 2 \cdot 79 + 31 \\ 79 &= 2 \cdot 31 + 17 \\ 31 &= 1 \cdot 17 + 14 && r' \text{ ist also } 7 \\ 17 &= 2 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1. \end{aligned}$$

Man sieht, dass die Anzahl der Divisionen mit Rest im zweiten Fall größer ist. □

Kurseinheit 5

Körper

Studierhinweise

Im ersten Kapitel von Kurseinheit 5 wird es theoretisch. Um im zweiten Kapitel nämlich zu den Kryptosystemen über endlichen Körpern zu kommen, sehen wir uns zunächst die endlichen Körper näher an. Schnell kann man sich klarmachen, dass die Anzahl der Elemente eines endlichen Körpers immer eine Primzahlpotenz ist. Andererseits werden wir zeigen, dass es zu jeder Primzahlpotenz p^n genau einen endlichen Körper mit p^n Elementen gibt. Dazu muss einige Theorie über Körpererweiterungen entwickelt werden. Diese Theorie lässt sich zum großen Teil nicht nur auf endliche Körper anwenden. Mit dem Gradsatz lässt sich zum Beispiel zeigen, dass es keinen Körper gibt, der „zwischen“ den Körpern $\mathbb{R}$ und $\mathbb{C}$ liegt, das heißt, es gibt keinen Körper, der $\mathbb{R}$ als echte Teilmenge enthält und der andererseits eine echte Teilmenge von $\mathbb{C}$ ist.

Für die endlichen Körper können wir sogar genau bestimmen, welcher endliche Körper in einem anderen endlichen Körper enthalten ist.

Anschließend werden die n-ten Einheitswurzeln kurz vorgestellt. Diese gibt es wieder über jedem Körper. Es sind einfach die Nullstellen (eventuell in einem größeren Körper) des Polynoms $T^n - 1$. Es stellt sich heraus, dass die n-ten Einheitswurzeln über einem Körper $\mathbb{K}$ eine zyklische Gruppe bilden. Die erzeugenden Elemente dieser Gruppe heißen primitive n-te Einheitswurzeln, und das n-te Kreisteilungpolynom ist ein Polynom, dessen Nullstellen gerade die primitiven n-ten Einheitswurzeln sind. Wir benötigen die n-ten Einheitswurzeln an einer Stelle in Kurseinheit 6 und entwickeln hier im Wesentlichen das, was in der nächsten Kurseinheit benötigt wird.

Die Spur eines Elementes ist wieder nur in einer endlichen Körpererweiterung $\mathbb{L}$ eines endlichen Körpers $\mathbb{K}$ definiert. Die Spur eines Elementes aus $\mathbb{L}$ ist ein Element aus $\mathbb{K}$, und wir werden sehen, dass die Spur eine lineare Abbildung von $\mathbb{L}$ nach $\mathbb{K}$ ist. Wir werden einige Eigenschaften dieser Abbildung, die später noch benötigt werden, näher beleuchten.

Es stellt sich die Frage, warum es nötig ist, alle endlichen Körper zu kennen.

Wenn bei einem Kryptosystem ein endlicher Körper verlangt wird, kann man doch einen Körper der Form $\mathbb{F}_p$ mit einer Primzahl p nehmen. Das stimmt in gewisser Weise und wird auch häufig gemacht. Schließlich kann man in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ effizient rechnen, indem man mit Rest durch p dividiert. Um Kryptografie über endlichen Körpern zu betreiben, reichen solche Körper vollkommen aus. Aber abgesehen von der Tatsache, dass es nie schaden kann, die Theorie der endlichen Körper zu kennen, fällt eine wichtige Klasse von geeigneten endlichen Körpern damit weg. Die Körper mit 2^n Elementen für ein $n \in \mathbb{N}$ sind von Interesse für die Kryptografie, weil sie einfach wie gemacht sind für die Behandlung durch einen Computer. Die Elemente eines solchen Körpers kann man nämlich ganz kompakt als Folge von Nullen und Einsen darstellen und die Arithmetik in diesem Körper dadurch extrem schnell machen. Wenn also bei den vorgestellten Kryptosystemen von endlichen Körpern die Rede ist, sollten Sie auch an diese Beispiele denken.

Im zweiten Kapitel dieser Kurseinheit werden nun also Kryptosysteme über endlichen Körpern vorgestellt. Alle diese Kryptosysteme spielen sich in der zyklischen Gruppe $\mathbb{K}^\times$ eines endlichen Körpers ab. Dabei wird ausgenutzt, dass der diskrete Logarithmus in dieser Gruppe schwer zu berechnen ist. Das bedeutet, dass es schwer ist – gegeben ein primitives Element $g \in \mathbb{K}^\times$ und außerdem g^a für ein $a \in \mathbb{Z}$ – dieses a dann zu berechnen. Vermutet wird, dass es keinen effizienten Algorithmus gibt, um dieses Problem zu lösen.

Es werden drei Kryptosysteme vorgestellt. Eins dient dazu einen Schlüssel auszutauschen, mit den anderen beiden können geheime Nachrichten übermittelt werden. Das erste aus dem Jahr 1976 ist von Diffie und Hellman ([DH]) und war das erste Public-Key-Kryptosystem überhaupt. Falls Sie sich übrigens für die Entstehungsgeschichte dieses Kryptosystems interessieren, empfehlen wir Ihnen das Buch [Si2]. Gerne hätten wir auch noch Systeme vorgestellt, die zur Authentifikation (stelle sicher, dass eine Nachricht von X wirklich von X ist) oder zur Feststellung der Integrität (stelle sicher, dass die Nachricht im Zuge der Übermittlung nicht verändert wurde) dienen, doch sie konnten in diesem Kurs nicht mehr untergebracht werden.

Kapitel 8

Körper

8.1 Beispiele endlicher Körper

In dieser Kurseinheit werden Körper behandelt. Dabei werden wir vor allem endliche Körper betrachten. Es wird jedoch auch Einiges ganz allgemein für beliebige Körper entwickelt.

Vorsichtshalber wiederholen wir Definition 5.1.5: Ein kommutativer Ring $(R, +, \cdot)$ mit $R \neq \{0\}$, bei dem $(R \setminus \{0\}, \cdot)$ eine Gruppe ist, wird ein **Körper** genannt.

Wir haben schon viele Beispiele für Körper kennen gelernt. Sowohl für unendliche, wie etwa $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$, als auch für endliche Körper, wie zum Beispiel die Körper $\mathbb{F}_p$, wobei p eine Primzahl ist. Das Hauptanliegen dieser Kurseinheit soll es sein, alle endlichen Körper zu charakterisieren. Bevor wir dies mit einem relativ großen Aufwand tun, sehen wir uns zunächst Beispiele für endliche Körper an, die nicht von der Form $\mathbb{F}_p$ für eine Primzahl p sind.

Sei $\mathbb{K}$ ein Körper. Wir haben in der letzten Kurseinheit in Proposition 5.7.3 gesehen, dass $\mathbb{K}[T]$ ein Hauptidealring ist. Die irreduziblen Polynome in $\mathbb{K}[T]$ sind die Primelemente in $\mathbb{K}[T]$. Mit 5.6.10 folgt:

8.1.1 Satz Sei $\mathbb{K}$ ein Körper, und sei $f \in \mathbb{K}[T]$ ein Polynom. Genau dann ist $\mathbb{K}[T]/(f)$ ein Körper, wenn f irreduzibel in $\mathbb{K}[T]$ ist. □

Wir wollen nun die Ringe -beziehungsweise die Körper- $\mathbb{K}[T]/(f)$, $f \in \mathbb{K}[T]$, genauer anschauen. Dazu sei f ein Polynom vom Grad $n > 0$ in $\mathbb{K}[T]$.

Zur Erinnerung: Der Faktorring $\mathbb{K}[T]/(f)$ besteht aus den Nebenklassen

$$[g] = g + (f) = \{g + hf \mid h \in \mathbb{K}[T]\}.$$

Die Verknüpfungen $[g] + [g']$ und $[g][g']$ sind durch $[g + g']$ beziehungsweise $[gg']$ definiert.

Zwei Nebenklassen $[g], [g']$ sind gleich, wenn $g - g' \in (f)$, wenn also $g - g'$ durch f teilbar ist. Dies ist äquivalent dazu, dass g und g' beim Teilen durch f denselben Rest lassen.

Jede Nebenklasse $[g]$ modulo (f) enthält genau ein Polynom r mit $\mathrm{Grad}(r) < \mathrm{Grad}(f)$. Das Polynom r ist gerade der Rest bei der Division von g durch f mit Rest.

Wir können nun die Elemente in $\mathbb{K}[T]/(f)$ explizit beschreiben: Es sind die Nebenklassen $[r] = r + (f)$, wobei r alle Polynome in $\mathbb{K}[T]$ mit $\mathrm{Grad}(r) < \mathrm{Grad}(f) = n$ sind.

Ist $\mathbb{K} = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, p eine Primzahl, ein Körper mit p Elementen, so gibt es p^n Polynome

$$a_0 + a_1 T + \ldots + a_{n-1} T^{n-1},$$

vom Grad $< n$, denn für jeden Koeffizienten a_i haben wir p Möglichkeiten.

8.1.2 Beispiel Sei $\mathbb{K} = \mathbb{F}_2$, und sei $f = T \in \mathbb{F}_2[T]$. Es ist $\mathrm{Grad}(f) = 1$. Es gibt 2 Polynome vom Grad < 1 in $\mathbb{F}_2[T]$, das Nullpolynom 0 und das konstante Polynom 1. Die Elemente in $\mathbb{F}_2[T]/(f)$ sind somit die Nebenklassen $[0]$ und $[1]$. Die Verknüpfungen in $\mathbb{F}_2[T]/(f)$ entsprechen denen in $\mathbb{F}_2$: Die Additions- beziehungsweise die Multiplikationstabelle von Elementen in $\mathbb{F}_2[T]/(f)$ ist:

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

und

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

8.1.3 Beispiel Sei $\mathbb{K} = \mathbb{F}_2$, und sei $f = T^2 + T + 1$. Wir haben in Beispiel 5.7.23 gesehen, dass f irreduzibel in $\mathbb{F}_2[T]$ ist. Somit ist $\mathbb{F}_2[T]/(f)$ mit Satz 8.1.1 ein Körper. Die Elemente von $\mathbb{F}_2[T]/(f)$ sind die Nebenklassen der Polynome in $\mathbb{F}_2[T]$ vom Grad < 2, also $[0], [1], [T], [T + 1]$. Die Addition und die Multiplikation dieser Restklassen erfolgt wie oben beschrieben. Hier müssen wir noch beachten, dass $\mathbb{F}_2[T]$ und $\mathbb{F}_2[T]/(f)$ die Charakteristik 2 haben. Beispielsweise ist $[T] + [T + 1] = [2T + 1] = [1]$ in $\mathbb{F}_2[T]/(f)$.

Als weiteres Beispiel: Es ist $[T][T + 1] = [T^2 + T] = [1]$, denn $T^2 + T = (T^2 + T + 1) + 1$, das heißt, bei der Division von $T^2 + T$ durch $T^2 + T + 1$ mit Rest bleibt der Rest 1.

Die vollständigen Additions- und Multiplikationstabellen von $\mathbb{F}_2[T]/(f)$ sind:

+	[0]	[1]	[T]	[T+1]
[0]	[0]	[1]	[T]	[T+1]
[1]	[1]	[0]	[T+1]	[T]
[T]	[T]	[T+1]	[0]	[1]
[T+1]	[T+1]	[T]	[1]	[0]

und

·	[0]	[1]	[T]	[T+1]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[T]	[T+1]
[T]	[0]	[T]	[T+1]	[1]
[T+1]	[0]	[T+1]	[1]	[T]

8.1.4 Aufgabe Geben Sie ein Beispiel für einen Körper mit 8 Elementen und bestimmen Sie seine Additions- und seine Multiplikationstabelle.

8.1.5 Beispiel Sei $\mathbb{K} = \mathbb{F}_2$, und sei $f = T^2 + 1 \in \mathbb{F}_2[T]$. Das Polynom f ist reduzibel in $\mathbb{F}_2[T]$, denn $T^2 + 1 = (T + 1)(T + 1)$ in $\mathbb{F}_2[T]$. Die Theorie, Satz 8.1.1, besagt, dass $\mathbb{F}_2[T]/(f)$ dann kein Körper sein kann. Berechnen wir die Additions- und die Multiplikationstabelle. Die Elemente in $\mathbb{F}_2[T]/(f)$ sind dieselben wie in Beispiel 8.1.3.

Die Additionstabelle in $\mathbb{F}_2[T]/(T^2 + 1)$ ist dieselbe wie in Beispiel 8.1.3:

+	[0]	[1]	[T]	[T+1]
[0]	[0]	[1]	[T]	[T+1]
[1]	[1]	[0]	[T+1]	[T]
[T]	[T]	[T+1]	[0]	[1]
[T+1]	[T+1]	[T]	[1]	[0]

Allerdings unterscheiden sich die Multiplikationstabellen. Die Multiplikationstabelle in $\mathbb{F}_2[T]/(T^2 + 1)$ ist

·	[0]	[1]	[T]	[T+1]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[T]	[T+1]
[T]	[0]	[T]	[1]	[T+1]
[T+1]	[0]	[T+1]	[T+1]	[0]

Es ist $[T][T] = [T^2] = [1]$, denn $T^2 = (T^2 + 1) + 1$ ist die Division von T^2 durch $T^2 + 1$ mit Rest.

Es ist $[T][T+1] = [T^2+T] = [T+1]$, denn $T^2+T = (T^2+1)+(T+1)$ ist die Division von T^2+T durch T^2+1 mit Rest.

Schließlich ist $[T+1][T+1] = [T^2+2T+1] = [T^2+1] = [0]$.

8.1.6 Aufgabe Beweisen Sie, dass $f = T^2+1$ irreduzibel in $\mathbb{F}_3[T]$ ist, und führen Sie folgende Rechnungen in $\mathbb{F}_3[T]/(f)$ aus.

(a) $[T+2][T+1]$

(b) $([T+1]+[2T+1])[T+2]$

(c) $[T+1]^3$

(d) $[T+2]-[2T-2]+[2]$

(e) $[T+1][2]+[T][2T+2]$

8.2 Körpererweiterungen

In diesem Abschnitt wird die Theorie bereitgestellt, um die endlichen Körper zu klassifizieren.

Analog zu den Gruppen- und Ringhomomorphismen definiert man auch Körperhomomorphismen. Diese sind nichts anderes als Ringhomomorphismen (siehe Definition 5.3.1), denn jeder Körper ist ja auch ein Ring.

8.2.1 Definition Seien $\mathbb{K}$ und $\mathbb{L}$ Körper. Eine Abbildung $\phi : \mathbb{K} \longrightarrow \mathbb{L}$ ist ein **Körperhomomorphismus**, wenn $\phi(k+k') = \phi(k)+\phi(k')$ und $\phi(kk') = \phi(k)\phi(k')$ für alle $k, k' \in \mathbb{K}$ gilt, und $\phi(1) = 1$ ist.

8.2.2 Bemerkungen Seien $\mathbb{K}$ und $\mathbb{L}$ Körper und sei $\phi : \mathbb{K} \longrightarrow \mathbb{L}$ ein Homomorphismus.

1. Es gilt $\phi(0) = 0$, denn: $\phi(0)+\phi(0) = \phi(0+0) = \phi(0)$. Addiert man nun das additive Inverse von $\phi(0)$ auf beiden Seiten dieser Gleichung, erhält man die Behauptung.
2. Sei $a \in \mathbb{K}^\times$. Dann gilt $\phi(a^{-1}) = \phi(a)^{-1}$. Es ist nämlich $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(1) = 1 = \phi(1) = \phi(a^{-1}a) = \phi(a^{-1})\phi(a)$, also folgt die Behauptung.
3. Sei $a \in \mathbb{K}$, dann ist $\phi(-a) = -\phi(a)$, denn $\phi(a)+\phi(-a) = \phi(a-a) = \phi(0) = 0$.

4. Ist $\phi : \mathbb{K} \longrightarrow \mathbb{L}$ ein Körperhomomorphismus, dann ist ϕ injektiv, denn angenommen, $\phi(k) = \phi(k')$ für $k, k' \in \mathbb{K}$, dann folgt $\phi(k - k') = 0$, also $k - k' = 0$, denn sonst wäre $\phi(k - k')$ mit 2. invertierbar. Also folgt $k = k'$.

Ein Körperhomomorphismus, der bijektiv ist, wird **Körperisomorphismus** genannt. Wenn es einen Körperisomorphismus von $\mathbb{K}$ nach $\mathbb{L}$ gibt, sagt man, dass $\mathbb{K}$ und $\mathbb{L}$ isomorph sind und schreibt $\mathbb{K} \simeq \mathbb{L}$.

8.2.3 Aufgaben Sei $\mathbb{K}$ ein Körper und $R \neq \{0\}$ ein Ring.

1. Sei $\phi : \mathbb{K} \longrightarrow R$ ein surjektiver Ringhomomorphismus. Folgt dann schon, dass R ein Körper ist?
2. Sei $\phi' : R \longrightarrow \mathbb{K}$ ein surjektiver Ringhomomorphismus. Ist R dann ein Körper?

Um die endlichen Körper zu charakterisieren, werden wir uns jetzt erstmal ausführlich mit Körpererweiterungen beschäftigen.

8.2.4 Definition Eine nichtleere Teilmenge $\mathbb{K}$ eines Körpers $\mathbb{L}$ heißt **Unterkörper** von $\mathbb{L}$, wenn $\mathbb{K}$ mit den Verknüpfungen $+$ und $\cdot$ in $\mathbb{L}$ ein Körper ist. In diesem Fall heißt $\mathbb{L}$ **Körpererweiterung** oder **Erweiterungskörper** von $\mathbb{K}$. Eine Körpererweiterung $\mathbb{L}$ von $\mathbb{K}$ wird mit $\mathbb{L} : \mathbb{K}$ notiert.

8.2.5 Beispiel $\mathbb{Q}$ ist ein Unterkörper von $\mathbb{R}$ und $\mathbb{C}$ ist ein Erweiterungskörper von $\mathbb{R}$, also ist $\mathbb{C} : \mathbb{R}$ eine Körpererweiterung. Der Körper $\mathbb{F}_2[T]/(f)$ aus Beispiel 8.1.3 ist ein Erweiterungskörper von $\mathbb{F}_2$, also $\mathbb{F}_2[T]/(f) : \mathbb{F}_2$. Dazu muss man allerdings die Restklasse $[0]$ beziehungsweise $[1]$ in $\mathbb{F}_2[T]/(f)$ mit den Körperelementen 0 beziehungsweise 1 identifizieren.

8.2.6 Bemerkung Ist $\mathbb{K}$ ein Unterkörper von $\mathbb{L}$, dann ist die 0 von $\mathbb{K}$ gleich der 0 von $\mathbb{L}$ und die 1 von $\mathbb{K}$ gleich der 1 von $\mathbb{L}$, denn sei $0'$ die Null in $\mathbb{K}$, dann ist $0' + 0' = 0' = 0' + 0$, also $0' = 0$, und analog $1'1' = 1' = 1'1$, also $1' = 1$ für das Einselement $1'$ von $\mathbb{K}$.

8.2.7 Aufgabe Sei $\mathbb{K}$ ein Körper, sei I eine nicht-leere Indexmenge und sei $(\mathbb{L}_i)_{i \in I}$ ein System von Unterkörpern von $\mathbb{K}$. Zeigen Sie, dass $\cap_{i \in I} \mathbb{L}_i$ ein Körper ist.

Nun definieren wir - ganz analog zu den Primringen in 5.5 - die Primkörper.

8.2.8 Definition Ein Körper $\mathbb{K}$, der keine Unterkörper enthält, die eine echte Teilmenge von $\mathbb{K}$ sind, wird **Primkörper** genannt.

8.2.9 Lemma Die Körper $\mathbb{Q}$ und $\mathbb{F}_p$, wobei p eine Primzahl ist, sind Primkörper.

Beweis: Sei $\mathbb{K} \subseteq \mathbb{Q}$ ein Unterkörper. Dann folgt $0, 1 \in \mathbb{K}$. Da $\mathbb{K}$ abgeschlossen unter Addition ist, folgt $\mathbb{Z} \subseteq \mathbb{K}$, und da $(\mathbb{K}^\times, \cdot)$ eine Gruppe ist, folgt $\mathbb{Q} \subseteq \mathbb{K}$. Also $\mathbb{K} = \mathbb{Q}$.

Sei nun p eine Primzahl und $\mathbb{K} \subseteq \mathbb{F}_p$ ein Unterkörper. Dann folgt $0, 1 \in \mathbb{K}$, und da $\mathbb{K}$ abgeschlossen unter Addition ist, folgt $\mathbb{F}_p \subseteq \mathbb{K}$, also $\mathbb{K} = \mathbb{F}_p$. □

Man kann nun zeigen, dass jeder Körper einen Primkörper als kleinsten Unterkörper enthält und dass die Primkörper aus Lemma 8.2.9 bis auf Isomorphie schon alle Primkörper sind.

8.2.10 Proposition Sei $\mathbb{K}$ ein Körper. Dann besitzt $\mathbb{K}$ einen Unterkörper $\mathbb{P}$, der ein Primkörper ist. Dabei gilt entweder $\mathbb{P} \simeq \mathbb{Q}$, wenn $\mathrm{char}(\mathbb{K}) = 0$ gilt, oder $\mathbb{P} \simeq \mathbb{F}_p$ für eine Primzahl p, wenn $\mathrm{char}(\mathbb{K}) = p$ gilt.

Beweis: Zunächst nehmen wir an, dass $\mathrm{char}(\mathbb{K}) = 0$ gilt. Sei

$$\mathbb{P} = \bigcap_{\mathbb{L} \text{ ist ein Unterkörper von } \mathbb{K}} \mathbb{L}.$$

Dann ist $\mathbb{P}$ mit Aufgabe 8.2.7 ein Körper. Es liegen $0, 1$ in jedem Unterkörper $\mathbb{L}$ von $\mathbb{K}$, also enthält jeder Unterkörper $\mathbb{L}$ auch $\{n \cdot 1 \mid n \in \mathbb{Z}\}$, also mit anderen Worten den Primring von $\mathbb{K}$. Da $\mathrm{char}(\mathbb{K}) = 0$ gilt, ist der Primring von $\mathbb{K}$ isomorph zu $\mathbb{Z}$. Da $(\mathbb{L}^\times, \cdot)$ für alle Unterkörper $\mathbb{L}$ eine abelsche Gruppe ist, enthält jeder Unterkörper $\mathbb{L}$ auch einen Unterkörper, der isomorph zu $\mathbb{Q}$ ist. Dieser Unterkörper ist dann gerade $\mathbb{P}$, und es gilt $\mathbb{P} \simeq \mathbb{Q}$.

Gilt $\mathrm{char}(\mathbb{K}) = p$, dann ist der Primring $P(\mathbb{K}) \simeq \mathbb{F}_p$ ein Körper. Das heißt, Primring und Primkörper stimmen überein. □

Folgendes ist eigentlich schon per Definition klar:

8.2.11 Lemma Sei $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung. Dann gilt:

1. $\mathrm{char}(\mathbb{K}) = \mathrm{char}(\mathbb{L})$.
2. Seien $\mathbb{P}(\mathbb{K})$ und $\mathbb{P}(\mathbb{L})$ die zu $\mathbb{K}$ beziehungsweise $\mathbb{L}$ gehörenden Primkörper. Dann gilt $\mathbb{P}(\mathbb{K}) = \mathbb{P}(\mathbb{L})$.

Beweis:

1. Da die Addition und die Multiplikation in $\mathbb{K}$ und $\mathbb{L}$ die gleichen sind, sind auch $\{n \cdot 1_{\mathbb{K}} \mid n \in \mathbb{Z}\}$ und $\{n \cdot 1_{\mathbb{L}} \mid n \in \mathbb{Z}\}$ gleich, also haben $\mathbb{K}$ und $\mathbb{L}$ denselben Primring.
2. Da der Primkörper $\mathbb{P}(\mathbb{K})$ von $\mathbb{K}$ der kleinste Unterkörper von $\mathbb{K}$ ist, gilt mit $\mathbb{P}(\mathbb{K}) \subseteq \mathbb{K} \subseteq \mathbb{L}$ dasselbe für $\mathbb{L}$. Also $\mathbb{P}(\mathbb{K}) = \mathbb{P}(\mathbb{L})$.

□

Ist $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung, dann ist $\mathbb{L}$ in natürlicher Weise ein $\mathbb{K}$-Vektorraum, denn $(\mathbb{L}, +)$ ist eine abelsche Gruppe, und man kann Elemente aus $\mathbb{L}$ mit „Skalaren“ aus $\mathbb{K}$ multiplizieren. Da $\mathbb{L}$ ein Körper ist, gelten auch die Distributivgesetze.

8.2.12 Definition Sei $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung. Der **Grad** der Körpererweiterung ist

$$[\mathbb{L} : \mathbb{K}] = \dim_{\mathbb{K}} \mathbb{L}.$$

Die Körpererweiterung $\mathbb{L} : \mathbb{K}$ heißt **endlich** oder **unendlich**, je nachdem, ob $[\mathbb{L} : \mathbb{K}]$ endlich oder unendlich ist.

8.2.13 Beispiele
1. $[\mathbb{C} : \mathbb{R}] = 2$, denn $(1, i)$ ist eine Basis von $\mathbb{C}$ über $\mathbb{R}$.
2. $[\mathbb{R} : \mathbb{Q}] = \infty$, wie Sie aus der Linearen Algebra I, 5.3.1, wissen.
3. $[\mathbb{F}_2[T]/(T^2 + T + 1) : \mathbb{F}_2] = 2$ mit Basis $([T], [1])$.
4. Jeder endliche Körper ist eine endliche Erweiterung seines Primkörpers.

8.2.14 Satz (Gradsatz) Seien $\mathbb{M} : \mathbb{L}$ und $\mathbb{L} : \mathbb{K}$ endliche Körpererweiterungen. Dann ist $\mathbb{M} : \mathbb{K}$ ebenfalls endlich, und es gilt

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}].$$

Beweis: Sei $[\mathbb{M} : \mathbb{L}] = m$ und $[\mathbb{L} : \mathbb{K}] = n$, und sei $(w_1, \ldots, w_m)$ eine Basis von $\mathbb{M}$ (über $\mathbb{L}$) und $(v_1, \ldots, v_n)$ eine Basis von $\mathbb{L}$ über $\mathbb{K}$.

Sei $x \in \mathbb{M}$ ein beliebiges Element aus $\mathbb{M}$. Dann gibt es $\alpha_1, \ldots, \alpha_m \in \mathbb{L}$ mit $x = \alpha_1 w_1 + \ldots + \alpha_m w_m$. Für alle $1 \leq j \leq m$ gibt es wiederum $\beta_{1j}, \ldots, \beta_{nj} \in \mathbb{K}$ mit $\alpha_j = \beta_{1j} v_1 + \ldots + \beta_{nj} v_n$. Also folgt

$$x = \sum_{j=1}^{m} \alpha_j w_j = \sum_{j=1}^{m} (\sum_{i=1}^{n} \beta_{ij} v_i) w_j = \sum_{j=1}^{m} \sum_{i=1}^{n} \beta_{ij} v_i w_j.$$

Dieses ist eine Linearkombination der nm Elemente $v_i w_j$, $1 \leq i \leq n$, $1 \leq j \leq m$, mit Koeffizienten aus $\mathbb{K}$. Damit ist gezeigt, dass diese Elemente ein Erzeugendensystem von $\mathbb{M}$ über $\mathbb{K}$ bilden. Es ist nun noch zu zeigen, dass sie linear unabhängig sind.

Für $1 \leq i \leq n$ und $1 \leq j \leq m$ seien also $\gamma_{ij} \in \mathbb{K}$ mit

$$\sum_{j=1}^{m} \sum_{i=1}^{n} \gamma_{ij} v_i w_j = 0.$$

Dann folgt

$$\sum_{j=1}^{m} (\sum_{i=1}^{n} \gamma_{ij} v_i) w_j = 0,$$

wobei für $1 \leq j \leq m$ dann $\sum_{i=1}^{n} \gamma_{ij} v_i \in \mathbb{L}$ gilt. Da $(w_1, \ldots, w_m)$ eine Basis von $\mathbb{M}$ über $\mathbb{L}$ ist, folgt $\sum_{i=1}^{n} \gamma_{ij} v_i = 0$ für $j = 1, \ldots, m$. Nun ist aber $(v_1, \ldots, v_n)$ eine Basis von $\mathbb{L}$ über $\mathbb{K}$, also folgt $\gamma_{ij} = 0$ für $1 \leq j \leq m$ und $1 \leq i \leq n$. Das heißt, $[\mathbb{M} : \mathbb{K}] = mn$. □

Der Gradsatz, beziehungsweise sein Korollar, liefern schon eine wichtige Tatsache über endliche Körpererweiterungen.

8.2.15 Korollar Seien $\mathbb{M} : \mathbb{L}$ und $\mathbb{L} : \mathbb{K}$ endliche Körpererweiterungen. Dann sind $[\mathbb{M} : \mathbb{L}]$ und $[\mathbb{L} : \mathbb{K}]$ Teiler von $[\mathbb{M} : \mathbb{K}]$.

Setzen wir in diesem Korollar beispielsweise $\mathbb{M} = \mathbb{C}$ und $\mathbb{K} = \mathbb{R}$, dann ergibt sich, dass es keinen echten „Zwischenkörper“ $\mathbb{L}$ mit $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{C}$ geben kann, denn $[\mathbb{C} : \mathbb{R}] = 2$, und dann wäre entweder $[\mathbb{C} : \mathbb{L}] = 1$, also $\mathbb{L} = \mathbb{C}$, oder $[\mathbb{L} : \mathbb{R}] = 1$, also $\mathbb{L} = \mathbb{R}$.

Wir definieren nun eine ganz wichtige Sorte von Körpererweiterungen. Es wird sich schnell herausstellen, dass alle endlichen Körpererweiterungen von diesem Typ sind.

8.2.16 Definition Sei $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung, und sei $a \in \mathbb{L}$. Ist a Nullstelle eines Polynoms $f \in \mathbb{K}[T]$, $f \neq 0$, dann heißt a **algebraisch** über $\mathbb{K}$. Eine Körpererweiterung $\mathbb{L} : \mathbb{K}$ heißt **algebraisch**, wenn jedes Element $a \in \mathbb{L}$ algebraisch über $\mathbb{K}$ ist.

8.2.17 Beispiele 1. Jedes Element $a \in \mathbb{K}$ ist algebraisch über $\mathbb{K}$, denn es ist Nullstelle von $T - a \in \mathbb{K}[T]$.

2. Das Element $i \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$, denn es ist Nullstelle von $T^2+1 \in \mathbb{R}[T]$.
3. Das Element $\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, denn es ist Nullstelle von $T^2 - 2 \in \mathbb{Q}[T]$.
4. Das Element $\pi \in \mathbb{R}$ ist nicht algebraisch über $\mathbb{Q}$, denn es gibt kein $0 \neq f \in \mathbb{Q}[T]$ mit $f(\pi) = 0$, wie man zeigen kann (wir aber nicht zeigen werden). Diese Tatsache wurde zuerst von C.L.F. von Lindemann (1852-1939) bewiesen. Er zeigte damit, dass die „Quadratur des Kreises“, ein Problem aus der klassischen griechischen Mathematik, nicht lösbar ist.

   Der Beweis, dass π nicht algebraisch ist, erfordert sehr viel Analysis und würde für diesen Kurs zu weit gehen.

8.2.18 Aufgabe Sei $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung, und sei $a \in \mathbb{L}$ algebraisch über $\mathbb{K}$. Sei $I = \{f \in \mathbb{K}[T] \mid f(a) = 0\}$. Zeigen Sie, dass I ein Ideal in $\mathbb{K}[T]$ ist.

Sei also $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung, und sei $a \in \mathbb{L}$ algebraisch. Sei $I \subseteq \mathbb{K}[T]$ definiert wie in Aufgabe 8.2.18. Dort haben Sie gezeigt, dass I ein Ideal in $\mathbb{K}[T]$ ist. Also gibt es mit Proposition 5.7.3 ein eindeutig bestimmtes, normiertes Polynom $g \in \mathbb{K}[T]$ mit $I = (g)$.

8.2.19 Definition Sei $a \in \mathbb{L}$ algebraisch über $\mathbb{K}$. Das eindeutig bestimmte normierte Polynom $g \in \mathbb{K}[T]$ mit $(g) = \{f \in \mathbb{K}[T] \mid f(a) = 0\}$ heißt **Minimalpolynom** von a. Der Grad von g wird auch als **Grad** von a über $\mathbb{K}$ bezeichnet.

8.2.20 Lemma Sei $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung und $a \in \mathbb{L}$ algebraisch über $\mathbb{K}$ mit Minimalpolynom g. Dann gilt:

1. g ist irreduzibel in $\mathbb{K}[T]$.
2. Für $f \in \mathbb{K}[T]$ gilt $f(a) = 0$ genau dann, wenn $g \mid f$ gilt.
3. g ist das normierte Polynom kleinsten Grades in $\mathbb{K}[T]$ mit $g(a) = 0$.

Beweis:

1. Angenommen, $g = h_1h_2$ mit $h_1, h_2 \in \mathbb{K}[T]$ und $1 \leq \mathrm{Grad}(h_1), \mathrm{Grad}(h_2) < \mathrm{Grad}(g)$. Dann gilt $0 = g(a) = h_1(a)h_2(a)$, also $h_1(a) = 0$ oder $h_2(a) = 0$. Es folgt $h_1 \in I$ oder $h_2 \in I$, ein Widerspruch, denn der Grad der Polynome in I (außer dem Nullpolynom) ist mindestens so groß wie der Grad von g.
2. Sei zunächst $f \in \mathbb{K}[T]$ mit $f(a) = 0$. Dann folgt $f \in I = (g)$, also gibt es $h \in \mathbb{K}[T]$ mit $f = gh$, und g teilt f. Nun gelte umgekehrt $g \mid f$. Es gibt also ein $h \in \mathbb{K}[T]$ mit $f = gh$. Dann ist $f(a) = g(a)h(a) = 0 \cdot h(a) = 0$.

3. Sei $h \in \mathbb{K}[T]$ normiert mit $h(a) = 0$. Dann folgt $h \in I = (g)$. Also gibt es ein Polynom $f \in \mathbb{K}[T]$ mit $h = fg$, das heißt, $\text{Grad}(h) \geq \text{Grad}(g)$.

□

8.2.21 Beispiel Das Minimalpolynom von $i \in \mathbb{C}$ über $\mathbb{R}$ ist $g = T^2 + 1 \in \mathbb{R}[T]$. Das Polynom g ist nämlich normiert, und es gilt $g(i) = 0$. Angenommen, es gibt ein normiertes Polynom $h \in \mathbb{R}[T]$ mit $h(i) = 0$ und $\text{Grad}(h) < \text{Grad}(g)$. Dann folgt $\text{Grad}(h) = 1$, also $h = T - \lambda$ für ein $\lambda \in \mathbb{R}$. Es kann aber i nicht Nullstelle eines solchen Polynoms sein. Also ist g das Minimalpolynom, und der Grad von i über $\mathbb{R}$ ist 2.

8.2.22 Aufgabe Sei $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung und sei $a \in \mathbb{L}$ algebraisch mit Minmalpolynom $g \in \mathbb{K}[T]$. Zeigen Sie, dass genau dann $a \in \mathbb{K}$ gilt, wenn $\text{Grad}(g) = 1$ gilt.

Vorsicht, bei dem Minimalpolynom oder dem Grad eines Elementes einer Körpererweiterung ist es ganz wichtig, zu spezifizieren, von welchem Körper man spricht. Natürlich beeinflusst das das Minimalpolynom. So ist zum Beispiel das Minimalpolynom von $i \in \mathbb{C}$ über $\mathbb{R}$ das Polynom $T^2 + 1$, wie wir in Beispiel 8.2.21 gesehen haben. Das Minimalpolynom von i über $\mathbb{C}$ ist $T - i$.

Nun werden wir sehen, dass die algebraischen Körpererweiterungen genau die Körpererweiterungen sind, die uns im Zusammenhang mit den endlichen Körpern interessieren.

8.2.23 Proposition Sei $\mathbb{K}$ ein Körper. Dann ist jede endliche Erweiterung von $\mathbb{K}$ algebraisch.

Beweis: Sei $\mathbb{L} : \mathbb{K}$ eine endliche Erweiterung von $\mathbb{K}$, und sei $[\mathbb{L} : \mathbb{K}] = n$. Sei $a \in \mathbb{L}$. Dann sind die $n + 1$ Elemente $1, a, a^2, \ldots, a^n$ linear abhängig über $\mathbb{K}$, das heißt, es gibt $\alpha_0, \ldots, \alpha_n \in \mathbb{K}$, so dass $\alpha_0 + \alpha_1 a + \ldots + \alpha_n a^n = 0$ gilt. Also ist a Nullstelle von $f = \sum_{i=0}^{n} \alpha_i T^i \in \mathbb{K}[T]$ und damit algebraisch. □

8.2.24 Korollar Jeder endliche Körper ist eine algebraische Erweiterung seines Primkörpers.

Beweis: Da jeder endliche Körper eine endliche Erweiterung über seinem Primkörper ist, ist diese Erweiterung auch algebraisch. □

8.2.25 Definition Sei $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung, und sei $M \subseteq \mathbb{L}$ eine Teilmenge von $\mathbb{L}$. Dann ist $\mathbb{K}(M)$ definiert als der Schnitt über alle Unterkörper von $\mathbb{L}$, die sowohl $\mathbb{K}$ als auch alle Elemente von M enthalten. Ist $M = \{a_1, \ldots, a_n\}$ endlich, so schreibt man auch $\mathbb{K}(a_1, \ldots, a_n)$ und sagt, dass dieser Körper aus $\mathbb{K}$ durch **Adjungieren** von $a_1, \ldots, a_n$ entstanden ist. Ist $M = \{a\}$ eine einelementige Menge, dann heißt $\mathbb{K}(a)$ **einfache Körpererweiterung** von $\mathbb{K}$. (Man spricht $\mathbb{K}(a)$ als „$\mathbb{K}$ adjungiert a“).

8.2.26 Beispiel Sei $\mathbb{K} = \mathbb{Q}$ und $a = \sqrt{2}$. Dann ist

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Beweis: Jeder Körper, der $\mathbb{Q}$ und $\sqrt{2}$ enthält, enthält auch die Menge $M = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Es ist also nur noch zu zeigen, dass M ein Körper ist. Klar ist, dass $+$ eine Verknüpfung auf dieser Menge ist. Seien nun $a+b\sqrt{2}, c+d\sqrt{2} \in M$ mit $a, b, c, d \in \mathbb{Q}$. Dann ist $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in M$, also ist auch $\cdot$ eine Verknüpfung auf M.

Die Elemente $0 = 0+0\cdot\sqrt{2}$ und $1 = 1+0\cdot\sqrt{2}$ liegen in M, und die Assoziativ- und Distributivgesetze gelten in M, denn M ist eine Teilmenge von $\mathbb{R}$. Zu zeigen ist deshalb nur noch, dass die Inversen bezüglich der Addition und der Multiplikation in M liegen. Zu $a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$ ist $(-a) + (-b)\sqrt{2}$ bezüglich der Addition invers, und das Inverse zu $a + b\sqrt{2} \neq 0$ bezüglich der Multiplikation ist

$$\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}.$$

Dabei ist $a^2 - 2b^2 \neq 0$, denn sonst wäre entweder $b = 0$ und dann auch $a = 0$, was wegen der Annahme $a + b\sqrt{2} \neq 0$ ausgeschlossen ist, oder $b \neq 0$ und $(\frac{a}{b})^2 = 2$. Auch das ist nicht möglich, denn $\sqrt{2} \notin \mathbb{Q}$. □

8.2.27 Aufgaben Seien $\mathbb{M} : \mathbb{L}$ und $\mathbb{L} : \mathbb{K}$ Körpererweiterungen und sei $S \subseteq \mathbb{M}$ eine beliebige Teilmenge. Zeigen Sie:

1. Ist $\mathbb{K}(S) = \mathbb{M}$, dann folgt $\mathbb{L}(S) = \mathbb{M}$.
2. Ist $\mathbb{L}(S) = \mathbb{M}$, dann folgt im Allgemeinen nicht, dass $\mathbb{K}(S) = \mathbb{M}$ gilt.

8.2.28 Satz Sei $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung, und sei $a \in \mathbb{L}$ algebraisch vom Grad n über $\mathbb{K}$ mit Minimalpolynom g. Dann gilt:

1. $\mathbb{K}(a) \simeq \mathbb{K}[T]/(g)$.
2. $[\mathbb{K}(a) : \mathbb{K}] = n$, und $(1, a, a^2, \ldots, a^{n-1})$ ist eine Basis von $\mathbb{K}(a)$ über $\mathbb{K}$.

3. Jedes $b \in \mathbb{K}(a)$ ist algebraisch über $\mathbb{K}$, und sein Grad über $\mathbb{K}$ ist ein Teiler von n.

Beweis:

1. Die Abbildung $\phi : \mathbb{K}[T] \longrightarrow \mathbb{K}(a)$ definiert durch $\phi(f) = f(a)$ ist ein Ringhomomorphismus: Es gilt $\phi(1) = 1$ und

$$\begin{aligned} \phi(f_1 + f_2) &= (f_1 + f_2)(a) = f_1(a) + f_2(a) = \phi(f_1) + \phi(f_2) \text{ und} \\ \phi(f_1 f_2) &= f_1 f_2(a) = f_1(a) f_2(a) = \phi(f_1)\phi(f_2) \end{aligned}$$

   für alle $f_1, f_2 \in \mathbb{K}[T]$. Der Kern von ϕ ist gerade $\text{Kern}(\phi) = (g)$, denn $f \in \text{Kern}(\phi)$ genau dann, wenn $f(a) = 0$ gilt. Sei also $B \subseteq \mathbb{K}(a)$ das Bild von ϕ. Dann liegen in B alle Elemente aus $\mathbb{K}$ (als Bilder der konstanten Polynome) und a (als Bild von T). Mit dem Homomorphiesatz für Ringe ist B als Ring isomorph zu $\mathbb{K}[T]/(g)$, und mit Satz 8.1.1 ist B ein Körper. Also ist $B \subseteq \mathbb{K}(a)$ ein Körper, der $\mathbb{K}$ und a enthält, das heißt, $B = \mathbb{K}(a)$.

2. Im ersten Teil haben wir gesehen, dass jedes Element in $\mathbb{K}(a)$ von der Form $f(a)$ mit $f \in \mathbb{K}[T]$ ist. Wir dividieren f durch g mit Rest und erhalten $f = qg + r$ mit $q, r \in \mathbb{K}[T]$ und $\text{Grad}(r) < \text{Grad}(g) = n$. Also gilt $f(a) = q(a)g(a) + r(a) = r(a)$, denn $g(a) = 0$. Sei $r = \sum_{i=0}^{n-1} \alpha_i T^i$ mit $\alpha_i \in \mathbb{K}$ für $0 \leq i \leq n-1$, dann ist $f(a) = r(a) = \sum_{i=0}^{n-1} \alpha_i a^i$. Damit folgt, dass $1, a, a^2, \ldots, a^{n-1}$ ein Erzeugendensystem von $\mathbb{K}(a)$ ist.

   Seien nun $\alpha_0, \ldots, \alpha_{n-1} \in \mathbb{K}$ mit $\sum_{i=0}^{n-1} \alpha_i a^i = 0$. Dann folgt $f(a) = 0$, wobei $f = \sum_{i=0}^{n-1} \alpha_i T^i \in \mathbb{K}[T]$ gilt. Es gilt also $f \in (g)$, das heißt, es gibt $h \in \mathbb{K}[T]$ mit $f = gh$. Angenommen, $h \neq 0$. Dann ist $\text{Grad}(f) = \text{Grad}(gh) \geq \text{Grad}(g) = n$, ein Widerspruch. Also ist $h = f = 0$ und $\alpha_0 = \alpha_1 = \ldots = \alpha_{n-1} = 0$.

3. Wie im zweiten Teil gezeigt wurde, ist $\mathbb{K}(a) : \mathbb{K}$ eine endliche Körpererweiterung, also mit Proposition 8.2.23 auch algebraisch. Damit ist b algebraisch über $\mathbb{K}$. Der Körper $\mathbb{K}(b)$ ist ein Unterkörper von $\mathbb{K}(a)$, und mit dem Gradsatz gilt:

$$n = [\mathbb{K}(a) : \mathbb{K}] = [\mathbb{K}(a) : \mathbb{K}(b)][\mathbb{K}(b) : \mathbb{K}].$$

   Also ist $[\mathbb{K}(b) : \mathbb{K}]$ ein Teiler von n, und mit dem zweiten Teil ist dies gerade der Grad von b über $\mathbb{K}$.

□

In Satz 8.2.28 stammt das Element a, das zu $\mathbb{K}$ adjungiert wird, aus einer Körpererweiterung $\mathbb{L}$ von $\mathbb{K}$. Das ist nötig, damit überhaupt von Potenzen und Linearkombinationen dieser Potenzen geredet werden kann. Der erste Teil von Satz 8.2.28

gibt aber schon einen Hinweis darauf, wie man ein Element zu einem Körper adjungieren kann, ohne dass es ein Element einer Körpererweiterung $\mathbb{L}$ sein muss.

8.2.29 Satz Sei $\mathbb{K}$ ein Körper und sei $f \in \mathbb{K}[T]$ irreduzibel. Dann ist $\mathbb{K}[T]/(f)$ eine einfache algebraische Erweiterung $\mathbb{K}(a) : \mathbb{K}$, wobei a eine Nullstelle von f ist.

Beweis: Der Ring $\mathbb{L} = \mathbb{K}[T]/(f)$ ist mit Satz 8.1.1 ein Körper. Die Elemente von $\mathbb{L}$ sind die Restklassen $[g] = g + (f)$ mit $g \in \mathbb{K}[T]$. Seien $\alpha, \beta \in \mathbb{K}$. Dann gilt $[\alpha] = [\beta]$ genau dann, wenn $\alpha - \beta \in (f)$ gilt, und wegen $\mathrm{Grad}(f) \geq 1$, folgt $\alpha = \beta$. Ist also $\alpha \neq \beta$, dann ist auch $[\alpha] \neq [\beta]$. Der Körper $\mathbb{K}$ kann also mit $\{[\alpha] \mid \alpha \in \mathbb{K}\}$ identifiziert werden, und auf diese Weise ist $\mathbb{L}$ eine Körpererweiterung von $\mathbb{K}$. Für jedes Polynom $g = \sum_{i=0}^{n} \alpha_i T^i \in \mathbb{K}[T]$ ist

$$[g] = [\sum_{i=0}^{n} \alpha_i T^i] = \sum_{i=0}^{n} [\alpha_i T^i] = \sum_{i=0}^{n} [\alpha_i][T^i] = \sum_{i=0}^{n} \alpha_i [T]^i,$$

wenn wir $[\alpha]$ mit α für $\alpha \in \mathbb{K}$ identifizieren. Jedes Element aus $\mathbb{K}[T]/(f)$ ist also eine endliche $\mathbb{K}$-Linearkombination von Potenzen von $[T]$. Jede solche Linearkombination ist auch in der einfachen Erweiterung $\mathbb{K}([T])$ enthalten, also $\mathbb{L} = \mathbb{K}([T])$. Außerdem gilt $f([T]) = [f] = 0$, also ist $[T]$ eine Nullstelle von f, und $\mathbb{L}$ ist eine einfache algebraische Erweiterung von $\mathbb{K}$. □

Nun betrachten wir noch einmal Beispiel 8.1.3, also $\mathbb{L} = \mathbb{F}_2[T]/(T^2 + T + 1)$. Die Elemente von $\mathbb{L}$ sind $[0], [1], [T], [T + 1]$, und mit Satz 8.2.29 ist $\mathbb{L} = \mathbb{F}_2([T])$. Sei $f = T^2+T+1$. Dann ist $f([T]) = [0]$, aber auch $f([T+1]) = [T+1]^2+[T+1]+[1] = [T^2+1+T+1+1] = [T^2+T+1] = [0]$. Da $[T] = [T+1]+[1]$ eine Linearkombination von Potenzen von $[T + 1]$ ist, gilt $\mathbb{F}_2([T]) = \mathbb{F}_2([T + 1])$, und $[T]$ und $[T + 1]$ sind beide Nullstellen von f. Wir werden sehen, dass das kein Zufall ist.

Vorher müssen wir uns jedoch noch ein paar Gedanken darüber machen, in welcher Weise ein Isomorphismus zwischen Körpern zu einem Isomorphismus der zugehörigen Polynomringe erweitert werden kann.

8.2.30 Lemma Seien $\mathbb{K}$ und $\mathbb{K}'$ Körper, und sei $\phi : \mathbb{K} \longrightarrow \mathbb{K}'$ ein Isomorphismus. Dann ist $\tilde{\phi} : \mathbb{K}[T] \longrightarrow \mathbb{K}'[T]$, definiert durch $\tilde{\phi}(\sum_{i=0}^{n} \alpha_i T^i) = \sum_{i=0}^{n} \phi(\alpha_i) T^i$, ein Isomorphismus von Ringen.

Beweis: Seien $f, g \in \mathbb{K}[T]$ mit $f = \sum_{i=0}^{n} \alpha_i T^i$ und $g = \sum_{i=0}^{m} \beta_i T^i$. Um die beiden Polynome zu addieren, nehmen wir an, dass $n \geq m$ gilt und setzen $\beta_{m+1} = \ldots =$

$\beta_n = 0$. Dann ist also $g = \sum_{i=0}^{n} \beta_i T^i$. Wir haben nun

$$\begin{aligned}
\tilde{\phi}(f+g) &= \tilde{\phi}(\sum_{i=0}^{n}(\alpha_i+\beta_i)T^i) = \sum_{i=0}^{n}\phi(\alpha_i+\beta_i)T^i \\
&= \sum_{i=0}^{n}\phi(\alpha_i)T^i + \sum_{i=0}^{n}\phi(\beta_i)T^i \\
&= \sum_{i=0}^{n}\phi(\alpha_i)T^i + \sum_{i=0}^{m}\phi(\beta_i)T^i \text{ denn } \phi(0)=0 \\
&= \tilde{\phi}(f)+\tilde{\phi}(g).
\end{aligned}$$

Außerdem ist

$$\begin{aligned}
\tilde{\phi}(fg) &= \tilde{\phi}(\sum_{i=0}^{n+m}(\sum_{j+k=i}\alpha_j\beta_k)T^i) = \sum_{i=0}^{n+m}\phi(\sum_{j+k=i}\alpha_j\beta_k)T^i \\
&= \sum_{i=0}^{n+m}(\sum_{j+k=i}\phi(\alpha_j)\phi(\beta_k))T^i = (\sum_{i=0}^{n}\phi(\alpha_i)T^i)(\sum_{i=0}^{m}\phi(\beta_i)T^i) \\
&= \tilde{\phi}(f)\tilde{\phi}(g).
\end{aligned}$$

Natürlich gilt auch $\tilde{\phi}(1) = 1$, also ist $\tilde{\phi}$ ein Ringhomomorphismus. Wir zeigen jetzt, dass $\tilde{\phi}$ surjektiv ist. Dazu sei $\sum_{i=0}^{n}\beta_i T^i \in \mathbb{K}'[T]$. Da ϕ surjektiv ist, gibt es $\alpha_0, \ldots, \alpha_n \in \mathbb{K}$ mit $\phi(\alpha_i) = \beta_i$ für $i = 0, \ldots, n$. Dann ist $\tilde{\phi}(\sum_{i=0}^{n}\alpha_i T^i) = \sum_{i=0}^{n}\phi(\alpha_i)T^i = \sum_{i=0}^{n}\beta_i T^i$, das heißt, $\tilde{\phi}$ ist surkjektiv.

Sei nun $\tilde{\phi}(\sum_{i=0}^{n}\alpha_i T^i) = 0$. Dann folgt

$$0 = \tilde{\phi}(\sum_{i=0}^{n}\alpha_i T^i) = \sum_{i=0}^{n}\phi(\alpha_i)T^i,$$

also $\phi(\alpha_i) = 0$ für $0 \le i \le n$. Da ϕ ein Isomorphismus ist, folgt $\alpha_i = 0$ für $0 \le i \le n$, also $\sum_{i=0}^{n}\alpha_i T^i = 0$, und $\tilde{\phi}$ ist injektiv. □

8.2.31 Aufgaben Seien $\mathbb{K}$ und $\mathbb{K}'$ Körper, sei $\phi : \mathbb{K} \longrightarrow \mathbb{K}'$ ein Isomorphismus, und sei $\tilde{\phi} : \mathbb{K}[T] \longrightarrow \mathbb{K}'[T]$ der in Lemma 8.2.30 definierte Isomorphismus. Zeigen Sie:

1. Ist $f \in \mathbb{K}[T]$ irreduzibel, dann ist auch $\tilde{\phi}(f)$ irreduzibel.
2. Seien $f, g \in \mathbb{K}[T]$, und es gelte $\tilde{\phi}(g) \mid \tilde{\phi}(f)$. Dann folgt $g \mid f$.

Da die folgende Proposition später noch einmal für den Beweis eines wichtigen Satzes benötigt wird, wird sie zunächst komplizierter formuliert als wir es momentan brauchen.

8.2.32 Proposition Seien $\mathbb{K}$ und $\mathbb{K}'$ Körper, und sei $\phi : \mathbb{K} \longrightarrow \mathbb{K}'$ ein Körperisomorphismus. Sei $f \in \mathbb{K}[T]$ irreduzibel über $\mathbb{K}$, und sei a eine Nullstelle von f. Sei b eine Nullstelle von $\tilde{\phi}(f) \in \mathbb{K}'[T]$, wobei $\tilde{\phi}$ definiert ist wie in Lemma 8.2.30. Dann gibt es einen Isomorphismus $\Phi : \mathbb{K}(a) \longrightarrow \mathbb{K}'(b)$ mit $\Phi(a) = b$ und $\Phi(k) = \phi(k)$ für alle $k \in \mathbb{K}$.

Beweis: Es ist a algebraisch über $\mathbb{K}$ und b algebraisch über $\mathbb{K}'$, das heißt $\mathbb{K}(a)$ ist eine einfache algebraische Erweiterung von $\mathbb{K}$ und $\mathbb{K}'(b)$ ist eine einfache algebraische Erweiterung von $\mathbb{K}'$. Die Elemente von $\mathbb{K}(a)$ beziehungsweise $\mathbb{K}'(b)$ sind also mit Satz 8.2.28 Linearkombinationen von Potenzen von a beziehungsweise b, das heißt, die Elemente sind von der Form $g(a)$ beziehungweise $g'(b)$ mit $g \in \mathbb{K}[T]$ beziehungweise $g' \in \mathbb{K}'[T]$.

Wir definieren nun $\Phi : \mathbb{K}(a) \longrightarrow \mathbb{K}'(b)$ durch $\Phi(g(a)) = \tilde{\phi}(g)(b)$ für alle $g \in \mathbb{K}[T]$.

Zunächst zeigen wir, dass Φ wohldefiniert ist, dass also $\Phi(g(a)) = \Phi(h(a))$ gilt, wenn $g(a) = h(a)$ ist. Angenommen, $g(a) = h(a)$, dann ist $(g - h)(a) = 0$. Sei $m \in \mathbb{K}[T]$ das Minimalpolynom von a über $\mathbb{K}$. Da m jedes Polynom p aus $\mathbb{K}[T]$ teilt, für das $p(a) = 0$ gilt, gilt also auch $m \mid f$. Andererseits ist f irreduzibel, und darum folgt $f = \alpha m$ mit $\alpha \in \mathbb{K}$. Wegen $(g - h)(a) = 0$, gilt $m \mid (g - h)$ und dann auch $f \mid (g - h)$. Es gibt also ein Polynom $p \in \mathbb{K}[T]$ mit $g - h = pf$ oder $g = h + pf$. Also ist

$$\begin{aligned} \Phi(g(a)) &= \tilde{\phi}(g)(b) = \tilde{\phi}(h + pf)(b) \\ &= \tilde{\phi}(h)(b) + \tilde{\phi}(pf)(b) = \tilde{\phi}(h)(b) + \tilde{\phi}(p)(b)\tilde{\phi}(f)(b) = \tilde{\phi}(h)(b) = \Phi(h(a)). \end{aligned}$$

Die Abbildung Φ ist also wohldefiniert. Außerdem gilt

$$\Phi(1) = \Phi(1(a)) = \tilde{\phi}(1)(b) = 1(b) = 1$$

und

$$\Phi(g(a) + h(a)) = \tilde{\phi}(g + h)(b) = \tilde{\phi}(g)(b) + \tilde{\phi}(h)(b) = \Phi(g(a)) + \Phi(h(a))$$

und

$$\Phi(g(a)h(a)) = \tilde{\phi}(gh(a)) = \tilde{\phi}(gh)(b) = \tilde{\phi}(g)(b)\tilde{\phi}(h)(b) = \Phi(g(a))\Phi(h(a))$$

für alle $g, h \in \mathbb{K}[T]$. Also ist Φ ein Homomorphismus. Die Abbildung Φ ist auch injektiv: Sei $\Phi(g(a)) = 0$, dann folgt $\tilde{\phi}(g)(b) = 0$. Sei $m \in \mathbb{K}'[T]$ das Minimalpolynom

von b über $\mathbb{K}'$. Da $\tilde{\phi}(f)(b) = 0$ gilt, gilt $m \mid \tilde{\phi}(f)$. Andererseits ist $\tilde{\phi}(f)$ irreduzibel mit Aufgabe 8.2.31, denn f ist irreduzibel. Also gibt es ein $0 \neq \beta \in \mathbb{K}'$ mit $\beta m = \tilde{\phi}(f)$. Nun gilt $\tilde{\phi}(g)(b) = 0$, also folgt $m \mid \tilde{\phi}(g)$ und damit auch $\tilde{\phi}(f) \mid \tilde{\phi}(g)$. Dann folgt - wieder mit Aufgabe 8.2.31 - $f \mid g$ und also $g(a) = 0$. Nun ist also nur noch zu zeigen, dass Φ surjektiv ist. Dazu sei $h \in \mathbb{K}'[T]$. Da $\tilde{\phi}$ ein Isomorphismus ist, gibt es ein $g \in \mathbb{K}[T]$ mit $\tilde{\phi}(g) = h$. Dann gilt auch $\Phi(g(a)) = \tilde{\phi}(g)(b) = h(b)$.

Es ist $\Phi(a) = \Phi(T(a)) = \tilde{\phi}(T)(b) = T(b) = b$ und $\Phi(k) = \Phi(k \cdot 1(a)) = \tilde{\phi}(k \cdot 1)(b) = \phi(k)$ für alle $k \in \mathbb{K}$. Also erfüllt Φ alle geforderten Bedingungen.

□

Wenn wir $\mathbb{K} = \mathbb{K}'$ und $\phi = \mathrm{id}_{\mathbb{K}}$ setzen, bekommen wir:

8.2.33 Korollar Sei $\mathbb{K}$ ein Körper, und sei $f \in \mathbb{K}[T]$ irreduzibel über $\mathbb{K}$. Seien a und b Nullstellen von f. Dann gibt es einen Isomorphismus $\Phi : \mathbb{K}(a) \longrightarrow \mathbb{K}(b)$ mit $\Phi(a) = b$ und $\Phi(k) = k$ für alle $k \in \mathbb{K}$.

In Beispiel 8.1.3 sähe der Isomorphismus also folgendermaßen aus:

$$\begin{aligned} \Phi \;:\; & \mathbb{F}_2([T]) \longrightarrow \mathbb{F}_2([T+1]) \\ & \alpha + \beta[T] \mapsto \alpha + \beta[T+1] = \alpha + \beta + \beta[T]. \end{aligned}$$

In diesem Beispiel zerfällt übrigens das irreduzible Polynom $f = T^2 + T + 1$ über dem Körper $\mathbb{F}_2([T])$ schon vollständig in Linearfaktoren:

$$f = (T + [T])(T + [T+1]) = T^2 + ([T] + [T+1])T + [T][T+1] = T^2 + T + 1.$$

Das nächste Beispiel zeigt, dass es nicht immer so sein muss, dass ein irreduzibles Polynom $f \in \mathbb{K}[T]$ ganz in Linearfaktoren zerfällt, wenn man eine Nullstelle von f zu $\mathbb{K}$ adjungiert.

8.2.34 Beispiel Sei $f = T^3 - 2 \in \mathbb{Q}[T]$. Dann ist f irreduzibel über $\mathbb{Q}$, denn es gibt kein $x \in \mathbb{Q}$ mit $x^3 = 2$. Sei $a = \sqrt[3]{2}$. Dann ist a eine Nullstelle von f, das heißt, f ist reduzibel in $\mathbb{Q}(\sqrt[3]{2})$. Es gilt

$$f = (T - \sqrt[3]{2})(T^2 + \sqrt[3]{2}T + (\sqrt[3]{2})^2)$$

in $\mathbb{Q}(\sqrt[3]{2})[T]$, und $T^2 + \sqrt[3]{2}T + (\sqrt[3]{2})^2$ ist irreduzibel über $\mathbb{Q}(\sqrt[3]{2})$, denn $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, während die beiden Nullstellen $-\frac{\sqrt[3]{2}}{2} \pm \frac{\sqrt{3}\sqrt[3]{2}}{2} i$ von $T^2 + \sqrt[3]{2}T + (\sqrt[3]{2})^2$ zwar in $\mathbb{C}$, aber nicht in $\mathbb{R}$ liegen.

Wir interessieren uns nun für solche Erweiterungen von $\mathbb{K}$, über denen $f \in \mathbb{K}[T]$ vollständig in Linearfaktoren zerfällt.

8.2.35 Definition Sei $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung, und sei $f \in \mathbb{K}[T]$ nicht konstant. Wir sagen, dass f über $\mathbb{L}$ **zerfällt**, wenn f über $\mathbb{L}$ als Produkt von Linearfaktoren geschrieben werden kann, also

$$f = a(T - a_1)(T - a_2)\dots(T - a_n) \text{ mit } a, a_1, \dots, a_n \in \mathbb{L}.$$

Der Körper $\mathbb{L}$ heißt **Zerfällungskörper** von f, wenn f über $\mathbb{L}$ zerfällt, und wenn $\mathbb{L} = \mathbb{K}(a_1, \dots, a_n)$ gilt.

Ein Zerfällungskörper ist also so etwas wie der kleinste Körper, über dem f zerfällt.

8.2.36 Lemma Sei $\mathbb{K}$ ein Körper und sei $f \in \mathbb{K}[T]$. Sei $\mathbb{L}$ Zerfällungskörper von f, und sei $\mathbb{M}$ ein Zwischenkörper von $\mathbb{L} : \mathbb{K}$ (das heißt, $\mathbb{L} : \mathbb{M}$ und $\mathbb{M} : \mathbb{K}$ sind Körpererweiterungen). Dann ist $\mathbb{L}$ auch Zerfällungskörper von f, aufgefasst als Element von $\mathbb{M}[T]$.

Beweis: Da $\mathbb{L}$ Zerfällungskörper von $f \in \mathbb{K}[T]$ ist, zerfällt f über $\mathbb{L}$. Sei $f = a(T - a_1)\dots(T - a_n)$ in $\mathbb{L}[T]$. Dann ist $\mathbb{L} = \mathbb{K}(a_1, \dots, a_n)$ und mit Aufgabe 8.2.27 (1) folgt auch $\mathbb{L} = \mathbb{M}(a_1, \dots, a_n)$. □

8.2.37 Aufgabe Bestimmen Sie den Grad des Zerfällungskörpers von $T^4 + 1$ über $\mathbb{Q}$.

Wir werden nun zeigen, dass es zu jedem Polynom $f \in \mathbb{K}[T]$ immer einen bis auf Isomorphie eindeutigen Zerfällungskörper gibt. Wegen der besseren Übersicht teilen wir den Beweis jedoch in zwei Teile.

8.2.38 Satz (Existenz eines Zerfällungskörpers) Sei $\mathbb{K}$ ein Körper und $f \in \mathbb{K}[T]$ ein Polynom vom Grad $n \geq 1$. Dann gibt es einen Zerfällungskörper $\mathbb{L} : \mathbb{K}$ von f mit $[\mathbb{L} : \mathbb{K}] \leq n!$.

Beweis: Wir beweisen den Satz durch Induktion nach $n = \text{Grad}(f)$. Sei zunächst $n = 1$, also $f = aT + b$ mit $a, b \in \mathbb{K}$ und $a \neq 0$. Dann ist $\mathbb{L} = \mathbb{K}$ ein Zerfällungskörper von f mit $[\mathbb{L} : \mathbb{K}] = 1 \leq n!$.

Sei nun also $\text{Grad}(f) = n > 1$. Sei $p \in \mathbb{K}[T]$ ein irreduzibler Faktor von f. Mit Satz 8.2.29 gibt es eine einfache algebraische Erweiterung $\mathbb{K}(a_1)$, wobei a_1 eine Nullstelle von p, also auch von f, ist. Außerdem gilt $[\mathbb{K}(a_1) : \mathbb{K}] = \text{Grad}(p) \leq n$. In

$\mathbb{K}(a_1)[T]$ ist also $f = (T-a_1)g$ mit $\mathrm{Grad}(g) = n-1$. Nach Induktionsvoraussetzung gibt es einen Zerfällungskörper $\mathbb{L} : \mathbb{K}(a_1)$, $a \in \mathbb{K}$ und $a_2, \ldots, a_n \in \mathbb{L}$ mit $g = a(T - a_2)\ldots(T - a_n)$ und $\mathbb{L} = \mathbb{K}(a_1)(a_2, \ldots, a_n)$ und $[\mathbb{L} : \mathbb{K}(a_1)] \leq (n-1)!$. Nun folgt aber $f = a(T-a_1)(T-a_2)\ldots(T-a_n)$ und $\mathbb{L} = \mathbb{K}(a_1)(a_2, \ldots, a_n) = \mathbb{K}(a_1, \ldots, a_n)$, also ist $\mathbb{L}$ ein Zerfällungskörper von f. Außerdem gilt

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}(a_1)][\mathbb{K}(a_1) : \mathbb{K}] \leq n(n-1)! = n!.$$

□

8.2.39 Beispiel Betrachten wir noch einmal $f = T^3 - 2 \in \mathbb{Q}[T]$. In Beispiel 8.2.34 haben wir bereits gesehen, dass $\sqrt[3]{2}$ eine Nullstelle von f ist, die nicht in $\mathbb{Q}$ liegt. Außerdem wurde dort gezeigt, dass $f = (T - \sqrt[3]{2})(T^2 + \sqrt[3]{2}T + (\sqrt[3]{2})^2)$ in $\mathbb{Q}(\sqrt[3]{2})[T]$ gilt. Sei nun $b = -\frac{1}{2} - \frac{\sqrt{3}}{2}i \in \mathbb{C}$. Dann gilt $b^3 = 1$ und $f = (T - \sqrt[3]{2})(T - \sqrt[3]{2}b)(T - \sqrt[3]{2}b^2)$. Es folgt, dass $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}b, \sqrt[3]{2}b^2) = \mathbb{Q}(\sqrt[3]{2}, b)$ ein Zerfällungskörper von f über $\mathbb{Q}$ ist. Es gilt $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, denn $T^3 - 2$ ist das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$. Weiter gilt $[\mathbb{K} : \mathbb{Q}(\sqrt[3]{2})] = 2$, denn b ist Nullstelle von $T^3 - 1 = (T-1)(T^2 + T + 1) \in \mathbb{Q}[T]$. Also ist $T^2 + T + 1$ das Minimalpolynom von b über $\mathbb{Q}$ und auch über $\mathbb{Q}(\sqrt[3]{2})$. Mit dem Gradsatz folgt, dass $[\mathbb{K} : \mathbb{Q}] = 6 = (\mathrm{Grad}(f))!$ gilt.

Nun wollen wir zeigen, dass Zerfällungskörper (bis auf Isomorphie) eindeutig sind. Wir beweisen dies durch Induktion, und um den Induktionsschritt beweisen zu können, müssen wir eine kompliziertere Aussage beweisen als wir eigentlich brauchen. Die Eindeutigkeit ergibt sich im folgenden Satz, wenn Sie $\mathbb{K} = \mathbb{K}'$ und $\phi = \mathrm{id}_{\mathbb{K}}$ setzen.

8.2.40 Satz Seien $\mathbb{K}$ und $\mathbb{K}'$ Körper und sei $\phi : \mathbb{K} \longrightarrow \mathbb{K}'$ ein Isomorphismus. Sei $f \in \mathbb{K}[T]$ ein Polynom mit $\mathrm{Grad}(f) \geq 1$ und sei $\mathbb{L}$ ein Zerfällungskörper von f über $\mathbb{K}$. Sei $\mathbb{L}'$ ein Zerfällungskörper von $\tilde{\phi}(f)$ über $\mathbb{K}'$, wobei $\tilde{\phi}$ wie in Lemma 8.2.30 definiert ist. Dann gibt es einen Isomorphismus $\Phi : \mathbb{L} \longrightarrow \mathbb{L}'$ mit $\Phi(k) = \phi(k)$ für alle $k \in \mathbb{K}$.

Beweis: Wir beweisen den Satz mit Induktion über $n = [\mathbb{L} : \mathbb{K}]$. Ist $[\mathbb{L} : \mathbb{K}] = 1$, also $\mathbb{L} = \mathbb{K}$, dann zerfällt f bereits über $\mathbb{K}$ in Linearfaktoren. Es gilt $f = a(T - a_1)\ldots(T - a_r)$ und $a, a_1, \ldots, a_r \in \mathbb{K}$. Dann ist $\tilde{\phi}(f) = \phi(a)(T - \phi(a_1))\ldots(T - \phi(a_r))$, und $\phi(a), \phi(a_1), \ldots, \phi(a_r) \in \mathbb{K}'$. Also ist $\mathbb{K}' = \mathbb{L}'$ Zerfällungskörper von $\tilde{\phi}(f)$ und wir können $\Phi = \phi$ setzen.

Sei nun der Satz richtig für alle Isomorphismen $\mathbb{M} \longrightarrow \mathbb{M}'$ und alle Polynome in $\mathbb{M}[T]$, so dass der Grad des Zerfällungskörpers über $\mathbb{M}$ kleiner als n ist.

Es gelte $[\mathbb{L} : \mathbb{K}] = n$. Sei $p \in \mathbb{K}[T]$ ein irreduzibler Faktor von f. Dann ist $\tilde{\phi}(p) \in \mathbb{K}'[T]$ mit Aufgabe 8.2.31 ein irreduzibler Faktor von $\tilde{\phi}(f)$. Nach Definition enthält $\mathbb{L}$ eine Nullstelle a von p, und $\mathbb{L}'$ enthält eine Nullstelle a' von $\tilde{\phi}(p)$. Mit Proposition 8.2.32 gibt es einen Isomorphismus $\phi' : \mathbb{K}(a) \longrightarrow \mathbb{K}'(a')$ mit $\phi'(k) = \phi(k)$ für alle $k \in \mathbb{K}$. Mit Lemma 8.2.36 ist $\mathbb{L}$ auch ein Zerfällungskörper von f über $\mathbb{K}(a)$, und $\mathbb{L}'$ ist ein Zerfällungskörper von $\tilde{\phi}(f)$ über $\mathbb{K}'(a')$. Mit dem Gradsatz ist $[\mathbb{L} : \mathbb{K}(a)] = \frac{[\mathbb{L}:\mathbb{K}]}{[\mathbb{K}(a):\mathbb{K}]} = \frac{n}{\mathrm{Grad}(p)} < n$. Nach Induktionsvoraussetzung gibt es also einen Isomorphismus $\Phi : \mathbb{L} \longrightarrow \mathbb{L}'$ mit $\Phi(k) = \phi'(k)$ für alle $k \in \mathbb{K}(a)$, also auch $\Phi(k) = \phi(k)$ für alle $k \in \mathbb{K}$. □

8.2.41 Korollar (Eindeutigkeit des Zerfällungskörpers) Sei $\mathbb{K}$ ein Körper und $f \in \mathbb{K}[T]$. Seien $\mathbb{L}$ und $\mathbb{L}'$ Zerfällungskörper von f über $\mathbb{K}$. Dann gibt es einen Isomorphismus $\Phi : \mathbb{L} \longrightarrow \mathbb{L}'$ mit $\Phi(k) = k$ für alle $k \in \mathbb{K}$.

8.3 Endliche Körper

In diesem Abschnitt soll gezeigt werden, dass es zu jeder Primzahl p und jedem $n \in \mathbb{N}$ bis auf Isomorphie genau einen Körper mit p^n Elementen gibt. Dazu rekapitulieren wir zunächst, was wir bereits über endliche Körper wissen:

- Zu jeder Primzahl p gibt es den Körper $\mathbb{F}_p$ mit p Elementen.
- Die Charakteristik eines endlichen Körpers ist immer eine Primzahl p.
- Jeder endliche Körper ist eine endliche Erweiterung seines Primkörpers.
- Ist $\mathbb{K}$ ein endlicher Körper mit $\mathrm{char}(\mathbb{K}) = p$, dann ist die Abbildung $a \mapsto a^p$ für alle $a \in \mathbb{K}$ ein Automorphismus.
- Die Anzahl der Elemente eines endlichen Körpers $\mathbb{K}$ ist p^n, wobei p die Charakteristik von $\mathbb{K}$ und n der Grad der Körpererweiterung von $\mathbb{K}$ über seinem Primkörper ist.
- Ist $\mathbb{K}$ ein endlicher Körper, dann ist $(\mathbb{K}^\times, \cdot)$ zyklisch. Daraus folgt direkt, dass $\mathbb{K}$ eine einfache algebraische Erweiterung seines Primkörpers $\mathbb{P}$ ist, nämlich $\mathbb{P}(a)$, wobei a ein primitives Element von $\mathbb{K}^\times$ ist.
- Wenn $\mathrm{char}(\mathbb{K}) = p$ gilt, dann ist $(a + b)^p = a^p + b^p$ für alle $a, b \in \mathbb{K}$.

Ein Weg, die Existenz von Körpern mit p^n Elementen für jede Primzahl p und jedes $n \in \mathbb{N}$ zu zeigen, wäre es, für jedes $n \in \mathbb{N}$ ein irreduzibles Polynom $f \in \mathbb{F}_p[T]$ vom Grad n zu finden. Dann ist $\mathbb{F}_p[T]/(f)$ ein Körper mit p^n Elementen. Wir

gehen jedoch den Umweg über Zerfällungskörper, und dazu brauchen wir folgendes Lemma:

8.3.1 Lemma Sei $\mathbb{K}$ ein endlicher Körper mit q Elementen. Dann gilt $a^q = a$ für alle $a \in \mathbb{K}$.

Beweis: Für $a = 0$ gilt $a^q = 0$. Die Elemente $a \in \mathbb{K}$ mit $a \neq 0$ bilden bezüglich der Multiplikation eine zyklische Gruppe mit $(q-1)$ Elementen. Also folgt aus dem Satz von Lagrange, dass $a^{q-1} = 1$ für alle $a \in \mathbb{K}$ mit $a \neq 0$ gilt. Multiplikation mit a ergibt $a^q = a$. □

8.3.2 Lemma Sei $\mathbb{L}$ ein Körper mit q Elementen, und sei $\mathbb{K} \subseteq \mathbb{L}$ ein Unterkörper von $\mathbb{L}$. Dann zerfällt das Polynom $f = T^q - T \in \mathbb{K}[T]$ über $\mathbb{L}$ in Linearfaktoren, und $\mathbb{L}$ ist ein Zerfällungskörper von f über $\mathbb{K}$.

Beweis: Für jedes $a \in \mathbb{L}$ gilt $a^q - a = 0$, also sind alle q Elemente von $\mathbb{L}$ Nullstellen von f. Da $\mathrm{Grad}(f) = q$ gilt, sind dies alle Nullstellen von f, und f zerfällt in Linearfaktoren $f = \prod_{a \in \mathbb{L}} (T - a)$. Es gilt $f' = (T^q - T)' = qT^{q-1} - 1 = -1 \neq 0$ in $\mathbb{K}[T]$, also hat f' keine Nullstelle. Mit Proposition 5.7.21 kann f deshalb keine mehrfachen Nullstellen haben. Also muss ein Körper, in dem f in Linearfaktoren zerfällt, mindestens q Elemente haben. Dies zeigt, dass es keinen kleineren Körper als $\mathbb{L}$ geben kann, in dem f zerfällt. □

8.3.3 Aufgabe Sei $\mathbb{K}$ ein Körper. Zeigen Sie, dass eine nicht-leere Teilmenge $L \subseteq \mathbb{K}$ mit $L \neq \{0\}$ genau dann ein Körper ist, wenn für alle $a, b \in L$ mit $b \neq 0$ gilt: $a - b \in L$ und $ab^{-1} \in L$.

Nun haben wir alle Zutaten zusammen, um die endlichen Körper charakterisieren zu können:

8.3.4 Satz (Existenz und Eindeutigkeit von endlichen Körpern) Sei p eine Primzahl und $n \in \mathbb{N}$. Dann existiert ein Körper mit p^n Elementen. Jeder endliche Körper mit $q = p^n$ Elementen ist isomorph zum Zerfällungskörper von $T^q - T$ über $\mathbb{F}_p$.

Beweis: Wir beweisen zunächst die Existenz. Sei also p eine Primzahl, $n \in \mathbb{N}$ und $q = p^n$. Sei $\mathbb{K}$ der Zerfällungskörper von $T^q - T \in \mathbb{F}_p[T]$. Sei $L = \{a \in \mathbb{K} \mid a^q - a = 0\}$. Dann ist L ein Körper: Seien $a, b \in L$ mit $b \neq 0$. Dann gilt $(a-b)^q = (a-b)^{p^n} = a^{p^n} - b^{p^n} = a^q - b^q = a - b$. Außerdem ist $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$, also $ab^{-1} \in L$. Damit folgt mit Aufgabe 8.3.3, dass L ein Körper ist. Da L alle Nullstellen von

$T^q - T$ enthält, folgt schon $L = \mathbb{K}$. Wie wir im Beweis zu Lemma 8.3.2 gesehen haben, hat $T^q - T$ keine mehrfachen Nullstellen. Das heißt, $L = \mathbb{K}$ hat q Elemente.

Die Eindeutigkeit folgt aus der Tatsache, dass jeder Körper $\mathbb{K}$ mit q Elementen eine Erweiterung seines Primkörpers und damit isomorph zu einer Erweiterung von $\mathbb{F}_p$ ist. Mit Lemma 8.3.2 ist $\mathbb{K}$ dann isomorph zu einem Zerfällungskörper von $T^q - T$ über $\mathbb{F}_p$. Die Aussage folgt nun aus der Eindeutigkeit des Zerfällungskörpers. □

Satz 8.3.4 berechtigt uns, von „dem“ Körper mit q Elementen zu sprechen, den wir mit $\mathbb{F}_q$ bezeichnen.

8.3.5 Beispiel Wir wollen uns anschauen, wie wir $\mathbb{F}_8$ konstruieren können. Dazu faktorisieren wir zunächst $T^8 - T$ über $\mathbb{F}_2$ in irreduzible Faktoren, wobei wir uns von dem Computeralgebrasystem MuPAD helfen lassen:

$$T^8 - T = T(T+1)(T^3 + T + 1)(T^3 + T^2 + 1).$$

Das Polynom $T^3 + T + 1$ ist also irreduzibel über $\mathbb{F}_2$. Damit ist $\mathbb{F}_8 = \mathbb{F}_2[T]/(T^3 + T + 1)$. Jetzt überzeugen wir uns aber noch, dass das auch wirklich der Zerfällungskörper von $T^8 - T$ ist. Dazu sei $\alpha = [T]$ in $\mathbb{F}_8$. Dann ist:

$$\begin{aligned} T(T+1) \quad & (T+\alpha)(T+\alpha+1)(T+\alpha^2)(T+\alpha^2+1)(T+\alpha^2+\alpha)(T+\alpha^2+\alpha+1) \\ & = T(T+1)(T^2+T+\alpha^2+\alpha)(T^2+T+\alpha)(T^2+T+\alpha^2) \\ & = T(T+1)(T^4+(\alpha^2+1)T^2+\alpha^2 T+(\alpha^2+\alpha+1))(T^2+T+\alpha^2) \\ & = T(T+1)(T^6+T^5+T^4+T^3+T^2+T+1) \\ & = T^8+T = T^8-T. \end{aligned}$$

Also ist $\mathbb{F}_8$ tatsächlich der Zerfällungskörper von $T^8 - T$. Statt des Polynoms $T^3 + T + 1$ hätten wir genauso das Polynom $T^3 + T^2 + 1$ nehmen können.

Nun untersuchen wir, wann ein Körper $\mathbb{F}_{p^m}$ Unterkörper von $\mathbb{F}_{p^n}$ ist.

8.3.6 Proposition Sei $n \in \mathbb{N}$ und sei $\mathbb{F}_{p^n}$ der Körper mit $q = p^n$ Elementen. Dann hat jeder Unterkörper p^m Elemente, wobei m ein Teiler von n ist. Außerdem besitzt $\mathbb{F}_q$ für jeden Teiler m von n genau einen Unterkörper $\mathbb{F}_{p^m}$.

Beweis: Der erste Teil der Aussage ist klar, denn es gilt für jeden Unterkörper $\mathbb{F}_{p^m}$ von $\mathbb{F}_q$

$$n = [\mathbb{F}_q : \mathbb{F}_p] = [\mathbb{F}_q : \mathbb{F}_{p^m}][\mathbb{F}_{p^m} : \mathbb{F}_p] = [\mathbb{F}_q : \mathbb{F}_{p^m}] \cdot m,$$

also ist m ein Teiler von n.

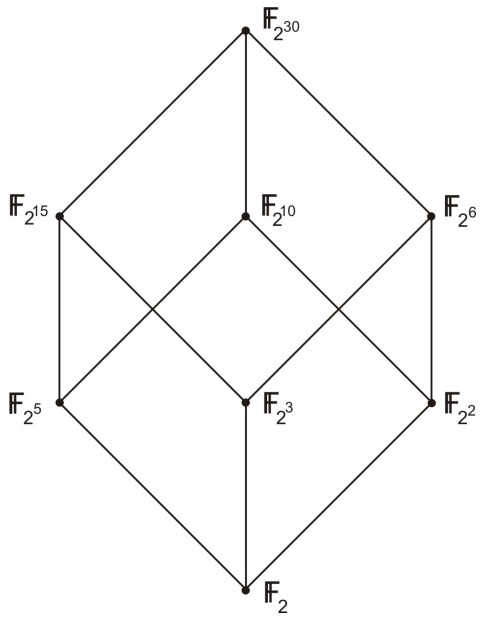


Abbildung 8.1: Die Unterkörper von $\mathbb{F}_{2^{30}}$

Sei nun m ein Teiler von n. Dann ist auch $p^m - 1$ ein Teiler von $p^n - 1$, denn dann ist $p^n - 1 = (p^m - 1)(p^{n-m} + p^{n-2m} + \ldots + p^m + 1)$. Für alle Elemente $a \neq 0$ aus $\mathbb{F}_{p^m}$ gilt also $a^{p^m-1} = 1$ und damit auch $a^{p^n-1} = 1$. Jedes Element aus $\mathbb{F}_{p^m}$ ist also auch Nullstelle von $T^{p^n} - T$ und gehört damit zu $\mathbb{F}_q$. Es folgt, dass $\mathbb{F}_q$ als Unterkörper einen Zerfällungskörper von $T^{p^m} - T$ über $\mathbb{F}_p$, also $\mathbb{F}_{p^m}$, enthält. Nehmen wir nun an, dass $\mathbb{F}_q$ zwei Unterkörper der Form $\mathbb{F}_{p^m}$ enthält. Dann enthielte $\mathbb{F}_q$ mehr als p^m Nullstellen von $T^{p^m} - T$, ein Widerspruch! □

Nun wissen wir also ziemlich genau über die endlichen Körper Bescheid. Abbildung 8.1 zeigt, welche Unterkörper wie in $\mathbb{F}_{2^{30}}$ enthalten sind.

Nun können wir auch zeigen, dass es zu jeder Primzahl p und zu jedem $n \in \mathbb{N}$ ein irreduzibles Polynom vom Grad n über $\mathbb{F}_p$ gibt.

8.3.7 Lemma Für jeden endlichen Körper $\mathbb{F}_q$ und jedes $n \in \mathbb{N}$ gibt es ein irreduzibles Polynom vom Grad n in $\mathbb{F}_q[T]$.

Beweis: Sei $\mathbb{F}_r$ der Oberkörper von $\mathbb{F}_q$ mit $r = q^n$ Elementen. Dann gilt $[\mathbb{F}_r : \mathbb{F}_q] = n$. Sei $a \in \mathbb{F}_r$ ein primitives Element von $\mathbb{F}_r$. Dann ist $\mathbb{F}_q(a) \subseteq \mathbb{F}_r$, und da $\mathbb{F}_q(a)$ die 0 und auch jedes andere Element von $\mathbb{F}_r$ enthält, gilt $\mathbb{F}_q(a) = \mathbb{F}_r$. Mit Satz 8.2.28 gilt, dass der Grad des Minimalpolynoms f von a über $\mathbb{F}_q$ gerade n ist, also ist f ein irreduzibles Polynom vom Grad n über $\mathbb{F}_q$. □

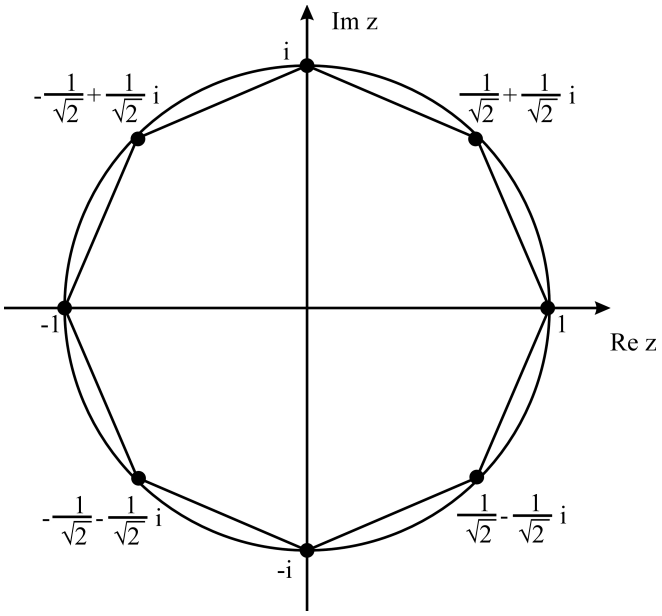


Abbildung 8.2: Die achten Einheitswurzeln

Wir wissen jetzt zwar, dass es für jedes $n \in \mathbb{N}$ und jede Primzahl p ein irreduzibles Polynom vom Grad n über $\mathbb{F}_p$ gibt, aber das heißt leider noch lange nicht, dass es einfach ist, ein solches irreduzibles Polynom auch zu berechnen.

8.3.8 Aufgabe Sei p eine Primzahl, und sei $f \in \mathbb{F}_p[T]$ irreduzibel. Zeigen Sie, dass $f \mid T^{p^n} - T$ genau dann gilt, wenn $\mathrm{Grad}(f) \mid n$ gilt.

8.4 Einheitswurzeln

In diesem Abschnitt betrachten wir den Zerfällungskörper des Polynoms $T^n - 1$ über einem beliebigen (nicht unbedingt endlichen) Körper.

8.4.1 Definition Sei $n \in \mathbb{N}$ und $\mathbb{K}$ ein Körper. Der Zerfällungskörper von $T^n - 1$ über $\mathbb{K}$ heißt n-ter **Kreisteilungkörper** und wird mit $\mathbb{K}^{(n)}$ bezeichnet. Die Nullstellen von $T^n - 1$ in $\mathbb{K}^{(n)}$ heißen n-te **Einheitswurzeln**, und die Menge der n-ten Einheitswurzeln wird mit $E^{(n)}$ bezeichnet.

8.4.2 Beispiel Ist $\mathbb{K} = \mathbb{Q}$, dann ist $E^{(n)}$ die Menge der komplexen n-ten Einheitswurzeln. In der komplexen Ebene sind dies gerade die Ecken eines regelmäßigen n-Ecks auf dem Einheitskreis, wie Sie in Abbildung 8.2 sehen.

Die dritten Einheitwurzeln haben wir für $\mathbb{K} = \mathbb{Q}$ bereits in Beispiel 8.2.39 berechnet:

$$E^{(3)} = \{1, b = -\frac{1}{2} - \frac{\sqrt{3}}{2}i, b^2 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i\}.$$

8.4.3 Aufgabe Sei $\xi \neq 1$ eine n-te Einheitswurzel über einem Körper $\mathbb{K}$. Zeigen Sie: $1 + \xi + \xi^2 + \ldots + \xi^{n-1} = 0$.

Der griechische Buchstabe ξ wird „xi“ ausgesprochen.

Der nächste Satz zeigt, dass die Struktur von $E^{(n)}$ davon abhängt, wie n sich zur Charakteristik von $\mathbb{K}$ verhält.

8.4.4 Satz Sei $n \in \mathbb{N}$ und sei $\mathbb{K}$ ein Körper der Charakteristik $p \geq 0$. Dann gilt:

1. Wenn p nicht n teilt, dann ist $E^{(n)}$ mit der Multiplikation in $\mathbb{K}^{(n)}$ eine zyklische Gruppe der Ordnung n.
2. Wenn $p \mid n$ gilt, dann sei $n = p^e m$, wobei $e, m \in \mathbb{N}$ und $\mathrm{ggT}(p, m) = 1$ gelte. Dann gilt $\mathbb{K}^{(n)} = \mathbb{K}^{(m)}$, $E^{(n)} = E^{(m)}$, und die Nullstellen von $T^n - 1$ in $\mathbb{K}^{(n)}$ sind die m Elemente von $E^{(m)}$, jedes mit Multiplizität p^e.

Beweis:

1. Für $n = 1$ ist die Behauptung klar. Sei nun $n > 1$. Dann ist $(T^n - 1)' = nT^{n-1}$. Da p nicht n teilt, ist 0 die einzige Nullstelle von $(T^n - 1)'$, das heißt, $(T^n - 1)$ und $(T^n - 1)'$ haben keine gemeinsamen Nullstellen und $T^n - 1$ hat keine mehrfachen Nullstellen. Also hat $E^{(n)}$ genau n Elemente.

   Seien $a, b \in E^{(n)}$, dann ist auch $ab^{-1} \in E^{(n)}$, denn $(ab^{-1})^n = a^n(b^{-1})^n = 1 \cdot 1^{-1} = 1$. Da außerdem $1 \in E^{(n)}$ gilt und $E^{(n)}$ also nicht leer ist, folgt mit dem Untergruppenkriterium, dass $E^{(n)}$ eine Gruppe ist, und zwar eine endliche Untergruppe von $(\mathbb{K}^{(n)})^\times$. Mit Satz 4.8.9 folgt, dass $E^{(n)}$ zyklisch ist.

2. Es ist $T^n - 1 = T^{p^e m} - 1 = (T^m - 1)^{p^e}$, denn $\mathrm{char}(\mathbb{K}) = p$. Also ist $E^{(n)} = E^{(m)}$ und $\mathbb{K}^{(n)} = \mathbb{K}^{(m)}$. Außerdem folgt sofort, dass jede Nullstelle von $T^n - 1$ ein Element von $E^{(m)}$ ist und mit Multiplizität p^e auftritt.

□

Die erzeugenden Elemente von $E^{(n)}$ bekommen wieder einen eigenen Namen:

8.4.5 Definition Sei $\mathbb{K}$ ein Körper mit $\mathrm{char}(\mathbb{K}) = p \geq 0$ und sei $n \in \mathbb{N}$ mit $p \nmid n$. Ein erzeugendes Element der zyklischen Gruppe $E^{(n)}$ wird **primitive** n-te Einheitswurzel genannt.

8.4.6 Beispiel Sei $\mathbb{K} = \mathbb{Q}$ und $n = 3$. Wir haben schon eine primitive dritte Einheitswurzel kennengelernt, nämlich $b = \frac{1}{2} - \frac{\sqrt{3}}{2}i$. Es gilt $E^{(3)} = \{b^0 = 1, b^1 = \frac{1}{2} - \frac{\sqrt{3}}{2}i, b^2 = \frac{1}{2} + \frac{\sqrt{3}}{2}i\}$.

8.4.7 Lemma Sei $\mathbb{K}$ ein Körper und sei $n \in \mathbb{N}$. Dann ist $\mathbb{K}^{(n)}$ eine einfache algebraische Erweiterung von $\mathbb{K}$.

Beweis: Ist $\mathrm{char}(\mathbb{K}) = p$ und gilt $p \nmid n$, dann gibt es eine primitive n-te Einheitswurzel ξ, und es gilt $\mathbb{K}^{(n)} = \mathbb{K}(\xi)$. Gilt $p \mid n$, dann ist $\mathbb{K}^{(n)} = \mathbb{K}^{(m)}$ mit m wie in Satz 8.4.4, und es gibt eine primitive m-te Einheitswurzel ξ. Es gilt $\mathbb{K}^{(n)} = \mathbb{K}^{(m)} = \mathbb{K}(\xi)$. □

Wenn $\mathbb{K}$ ein Körper mit $\mathrm{char}(\mathbb{K}) = p \geq 0$ und $n \in \mathbb{N}$ mit $\mathrm{ggT}(n, p) = 1$ ist, dann ist $E^{(n)}$ eine zyklische Gruppe mit n Elementen. Es gibt also $\varphi(n)$ viele primitive n-te Einheitswurzeln. Ist ξ eine solche Einheitswurzel, dann sind alle alle anderen primitiven n-ten Einheitswurzeln von der Form ξ^i mit $\mathrm{ggT}(i, n) = 1$. Interessanterweise gibt es ein Polynom in $\mathbb{K}[T]$, dessen Nullstellen genau die primitiven n-ten Einheitswurzeln sind.

8.4.8 Definition Sei $\mathbb{K}$ ein Körper mit $\mathrm{char}(\mathbb{K}) = p \geq 0$, und sei $n \in \mathbb{N}$ mit $p \nmid n$. Sei ξ eine primitive n-te Einheitswurzel über $\mathbb{K}$. Dann heißt das Polynom

$$Q_n = \prod_{\substack{i=1 \\ \mathrm{ggT}(i,n)=1}}^{n} (T - \xi^i)$$

das n-te **Kreisteilungspolynom** über $\mathbb{K}$.

Klar ist, dass Q_n nicht von der Wahl von ξ abhängt. Außerdem ist klar, dass $\mathrm{Grad}(Q_n) = \varphi(n)$ und $Q_n \in \mathbb{K}^{(n)}[T]$ gilt. Nun zeigen wir, dass Q_n in $\mathbb{P}[T]$ liegt, wobei $\mathbb{P}$ der Primkörper von $\mathbb{K}$ ist.

8.4.9 Proposition Sei $\mathbb{K}$ ein Körper mit $\mathrm{char}(\mathbb{K}) = p \geq 0$, und sei $n \in \mathbb{N}$ mit $p \nmid n$. Dann gilt:

1. $T^n - 1 = \prod_{d|n} Q_d$.
2. $Q_n \in \mathbb{P}[T]$, wobei $\mathbb{P}$ der Primkörper von $\mathbb{K}$ ist. Ist $\mathrm{char}(\mathbb{K}) = 0$, dann gilt sogar $Q_n \in \mathbb{Z}[T]$.

Beweis:

1. Sei ξ eine primitive n-te Einheitswurzel. Dann ist ξ^i für $1 \leq i \leq n$ mit Proposition 4.8.5 eine primitive d-te Einheitswurzel, wobei $d = \frac{n}{\mathrm{ggT}(n,i)}$ gilt.

   Nun ist $T^n - 1 = \prod_{i=1}^{n}(T - \xi^i)$, und wenn man nun jeweils alle Potenzen von ξ^i zusammenfasst, die eine primitive $d = \frac{n}{\mathrm{ggT}(n,i)}$-te Einheitswurzel sind, folgt die Behauptung.

2. Wir benutzen Induktion über n. Für $n = 1$ ist $Q_1 = (T-1)$, die Behauptung ist also wahr. Die Behauptung gelte nun für alle Q_d mit $1 \leq d < n$. Mit dem ersten Teil gilt

$$T^n - 1 = \prod_{d|n} Q_d = Q_n \prod_{\substack{d|n \\ d<n}} Q_d,$$

   also

$$Q_n = \frac{T^n - 1}{\prod_{\substack{d|n \\ d<n}} Q_d}.$$

   Nach Induktionsvoraussetzung gilt $\prod_{\substack{d|n \\ d<n}} Q_d \in \mathbb{P}[T]$ und $\prod_{\substack{d|n \\ d<n}} Q_d \in \mathbb{Z}[T]$, falls $\mathbb{P} \simeq \mathbb{Q}$ gilt. Außerdem ist $\prod_{\substack{d|n \\ d<n}} Q_d$ normiert, und Polynomdivision zeigt nun, dass auch $Q_n \in \mathbb{P}[T]$ beziehungsweise $Q_n \in \mathbb{Z}[T]$ gilt.

□

8.4.10 Beispiele 1. Sei $n = 12$, und sei ξ eine primitive 12-te Einheitswurzel. Dann ist

$$\begin{aligned} T^{12} - 1 \;=\; \prod_{i=1}^{12}(T - \xi^i) = {} & \underbrace{(T-1)}_{Q_1}\underbrace{(T-\xi^6)}_{Q_2}\underbrace{(T-\xi^4)(T-\xi^8)}_{Q_3} \\ & \cdot \underbrace{(T-\xi^3)(T-\xi^9)}_{Q_4}\underbrace{(T-\xi^2)(T-\xi^{10})}_{Q_6} \\ & \cdot \underbrace{(T-\xi)(T-\xi^5)(T-\xi^7)(T-\xi^{11})}_{Q_{12}}. \end{aligned}$$

2. Sei p eine Primzahl. Dann gilt

$$Q_p = \frac{T^p - 1}{T - 1} = T^{p-1} + T^{p-2} + \ldots + T + 1.$$

3. Sei p eine Primzahl, und sei $k \in \mathbb{N}$. Dann ist:

$$\begin{aligned} Q_{p^k} &= \frac{T^{p^k}-1}{Q_{p^{k-1}}Q_{p^{k-2}}\ldots Q_pQ_1} = \frac{T^{p^k}-1}{T^{p^{k-1}}-1} \\ &= T^{(p-1)p^{k-1}} + T^{(p-2)p^{k-1}} + \ldots + T^{p^{k-1}} + 1. \end{aligned}$$

Wir können nun nach und nach mit Proposition 8.4.9 und Beispiel 8.4.10 alle Kreisteilungspolynome berechnen. Hier sei $\mathbb{K} = \mathbb{Q}$.

$$\begin{aligned} Q_1 &= T-1 \\ Q_2 &= \frac{T^2-1}{T-1} = T+1 \\ Q_3 &= T^2+T+1 \\ Q_4 &= T^2+1 \\ Q_5 &= T^4+T^3+T^2+T+1 \\ Q_6 &= \frac{T^6-1}{(T-1)(T+1)(T^2+T+1)} = T^2-T+1 \\ Q_7 &= T^6+T^5+T^4+T^3+T^2+T+1 \\ Q_8 &= T^4+1 \\ Q_9 &= T^6+T^3+1 \\ Q_{10} &= \frac{T^{10}-1}{(T-1)(T+1)(T^4+T^3+T^2+T+1)} = T^4-T^3+T^2-T+1 \\ Q_{11} &= T^{10}+T^9+T^8+T^7+T^6+T^5+T^4+T^3+T^2+T+1 \\ Q_{12} &= \frac{T^{12}-1}{(T-1)(T+1)(T^2+T+1)(T^2+1)(T^2-T+1)} = T^4-T^2+1. \end{aligned}$$

8.4.11 Aufgabe Berechnen Sie Q_{13}, Q_{14}, Q_{15} und Q_{16} für $\mathbb{K} = \mathbb{Q}$.

Natürlich kann man noch sehr viel mehr zu Kreisteilungskörpern und -polynomen sagen, aber wir haben nun den Stoff zusammen, den wir in Kurseinheit 6 benötigen, und wollen es an dieser Stelle dabei bewenden lassen.

8.5 Die Spur

In diesem Abschnitt betrachten wir eine Körpererweiterung $\mathbb{L} : \mathbb{K}$ mit $\mathbb{K} = \mathbb{F}_q$ (und $q = p^n$) und $\mathbb{L} = \mathbb{F}_{q^m}$, wobei $m, n \in \mathbb{N}$ gilt. Wir betrachten $\mathbb{L}$ als $\mathbb{K}$-Vektorraum und untersuchen eine lineare Abbildung von $\mathbb{L}$ nach $\mathbb{K}$.

8.5.1 Definition Sei $\mathbb{K} = \mathbb{F}_q$ mit $q = p^n$ für eine Primzahl p und $n \in \mathbb{N}$ und $\mathbb{L} = \mathbb{F}_{q^m}$ für ein $m \in \mathbb{N}$. Für jedes $\alpha \in \mathbb{L}$ ist die **Spur** von α über $\mathbb{K}$ definiert als

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}.$$

(Die Bezeichnung „Tr“ kommt vom englischen „Trace“ = Spur.) Ist $\mathbb{K}$ der Primkörper von $\mathbb{L}$, dann wird die Spur einfach mit $\mathrm{Tr}_{\mathbb{L}}(\alpha)$ bezeichnet.

In der folgenden Proposition sind die wichtigsten Eigenschaften der Abbildung Tr aufgelistet.

8.5.2 Proposition Seien $\mathbb{K} = \mathbb{F}_q$ und $\mathbb{L} = \mathbb{F}_{q^m}$ wie in Definition 8.5.1. Dann gilt:

1. $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) \in \mathbb{K}$ für alle $\alpha \in \mathbb{L}$.
2. $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha + \beta) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) + \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\beta)$ für alle $\alpha, \beta \in \mathbb{L}$.
3. $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(c\alpha) = c\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha)$ für alle $\alpha \in \mathbb{L}$ und alle $c \in \mathbb{K}$.
4. $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ ist eine surjektive lineare Abbildung von $\mathbb{L}$ nach $\mathbb{K}$, wobei beide Körper als $\mathbb{K}$-Vektorräume betrachtet werden.
5. $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = m\alpha$ für alle $\alpha \in \mathbb{K}$.
6. $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha^q) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha)$ für alle $\alpha \in \mathbb{L}$.

Beweis:

1. Sei $\alpha \in \mathbb{L}$. Dann ist

$$\begin{aligned}(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha))^q &= (\alpha + \alpha^q + \ldots + \alpha^{q^{m-1}})^q \\ &= \alpha^q + \alpha^{q^2} + \ldots \alpha^{q^m} \quad (\text{ denn in } \mathbb{L} \text{ gilt } (\alpha+\beta)^q = \alpha^q + \beta^q) \\ &= \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{m-1}} + \alpha (\text{denn in } \mathbb{L} \text{ gilt } \alpha^{q^m} = \alpha \text{ für alle } \alpha) \\ &= \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha).\end{aligned}$$

   Es folgt, dass $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) \in \mathbb{K}$ gilt.

2. Seien $\alpha, \beta \in \mathbb{L}$. Dann ist

$$\begin{aligned}\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha+\beta) &= (\alpha+\beta) + (\alpha+\beta)^q + \ldots + (\alpha+\beta)^{q^{m-1}} \\ &= \alpha + \beta + \alpha^q + \beta^q + \ldots + \alpha^{q^{m-1}} + \beta^{q^{m-1}} \\ &= \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) + \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\beta).\end{aligned}$$

3. Seien $\alpha \in \mathbb{L}$ und $c \in \mathbb{K}$. Dann gilt

$$\begin{aligned} \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(c\alpha) &= (c\alpha) + (c\alpha)^q + \ldots + (c\alpha)^{q^{m-1}} \\ &= c\alpha + c^q\alpha^q + \ldots + c^{q^{m-1}}\alpha^{q^{m-1}} \\ &= c\alpha + c\alpha^q + \ldots + c\alpha^{q^{m-1}} \text{ (denn } c \in \mathbb{K}, \text{ also } c^q = c) \\ &= c\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha). \end{aligned}$$

4. Aus den ersten drei Teilen folgt, dass $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}} : \mathbb{L} \longrightarrow \mathbb{K}$ linear ist. Es ist also nur noch zu zeigen, dass $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ surjektiv ist. Dazu reicht es zu zeigen, dass $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ nicht die Nullabbildung ist. Jedes Element $\alpha \in \mathbb{L}$, das auf 0 abgebildet wird, ist eine Nullstelle des Polynoms $T + T^q + \ldots + T^{q^{m-1}} \in \mathbb{K}[T]$. Dies ist ein Polynom vom Grad q^{m-1}, es kann also höchstens q^{m-1} Nullstellen haben. Damit kann $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ nicht die Nullabbildung sein, denn $\mathbb{L}$ hat q^m Elemente. Also ist $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ surjektiv.

5. Sei $\alpha \in \mathbb{K}$. Dann gilt

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}} = \alpha + \alpha + \ldots + \alpha = m\alpha.$$

6. Sei $\alpha \in \mathbb{L}$. Dann ist

$$\begin{aligned} \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha^q) &= \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^m} \\ &= \alpha^q + \alpha^{q^2} + \ldots + \alpha \text{ (denn } \alpha^{q^m} = \alpha) \\ &= \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha). \end{aligned}$$

□

8.5.3 Proposition Seien $\mathbb{K}, \mathbb{L}, \mathbb{M}$ endliche Körper, und seien $\mathbb{L} : \mathbb{K}$ und $\mathbb{M} : \mathbb{L}$ Körpererweiterungen. Sei $\alpha \in \mathbb{M}$. Dann gilt:

$$\mathrm{Tr}_{\mathbb{M}/\mathbb{K}}(\alpha) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\mathrm{Tr}_{\mathbb{M}/\mathbb{L}}(\alpha)).$$

Beweis: Sei $\mathbb{K} = \mathbb{F}_q$, $\mathbb{L} = \mathbb{F}_{q^n}$ und $\mathbb{M} = \mathbb{F}_{q^{nm}}$ mit $n, m \in \mathbb{N}$, also $[\mathbb{L} : \mathbb{K}] = n$, $[\mathbb{M} : \mathbb{L}] = m$ und $[\mathbb{M} : \mathbb{K}] = nm$. Wir haben

$$\begin{aligned} \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\mathrm{Tr}_{\mathbb{M}/\mathbb{L}}(\alpha)) &= \mathrm{Tr}_{\mathbb{M}/\mathbb{L}}(\alpha) + (\mathrm{Tr}_{\mathbb{M}/\mathbb{L}}(\alpha))^q + \ldots + (\mathrm{Tr}_{\mathbb{M}/\mathbb{L}}(\alpha))^{q^{n-1}} \\ &= (\alpha + \alpha^{q^n} + \ldots + \alpha^{q^{n(m-1)}}) + (\alpha + \alpha^{q^n} + \ldots + \alpha^{q^{n(m-1)}})^q \\ &\quad + \ldots + (\alpha + \alpha^{q^n} + \ldots + \alpha^{q^{n(m-1)}})^{q^{n-1}} \end{aligned}$$

Nun multiplizieren wir die Klammern aus und erhalten:

$$\begin{array}{lllll} = & \alpha & +\alpha^{q^n} & +\ldots & +\alpha^{q^{nm-n}} \\ + & \alpha^q & +\alpha^{q^{n+1}} & +\ldots & +\alpha^{q^{nm-n+1}} \\ & \vdots & & & \\ + & \alpha^{q^{n-1}} & +\alpha^{q^{2n-1}} & +\ldots & +\alpha^{q^{nm-1}} \end{array}$$

Jetzt wird spaltenweise summiert, und es ergibt sich:

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\mathrm{Tr}_{\mathbb{M}/\mathbb{L}})(\alpha) = \sum_{i=0}^{nm-1} \alpha^{q^i} = \mathrm{Tr}_{\mathbb{M}/\mathbb{K}}(\alpha).$$

□

8.5.4 Aufgabe Seien $\mathbb{K} = \mathbb{F}_q$ und $\mathbb{L} = \mathbb{F}_{q^m}$ wie in Definition 8.5.1. Sei $a \in \mathbb{L}$, und das Minimalpolynom von a über $\mathbb{K}$ habe den Grad d. Zeigen Sie:

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(a) = \frac{m}{d}\mathrm{Tr}_{\mathbb{K}(a)/\mathbb{K}}(a).$$

Sie fragen sich vielleicht, ob die Spur etwas mit der Spur einer Matrix zu tun hat, die Ihnen aus der Linearen Algebra bekannt ist. Dazu sehen wir uns $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ einmal aus einem anderen Blickwinkel an: Sei $\alpha \in \mathbb{L}$ und sei $g \in \mathbb{K}[T]$ das Minimalpolynom von α über $\mathbb{K}$. Dann ist der Grad d von g mit Satz 8.2.28 ein Teiler von m, wobei m der Grad der Körpererweiterung von $\mathbb{L} : \mathbb{K}$ ist. Sei $f = g^{\frac{m}{d}}$. Dann gilt $\mathrm{Grad}(f) = m$, und f wird das charakteristische Polynom von α genannt. Sei $f = \sum_{i=0}^{m} a_i T^i$ mit $a_0, \ldots, a_m \in \mathbb{K}$ und sei $g = \sum_{i=0}^{d} b_i T^i$ mit $b_0, \ldots, b_d \in \mathbb{K}$. Nach Voraussetzung gilt $g(\alpha) = 0$, und damit ist für $1 \leq k \leq d-1$ auch

$$\begin{aligned} g(\alpha^{q^k}) &= \sum_{i=0}^{d} b_i(\alpha^{q^k})^i = \sum_{i=0}^{d} b_i(\alpha^i)^{q^k} = \sum_{i=0}^{d} b_i^{q^k}(\alpha^i)^{q^k} \\ &= \sum_{i=0}^{d}(b_i\alpha^i)^{q^k} = (\sum_{i=0}^{d} b_i\alpha^i)^{q^k} = (g(\alpha))^{q^k} = 0. \end{aligned}$$

Es sind also $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ Nullstellen von g. Außerdem gilt $\alpha^{q^i} \neq \alpha^{q^j}$ für $0 \leq i < j \leq d-1$, denn angenommen $\alpha^{q^i} = \alpha^{q^j}$, dann folgt $\alpha = \alpha^{q^{j-i+1}}$, und $2 \leq j-i+1 \leq d-1$, also $\alpha \in \mathbb{F}_{q^{j-i+1}}$, ein Widerspruch. Also sind $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ die d verschiedenen Nullstellen von g und $g = (T-\alpha)\cdots(T-\alpha^{q^{d-1}})$. Jede Nullstelle

von g ist eine $\frac{m}{d}$-fache Nullstelle von f, also

$$\begin{aligned} f &= (T-\alpha)^{\frac{m}{d}} \cdots (T-\alpha^{q^{d-1}})^{\frac{m}{d}} \\ &= \Big((T-\alpha)(T-\alpha^{q^d})(T-\alpha^{q^{2d}}) \cdots (T-\alpha^{q^{m-d}})\Big) \cdots \Big((T-\alpha^{q^{d-1}}) \cdots (T-\alpha^{q^{m-1}})\Big) \\ &= (T-\alpha)(T-\alpha^q) \ldots (T-\alpha^{q^{m-1}}), \end{aligned}$$

denn $\alpha^{q^d} = \alpha$. Koeffizientenvergleich zeigt, dass $a_{m-1} = -(\alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}) = -\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha)$ gilt. Dies ist - wie Sie sich sicher aus der Linearen Algebra erinnern - analog zu den Matrizen über einem Körper. Sei nämlich $A \in M_{mm}(\mathbb{K})$ mit charakteristischem Polynom $\chi_A = \sum_{i=0}^{m} a_i T^i$, dann gilt $a_{m-1} = -\mathrm{Spur}(A)$.

Lösungen der Aufgaben

Lösungen der Aufgaben in Kapitel 8

Aufgabe 8.1.4 Gesucht ist ein Beispiel für einen Körper mit 8 Elementen.

Dazu wird ein irreduzibles Polynom in $\mathbb{F}_2[T]$ vom Grad 3 benötigt. Aus Beispiel 5.7.23 wissen wir, dass zum Beispiel das Polynom $T^3 + T + 1$ über $\mathbb{F}_2$ irreduzibel ist. Dann ist $\mathbb{F}_2[T]/(T^3 + T + 1)$ ein Körper mit 8 Elementen. Diese sind $[0], [1], [T], [T+1], [T^2], [T^2+1], [T^2+T], [T^2+T+1]$. Die vollständigen Additions- und Multiplikationstabellen von $\mathbb{F}_2[T]/(T^3 + T + 1)$ sind:

$+$	$[0]$	$[1]$	$[T]$	$[T+1]$	$[T^2]$	$[T^2+1]$	$[T^2+T]$	$[T^2+T+1]$
$[0]$	$[0]$	$[1]$	$[T]$	$[T+1]$	$[T^2]$	$[T^2+1]$	$[T^2+T]$	$[T^2+T+1]$
$[1]$	$[1]$	$[0]$	$[T+1]$	$[T]$	$[T^2+1]$	$[T^2]$	$[T^2+T+1]$	$[T^2+T]$
$[T]$	$[T]$	$[T+1]$	$[0]$	$[1]$	$[T^2+T]$	$[T^2+T+1]$	$[T^2]$	$[T^2+1]$
$[T+1]$	$[T+1]$	$[T]$	$[1]$	$[0]$	$[T^2+T+1]$	$[T^2+T]$	$[T^2+1]$	$[T^2]$
$[T^2]$	$[T^2]$	$[T^2+1]$	$[T^2+T]$	$[T^2+T+1]$	$[0]$	$[1]$	$[T]$	$[T+1]$
$[T^2+1]$	$[T^2+1]$	$[T^2]$	$[T^2+T+1]$	$[T^2+T]$	$[1]$	$[0]$	$[T+1]$	$[T]$
$[T^2+T]$	$[T^2+T]$	$[T^2+T+1]$	$[T^2]$	$[T^2+1]$	$[T]$	$[T+1]$	$[0]$	$[1]$
$[T^2+T+1]$	$[T^2+T+1]$	$[T^2+T]$	$[T^2+1]$	$[T^2]$	$[T+1]$	$[T]$	$[1]$	$[0]$

und

$\cdot$	$[0]$	$[1]$	$[T]$	$[T+1]$	$[T^2]$	$[T^2+1]$	$[T^2+T]$	$[T^2+T+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[T]$	$[T+1]$	$[T^2]$	$[T^2+1]$	$[T^2+T]$	$[T^2+T+1]$
$[T]$	$[0]$	$[T]$	$[T^2]$	$[T^2+T]$	$[T+1]$	$[1]$	$[T^2+T+1]$	$[T^2+1]$
$[T+1]$	$[0]$	$[T+1]$	$[T^2+T]$	$[T^2+1]$	$[T^2+T+1]$	$[T^2]$	$[1]$	$[T]$
$[T^2]$	$[0]$	$[T^2]$	$[T+1]$	$[T^2+T+1]$	$[T^2+T]$	$[T]$	$[T^2+1]$	$[1]$
$[T^2+1]$	$[0]$	$[T^2+1]$	$[1]$	$[T^2]$	$[T]$	$[T^2+T+1]$	$[T+1]$	$[T^2+T]$
$[T^2+T]$	$[0]$	$[T^2+T]$	$[T^2+T+1]$	$[1]$	$[T^2+1]$	$[T+1]$	$[T]$	$[T^2]$
$[T^2+T+1]$	$[0]$	$[T^2+T+1]$	$[T^2+1]$	$[T]$	$[1]$	$[T^2+T]$	$[T^2]$	$[T+1]$

□

Aufgabe 8.1.6

Behauptung $f = T^2 + 1$ ist irreduzibel in $\mathbb{F}_3[T]$.

Beweis: Da $\text{Grad}(f) = 2$ gilt, ist f genau dann irreduzibel, wenn f in $\mathbb{F}_3$ keine Nullstelle hat. Es gilt $f(0) = 1$, $f(1) = 2$ und $f(2) = 2$, also ist f irreduzibel. □

In $\mathbb{F}_3[T]/(f)$ gilt

(a) $[T+2][T+1] = [T^2+3T+2] = [T^2+2] = [T^2+1]+[1] = [1]$.

(b) $([T+1]+[2T+1])[T+2] = [3T+2][T+2] = [2][T+2] = [2T+1]$.

(c) $[T+1]^3 = [T+1][T^2+2T+1] = [T+1]([T^2+1]+[2T]) = [T+1][2T] = [2T^2+2T] = [2T^2+2]+[2T+1] = 2[T^2+1]+[2T+1] = [2T+1]$.

(d) $[T+2]-[2T-2]+[2] = [2T+1]+[2] = [2T]$.

(e) $[T+1][2]+[T][2T+2] = [2T+2]+[2T^2+2T] = [2T^2+T+2] = [2T^2+2]+[T] = 2[T^2+1]+[T] = [T]$.

□

Aufgabe 8.2.3 Sei $\mathbb{K}$ ein Körper und $R \neq \{0\}$ ein Ring.

1. **Behauptung** Ist $\phi : \mathbb{K} \longrightarrow R$ ein surjektiver Ringhomomorphismus, dann folgt schon, dass R ein Körper ist.

   Beweis: Die einzigen Ideale in $\mathbb{K}$ sind mit Proposition 5.2.6 (0) und $\mathbb{K}$. Nun ist aber $\mathrm{Kern}(\phi)$ ein Ideal in $\mathbb{K}$, es gilt also $\mathrm{Kern}(\phi) = (0)$ oder $\mathrm{Kern}(\phi) = \mathbb{K}$. Die letzte Möglichkeit kann nicht sein, denn wir fordern immer $\phi(1) = 1$ für einen Ringhomomorphismus, und in R ist nach Voraussetzung $1 \neq 0$. Also gilt $\mathrm{Kern}(\phi) = (0)$. Mit dem Homomorphisatz für Ringe folgt $R \simeq \mathbb{K}$, also ist R ein Körper. □

2. Ist p eine Primzahl, dann ist die Abbildung $\phi' : \mathbb{Z} \longrightarrow \mathbb{F}_p$ mit $\phi'(z) = z \bmod p$ ein surjektiver Ringhomomorphismus. Es folgt also nicht unbedingt, dass R ein Körper ist. □

Aufgabe 8.2.7 Sei $\mathbb{K}$ ein Körper, sei I eine nicht-leere Indexmenge und sei $(\mathbb{L}_i)_{i\in I}$ ein System von Unterkörpern von $\mathbb{K}$.

Behauptung $\cap_{i\in I}\mathbb{L}_i$ ist ein Körper.

Beweis: Sei $M = \cap_{i\in I}\mathbb{L}_i$.

- Seien $a, b \in M$. Dann gilt $a, b \in \mathbb{L}_i$ für alle $i \in I$, also $a+b \in \mathbb{L}_i$ und $ab \in \mathbb{L}_i$ für alle $i \in I$, das heißt, $a+b \in M$ und $ab \in M$. Dies zeigt, dass $+$ und $\cdot$ Verknüpfungen auf M sind.
- Die 0 und die 1 aus $\mathbb{K}$ liegen mit Bemerkung 8.2.6 in jedem Unterkörper $\mathbb{L}_i$ von $\mathbb{K}$, also gilt $0 \in M$ und $1 \in M$.
- Sei $a \in M$. Dann gilt $a \in \mathbb{L}_i$ für alle $i \in I$, also auch $-a \in \mathbb{L}_i$ und, falls $a \neq 0$ gilt, $a^{-1} \in \mathbb{L}_i$ für alle $i \in I$. Es folgt $-a \in M$ und für $a \neq 0$ auch $a^{-1} \in M$.

- Da M eine Teilmenge von $\mathbb{K}$ ist, gelten in M das Assoziativgesetz für die Addition und für die Multiplikation und die Distributivgesetze. Außerdem sind Addition und Multiplikation kommutativ.

Alles zusammen zeigt, dass M ein Körper ist. □

Aufgabe 8.2.18 Sei $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung, und sei $a \in \mathbb{L}$ algebraisch über $\mathbb{K}$. Sei $I = \{f \in \mathbb{K}[T] \mid f(a) = 0\}$.

Behauptung I ist ein Ideal in $\mathbb{K}[T]$.

Beweis: Es gilt $0 \in I$, und für $f, g \in I$ ist $(f-g)(a) = f(a)+(-g)(a) = 0+0 = 0$, also $f - g \in I$. Mit dem Untergruppenkriterium ist also I eine Untergruppe von $\mathbb{K}[T]$. Sei $f \in I$ und $g \in \mathbb{K}[T]$. Dann gilt $(fg)(a) = f(a)g(a) = 0 \cdot g(a) = 0$, also $fg \in I$. Dies zeigt, dass I ein Ideal ist. □

Aufgabe 8.2.22 Sei $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung und sei $a \in \mathbb{L}$ algebraisch mit Minimalpolynom $g \in \mathbb{K}[T]$.

Behauptung Es gilt genau dann $a \in \mathbb{K}$, wenn $\mathrm{Grad}(g) = 1$ gilt.

Beweis: Wir nehmen zunächst an, dass $a \in \mathbb{K}$ gilt. Dann ist $f = T - a \in \mathbb{K}[T]$ ein normiertes Polynom vom Grad 1 mit $f(a) = 0$. Das einzige normierte Polynom mit echt kleinerem Grad ist die Konstante 1. Da aber $1(a) \neq 0$ gilt, ist f schon das Minimalpolynom von a.

Es gelte nun umgekehrt $\mathrm{Grad}(g) = 1$. Dann ist g von der Form $T - \alpha$ mit $\alpha \in \mathbb{K}$. Die einzige Nullstelle von g ist α, also $a = \alpha \in \mathbb{K}$. □

Aufgabe 8.2.27 Seien $\mathbb{M} : \mathbb{L}$ und $\mathbb{L} : \mathbb{K}$ Körpererweiterungen und sei $S \subseteq \mathbb{M}$ eine beliebige Teilmenge.

1. **Behauptung** Ist $\mathbb{K}(S) = \mathbb{M}$, dann folgt $\mathbb{L}(S) = \mathbb{M}$.

   Beweis: Es gilt sicher $\mathbb{L}(S) \subseteq \mathbb{M}$, denn $\mathbb{M}$ ist ein Körper, der $\mathbb{L}$ und S enthält. Außerdem ist $\mathbb{L}(S)$ ein Körper, der $\mathbb{K}$ und S enthält, also folgt $\mathbb{K}(S) \subseteq \mathbb{L}(S)$. Aus $\mathbb{K}(S) = \mathbb{M}$ folgt dann schon $\mathbb{K}(S) = \mathbb{L}(S) = \mathbb{M}$. □

2. **Behauptung** Ist $\mathbb{L}(S) = \mathbb{M}$, dann folgt im Allgemeinen nicht, dass $\mathbb{K}(S) = \mathbb{M}$ gilt.

   Beweis: Sei $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{R}$ und $\mathbb{M} = \mathbb{C}$. Sei außerdem $S = \{i\}$. Dann gilt $\mathbb{R}(i) = \mathbb{C}$, aber $\mathbb{Q}(i) \neq \mathbb{C}$, denn zum Beispiel gilt $\sqrt{2} \notin \mathbb{Q}(i)$. □

Aufgabe 8.2.31 Seien $\mathbb{K}$ und $\mathbb{K}'$ Körper, sei $\phi : \mathbb{K} \longrightarrow \mathbb{K}'$ ein Isomorphismus, und sei $\tilde{\phi} : \mathbb{K}[T] \longrightarrow \mathbb{K}'[T]$ der in Lemma 8.2.30 definierte Isomorphismus.

1. **Behauptung** Sei $f \in \mathbb{K}[T]$ irreduzibel. Dann ist auch $\tilde{\phi}(f)$ irreduzibel.

   Beweis: Angenommen, $\tilde{\phi}(f)$ ist reduzibel. Dann gibt es $\tilde{g}, \tilde{h} \in \mathbb{K}'[T]$ mit $\tilde{\phi}(f) = \tilde{g}\tilde{h}$ und der Grad von beiden Polynomen ist mindestens 1. Da $\tilde{\phi}$ ein Isomorphismus ist, gibt es $g, h \in \mathbb{K}[T]$ mit $\tilde{\phi}(g) = \tilde{g}$ und $\tilde{\phi}(h) = \tilde{h}$. Dann gilt

   $$\tilde{\phi}(gh) = \tilde{\phi}(g)\tilde{\phi}(h) = \tilde{g}\tilde{h} = \tilde{\phi}(f),$$

   und da $\tilde{\phi}$ ein Isomorphismus ist, folgt $f = gh$. Außerdem gilt $\mathrm{Grad}(g) = \mathrm{Grad}(\tilde{g}) \geq 1$ und $\mathrm{Grad}(h) = \mathrm{Grad}(\tilde{h}) \geq 1$. Also ist f auch reduzibel, ein Widerspruch. □

2. **Behauptung** Seien $f, g \in \mathbb{K}[T]$, und es gelte $\tilde{\phi}(g) \mid \tilde{\phi}(f)$. Dann folgt $g \mid f$.

   Beweis: Nach Voraussetzung gibt es ein $\tilde{h} \in \mathbb{K}'[T]$ mit $\tilde{\phi}(f) = \tilde{h}\tilde{\phi}(g)$. Da $\tilde{\phi}$ ein Isomorphismus ist, gibt es ein $h \in \mathbb{K}[T]$ mit $\tilde{\phi}(h) = \tilde{h}$. Es folgt

   $$\tilde{\phi}(hg) = \tilde{\phi}(h)\tilde{\phi}(g) = \tilde{h}\tilde{\phi}(g) = \tilde{\phi}(f),$$

   und da $\tilde{\phi}$ ein Isomorphismus ist, folgt $f = gh$. Also gilt $g \mid f$. □

Aufgabe 8.2.37 Bestimmen Sie den Grad des Zerfällungskörpers von $T^4 + 1$ über $\mathbb{Q}$.

Sei $a = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i \in \mathbb{C}$. Dann ist $a^2 = i$ und $a^4 = -1$. Also ist a eine Nullstelle von $T^4 + 1$. Weiter gilt $(a^3)^4 = (a^4)^3 = (-1)^3 = -1$, $(a^5)^4 = (a^4)^5 = (-1)^5 = -1$ und $(a^7)^4 = (a^4)^7 = (-1)^7 = (-1)$. Außerdem sind a, a^3, a^5, a^7 alle verschieden, das heißt, wir haben alle Nullstellen von $T^4 + 1$ gefunden, und der Zerfällungskörper von T^4+1 über $\mathbb{Q}$ ist $\mathbb{Q}(a, a^3, a^5, a^7) = \mathbb{Q}(a)$. Da T^4+1 irreduzibel über $\mathbb{Q}$ ist, denn $T^4 + 1 = (T^2 + \sqrt{2}T + 1)(T^2 - \sqrt{2}T + 1)$ in $\mathbb{R}[T]$, ist $T^4 + 1$ das Minimalpolynom von a, und es gilt $[\mathbb{Q}(a) : \mathbb{Q}] = 4$. □

Aufgabe 8.3.3 Sei $\mathbb{K}$ ein Körper.

Behauptung Eine nicht-leere Teilmenge $\{0\} \neq L \subseteq \mathbb{K}$ ist genau dann ein Körper, wenn für alle $a, b \in L$ mit $b \neq 0$ gilt: $a - b \in L$ und $ab^{-1} \in L$.

Beweis: Die eine Richtung der Behauptung ist klar: Wenn L ein Körper ist, dann gelten die beiden Bedingungen. Sei nun also L eine nicht-leere Teilmenge eines Körpers $\mathbb{K}$ mit $L \neq \{0\}$, und für alle $a, b \in L$ mit $b \neq 0$ gelte $a - b \in L$ und $ab^{-1} \in L$.

- Sei $0 \neq b \in L$. Mit $a = b$ folgt $a-b = b-b = 0 \in L$ und $ab^{-1} = bb^{-1} = 1 \in L$.
- Sei $0 \neq b \in L$. Mit $a = 0$ folgt $a - b = -b \in L$ und mit $a = 1$ folgt $ab^{-1} = 1 \cdot b^{-1} = b^{-1} \in L$.
- Seien nun $a, b \in L$ und sei $b \neq 0$. Dann gilt auch $-b \in L$ und $b^{-1} \in L$, also auch $a - (-b) = a + b \in L$ und $a(b^{-1})^{-1} = ab \in L$.
- Das Assoziativgesetz der Addition und der Multiplikation und die Distributivgesetze gelten in L, weil L eine Teilmenge von $\mathbb{K}$ ist. Außerdem sind die Addition und die Multiplikation aus diesem Grunde kommutativ.

Alles zusammen zeigt, dass L ein Körper ist. □

Aufgabe 8.3.8 Sei p eine Primzahl, und sei $f \in \mathbb{F}_p[T]$ irreduzibel.

Behauptung $f \mid T^{p^n} - T$ genau dann, wenn $\mathrm{Grad}(f) \mid n$ gilt.

Beweis: Es gelte $f \mid T^{p^n} - T$. Dann sind alle Nullstellen von f (im Zerfällungskörper von f über $\mathbb{F}_p$) auch Nullstellen von $T^{p^n} - T$. Insbesondere gilt $\mathbb{F}_p \subseteq \mathbb{F}_p[T]/(f) \subseteq \mathbb{F}_{p^n}$, denn der Zerfällungskörper von $T^{p^n} - T$ ist $\mathbb{F}_{p^n}$. Das heißt, $\mathbb{F}_p[T]/(f)$ ist ein Unterkörper von $\mathbb{F}_{p^n}$. Dies ist mit Proposition 8.3.6 nur möglich, wenn der Grad von f, welches gleichzeitig der Grad der Körpererweiterung $\mathbb{F}_p[T]/(f) : \mathbb{F}_p$ ist, ein Teiler von n ist.

Es gelte nun $\mathrm{Grad}(f) \mid n$. Sei $m = \mathrm{Grad}(f)$ und sei a eine Nullstelle von f im Zerfällungskörper von f über $\mathbb{F}_p$. Dann gilt $\mathbb{F}_p(a) \simeq \mathbb{F}_{p^m}$, das heißt, $a^{p^m} - a = 0$. Dann ist $a^{p^m-1} = 1$, und mit $m \mid n$ folgt auch $p^m - 1 \mid p^n - 1$, also $a^{p^n-1} = 1$ und $a^{p^n} = a$. Das heißt, a ist eine Nullstelle von $T^{p^n} - T$. Wenn aber alle Nullstellen von f Nullstellen von $T^{p^n} - T$ sind, dann folgt $f \mid T^{p^n} - T$. □

Aufgabe 8.4.3 Sei $\xi \neq 1$ ein n-te Einheitswurzel über einem Körper $\mathbb{K}$.

Behauptung $1 + \xi + \xi^2 + \ldots + \xi^{n-1} = 0$.

Beweis: Da ξ eine n-te Einheitswurzel ist, ist ξ eine Nullstelle von $T^n - 1$. Es gilt $T^n - 1 = (T-1)(T^{n-1} + \ldots + T + 1)$. Da $\xi \neq 1$ ist, ist ξ eine Nullstelle von $T^{n-1} + \ldots + T + 1$. Es folgt die Behauptung. □

Aufgabe 8.4.11 Berechnen Sie Q_{13}, Q_{14}, Q_{15} und Q_{16} für $\mathbb{K} = \mathbb{Q}$.

Es gilt

$$Q_{13} = \frac{T^{13} - 1}{T - 1} = T^{12}+T^{11}+T^{10}+T^9+T^8+T^7+T^6+T^5+T^4+T^4+T^3+T^2+T+1$$

mit Beispiel 8.4.10. Weiter ist

$$\begin{aligned} Q_{14} &= \frac{T^{14}-1}{(T-1)(T+1)(T^6+T^5+T^4+T^3+T^2+T+1)} = \frac{T^{14}-1}{T^8+T^7-T-1} \\ &= T^6-T^5+T^4-T^3+T^2-T+1 \end{aligned}$$

und

$$\begin{aligned} Q_{15} &= \frac{T^{15}-1}{(T-1)(T^2+T+1)(T^4+T^3+T^2+T+1)} = \frac{T^{15}-1}{T^7+T^6+T^5-T^2-T-1} \\ &= T^8-T^7+T^5-T^4+T^3-T+1. \end{aligned}$$

Außerdem gilt $Q_{16} = Q_{2^4} = T^8+1$ wieder mit Beispiel 8.4.10. □

Aufgabe 8.5.4 Seien $\mathbb{K} = \mathbb{F}_q$ und $\mathbb{L} = \mathbb{F}_{q^m}$ wie in Definition 8.5.1. Sei $a \in \mathbb{L}$, und das Minimalpolynom von a über $\mathbb{K}$ habe den Grad d.

Behauptung $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(a) = \frac{m}{d}\mathrm{Tr}_{\mathbb{K}(a)/\mathbb{K}}(a)$.

Beweis: Es gilt $[\mathbb{K}(a):\mathbb{K}] = d$, also

$$m = [\mathbb{L}:\mathbb{K}] = [\mathbb{L}:\mathbb{K}(a)][\mathbb{K}(a):\mathbb{K}] = d[\mathbb{L}:\mathbb{K}(a)].$$

Es folgt $[\mathbb{L}:\mathbb{K}(a)] = \frac{m}{d}$. Nun gilt

$$\begin{aligned} \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(a) &= \mathrm{Tr}_{\mathbb{K}(a)/\mathbb{K}}(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}(a)}(a)) \qquad \text{mit Proposition 8.5.3} \\ &= \mathrm{Tr}_{\mathbb{K}(a)/\mathbb{K}}(\frac{m}{d}a) \qquad \text{mit Proposition 8.5.2} \\ &= \frac{m}{d}\mathrm{Tr}_{\mathbb{K}(a)/\mathbb{K}}(a). \end{aligned}$$

□

Kapitel 9

Kryptoverfahren über endlichen Körpern

9.1 Der diskrete Logarithmus

Wir werden in diesem Teil Public-Key-Kryptosysteme vorstellen, die darauf beruhen, dass der diskrete Logarithmus über endlichen Körper schwer zu berechnen ist. Die Aufgabe ist - wie beim Faktorisieren von ganzen Zahlen - leicht zu formulieren:

9.1.1 Problem (Diskreter-Logarithmus-Problem) Sei $\mathbb{K}$ ein endlicher Körper, und sei $g \in \mathbb{K}^\times$ ein primitives Element von $\mathbb{K}^\times$. Gegeben sei $a \in \mathbb{K}^\times$. Bestimme $x \in \mathbb{Z}$ mit $a = g^x$.

Das gesuchte Element $x \in \mathbb{Z}$ wird der **diskrete Logarithmus** von a zur Basis g genannt - in Analogie zum Logarithmus über den reellen oder komplexen Zahlen.

Über den diskreten Logarithmus über endlichen Körpern gilt folgende Vermutung, auf der die Sicherheit der in diesem Kapitel vorgestellten Kryptosysteme beruht:

9.1.2 Vermutung Es gibt keinen effizienten Algorithmus, um das diskreter-Logarithmus-Problem über endlichen Körpern zu lösen.

Diese Vermutung wird dadurch bestätigt, dass der diskrete Logarithmus im Mittelpunkt intensiver Forschungen steht, ohne dass auch nur ein Anzeichen für einen effizienten Algorithmus gefunden werden konnte. In dieser Hinsicht gleicht also das diskrete-Logarithmus-Problem dem Problem des Faktorisierens großer Zahlen, auf dem RSA beruht.

Es gibt jedoch natürlich Algorithmen, um das diskrete-Logarithmus-Problem für endliche Körper zu lösen. Diese sind zwar nicht effizient, aber doch immerhin so gut, dass man die endlichen Körper schon recht groß wählen muss, um sicher zu sein. Nach dem heutigen Stand der Technik (2003) sollte der endliche Körper zwischen 2^{1024} und 2^{4096} Elementen haben. Außerdem gibt es noch weitere Anforderungen an den endlichen Körper, die sicherstellen, dass das diskrete-Logarithmus-Problem wirklich schwer zu lösen ist. Es ist effizient möglich zu überprüfen, ob der Körper diese Anforderungen erfüllt. Algorithmen, um das diskrete-Logarithmus-Problem zu lösen, und auch Anforderungen an die endlichen Körper, damit das diskrete-Logarithmus-Problem nicht zu leicht zu lösen ist, finden Sie beispielsweise in [St].

9.1.3 Aufgabe Im Körper $\mathbb{F}_{37}$ ist 2 ein primitives Element. Bestimmen Sie den diskreten Logarithmus von 15 zur Basis 2.

9.2 Das Diffie-Hellman-Verfahren

Wir werden nun einige Public-Key-Kryptosysteme vorstellen, die auf dem diskreter-Logarithmus-Problem beruhen. Historisch gesehen waren dies die ersten Public-Key-Kryptosysteme, jedenfalls das von Whitfield Diffie und M. Hellman, die als die Erfinder der Public-Key-Kryptografie gelten. Deshalb wird auch das erste Kryptosystem, das wir vorstellen, von Diffie und Hellman sein (siehe [DH]). Es dient nicht dazu, eine bestimmte Nachricht von Alice zu Bob zu schicken, sondern dazu, einen Schlüssel zwischen beiden festzulegen. Das ist auch genau der Zweck, zu dem Public-Key-Kryptosysteme oft benutzt werden. Da für solche Systeme oft viel komplizierte Mathematik benötigt wird, sind sie in der Regel langsamer als symmetrische Kryptosysteme. Jedoch gibt es bei den symmetrischen Kryptosystemen das Problem mit den Schlüsseln. Irgendwie muss sichergestellt werden, dass regelmäßig die benötigten Schlüssel auf sicherem Wege von Alice zu Bob oder umgekehrt gelangen. Und für die relativ kurzen Schlüssel eignen sich die Public-Key-Kryptosysteme hervorragend.

Beim Diffie-Hellman-Schlüsselaustauschverfahren (1976) geht man nun folgendermaßen vor: Öffentlich bekannt gegeben werden ein (großer) endlicher Körper $\mathbb{K}$ und ein primitives Element $g \in \mathbb{K}^\times$.

Alice und Bob möchten ein zufällig gewähltes Element aus $\mathbb{K}^\times$ als Schlüssel für ihr symmetrisches Kryptosystem vereinbaren. Dabei müssen sie sich natürlich vorher geeinigt haben, wie aus einem Element eines endlichen Körpers ein Schlüssel, also zum Beispiel eine natürliche Zahl oder eine Matrix, wird. Alice wählt zufällig ein

$a \in \mathbb{Z}$ (wobei sinnvollerweise $1 \leq a \leq |\mathbb{K}^\times|$ gilt) und bildet g^a. Dieses Element gibt sie bekannt. Bob wählt analog $b \in \mathbb{Z}$ mit $1 \leq b \leq |\mathbb{K}^\times|$, berechnet g^b und gibt dieses Element aus $\mathbb{K}^\times$ bekannt. Der Schlüssel ist dann das Element g^{ab}. Alice und Bob können ihn beide berechnen, denn Alice kennt g^b und a und berechnet $(g^b)^a$, und Bob berechnet g^{ab} als $(g^a)^b$.

Wenn nun Oscar das diskreter-Logarithmus-Problem in $\mathbb{K}$ lösen kann, dann kann er aus den Elementen g^a und g^b die Zahlen a und b und damit auch den Schlüssel g^{ab} berechnen. Es gilt jedoch folgende Vermutung:

9.2.1 Vermutung Wenn Oscar das Diffie-Hellman-Schlüsselaustauschsystem brechen kann, dann kann er auch das diskreter-Logarithmus-Problem über endlichen Körpern lösen.

Auch hier ist es wieder noch niemandem gelungen, diese Vermutung zu beweisen. Pessimisten werden nun behaupten, dass die Sicherheit des Diffie-Hellman-Schlüsselaustauschsystems auf bloßen Vermutungen beruht, und damit haben sie natürlich Recht. Der Grund dafür, dass es trotzdem benutzt wird, ist die (realistische) Annahme, dass es wohl sehr schnell bekannt würde, wenn sich eine der Vermutungen als falsch herausstellen sollte, da sich viele Wissenschaftler - und nicht nur Geheimdienstler - mit diesen Vermutungen beschäftigen.

9.2.2 Aufgaben

1. Zeigen Sie, dass mit dem Verfahren von Diffie und Hellman ein Schlüssel effizient berechnet werden kann.
2. Alice und Bob möchten mit dem Diffie-Hellman-Verfahren einen Schlüssel austauschen. Sie wählen $\mathbb{K} = \mathbb{F}_{19}$ und $g = 2$. Alice schickt 11 an Bob, und Bob schickt 3 an Alice. Was ist der Schlüssel?

9.3 Das Massey-Omura-Kryptosystem

Bei diesem Kryptosystem von 1983, benannt nach James L. Massey und Jim K. Omura, soll eine geheime Nachricht von Alice an Bob gehen. Wir nehmen an, dass die Nachricht aus einem Element oder einer Folge von Elementen aus $\mathbb{K}^\times$ besteht, wobei $\mathbb{K}$ ein großer Körper mit q Elementen ist. Alice und Bob müssen sich also vorher einigen, wie sie aus einer Nachricht ein oder mehrere Elemente aus $\mathbb{K}$ machen und umgekehrt. Wir nehmen nun an, dass das Element $N \in \mathbb{K}^\times$ übermittelt werden soll.

Der Körper $\mathbb{K}$ wird öffentlich bekannt gegeben. Alice wählt zufällig eine Zahl $e_A \in \mathbb{N}$ mit $1 \leq e_A \leq q-1$ und $\mathrm{ggT}(e_A, q-1) = 1$. Mit dem erweiterten Euklidischen

Algorithmus berechnet sie $d_A \in \mathbb{Z}$ mit $d_A e_A \equiv 1 \bmod q-1$. Nun schickt sie N^{e_A} an Bob. Bob kann N aus N^{e_A} ohne einen weiteren Hinweis nicht berechnen. Um diesen Hinweis zu bekommen, wählt er zufällig $e_B \in \mathbb{N}$ mit $1 \leq e_B \leq q-1$ und $\mathrm{ggT}(e_B, q-1) = 1$, berechnet d_B mit $e_B d_B \equiv 1 \bmod q-1$ und schickt $(N^{e_A})^{e_B} = N^{e_A e_B}$ zurück an Alice. Diese bildet

$$(N^{e_A e_B})^{d_A} = (N^{e_A d_A})^{e_B} = N^{e_B},$$

denn $e_A d_A \equiv 1 \bmod q-1$, also $e_A d_A = 1 + a(q-1)$ für ein $a \in \mathbb{Z}$, also

$$N^{e_A d_A} = N^{1+a(q-1)} = N(N^{q-1})^a = N \cdot 1^a = N.$$

Alice schickt nun also N^{e_B} zurück an Bob, und Bob berechnet $(N^{e_B})^{d_B} = N^{e_B d_B} = N$ mit der gleichen Argumentation wie eben.

Wieder ist klar, dass Oscar das Kryptosystem brechen kann, wenn er diskrete Logarithmen berechnen kann. Und wieder gilt:

9.3.1 Vermutung Oscar kann das Massey-Omura-Kryptosystem nicht brechen, ohne das diskreter-Logarithmus-Problem zu lösen.

9.3.2 Aufgaben

1. Zeigen Sie, dass alle Daten, die beim Massey-Omura-System benötigt werden, effizient berechnet werden können.
2. Stellen Sie sich vor, Sie sind Oscar und können diskrete Logarithmen in $\mathbb{K}$ berechnen. Wie können Sie aus den versendeten Informationen N^{e_A}, N^{e_B} und $N^{e_A e_B}$ die Nachricht N berechnen?

Zum Abschluss noch eine Warnung. Wenn Oscar die Nachricht N^{e_A} von Alice abfängt, sein eigenes e_O wählt und $N^{e_A e_O}$ als Bob an Alice schickt, dann schickt Alice N^{e_O} zurück, und Oscar kann N berechnen. Alice muss sich also sicher sein, dass die Nachrichten auch wirklich von Bob kommen, was zum Problem der Authentifikation (stelle sicher, dass eine Nachricht von X wirklich von X ist) beziehungsweise der Integrität (stelle sicher, dass die Nachricht im Zuge der Übermittlung nicht verändert wurde) führt. Leider können wir diese Themen hier nicht behandeln.

9.4 Das ElGamal-Kryptosystem

Auch bei diesem nach Taher ElGamal benannten Kryptosystem von 1985 ist das Szenario so, dass Alice eine Nachricht an Bob schicken möchte. Öffentlich bekannt gegeben werden ein großer endlicher Körper $\mathbb{K}$ mit q Elementen und ein primitives

Element $g \in \mathbb{K}^\times$. Außerdem gibt Bob noch g^a für ein zufällig gewähltes $a \in \mathbb{N}$ mit $1 \leq a \leq q-1$ bekannt. Alice möchte die Nachricht $N \in \mathbb{K}^\times$ verschicken. Dazu schickt sie Bob das Paar (g^k, Ng^{ak}) von Elementen aus $\mathbb{K}^\times$, wobei $k \in \mathbb{N}$ mit $1 \leq k \leq q-1$ zufällig gewählt ist. Bob, der ja a kennt, bildet

$$(g^k)^{q-1-a} = g^{k(q-1)-ka} = (g^{q-1})^k \cdot g^{-ka} = g^{-ka}$$

und anschließend $g^{-ka}Ng^{ak} = N$.

Oscar kann nur die Körperelemente g^a, g^k und Ng^{ak} sehen. Daraus a und k und damit N zu berechnen, würde bedeuten, dass Oscar diskrete Logarithmen berechnen kann.

9.4.1 Vermutung Es ist zwingend notwendig, diskrete Logarithmen zu berechnen, um das ElGamal-Kryptosystem zu brechen.

Theoretisch kann es wieder sein, dass sich das Kryptosystem auf einem völlig anderen Wege brechen lässt, der mit diskreten Logarithmen nichts zu tun hat. Von den Spezialisten in der Kryptologie würde aber sicher niemand darauf wetten.

9.4.2 Aufgabe Zeigen Sie, dass alle Elemente, die beim ElGamal-System benötigt werden, effizient berechnet werden können.

Lösungen der Aufgaben

Lösungen der Aufgaben in Kapitel 9

Aufgabe 9.1.3 Im Körper $\mathbb{F}_{37}$ ist 2 ein primitives Element. Bestimmen Sie den diskreten Logarithmus von 15 zur Basis 2.

Hier bleibt uns nichts Anderes übrig als in $\mathbb{F}_{37}$ zu rechnen: $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 27$, $2^7 = 17$, $2^8 = 34$, $2^9 = 31$, $2^{10} = 25$, $2^{11} = 13$, $2^{12} = 26$, $2^{13} = 15$. Also ist der diskrete Logarithmus von 15 zur Basis 2 gleich 13. □

Aufgabe 9.2.2

1. **Behauptung** Mit dem Verfahren von Diffie und Hellman kann ein Schlüssel effizient berechnet werden.

   Beweis: Alice und Bob berechnen g^a beziehungsweise g^b mit Wiederholtem Quadrieren und g^{ab} wieder mit Wiederholtem Quadrieren. Der Schlüssel lässt sich also effizient berechnen. □

2. Alice und Bob möchten mit dem Diffie-Hellman-Verfahren einen Schlüssel austauschen. Sie wählen $\mathbb{K} = \mathbb{F}_{19}$ und $g = 2$. Alice schickt 11 an Bob, und Bob schickt 3 an Alice. Was ist der Schlüssel?

   In $\mathbb{F}_{19}$ gilt $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 13$, $2^6 = 7$, $2^7 = 14$, $2^8 = 9$, $2^9 = 18$, $2^{10} = 17$, $2^{11} = 15$, $2^{12} = 11$ und $2^{13} = 3$. Also gilt $a = 12$ und $b = 13$. Damit ist der Schlüssel $2^{12 \cdot 13} \equiv 2^{156} \equiv 2^{8 \cdot 18 + 12} \equiv 2^{12} \equiv 11 (\mathrm{mod} 19)$. □

Aufgabe 9.3.2

1. **Behauptung** Alle Daten, die beim Massey-Omura-System benötigt werden, können effizient berechnet werden.

Beweis: Alice muss einmal den erweiterten Euklidischen Algorithmus anwenden und N^{e_A} und $(N^{e_A \cdot e_B})^{d_A}$ mit Wiederholtem Quadrieren berechnen. Bob muss ebenfalls einmal den erweiterten Euklidischen Algorithmus anwenden und $(N^{e_A})^{e_B}$ und $(N^{e_B})^{d_B}$ mit Wiederholtem Quadrieren berechnen. Es lassen sich also alle Daten effizient berechnen. □

2. Stellen Sie sich vor, Sie sind Oscar und können diskrete Logarithmen in $\mathbb{K}$ berechnen. Wie können Sie aus den versendeten Informationen N^{e_A}, N^{e_B} und $N^{e_A e_B}$ die Nachricht N berechnen?

   Oscar weiß, dass die zweite Information $N^{e_A e_B}$ eine Potenz von N^{e_A} ist. Da er diskrete Logarithmen berechnen kann, kann er e_B berechnen. Mit dem erweiterten Euklidischen Algorithmus berechnet er nun d_B mit $e_B d_B \equiv 1 (\mathrm{mod} q-1)$, und dann ist $(N^{e_B})^{d_B} \equiv N (\mathrm{mod} q-1)$. □

Aufgabe 9.4.2

Behauptung Alle Elemente, die beim ElGamal-System benötigt werden, können effizient berechnet werden.

Beweis: Bob berechnet g^a effizient mit Wiederholtem Quadrieren. Anschließend berechnet Alice g^k und g^{ak} mit Wiederholtem Quadrieren und Ng^{ak} durch eine Multiplikation in $\mathbb{K}$. Nun bildet Bob $(g^k)^{q-1-a}$ durch Wiederholtes Quadrieren und anschließend noch $g^{-ak}N$ und $g^{-ak}Ng^{ak}$ durch eine Multiplikation in $\mathbb{K}$. Also lassen sich alle Elemente effizient berechnen. □

Kurseinheit 6

Kryptosysteme über elliptischen Kurven

Studierhinweise

Ziel dieser Kurseinheit ist es, Kryptosysteme zu beschreiben, die auf elliptischen Kurven basieren. Diese Kryptosysteme sind relativ neu (seit etwa 1985 werden Kryptosysteme über elliptischen Kurven betrachtet) und ein gutes Beispiel dafür, wie ein Gebiet der Mathematik, das zuvor für ein Gebiet ohne Anwendungen gehalten wurde, plötzlich den Hintergrund für neue, bessere Verfahren in der Kryptologie liefern konnte.

Elliptische Kurven sind schon sehr lange Gegenstand mathematischer Forschung. Meistens wurden jedoch elliptische Kurven über den reellen oder den komplexen Zahlen betrachtet. Wie der Name schon sagt, sind elliptische Kurven Kurven, das heißt, eine Menge von Punkten im zweidimensionalen Raum (über dem betrachteten Körper $\mathbb{K}$). Das Interessante an den elliptischen Kurven ist aber, dass man diese Punkte nach bestimmten Vorschriften addieren kann und auf diese Art und Weise eine abelsche Gruppe erhält. Ist der zugrunde liegende Körper ein endlicher Körper, dann erhält man so eine endliche abelsche Gruppe, in der man effizient rechnen kann. Wir stellen uns wieder vor, dass die endlichen Körper, über denen gerechnet wird, entweder von der Form $\mathbb{F}_p$ für eine Primzahl p oder von der Form $\mathbb{F}_{2^n}$ für ein $n \in \mathbb{N}$ sind. Um die Formeln für die Addition von Punkten herzuleiten, müssen diese beiden Fälle unterschieden werden. Die Formeln für die Addition von Punkten unterscheiden sich dann auch, je nachdem, in welchem der beiden Fälle wir uns befinden. Den vollständigen Beweis, dass die elliptische Kurve zusammen mit der von uns definierten Addition eine Gruppe bildet, müssen wir leider schuldig bleiben. Nachzulesen ist er entweder in [Sil] - dies ist ein Buch, in dem alle Ergebnisse, die hier vorgestellt werden, auch bewiesen werden - oder in [Kn], wo das Assoziativgesetz geometrisch bewiesen wird.

Untersucht man nun die Struktur der definierten abelschen Gruppe, sieht man, dass diese Gruppe nicht immer zyklisch ist, aber das ist bei den Kryptosystemen auch nicht unbedingt notwendig. Jedenfalls erhält man eine endliche abelsche Gruppe, in der diskrete Logarithmen schwer zu berechnen sind. In diesem Fall sieht das diskreter-Logarithmus-Problem folgendermaßen aus: Gegeben sind ein Punkt P

auf der elliptischen Kurve und ein Vielfaches aP von P mit $a \in \mathbb{Z}$. Das Problem ist, a zu berechnen.

Es stellt sich heraus, dass das diskreter-Logarithmus-Problem für die elliptischen Kurven scheinbar schwerer zu lösen ist als das über den endlichen Körpern. Das soll heißen, dass man die Größe des endlichen Körpers für Kryptoverfahren über endlichen Körpern sehr viel größer wählen muss als bei den elliptischen Kurven, um die gleiche Sicherheitsstufe zu erreichen. Das ist der große Vorteil der Kryptoverfahren über elliptischen Kurven, dass die Körpergröße relativ klein gewählt werden kann und damit wenig Speicherplatz verbraucht wird und auch schneller gerechnet werden kann. Dies führt dazu, dass die elliptischen Kurven immer öfter verwendet werden.

Die Kryptoverfahren aus Kapitel 9 können nun also auch über elliptischen Kurven durchgeführt werden. Das war auf den ersten Blick überraschend, denn die Theorie der elliptischen Kurven ist sehr tiefliegend und abstrakt, und Anwendungen außerhalb der reinen Mathematik waren bis dahin nicht bekannt. Wir werden die Kryptoverfahren aus Kapitel 9 nochmals für die elliptischen Kurven formulieren. Anschließend geht es noch um einige technische Details bei den Kryptosystemen über elliptischen Kurven. So muss man sich zum Beispiel überlegen, wie man aus einer Nachricht, die geschickt werden soll, einen Punkt auf einer elliptischen Kurve findet, und zwar so, dass man aus dem Punkt die Nachricht wieder rekonstruieren kann. Relativ ausführlich beschäftigen wir uns damit, wie überhaupt ein Punkt auf einer vorgegebenen elliptischen Kurve gefunden werden kann. Das einfachste und schnellste Verfahren ist, einen x-Wert zufällig zu raten und dann zu versuchen, einen zugehörigen y-Wert zu finden. Bei diesem Verfahren müssen quadratische Gleichungen über endlichen Körpern gelöst werden, und wir stellen Algorithmen dazu vor.

Kapitel 10

Kryptosysteme über elliptischen Kurven

10.1 Elliptische Kurven als abelsche Gruppe

Da elliptische Kurven hier nur im Zusammenhang mit Kryptologie benötigt werden, werden wir nur elliptische Kurven über endlichen Körpern betrachten. Klassischerweise werden eher elliptische Kurven über den rellen und komplexen Zahlen studiert. Bei den elliptischen Kurven über den endlichen Körpern werden in der Regel die Fälle, dass die Charakteristik des betrachteten Körpers $\mathbb{K}$ größer als 3 ist und die Fälle $\text{char}(\mathbb{K}) = 2$ und $\text{char}(\mathbb{K}) = 3$ getrennt betrachtet. Anwendung in der Kryptografie finden entweder elliptische Kurven über $\mathbb{F}_p$, wobei p eine große Primzahl ist, oder elliptische Kurven über $\mathbb{F}_{2^n}$ für großes $n \in \mathbb{N}$. Deshalb werden hier nur die Fälle $\text{char}(\mathbb{K}) > 3$ und $\text{char}(\mathbb{K}) = 2$ behandelt.

10.1.1 Der Fall $\text{char}(\mathbb{K}) > 3$

In diesem Abschnitt sei $\mathbb{K}$ ein endlicher Körper mit $\text{char}(\mathbb{K}) > 3$. Für die Kryptografie wird dies meistens ein Körper der Form $\mathbb{F}_p$ mit einer sehr großen Primzahl p sein.

10.1.1 Definition Seien $a, b \in \mathbb{K}$ mit $4a^3 + 27b^2 \neq 0$. Die Menge $E(a, b, \mathbb{K})$ aller Punkte (x, y) mit $x, y \in \mathbb{K}$, die die Gleichung

$$y^2 = x^3 + ax + b$$

erfüllen, zusammen mit einem weiteren Punkt, der $\mathcal{O}$ genannt wird (und „O“ ausgesprochen wird), heißt eine **elliptische Kurve** über $\mathbb{K}$. Mit anderen Worten

$$E(a,b,\mathbb{K}) = \{(x,y) \mid x,y \in \mathbb{K} \text{ und } y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

10.1.2 Beispiel Sei $\mathbb{K} = \mathbb{F}_5$, und seien $a = 0$ und $b = 1$. Es gilt $4a^3 + 27b^2 \equiv 2(\mathrm{mod}5)$. Also ist die Menge aller (x,y) mit $x,y \in \mathbb{F}_5$ und $y^2 = x^3 + 1$ zusammen mit $\mathcal{O}$ eine elliptische Kurve über $\mathbb{F}_5$. Es gilt

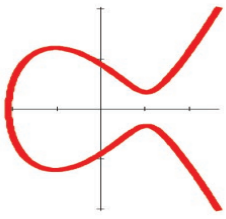
$$E(0,1,\mathbb{F}_5) = \{(0,1),(0,4),(2,2),(2,3),(4,0),\mathcal{O}\}.$$

10.1.3 Bemerkung Der Punkt $\mathcal{O}$, der zu jeder elliptischen Kurve gehört, wird der „Punkt bei Unendlich“ genannt. Um seine Bedeutung genau zu verstehen, müsste man die Grundlagen der projektiven Geometrie beherrschen. Das würde in diesem Kurs aber zu weit führen, deshalb begnügen wir uns mit der Tatsache, dass der Punkt immer dazugehört.

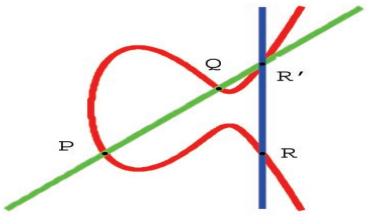
Bis jetzt ist eine elliptische Kurve für uns nur eine Menge von Punkten (x,y) mit $x,y \in \mathbb{K}$. Nun soll auf dieser Menge eine Addition definiert werden. Dazu schauen wir uns zunächst die elliptischen Kurven über den reellen Zahlen an. Diese sind genauso definiert wie die elliptischen Kurven über den endlichen Körpern. Man nimmt also $a,b \in \mathbb{R}$, so dass $4a^3 + 27b^2 \neq 0$ ist. Dann ist

$$E(a,b,\mathbb{R}) = \{(x,y) \mid x,y \in \mathbb{R} \text{ und } y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

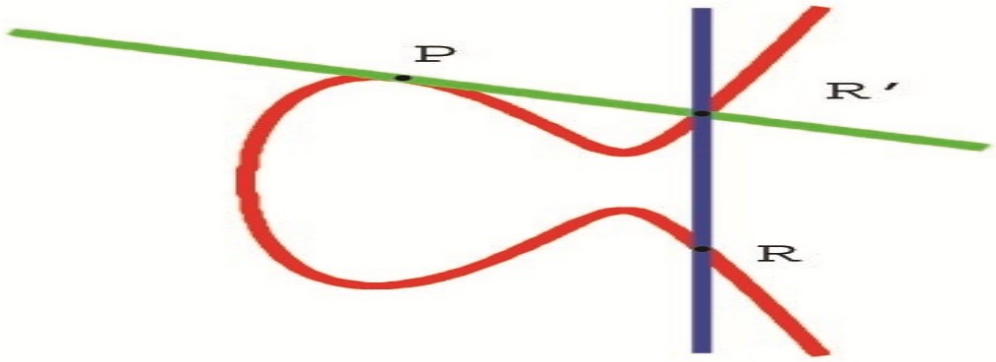
eine elliptische Kurve über $\mathbb{R}$. Für $a = -5$ und $b = 5$ ist das hier zu sehen (alle Beispiele wurden übrigens mit dem Computeralgebrasystem MuPAD erzeugt):



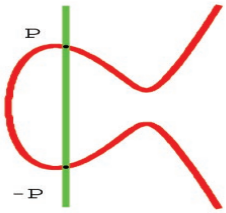
Über den reellen Zahlen wird es etwas klarer, warum wir die Bedingung $4a^3+27b^2 \neq 0$ benötigen. Diese Bedingung stellt nämlich sicher, dass es keine sogenannten Singularitäten auf der Kurve gibt. Das sind zum Beispiel Spitzen oder Punkte, an denen sich die Kurve selbst schneidet. Man definiert nun folgendermaßen eine Gruppenstruktur auf $E(a, b, \mathbb{R})$: Das neutrale Element bezüglich der Addition ist der Punkt $\mathcal{O}$, das heißt, es gilt $P + \mathcal{O} = \mathcal{O} + P = P$ für alle $P \in E(a, b, \mathbb{R})$. Sind zwei Punkte $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ in $E(a, b, \mathbb{R})$ gegeben, dann verbindet man diese beiden Punkte durch eine Gerade. Diese Gerade schneidet die elliptische Kurve in einem weiteren Punkt $R' = (x'_3, y'_3)$. Die Summe $P+Q$ ist dann der an der x-Achse gespiegelte Punkt $R = (x_3, y_3)$, also $x_3 = x'_3$ und $y_3 = -y'_3$. Anschaulich ist das hier zu sehen:



Gilt $P = Q$, so geht man vor wie oben, nimmt aber die Tangente in P an der Kurve (anschaulich ist das die Gerade, die die Kurve in P „berührt“). Diese schneidet dann wieder in einem weiteren Punkt R' die Kurve, und $P + P = 2P = R$, wobei R der an der x-Achse gespiegelte Punkt R' ist:



Um zu einem Punkt P das Inverse, also $-P$, zu bekommen, spiegelt man den Punkt an der x-Achse:



10.1.4 Aufgabe Zeigen Sie, dass für $(x, y) \in E(a, b, \mathbb{K})$ mit $\mathbb{K} = \mathbb{R}$ oder $\text{char}(\mathbb{K}) > 3$ immer $(x, -y) \in E(a, b, \mathbb{K})$ gilt.

Mit diesen Vorschriften wird eine Addition auf $E(a, b, \mathbb{R})$ definiert, die sich am besten durch folgende Merkregel beschreiben lässt (die dann auch über den endlichen Körpern gelten wird):

10.1.5 Satz (Merkregel) Liegen drei Punkte $P, Q, R \in E(a, b, \mathbb{R})$ auf einer Geraden, dann gilt $P + Q + R = \mathcal{O}$. □

Betrachten wir die Addition aus einem anderen Blickwinkel: Wir fangen mit der Merkregel an: $P + Q + R = \mathcal{O}$ für je drei Punkte, die auf einer Geraden liegen. Sei also $P \in E(a, b, \mathbb{R})$. Auf der Geraden durch P parallel zur y-Achse liegen drei Punkte aus $E(a, b, \mathbb{R})$: Wenn $P = (x, y)$ ist, dann liegt auch $P' = (x, -y)$ auf der Geraden und in $E(a, b, \mathbb{R})$, denn $E(a, b, \mathbb{R})$ ist symmetrisch zur x-Achse. Außerdem liegt auch der Punkt $\mathcal{O}$ auf dieser Geraden. Man kann sich diesen Punkt nämlich so vorstellen, dass er auf jeder Geraden liegt, die parallel zur y-Achse verläuft, und zwar im „Unendlichen“. Wenn wir das einmal so glauben, gilt also $P + P' + \mathcal{O} = \mathcal{O}$, oder $P' = -P$, denn $\mathcal{O}$ ist ja das neutrale Element. Um zwei Punkte P und Q zu addieren, nehmen wir den dritten Punkt auf der Gerade durch P und Q. Dieser Punkt sei R'. Dann gilt $P + Q + R' = \mathcal{O}$, also $P + Q = -R'$.

Nun müssen die Regeln für die Addition über $\mathbb{R}$ auf die endlichen Körper übertragen werden. Dabei werden wir gleichzeitig Formeln für die Addition von zwei Punkten herleiten, die aus algebraischen Ausdrücken in den Koordinaten der Punkte bestehen. Diese Formeln können dann mit einem Computer leicht berechnet werden.

Sei also nun wieder $\mathbb{K}$ ein endlicher Körper mit $\text{char}(\mathbb{K}) > 3$. Seien $a, b \in \mathbb{K}$, so dass $4a^3 + 27b^2 \neq 0$ in $\mathbb{K}$ gilt. Die ersten beiden Regeln sind folgende:

(R1) Das neutrale Element der Addition ist $\mathcal{O}$. Es gilt also $P + \mathcal{O} = \mathcal{O} + P = P$ für alle $P \in E(a, b, \mathbb{K})$.

(R2) Ist $P = (x, y) \in E(a, b, \mathbb{K})$ (also $P \neq \mathcal{O}$), dann ist $-P = (x, -y) \in E(a, b, \mathbb{K})$.

Wie bei abelschen Gruppen üblich, schreibt man $P - Q$ statt $P + (-Q)$ für alle $P, Q \in E(a, b, \mathbb{K})$. Seien nun $P = (x_1, y_1), Q = (x_2, y_2) \in E(a, b, \mathbb{K})$, wobei $x_1 \neq x_2$ gelte. Ist nämlich $x_1 = x_2$, dann ist $y_1^2 = y_2^2$, also besagt diese Bedingung gerade, dass $P \neq Q$ und $P \neq -Q$ gelten soll. Die Gleichung der Gerade G durch P und Q ist dann

$$y = (\frac{y_2 - y_1}{x_2 - x_1})x + \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1},$$

das heißt, G ist die Menge aller Punkte (x, y) mit $x, y \in \mathbb{K}$, die die obige Gleichung erfüllen.

10.1.6 Aufgabe Prüfen Sie nach, ob P und Q wirklich in G liegen.

Wir setzen

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ und } \mu = \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1},$$

das heißt, G ist dann die Menge aller Punkte (x, y) mit $x, y \in \mathbb{K}$ und $y = \lambda x + \mu$. Um den dritten Schnittpunkt von G mit $E(a, b, \mathbb{K})$ zu berechnen, setzen wir $y = \lambda x + \mu$ in die Gleichung $y^2 = x^3 + ax + b$ ein. Also

$$\begin{aligned} (\lambda x + \mu)^2 &= x^3 + ax + b \\ \Leftrightarrow \lambda^2 x^2 + 2\lambda\mu x + \mu^2 &= x^3 + ax + b \\ \Leftrightarrow x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + (b - \mu^2) &= 0. \end{aligned}$$

Die linke Seite der letzten Gleichung ist ein Polynom dritten Grades in x, von dem wir schon zwei Nullstellen kennen, nämlich x_1 und x_2. Das folgende Lemma hilft jetzt weiter:

10.1.7 Lemma Sei $\mathbb{K}$ ein Körper, und sei $T^3 + \alpha T^2 + \beta T + \gamma \in \mathbb{K}[T]$ ein normiertes Polynom dritten Grades. Seien $x_1, x_2, x_3 \in \mathbb{K}$ Nullstellen des Polynoms. Dann gilt $\alpha = -(x_1 + x_2 + x_3)$.

Beweis: Sind $x_1, x_2, x_3 \in \mathbb{K}$ Nullstellen des Polynoms, dann gilt

$$\begin{aligned} T^3 + \alpha T^2 + \beta T + \gamma &= (T - x_1)(T - x_2)(T - x_3) \\ &= T^3 - (x_1 + x_2 + x_3)T^2 + (x_1 x_2 + x_1 x_3 + x_2 x_3)T - x_1 x_2 x_3. \end{aligned}$$

Koeffizientenvergleich ergibt die Behauptung. □

Sei nun $R' = (x'_3, y'_3)$ der dritte Schnittpunkt von G mit $E(a, b, \mathbb{K})$. Dann ist x'_3 die dritte Nullstelle des Polynoms

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + (b - \mu^2),$$

also gilt mit Lemma 10.1.7, dass $-\lambda^2 = -(x_1 + x_2 + x'_3)$ gilt, oder

$$x'_3 = \lambda^2 - x_1 - x_2 = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2.$$

Außerdem gilt natürlich

$$\begin{aligned} y'_3 &= \lambda x'_3 + \mu = \frac{y_2 - y_1}{x_2 - x_1} x'_3 + \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1} \\ &= (\frac{y_2 - y_1}{x_2 - x_1}) x'_3 + \frac{y_1 x_2 - y_1 x_1 + x_1 y_1 - x_1 y_2}{x_2 - x_1} \\ &= (\frac{y_2 - y_1}{x_2 - x_1}) x'_3 + y_1 (\frac{x_2 - x_1}{x_2 - x_1}) - x_1 (\frac{y_2 - y_1}{x_2 - x_1}) \\ &= (\frac{y_2 - y_1}{x_2 - x_1})(x'_3 - x_1) + y_1. \end{aligned}$$

Um das Ergebnis der Addition $P + Q$ zu erhalten, muss nun noch $R' = (x'_3, y'_3)$ an der x-Achse gespiegelt werden, und dies liefert den Punkt $R = (x_3, y_3)$ mit $x_3 = x'_3$ und $y_3 = -y'_3$. Also folgt

(R3) Sind $P = (x_1, y_1), Q = (x_2, y_2) \in E(a, b, \mathbb{K})$ mit $x_1 \neq x_2$ (also $Q \neq P$ und $Q \neq -P$), dann ist $P + Q = R = (x_3, y_3)$ mit

$$\begin{aligned} x_3 &= (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2 \text{ und} \\ y_3 &= (\frac{y_2 - y_1}{x_2 - x_1})(x_1 - x_3) - y_1. \end{aligned}$$

10.1.8 Beispiel Wir betrachten die Kurve aus Beispiel 10.1.2. Dann ist $(0, 1) + (4, 0) = (x_3, y_3)$ mit

$$\begin{aligned} x_3 &\equiv (\frac{0 - 1}{4 - 0})^2 - 0 - 4 \equiv 1^2 - 4 \equiv 2 (\mathrm{mod} 5), \\ y_3 &\equiv (\frac{0 - 1}{4 - 0}) \cdot (0 - 2) - 1 \equiv 1 \cdot (-2) - 1 \equiv 2 (\mathrm{mod} 5). \end{aligned}$$

Also $(0, 1) + (4, 0) = (2, 2)$.

Nun fehlt noch eine Regel, wie $2P$ für $P = (x_1, y_1) \in E(a, b, \mathbb{K})$ gebildet werden kann. Hier nehmen wir an, dass $y_1 \neq 0$ gilt, denn für $y_1 = 0$ ist $P = -P$, also $2P = \mathcal{O}$. Eine Gleichung für die Tangente in P berechnet sich folgendermaßen:

10.1.9 Definition Wenn die Gleichung einer elliptischen Kurve durch $f(x, y) = 0$ gegeben ist, dann ist die **Tangente** in einem Punkt $P = (x_1, y_1)$ auf dieser Kurve die Menge aller (x, y) mit $x, y \in \mathbb{K}$ und

$$\frac{\partial f}{\partial x}(x_1, y_1)(x - x_1) + \frac{\partial f}{\partial y}(x_1, y_1)(y - y_1) = 0.$$

In unserem Fall ist $f(x, y) = y^2 - x^3 - ax - b$, also

$$\frac{\partial f}{\partial x}(x, y) = -3x^2 - a \text{ und } \frac{\partial f}{\partial y}(x, y) = 2y.$$

Die Gleichung für die Tangente in $P = (x_1, y_1)$ ist also

$$(-3x_1^2 - a)(x - x_1) + 2y_1(y - y_1) = 0.$$

Diese Gleichung kann man umformen:

$$\begin{aligned}
& (-3x_1^2 - a)(x - x_1) + 2y_1(y - y_1) = 0 \\
\Leftrightarrow\ & (-3x_1^2 - a)x + (3x_1^2 + a)x_1 + 2y_1y - 2y_1^2 = 0 \\
\Leftrightarrow\ & (2y_1)y = (3x_1^2 + a)x + (-3x_1^3 - ax_1 + 2y_1^2) \\
\Leftrightarrow\ & y = \frac{3x_1^2 + a}{2y_1}x - \frac{3x_1^2 + a}{2y_1}x_1 + y_1, \text{ denn } y_1 \neq 0 \text{ und } \mathrm{char}(\mathbb{K}) > 3.
\end{aligned}$$

Nun wird $\lambda = \frac{3x_1^2+a}{2y_1}$ und $\mu = -\frac{3x_1^2+a}{2y_1}x_1 + y_1$ gesetzt, und die Tangente T an P ist die Menge aller (x, y) mit $x, y \in \mathbb{K}$ und $y = \lambda x + \mu$.

10.1.10 Aufgabe Prüfen Sie nach, dass $P \in T$ gilt.

Um den weiteren Schnittpunkt von T mit $E(a, b, \mathbb{K})$ zu bestimmen, wird die Gleichung für T, also $y = \lambda x + \mu$, in die Gleichung für $E(a, b, \mathbb{K})$ eingesetzt. Dies haben wir ja oben schon einmal getan und die Gleichung

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + (b - \mu^2) = 0$$

erhalten.

10.1.11 Aufgabe Sei $f(x) = x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + (b - \mu^2)$. Zeigen Sie, dass $f'(x_1) = 0$ gilt, dass also x_1 doppelte Nullstelle von f ist.

Wie Sie in Aufgabe 10.1.11 gezeigt haben, ist x_1 doppelte Nullstelle des Polynoms $x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + (b - \mu^2)$, und mit Lemma 10.1.7 ergibt sich für die weitere Nullstelle x_3', dass $-\lambda^2 = -(2x_1 + x_3')$, also $x_3' = \lambda^2 - 2x_1$ gilt. Ist also $2P = R = (x_3, y_3)$, dann ist

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1 = (\frac{3x_1^2 + a}{2y_1})^2 - 2x_1 \text{ und} \\ y_3 &= -\lambda x_3 - \mu = -(\frac{3x_1^2 + a}{2y_1})x_3 + \frac{3x_1^2 + a}{2y_1}x_1 - y_1. \end{aligned}$$

Jetzt kann die vierte und letzte Regel formuliert werden:

(R4) Ist $P = (x_1, y_1) \in E(a, b, \mathbb{K})$ und ist $y_1 = 0$, dann ist $2P = \mathcal{O}$. Ist $y_1 \neq 0$, dann ist $2P = R = (x_3, y_3)$ mit

$$\begin{aligned} x_3 &= (\frac{3x_1^2 + a}{2y_1})^2 - 2x_1 \text{ und} \\ y_3 &= -(\frac{3x_1^2 + a}{2y_1})x_3 + \frac{3x_1^2 + a}{2y_1}x_1 - y_1 = (\frac{3x_1^2 + a}{2y_1})(x_1 - x_3) - y_1. \end{aligned}$$

10.1.12 Beispiel Wir nehmen wieder Beispiel 10.1.2 und berechnen $2(2, 2)$. Es ist $2(2, 2) = (x_3, y_3)$ mit

$$\begin{aligned} x_3 &\equiv (\frac{3 \cdot 4 + 0}{4})^2 - 4 \equiv 0 (\mathrm{mod} 5) \\ y_3 &\equiv (\frac{3 \cdot 4 + 0}{4})(2 - 0) - 2 \equiv 4 (\mathrm{mod} 5). \end{aligned}$$

10.1.13 Satz Mit den Regeln (R1)-(R4) wird $E(a, b, \mathbb{K})$ zu einer abelschen Gruppe.

Beweis: Die Summe von zwei Elementen aus $E(a, b, \mathbb{K})$ ist wieder ein Element aus $E(a, b, \mathbb{K})$, das ist klar mit der Konstruktion der Summe und Aufgabe 10.1.4. Weiterhin ist $\mathcal{O}$ das neutrale Element nach Definition. Außerdem haben wir zu jedem $P \in E(a, b, \mathbb{K})$ ein Element $(-P) \in E(a, b, \mathbb{K})$ definiert, so dass $P - P = (-P) + P = \mathcal{O}$ gilt. Ebenfalls direkt aus den Regeln (R1)-(R4) wird klar, dass $P + Q = Q + P$ für alle $P, Q \in E(a, b, \mathbb{K})$ gilt. Es bleibt also nur noch zu zeigen, dass die Addition assoziativ ist. Dazu kann man natürlich die von uns hergeleiteten Formeln für die Addition nehmen und das Assoziativgesetz direkt nachrechnen. Das führt allerdings zu aufwändigen Rechnungen mit vielen Fallunterscheidungen. Die eher theoretischen Beweise gehen aber für diesen Text zu weit, und wir müssen auf die in den Studierhinweisen aufgeführte Literatur verweisen. □

Da die Koordinaten der Summe von zwei Punkten durch Addieren, Subtrahieren, Multiplizieren und Dividieren im endlichen Körper $\mathbb{K}$ errechnet werden können, gilt außerdem

10.1.14 Proposition Die Summe von zwei Punkten in $E(a, b, \mathbb{K})$ kann effizient berechnet werden.

10.1.15 Aufgabe Berechnen Sie alle Punkte von $E(1, 0, \mathbb{F}_7)$ und bestimmen Sie $(1, 3) + (1, 4)$, $(1, 3) + (3, 3)$ und $2(1, 3)$.

10.1.2 Der Fall char$(\mathbb{K}) = 2$

In diesem Abschnitt ist $\mathbb{K}$ ein endlicher Körper mit $\text{char}(\mathbb{K}) = 2$. Hier sollten Sie sich den Körper $\mathbb{F}_{2^n}$ mit großem $n \in \mathbb{N}$ vorstellen.

10.1.16 Definition Seien $a, b \in \mathbb{K}$, und sei $b \neq 0$. Die **elliptische Kurve** $E(a, b, \mathbb{K})$ ist die Menge aller Punkte (x, y) mit $x, y \in \mathbb{K}$ und

$$y^2 + xy = x^3 + ax^2 + b,$$

zusammen mit einem weiteren Punkt $\mathcal{O}$, also

$$E(a, b, \mathbb{K}) = \{(x, y) \mid x, y \in \mathbb{K} \text{ und } y^2 + xy = x^3 + ax^2 + b\} \cup \{\mathcal{O}\}.$$

10.1.17 Bemerkung Dies ist nicht die allgemeinst mögliche Definition einer elliptischen Kurve über einem Körper der Charakteristik 2. Jedoch ist die andere Sorte elliptischer Kurven für die Kryptografie nicht geeignet.

10.1.18 Beispiel Sei $\mathbb{K} = \mathbb{F}_4 = \mathbb{F}_2[T]/(T^2 + T + 1)$, also $\mathbb{K} = \{0, 1, \alpha, \alpha + 1\}$, wobei $\alpha = [T]$ gilt. Seien $a = 0$ und $b = 1$. Dann ist $E(0, 1, \mathbb{K})$ die Menge aller (x, y) mit $x, y \in \mathbb{K}$ und $y^2 + xy = x^3 + 1$, zusammen mit $\mathcal{O}$. Um alle Punkte in $E(a, b, \mathbb{K})$ zu berechnen, setzen wir nacheinander alle Elemente aus $\mathbb{K}$ für x ein und berechnen die zugehörigen Werte für y:

$$\begin{aligned} x = 0 &\Rightarrow y^2 = 1 \Rightarrow y = 1. \\ x = 1 &\Rightarrow y^2 + y = 0 \Rightarrow y = 0 \text{ oder } y = 1. \\ x = \alpha &\Rightarrow y^2 + \alpha y = 0 \Rightarrow y = 0 \text{ oder } y = \alpha. \\ x = \alpha + 1 &\Rightarrow y^2 + (\alpha + 1)y = 0 \Rightarrow y = 0 \text{ oder } y = \alpha + 1. \end{aligned}$$

Die Kurve ist also

$$E(0, 1, \mathbb{K}) = \{(0, 1), (1, 0), (1, 1), (\alpha, 0), (\alpha, \alpha), (\alpha + 1, 0), (\alpha + 1, \alpha + 1), \mathcal{O}\}.$$

Nun soll auch auf $E(a,b,\mathbb{K})$ eine Addition definiert werden. Dabei gehen wir vor wie beim Fall $\text{char}(\mathbb{K}) > 3$. Die erste Regel ist schon bekannt:

(R1) Das neutrale Element der Addition ist $\mathcal{O}$, es gilt also $\mathcal{O} + P = P = P + \mathcal{O}$ für alle $P \in E(a,b,\mathbb{K})$.

Nun soll das Inverse eines Punktes $P = (x,y) \in E(a,b,\mathbb{K})$ definiert werden. Wir müssen wieder – getreu unserer Merkregel – einen weiteren Schnittpunkt der Kurve mit der Gerade suchen, die parallel zur y-Achse durch P verläuft. Das ist diesmal nicht einfach der Punkt $(x,-y)$. Das würde hier auch keinen Sinn machen, denn über $\mathbb{K}$ gilt ja $y = -y$, dann wäre also $P = -P$ für alle $P \in E(a,b,\mathbb{K})$. Ist jedoch $(x,y) \in E(a,b,\mathbb{K})$, dann ist auch $(x, x+y) \in E(a,b,\mathbb{K})$, denn es gilt

$$\begin{aligned}(x+y)^2 + x(x+y) &= (x+y)(x+y) + x(x+y) = (2x+y)(x+y)\\ &= y(x+y) = y^2 + xy = x^3 + ax^2 + b.\end{aligned}$$

Es soll deshalb folgende Regel gelten:

(R2) Ist $P = (x,y) \in E(a,b,\mathbb{K})$, dann ist $-P = (x, x+y) \in E(a,b,\mathbb{K})$, es gilt also $P + (-P) = \mathcal{O} = (-P) + P$.

Seien nun $P = (x_1,y_1), Q = (x_2,y_2) \in E(a,b,\mathbb{K})$, und es gelte $x_1 \neq x_2$ (denn sonst wäre $Q = P$ oder $Q = -P$). Die Gerade G durch P und Q ist wie im letzten Abschnitt die Menge aller Punkte (x,y) mit $x,y \in \mathbb{K}$ und

$$y = \frac{y_2 + y_1}{x_2 + x_1}x + \frac{y_1x_2 + x_1y_2}{x_2 + x_1}.$$

(bedenken Sie, dass $\text{char}(\mathbb{K}) = 2$ gilt!). Wir setzen wieder $\lambda = \frac{y_2+y_1}{x_2+x_1}$ und $\mu = \frac{y_1x_2+x_1y_2}{x_2+x_1}$. Dann ist G also die Menge aller Punkte (x,y) mit $x,y \in \mathbb{K}$ und $y = \lambda x + \mu$. Nun wird wieder in die Gleichung für $E(a,b,\mathbb{K})$ eingesetzt:

$$\begin{aligned}&(\lambda x + \mu)^2 + x(\lambda x + \mu) = x^3 + ax^2 + b\\ \Leftrightarrow\ &\lambda^2x^2 + \mu^2 + \lambda x^2 + \mu x = x^3 + ax^2 + b\\ \Leftrightarrow\ &x^3 + (\lambda^2 + \lambda + a)x^2 + \mu x + (b + \mu^2) = 0.\end{aligned}$$

Dies ist ein Polynom dritten Grades in x, und wir kennen zwei Nullstellen, nämlich x_1 und x_2. Mit Lemma 10.1.7 gilt für die dritte Nullstelle

$$x_3' = \lambda^2 + \lambda + a + x_1 + x_2 = (\frac{y_2 + y_1}{x_2 + x_1})^2 + \frac{y_2 + y_1}{x_2 + x_1} + a + x_1 + x_2.$$

Ist $R' = (x'_3, y'_3)$ der dritte Schnittpunkt von G mit $E(a, b, \mathbb{K})$, dann gilt außerdem

$$\begin{aligned} y'_3 &= \lambda x'_3 + \mu = \frac{y_2 + y_1}{x_2 + x_1} x'_3 + \frac{y_1 x_2 + x_1 y_2}{x_2 + x_1} \\ &= \frac{y_1 + y_2}{x_1 + x_2} x'_3 + \frac{y_1 x_2 + y_1 x_1 + y_1 x_1 + x_1 y_2}{x_2 + x_1} \\ &= \frac{y_1 + y_2}{x - 1 + x_2} x'_3 + y_1 \frac{x_2 + x_1}{x_2 + x_1} + x_1 \frac{y_1 + y_2}{x_1 + x_2} \\ &= \frac{y_1 + y_2}{x_1 + x_2}(x_1 + x'_3) + y_1. \end{aligned}$$

Um die Koordinaten (x_3, y_3) von $P + Q$ zu erhalten, muss nun noch $x_3 = x'_3$ und $y_3 = y'_3 + x_3$ gebildet werden. Es gilt also

(R3) Seien $P = (x_1, y_1), Q = (x_2, y_2) \in E(a, b, \mathbb{K})$, und es gelte $x_1 \neq x_2$. Dann ist $P + Q = R = (x_3, y_3)$ mit

$$\begin{aligned} x_3 &= (\frac{y_2 + y_1}{x_2 + x_1})^2 + \frac{y_2 + y_1}{x_2 + x_1} + a + x_1 + x_2 \text{ und} \\ y_3 &= (\frac{y_2 + y_1}{x_2 + x_1})(x_1 + x_3) + y_1 + x_3. \end{aligned}$$

10.1.19 Beispiel Sei $E(0, 1, \mathbb{F}_4)$ wie in Beispiel 10.1.18. Dann ist $(1, 0) + (\alpha + 1, \alpha + 1) = (x_3, y_3)$ mit

$$\begin{aligned} x_3 &= (\frac{\alpha + 1}{\alpha})^2 + (\frac{\alpha + 1}{\alpha}) + 1 + (\alpha + 1) \\ &= (\alpha + 1)^4 + (\alpha + 1)^2 + 1 + (\alpha + 1), \text{ denn } \alpha^{-1} = \alpha + 1 \text{ in } \mathbb{F}_4 \\ &= \alpha^2 + \alpha + 1 + \alpha + 1, \text{ denn } (\alpha + 1)^2 = \alpha \text{ in } \mathbb{F}_4 \\ &= \alpha^2 = \alpha + 1. \\ y_3 &= (\frac{\alpha + 1}{\alpha})\alpha + 0 + \alpha + 1 \\ &= (\alpha + 1) + (\alpha + 1) = 0. \end{aligned}$$

Also gilt $(1, 0) + (\alpha + 1, \alpha + 1) = (\alpha + 1, 0)$.

Zu guter Letzt fehlt noch eine Regel zur Verdopplung eines Punktes.

WARNUNG: Wir befinden uns hier zwar über einem Körper mit Charakteristik 2, das heißt, in $\mathbb{K}$ gilt $2x = 0$ für alle $x \in \mathbb{K}$, das gilt aber nicht für die Gruppe $E(a, b, \mathbb{K})$. Hier kann und wird in der Regel durchaus $2P \neq 0$ gelten.

Sei also $P = (x_1, y_1) \in E(a, b, \mathbb{K})$ und sei $x_1 \neq 0$. Ist nämlich $x_1 = 0$, dann ist $y_1 + x_1 = y_1$, und es gilt $P = -P$, also $2P = \mathcal{O}$. Gesucht ist zuerst wieder die

Tangente an $E(a,b,\mathbb{K})$ in P. Definition 10.1.9 beschreibt eine Gleichung für diese Tangente. In diesem Fall ist die Funktion, die die Kurve beschreibt

$$\begin{aligned} f(x,y) &= y^2+xy+x^3+ax^2+b=0, \text{ also} \\ \frac{\partial f}{\partial x}(x,y) &= y+3x^2+2ax = y+x^2 \text{ und} \\ \frac{\partial f}{\partial y}(x,y) &= 2y+x = x. \end{aligned}$$

Also ist die Tangente T in P die Menge aller Punkte (x,y) mit $x,y \in \mathbb{K}$ und

$$\begin{aligned} & (y_1+x_1^2)(x+x_1)+x_1(y+y_1)=0 \\ \Leftrightarrow\ & (y_1+x_1^2)x+(y_1+x_1^2)x_1+x_1y+x_1y_1=0 \\ \Leftrightarrow\ & x_1y=(y_1+x_1^2)x+x_1^3 \\ \Leftrightarrow\ & y=\frac{y_1+x_1^2}{x_1}x+x_1^2, \text{ denn } x_1\neq 0. \end{aligned}$$

Wir setzen $\lambda=(\frac{y_1}{x_1}+x_1)$ und $\mu=x_1^2$. Dann ist T die Menge aller Punkte (x,y) mit $x,y\in\mathbb{K}$ und $y=\lambda x+\mu$. Um die Schnittpunkte von T mit $E(a,b,\mathbb{K})$ zu bestimmen, wird die Gleichung von T in die von $E(a,b,\mathbb{K})$ eingesetzt. Dies ist oben bereits geschehen, und es folgt

$$x^3+(\lambda^2+\lambda+a)x^2+\mu x+(b+\mu^2)=0.$$

Da T die Tangente in P ist, ist x_1 doppelte Nullstelle dieses Polynoms in x, und mit Lemma 10.1.7 folgt, dass für den weiteren Schnittpunkt $R'=(x_3',y_3')$ mit $E(a,b,\mathbb{K})$ gilt:

$$\begin{aligned} x_3' &= \lambda^2+\lambda+a+2x_1=(\frac{y_1}{x_1}+x_1)^2+(\frac{y_1}{x_1}+x_1)+a \\ &= \frac{y_1^2}{x_1^2}+x_1^2+\frac{y_1}{x_1}+x_1+a=\frac{y_1^2+x_1y_1+x_1^3+ax_1^2}{x_1^2}+x_1^2 \\ &= \frac{b}{x_1^2}+x_1^2 \end{aligned}$$

und $y_3'=\lambda x_3'+\mu=(\frac{y_1}{x_1}+x_1)x_3'+x_1^2$. Ist also $2P=R=(x_3,y_3)$, dann gilt

$$x_3=\frac{b}{x_1^2}+x_1^2 \text{ und } y_3=(\frac{y_1}{x_1}+x_1+1)x_3+x_1^2,$$

denn es ist ja $y_3=y_3'+x_3$. Die vierte Regel lautet also:

(R4) Ist $P = (x_1, y_1) \in E(a, b, \mathbb{K})$ und ist $x_1 = 0$, dann ist $2P = \mathcal{O}$. Ist $x_1 \neq 0$, dann ist $2P = (x_3, y_3)$ mit

$$x_3 = x_1^2 + \frac{b}{x_1^2} \text{ und } y_3 = (\frac{y_1}{x_1} + x_1 + 1)x_3 + x_1^2.$$

10.1.20 Beispiel Sei $E(0, 1, \mathbb{F}_4)$ wie in Beispiel 10.1.18. Dann ist $2(\alpha, 0) = (x_3, y_3)$ mit $x_3 = \alpha^2 + \frac{1}{\alpha^2} = \alpha + 1 + \alpha = 1$ und $y_3 = \alpha + 1 + \alpha^2 = 0$. Also ist $2(\alpha, 0) = (1, 0)$.

10.1.21 Satz Mit den Regeln (R1)-(R4) wird $E(a, b, \mathbb{K})$ zu einer abelschen Gruppe.

Beweis: Wie zu Satz 10.1.13. □

Und natürlich gilt auch wieder:

10.1.22 Proposition In $E(a, b, \mathbb{K})$ können die Koordinaten der Summe von zwei Punkten effizient berechnet werden.

10.1.23 Aufgabe Sei $\mathbb{F}_4 = \mathbb{F}_2[T]/(T^2 + T + 1)$ und $\alpha = [T]$. Berechnen Sie alle Punkte von $E(1, \alpha, \mathbb{F}_4)$ und berechnen Sie $(0, \alpha + 1) + (\alpha, \alpha)$ und $2(\alpha, \alpha)$.

10.1.3 Einige Eigenschaften der Gruppe $E(a, b, \mathbb{K})$

In diesem Abschnitt sei $\mathbb{K}$ entweder ein endlicher Körper mit $\text{char}(\mathbb{K}) > 3$, und dann ist $E(a, b, \mathbb{K})$ eine elliptische Kurve wie in Abschnitt 10.1.1, oder $\text{char}(\mathbb{K}) = 2$ und $E(a, b, \mathbb{K})$ ist wie in 10.1.2.

Eine der ersten Fragen, die im Zusammenhang mit elliptischen Kurven über endlichen Körpern auftreten, ist die nach der Anzahl der Punkte. Eine erste Abschätzung der Anzahl der Punkte können Sie selbst vornehmen:

10.1.24 Aufgabe Sei q eine Primzahl, die größer als drei ist, oder eine Zweierpotenz, und sei N die Anzahl der Punkte einer elliptischen Kurve $E(a, b, \mathbb{F}_q)$. Zeigen Sie: $N \leq 2q + 1$.

Man kann die Abschätzung aber noch viel genauer machen, und zwar mit dem Satz von Hasse aus dem Jahr 1933:

10.1.25 Satz (Helmut Hasse (1898-1979)) Sei N die Anzahl der Punkte einer elliptischen Kurve $E(a, b, \mathbb{K})$, wobei $\mathbb{K} = \mathbb{F}_q$ ist. Dann gilt:

$$|N - (q + 1)| \leq 2\sqrt{q}.$$

Der Beweis dieses Satzes kann in den beiden in den Studierhinweisen aufgeführten Büchern gefunden werden. Jedoch wollen wir die Aussage des Satzes noch etwas näher ansehen. Für kryptogafische Zwecke nehmen wir an, dass q sehr groß ist. Dann ist jedoch $\sqrt{q}$ im Vergleich dazu relativ klein, so dass die mögliche Anzahl der Punkte von $E(a, b, \mathbb{K})$ wirklich eingeschränkt wird. Und zwar kann man sagen, dass die Anzahl der Punkte ungefähr q ist oder dass die Anzahl der Punkte die gleiche Größenordung wie q hat. Inzwischen gibt es auch Algorithmen, die die Anzahl der Punkte einer vorgegebenen elliptischen Kurve effizient bestimmen können. Diese beruhen auf dem Algorithmus von Schoof aus dem Jahr 1995, siehe [Sch]. Effizient ist hier allerdings wirklich im Sinne der Definition zu verstehen. In der Praxis sind diese Algorithmen recht aufwändig.

10.1.26 Aufgabe Sei $p > 3$ eine Primzahl. Zeigen Sie, dass die Anzahl der Punkte von $E(0, 1, \mathbb{F}_p)$ immer gerade ist.

Bei den Kryptosystemen über $\mathbb{F}_q^\times$, wobei $\mathbb{F}_q$ ein endlicher Körper ist, weiß man, dass die unterliegende Gruppe, also $(\mathbb{F}_q^\times, \cdot)$, zyklisch ist (vergleiche Satz 4.8.9). Wie ist das bei der Gruppe $E(a, b, \mathbb{K})$? Diese Gruppen sind nicht immer zyklisch, aber es gilt:

10.1.27 Satz Sei $E(a, b, \mathbb{K})$ eine elliptische Kurve über einem endlichen Körper der Charakteristik > 3 oder $= 2$. Dann ist

$$E(a, b, \mathbb{K}) \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}),$$

wobei $d_1 \mid d_2$ gilt. Der Fall $d_1 = 1$, das heißt, $E(a, b, \mathbb{K})$ ist zyklisch, ist möglich.

Leider können wir auch diesen Satz hier nicht beweisen und müssen auf die Literatur verweisen, die am Anfang dieses Kapitels aufgeführt wurde.

10.1.28 Beispiel Wir wollen die Struktur der Gruppe $E(0, 1, \mathbb{F}_4)$ aus Beispiel 10.1.18 berechnen. Wir hatten schon

$$E(0, 1, \mathbb{F}_4) = \{(0, 1), (1, 0), (1, 1), (\alpha, 0), (\alpha, \alpha), (\alpha + 1, 0), (\alpha + 1, \alpha + 1), \mathcal{O}\}$$

berechnet. $E(0, 1, \mathbb{F}_4)$ hat also 8 Elemente. Das heißt, es gilt entweder

$$E(0, 1, \mathbb{F}_4) \simeq \mathbb{Z}/8\mathbb{Z} \text{ oder } E(0, 1, \mathbb{F}_4) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Um herauszufinden, welcher der beiden Fälle vorliegt, berechnen wir die Ordnungen der Elemente und stellen fest, dass $2(\alpha, 0) = (1, 0)$ und $4(\alpha, 0) = (0, 1)$, also $\text{ord}(\alpha, 0) = 8$ gilt, denn $5, 6$ und 7 teilen die Gruppenordnung, also 8, nicht. Es gibt in $E(0, 1, \mathbb{F}_4)$ also ein Element der Ordnung 8, und damit gilt $E(0, 1, \mathbb{F}_4) \simeq \mathbb{Z}/8\mathbb{Z}$, denn in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ gibt es kein Element der Ordnung 8.

10.1.29 Aufgaben 1. Bestimmen Sie die Ordnungen der Elemente in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ und in $\mathbb{Z}/8\mathbb{Z}$.

2. Berechnen Sie die Struktur der Gruppe $E(0, 1, \mathbb{F}_{19})$.

10.1.4 Das diskreter-Logarithmus-Problem für elliptische Kurven

Auch in diesem Abschnitt sei $\mathbb{K}$ entweder ein endlicher Körper mit $\text{char}(\mathbb{K}) > 3$ und $E(a, b, \mathbb{K})$ eine elliptische Kurve wie in 10.1.1, oder es sei $\text{char}(\mathbb{K}) = 2$ und $E(a, b, \mathbb{K})$ wie in 10.1.2. Da $E(a, b, \mathbb{K})$ eine additive Gruppe ist, lautet das diskreter-Logarithmus-Problem (DLP) für elliptische Kurven folgendermaßen:

10.1.30 Problem (Diskreter-Logarithmus-Problem(DLP)) Gegeben seien eine elliptische Kurve $E(a, b, \mathbb{K})$ und $P \in E(a, b, \mathbb{K})$. Sei Q ein Vielfaches von P. Finde den diskreten Logarithmus von Q zur Basis P, das heißt, finde eine Zahl $x \in \mathbb{Z}$ mit $Q = xP$.

10.1.31 Vermutung Es gibt keinen effizienten Algorithmus, um das diskreter-Logarithmus-Problem für elliptische Kurven zu lösen.

Es wird sogar noch mehr vermutet:

10.1.32 Vermutung Das diskreter-Logarithmus-Problem für elliptische Kurven ist schwerer zu lösen als das für endliche Körper.

Die zweite Vermutung bedeutet Folgendes: Selbst, wenn es einmal einen effizienten oder fast effizienten Algorithmus für das DLP für endliche Körper geben sollte, dann heißt das wahrscheinlich noch nicht, dass es auch einen für elliptische Kurven gibt.

Das Problem ist dasselbe wie beim diskreter-Logarithmus-Problem für endliche Körper: Beweisen kann das alles (bisher) keiner. Der einzige Beweis ist, dass schon sehr viele versucht haben, effiziente Algorithmen zu finden, und es ist noch niemandem gelungen. Natürlich gibt es Algorithmen, um das DLP für elliptische Kurven zu lösen, aber die sind weit davon entfernt, effizient zu sein. Immerhin sind sie aber so gut, dass auch bei elliptischen Kurven der zugrunde liegende Körper nicht zu klein gewählt werden sollte. Heutzutage (2003) wählt man die Größe des Körpers etwa zwischen 2^{160} und 2^{190} Elementen. Es gibt auch noch weitere Einschränkungen für die Auswahl der elliptischen Kurve, denn für bestimmte Familien von elliptischen Kurven gibt es relativ gute Algorithmen, um das DLP zu lösen.

10.2 Kryptografische Verfahren über elliptischen Kurven

Nachdem in 10.1 dargelegt wurde, auf welche Weise elliptische Kurven zu abelschen Gruppen werden, und wir gesehen haben, dass das Diskreter-Logarithmus-Problem über elliptischen Kurven schwer ist, können nun die Verfahren aus Kapitel 9 auf die elliptischen Kurven übertragen werden. Dabei benutzen wir, dass wir in Kapitel 9 eigentlich nur Gruppen benötigen, in denen die Verknüpfung effizient berechnet werden kann und in denen das diskreter-Logarithmus-Problem schwer zu lösen ist. Die Verfahren selbst funktionieren in jeder solcher Gruppe.

10.2.1 Das Diffie-Hellman Verfahren

Es sei daran erinnert, dass das Diffie-Hellman Schlüssel-Austauschverfahren dazu dient, Schlüssel (zum Beispiel für ein symmetrisches Verfahren) über einen unsicheren Kanal auszutauschen.

Bekanntgegeben werden ein endlicher Körper $\mathbb{K}$ mit

$$\text{char}(\mathbb{K}) > 3 \text{ oder } \text{char}(\mathbb{K}) = 2,$$

eine entsprechende elliptische Kurve $E(a, b, \mathbb{K})$ und ein zufällig gewählter Punkt $P \in E(a, b, \mathbb{K})$. Der Punkt P sollte so gewählt sein, dass die von P erzeugte Untergruppe in $E(a, b, \mathbb{K})$ möglichst groß ist, also ungefähr so groß wie $E(a, b, \mathbb{K})$ selbst. Mehr dazu in Abschnitt 10.3.4.

Alice und Bob möchten einen zufällig gewählten Punkt $Q \in E(a, b, \mathbb{K})$ – oder genauer: in der von P erzeugten Untergruppe von $E(a, b, \mathbb{K})$ – als Schlüssel für ihr Kryptosystem vereinbaren. In welcher Weise sie aus einem Punkt der elliptischen Kurve einen passenden Schlüssel für ihr Kryptosystem machen, darauf müssen sie sich vorher geeinigt haben. Benötigen sie ein Element aus $\mathbb{K}$, so können sie ja zum Beispiel einfach die x-Koordinate von Q nehmen.

Alice wählt nun zufällig eine Zahl $e_A \in \mathbb{N}$. Da man mit dem Satz von Hasse annehmen kann, dass die Anzahl der Elemente von $E(a, b, \mathbb{K})$ ungefähr q, also die Anzahl der Elemente von $\mathbb{K}$ ist, und da man außerdem hofft (oder weiß), dass die von P erzeugte Untergruppe ungefähr genauso viele Elemente hat, ist es sinnvoll, e_A irgendwo in der Größenordnung von q zu wählen. Alice bildet $e_A P$ – das ist effizient möglich, wenn man das Analogon zum Wiederholten Quadrieren für additive Gruppen benutzt – und gibt diesen Punkt bekannt.

Bob wählt analog $e_B \in \mathbb{N}$, wieder in der gleichen Größenordnung wie q, berechnet $e_B P$ und gibt diesen Punkt bekannt. Der neue Schlüssel ist dann $e_A e_B P$. Beide können ihn effizient berechnen: Alice berechnet $e_A(e_B P)$ und Bob berechnet $e_B(e_A P)$. Oscar kennt jedoch nur P, $e_A P$ und $e_B P$. Wenn Oscar das DLP für elliptische Kurven lösen kann, dann kann Oscar sicher $e_A e_B P$ berechnen. Jedoch gilt wieder:

10.2.1 Vermutung Oscar kann das Diffie-Hellman-System nicht brechen, ohne diskrete Logarithmen für elliptische Kurven zu berechnen.

10.2.2 Aufgabe Alice und Bob möchten mit dem Diffie-Hellman-Verfahren einen Schlüssel festlegen. Sie geben $E(1, 0, \mathbb{F}_7)$ und $(3, 3)$ bekannt. Alice schickt $(0, 0)$ an Bob und Bob schickt $(5, 2)$ an Alice. Was ist der Schlüssel?

10.2.2 Das Massey-Omura Kryptosystem

Bei diesem Kryptosystem möchten sich Alice und Bob geheime Nachrichten schicken. Öffentlich bekannt gegeben werden ein endlicher Körper $\mathbb{K}$ mit $\mathrm{char}(\mathbb{K}) > 3$ oder $\mathrm{char}(\mathbb{K}) = 2$ und eine entsprechende elliptische Kurve $E(a, b, \mathbb{K})$ über $\mathbb{K}$. Außerdem muss bei diesem Verfahren auch die Anzahl N der Punkte von $E(a, b, \mathbb{K})$ bekannt sein. In 10.1.3 wurde schon erwähnt, dass es mit dem Algorithmus von Schoof effizient möglich ist, die Anzahl der Punkte einer elliptischen Kurve zu bestimmen.

Die Nachrichten oder Nachrichteneinheiten m werden als Punkte $P_m \in E(a, b, \mathbb{K})$ kodiert, und zwar so, dass man m eindeutig ermitteln kann, wenn man P_m kennt. Eine Möglichkeit, wie eine solche Kodierung aussehen kann, wird in 10.3.3 vorgestellt. Wir können jetzt also annehmen, dass die geheimen Nachrichten, die verschickt werden sollen, Punkte auf $E(a, b, \mathbb{K})$ sind.

Alice möchte den Punkt P als Nachricht verschicken. Sie wählt zufällig eine Zahl $e_A \in \mathbb{N}$ mit $0 \leq e_A \leq N$ und $\mathrm{ggT}(e_A, N) = 1$. Außerdem berechnet sie mit Hilfe des erweiterten Euklidischen Algorithmus' ein $d_A \in \mathbb{N}$ mit $e_A d_A \equiv 1 (\mathrm{mod} N)$. Alice bildet $e_A P$ und schickt diesen Punkt an Bob. Bob wählt ebenfalls zufällig $e_B \in \mathbb{N}$ mit $0 \leq e_B \leq N$ und $\mathrm{ggT}(e_B, N) = 1$ und berechnet mit Hilfe des erweiterten Euklidischen Algorithmus' ein $d_B \in \mathbb{N}$ mit $e_B d_B \equiv 1 (\mathrm{mod} N)$. Bob bildet $e_B(e_A P)$ und schickt diesen Punkt zurück an Alice. Nun bildet Alice $d_A(e_B e_A P) = d_A e_A e_B P = e_B P$, da $e_A d_A \equiv 1 (\mathrm{mod} N)$ gilt und N die Ordnung der Gruppe $E(a, b, \mathbb{K})$ ist. (Wenn nämlich $NQ = \mathcal{O}$ für alle $Q \in E(a, b, \mathbb{K})$ ist und $e_A d_A = 1 + kN$ für ein $k \in \mathbb{Z}$ ist, dann ist

$$d_A e_A Q = (1 + kN)Q = Q + kNQ = Q + k\mathcal{O} = Q + \mathcal{O} = Q$$

für alle $Q \in E(a, b, \mathbb{K})$.)

Alice schickt $e_B P$ an Bob. Dieser berechnet $d_B e_B P = P$ und kennt damit die geheime Nachricht. Oscar dagegen sieht nur die Nachrichten $e_A P, e_B e_A P$ und $e_B P$. Wenn er das DLP für elliptische Kurven lösen kann, dann kann er auch P berechnen.

10.2.3 Vermutung Oscar kann das Massey-Omura-System nicht brechen, ohne diskrete Logarithmen zu berechnen.

10.2.4 Aufgabe Stellen Sie sich vor, Sie sind Oscar und können diskrete Logarithmen in $E(a, b, \mathbb{K})$ berechnen. Wie können Sie aus $e_A P$, $e_B P$ und $e_A e_B P$ die geheime Nachricht P berechnen?

10.2.3 Das ElGamal-Kryptosystem

Auch bei diesem Kryptosystem soll eine Nachricht über einen unsicheren Kanal verschickt werden. Es werden ein endlicher Körper $\mathbb{K}$ mit $\text{char}(\mathbb{K}) > 3$ oder $\text{char}(\mathbb{K}) = 2$, eine entsprechende elliptische Kurve $E(a, b, \mathbb{K})$ und ein Punkt $S \in E(a, b, \mathbb{K})$ bekannt gegeben. Bei diesem Verfahren ist es nicht nötig, die Anzahl der Punkte von $E(a, b, \mathbb{K})$ zu kennen. Jedoch sollte die von S erzeugte Untergruppe von $E(a, b, \mathbb{K})$ möglichst groß sein.

Wir nehmen wieder an, dass die Nachricht, die übermittelt werden soll, ein Punkt $P \in E(a, b, \mathbb{K})$ ist. Bob wählt nun geheim und zufällig ein $e_B \in \mathbb{N}$ und gibt $e_B S$ bekannt. Alice wählt zufällig eine ganze Zahl e_A und schickt $(e_A S, P + e_A(e_B S))$ an Bob. Um die Nachricht zu entschlüsseln, berechnet Bob zunächst $e_B(e_A S)$ und dann $P + e_A(e_B S) - e_B(e_A S) = P$. Oscar kann aus den verschickten Informationen $e_B S$, $e_A S$ und $P + e_A(e_B S)$ natürlich P berechnen, wenn er das DLP für elliptische Kurven lösen kann.

10.2.5 Vermutung Wenn Oscar das ElGamal-System brechen kann, dann kann er auch das diskreter-Logarithmus-Problem für elliptische Kurven lösen.

10.3 Technische Probleme

In diesem Abschnitt wird es um die Probleme gehen, die auftreten, wenn man Kryptologie über elliptischen Kurven betreibt. Es wird darum gehen, wie man einen Punkt auf einer vorgegebenen elliptischen Kurve findet, wie man einer Nachricht

einen Punkt auf der Kurve zuordnet und darum, wie man überhaupt zu einer geeigneten Kurve kommt.

10.3.1 Das Lösen quadratischer Gleichungen

Um Punkte auf einer vorgegebenen elliptischen Kurve zu finden, muss man quadratische Gleichungen über dem Grundkörper $\mathbb{K}$ lösen können. Im Folgenden wird ein Verfahren zum Lösen quadratischer Gleichungen vorgestellt wie sie im Zusammenhang mit den elliptischen Kurven auftreten.

Zuerst betrachten wir den Fall, dass $\mathbb{K}$ ein Körper der Form $\mathbb{F}_p$ ist, wobei $p > 3$ eine Primzahl ist. Gelöst werden soll die Gleichung

$$x^2 \equiv a(\mathrm{mod} p) \text{ oder } x^2 - a = 0 \text{ in } \mathbb{F}_p. \tag{10.1}$$

Gesucht wird also eine (oder beide) Quadratwurzel(n) aus $a \in \mathbb{F}_p$. In 7.3 wurde gezeigt, dass man mit Hilfe des Legendre-Symbols $(\frac{a}{p})$ feststellen kann, ob Gleichung (10.1) in $\mathbb{F}_p$ überhaupt eine Lösung besitzt. Außerdem wurde in 7.3 gezeigt, wie man das Legendre- beziehungsweise das Jacobi-Symbol effizient berechnet. Wir können hier also annehmen, dass $(\frac{a}{p}) = 1$ gilt, denn sonst hätte Gleichung (10.1) keine (für $(\frac{a}{p}) = -1$) oder genau eine (für $(\frac{a}{p}) = 0$) Lösung.

Wir nehmen zunächst an, dass wir ein $n \in \mathbb{F}_p$ mit $(\frac{n}{p}) = -1$ kennen. Sei $p-1 = 2^r s$, wobei s ungerade ist. 2^r ist also die größte Zweierpotenz, die in $p-1$ enthalten ist. Setze

$$b = n^s \bmod p \text{ und } q = a^{\frac{s+1}{2}} \bmod p.$$

10.3.1 Lemma Es gilt

$$(\frac{q^2}{a})^{2^{r-1}} \equiv 1(\mathrm{mod} p).$$

Beweis: Es gilt

$$(\frac{q^2}{a})^{2^{r-1}} \equiv (\frac{a^{s+1}}{a})^{2^{r-1}} \equiv a^{s \cdot 2^{r-1}} \equiv a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \equiv 1(\mathrm{mod} p).$$

□

Gesucht ist ein $x \in \mathbb{F}_p$ mit $\frac{x^2}{a} = 1$, das heißt, q ist als erste Näherung für x gar nicht so schlecht. Die Zahl q wird jetzt schrittweise modifiziert, und zwar so, dass nach Schritt k gilt

$$(\frac{q^2}{a})^{2^{r-1-k}} \equiv 1(\mathrm{mod} p).$$

Also ist nach spätestens $r-1$ Schritten die Lösung gefunden. Um q zu modifizieren, kommt b ins Spiel.

10.3.2 Lemma $b \bmod p$ ist eine primitive 2^r-te Einheitswurzel in $\mathbb{F}_p^\times$.

Beweis: Es gilt

$$b^{2^r} \equiv (n^s)^{2^r} \equiv n^{s\cdot 2^r} \equiv n^{p-1} \equiv 1(\mathrm{mod}p)$$

mit Fermats kleinem Satz. Dann gilt also $b \equiv g^l(\mathrm{mod}p)$ für eine primitive 2^r-te Einheitswurzel $g \in \mathbb{F}_p^\times$. Angenommen, $b^k \equiv 1(\mathrm{mod}p)$ für ein $k < 2^r$. Dann ist $g^{lk} \equiv 1(\mathrm{mod}p)$, also folgt $2^r \mid lk$. Da $k < 2^r$ gilt, ist l gerade, also ist b ein quadratischer Rest modulo p. Das ist aber nicht möglich, denn mit Lemma 7.3.7 gilt

$$(\frac{b}{p}) = (\frac{n^s}{p}) = (\frac{n}{p})^s = (-1)^s = (-1),$$

weil s ungerade ist. □

Da $b \bmod p$ eine primitive 2^r-te Einheitswurzel ist, ist $b^2 \bmod p$ eine primitive 2^{r-1}-te Einheitswurzel, wie wir aus Proposition 4.8.5 wissen. Nun gilt aber $(\frac{q^2}{a})^{2^{r-1}} \equiv 1(\bmod p)$ mit Lemma 10.3.1, also gibt es ein $j \in \mathbb{N}$, $0 \le j \le 2^{r-1}$, mit $\frac{q^2}{a} \equiv (b^2)^j \equiv b^{2j}(\mathrm{mod}p)$. Es folgt

$$\begin{aligned} 1 &\equiv \frac{q^2}{a}b^{-2j} \equiv \frac{q^2}{a}b^{2^r-2j}, \text{ denn } b^{2^r} \equiv 1(\mathrm{mod}p) \\ &\equiv \frac{(qb^{2^{r-1}-j})^2}{a}(\mathrm{mod}p), \end{aligned}$$

und $qb^{2^{r-1}-j} \bmod p$ ist das gesuchte x. Wichtig ist, dass es einen Exponenten $\alpha \in \mathbb{N}$, $0 \le \alpha \le 2^{r-1}$, gibt, so dass $(qb^\alpha)^2 \equiv a(\mathrm{mod}p)$ gilt, das heißt, $qb^\alpha \bmod p$ ist eine Lösung von Gleichung (10.1). Dabei gilt sogar $\alpha < 2^{r-1}$, denn $b^{2^{r-1}} \equiv -1(\mathrm{mod}\ p)$, weil $(b^{2^{r-1}})^2 \equiv b^{2^r} \equiv 1(\mathrm{mod}p)$ und $b^{2^{r-1}} \not\equiv 1(\mathrm{mod}p)$ gilt. Also ist $b^{2^{r-1}}q \equiv -q(\mathrm{mod}p)$.

Der Exponent α, beziehungsweise die Lösung q, soll nun berechnet werden. Um es übersichtlicher zu machen, werden wir wieder einen Algorithmus formulieren. Dieser Algorithmus ist übrigens von Daniel Shanks (1917-1996) und wird auch im Computeralgebra-System MuPAD verwendet.

10.3.3 Algorithmus (Lösung quadratischer Gleichungen)

Eingabe Eine Primzahl $p > 3$ und ein $a \in \mathbb{N}$ mit $1 \le a < p$ und $(\frac{a}{p}) = 1$.

Ausgabe Ein $x \in \mathbb{N}$ mit $x^2 \equiv a(\mathrm{mod}p)$.

1. Berechne $r, s \in \mathbb{N}$ mit $p-1 = 2^r s$ und s ist ungerade.

2. Berechne $n \in \mathbb{N}$ mit $1 \leq n < p$ und $(\frac{n}{p}) = -1$.

3. $b_{-1} \leftarrow n^s \bmod p$ und $q_{-1} \leftarrow a^{\frac{s+1}{2}} \bmod p$.

4. **for** $k = 0, \ldots, r-2$ **do**

5. **if** $(\frac{q_{k-1}^2}{a})^{2^{r-2-k}} \equiv 1 (\mathrm{mod} p)$

6. **then** $q_k \leftarrow q_{k-1}$

7. **else** $q_k \leftarrow q_{k-1} b_{k-1} \bmod p$

8. $b_k \leftarrow (b_{k-1})^2 \bmod p$

9. **übergebe** q_{r-2}.

Nun müssen wir natürlich wieder zeigen, dass der Algorithmus auch das richtige Ergebnis liefert.

10.3.4 Lemma Sei $0 \leq k \leq r-2$. Dann gilt

$$(\frac{q_k^2}{a})^{2^{r-2-k}} \equiv 1 (\mathrm{mod} p) \text{ und } b_k \equiv b^{2^{k+1}} (\mathrm{mod} p),$$

wobei $b = n^s \bmod p$ gilt.

Beweis: Wir beweisen die Behauptung durch Induktion nach k. Sei $k = 0$. Mit Lemma 10.3.1 gilt $(\frac{q_{-1}^2}{a})^{2^{r-1}} \equiv 1 (\mathrm{mod} p)$. Also folgt $(\frac{q_{-1}^2}{a})^{2^{r-2}} \equiv \pm 1 (\mathrm{mod} p)$. Ist $(\frac{q_{-1}^2}{a})^{2^{r-2}} \equiv 1 (\mathrm{mod} p)$, dann ist $q_0 = q_{-1}$, also $(\frac{q_0^2}{a})^{2^{r-2}} \equiv 1 (\mathrm{mod} p)$. Ist $(\frac{q_{-1}}{a})^{2^{r-2}} \equiv -1 (\mathrm{mod} p)$, dann ist $q_0 = q_{-1} b_{-1} = q_{-1} b$, also

$$(\frac{q_0^2}{a})^{2^{r-2}} \equiv (\frac{q_{-1}^2 b^2}{a})^{2^{r-2}} \equiv (\frac{q_{-1}^2}{a})^{2^{r-2}} b^{2^{r-1}} \equiv (-1)(-1) \equiv 1 (\mathrm{mod} p).$$

Außerdem gilt $b_0 \equiv (b_{-1})^2 \equiv b^2 \equiv b^{2^1} (\mathrm{mod} p)$. Sei nun $0 \leq k < r-2$. Mit Induktionsvoraussetzung ist $(\frac{q_k^2}{a})^{2^{r-2-k}} \equiv 1 (\mathrm{mod} p)$, also $(\frac{q_k^2}{a})^{2^{r-2-(k+1)}} \equiv \pm 1 (\mathrm{mod}\ p)$. Ist $(\frac{q_{k-1}^2}{a})^{2^{r-2-k}} \equiv 1 (\mathrm{mod} p)$, dann ist

$$(\frac{q_k^2}{a})^{2^{r-2-k}} \equiv (\frac{q_{k-1}^2}{a})^{2^{r-2-k}} \equiv 1 (\mathrm{mod} p),$$

und ist $(\frac{q_{k-1}^2}{a})^{2^{r-2-k}} \equiv -1 (\mathrm{mod} p)$, dann ist

$$(\frac{q_k^2}{a})^{2^{r-2-k}} \equiv (\frac{q_{k-1}^2}{a} b_{k-1})^{2^{r-2-k}} \equiv (\frac{q_{k-1}^2}{a})^{2^{r-2-k}} b^{2^{r-1}} \equiv (-1)(-1) \equiv 1 (\mathrm{mod} p).$$

Außerdem ist $b_k \equiv (b_{k-1})^2 \equiv (b^{2^k})^2 \equiv b^{2^{k+1}} (\mathrm{mod} p)$. □

Für $k = r - 2$ ist dann also

$$(\frac{q_{r-2}^2}{a})^{2^0} \equiv \frac{q_{r-2}^2}{a} \equiv 1(\mathrm{mod}p),$$

das heißt, $x = q_{r-2}$ ist eine Lösung von Gleichung (10.1).

Es bleibt jetzt nur noch die Frage zu klären, wie man ein n mit $(\frac{n}{p}) = -1$ finden kann. Doch das kann man einfach durch Ausprobieren tun. Wenn man n zufällig wählt mit $0 < n < p$, dann gilt mit Wahrscheinlichkeit $\frac{1}{2}$, dass $(\frac{n}{p}) = -1$ ist, wie in 7.3 gezeigt wurde. Das heißt, die Wahrscheinlichkeit, nach k Versuchen immer noch kein n mit $(\frac{n}{p}) = -1$ gefunden zu haben, ist nur $\frac{1}{2^k}$, so dass man damit rechnen kann, schon nach wenigen Versuchen ein n gefunden zu haben. Die Tatsache, dass n zufällig gewählt wird, macht den oben angeführten Algorithmus zu einem effizienten, probabilistischen Algorithmus. Bei gleicher Eingabe können unterschiedlich viele und unterschiedliche Schritte ausgeführt werden. Das Ergebnis ist jedoch im Gegensatz zu den Primzahltests aus Kapitel 7 immer das gleiche und immer korrekt.

10.3.5 Beispiel Sei $p = 113$ und $a = 50$. Wir berechnen

$$(\frac{50}{113}) = (\frac{2}{113})(\frac{5}{113})^2 = (\frac{2}{113}) = 1,$$

denn $113 \bmod 8 = 1$, also $(\frac{2}{113}) = 1$ mit Proposition 7.3.22. Es ist also $x^2 = 50$ in $\mathbb{F}_{113}$ lösbar.

Eingabe $p = 113$ und $a = 50$.

1. $113 - 1 = 112 = 2^4 \cdot 7$, also $r = 4$ und $s = 7$.

2. Durch Ausprobieren berechnen wir $n = 3$.

3. $b_{-1} \leftarrow 3^7 \bmod 113 = 40$ und $q_{-1} \leftarrow 50^4 \bmod 113 = 83$.

4. $k = 0$.

5. $(\frac{q_{-1}^2}{a})^4 \equiv -1(\mathrm{mod}113)$, also

7. $q_0 \leftarrow q_{-1} \cdot b_{-1} \bmod 113 = 43$.

8. $b_0 \leftarrow b_{-1}^2 \bmod 113 = 18$.

4. $k = 1$.

5. $(\frac{q_0^2}{a})^2 \equiv -1(\mathrm{mod}113)$, also

7. $q_1 = q_0 \cdot b_0 \bmod 113 = 96$.

8. $b_1 \leftarrow b_0^2 \bmod 113 = 98$.

4. $k = 2$.

5. $(\frac{q_1^2}{a}) \equiv -1 (\mathrm{mod} 113)$, also

7. $q_2 = q_1 b_1 \bmod 113 = 29$.

8. $b_2 \leftarrow b_1^2 \bmod 113 = 112$.

9. Das Ergebnis ist $x = 29$.

10.3.6 Aufgabe Sei p eine Primzahl mit $p \equiv 3 \bmod 4$, und sei $a \in \mathbb{Z}$ mit $(\frac{a}{p}) = 1$. Welche Lösung der Gleichung $x^2 \equiv a (\mathrm{mod} p)$ wird mit dem Algorithmus von Shanks berechnet? Zeigen Sie für die so berechnete Lösung x direkt, dass $x^2 \equiv a (\mathrm{mod} p)$ gilt.

Nun muss noch der Fall $\mathrm{char}(\mathbb{K}) = 2$ betrachtet werden. Die Gleichung $x^2 = a$ ist über einem Körper $\mathbb{K}$ mit $\mathrm{char}(\mathbb{K}) = 2$ einfach zu lösen. Gilt nämlich $\mathbb{K} = \mathbb{F}_{2^n}$ für ein $n > 1$, dann ist $a^{2^n} = a$ für alle $a \in \mathbb{F}_{2^n}$, also ist für $x = a^{2^{n-1}}$ die Gleichung $x^2 = a$ erfüllt (und x ist die einzige Lösung dieser Gleichung).

Für das Finden von Punkten auf elliptischen Kurven müssen jedoch auch quadratische Gleichungen der Form $x^2 + ax + b = 0$ für $a \neq 0$ gelöst werden. Diese werden zunächst auf die Form $x^2 + x + \beta = 0$ gebracht, indem man $x = ax'$ setzt. Dann ist nämlich

$$a^2 x'^2 + a^2 x' + b = 0 \Leftrightarrow x'^2 + x' + \frac{b}{a^2} = 0.$$

Kann man also Gleichungen der Form $x^2 + x + \beta = 0$ lösen, dann auch solche der Form $x^2 + ax + b = 0$.

Gegeben sei also die Gleichung

$$x^2 + x + \beta = 0 \tag{10.2}$$

mit $\beta \in \mathbb{K} = \mathbb{F}_{2^n}$. Ob es überhaupt eine Lösung für Gleichung (10.2) gibt, lässt sich leicht feststellen, man muss nur die Spur von β berechnen.

10.3.7 Proposition Gleichung (10.2) hat genau dann eine Lösung in $\mathbb{K} = \mathbb{F}_{2^n}$, wenn $\mathrm{Tr}_{\mathbb{K}}(\beta) = 0$ gilt.

Beweis: Wir zeigen zunächst, dass $\mathrm{Tr}_{\mathbb{K}}(\beta) = 0$ gilt, wenn Gleichung (10.2) eine Lösung hat. Dann gilt nämlich $x^2 + x + \beta = (x + a)(x + b)$ mit $a, b \in \mathbb{K}$. Also folgt

$x^2+x+\beta = x^2+(a+b)x+ab$. Koeffizientenvergleich ergibt $a+b=1$ und $ab=\beta$, also $b=1+a$ und $\beta = a(a+1) = a^2+a$. Es folgt

$$\mathrm{Tr}_{\mathbb{K}}(\beta) = \mathrm{Tr}_{\mathbb{K}}(a^2+a) = \mathrm{Tr}_{\mathbb{K}}(a^2) + \mathrm{Tr}_{\mathbb{K}}(a) = 2\mathrm{Tr}_{\mathbb{K}}(a) = 0$$

mit Proposition 8.5.2.

Nun werden wir zeigen, wie man eine Lösung für Gleichung (10.2) berechnet, wenn $\mathrm{Tr}_{\mathbb{K}}(\beta) = 0$ gilt. Dabei werden zwei Fälle unterschieden. Zunächst betrachten wir den Fall, dass n ungerade ist. Dann ist

$$\tau(\beta) = \sum_{j=0}^{\frac{n-1}{2}} \beta^{2^{2j}}$$

eine Lösung von Gleichung (10.2), denn

$$\begin{aligned}
\tau(\beta)^2+\tau(\beta)+\beta &= (\sum_{j=0}^{\frac{n-1}{2}} \beta^{2^{2j}})^2 + \sum_{j=0}^{\frac{n-1}{2}} \beta^{2^{2j}} + \beta \\
&= \sum_{j=0}^{\frac{n-1}{2}} \beta^{2^{2j+1}} + \sum_{j=0}^{\frac{n-1}{2}} \beta^{2^{2j}} + \beta, \text{ denn } (a+b)^2 = a^2+b^2 \text{ in } \mathbb{F}_{2^n} \\
&= \sum_{i=0}^{n} \beta^{2^i} + \beta \\
&= \sum_{i=0}^{n-1} \beta^{2^i} + 2\beta, \text{ denn } \beta^{2^n} = \beta \\
&= \sum_{i=0}^{n-1} \beta^{2^i} = \mathrm{Tr}_{\mathbb{K}}(\beta) = 0.
\end{aligned}$$

Ist n gerade, dann muss zunächst ein Element $\delta \in \mathbb{F}_{2^n}$ gesucht werden mit $\mathrm{Tr}_{\mathbb{K}}(\delta) = 1$. Am einfachsten ist es, zufällig Elemente von $\mathbb{F}_{2^n}$ zu probieren. In Proposition 8.5.2 haben wir nämlich gezeigt, dass $\mathrm{Tr}_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{F}_2$ surjektiv ist, das heißt, $\dim \mathrm{Kern}(\mathrm{Tr}_{\mathbb{K}}) = n-1$, und das heißt, dass 2^{n-1} Elemente von $\mathbb{K}$ auf 0 abgebildet werden. Die anderen 2^{n-1} Elemente werden auf 1 abgebildet. Bei jedem Versuch ist also die Wahrscheinlichkeit $\frac{1}{2}$, dass ein Element mit Spur 1 gefunden wird. Nach k Versuchen ist die Wahrscheinlichkeit, ein passendes Element gefunden zu haben, dann schon $1-\frac{1}{2^k}$.

Sei also $\delta \in \mathbb{F}_{2^n}$ mit $\mathrm{Tr}_{\mathbb{K}}(\delta) = 1$. Eine Lösung von Gleichung (10.2) ist dann

$$x = \sum_{i=0}^{n-2} (\sum_{j=i+1}^{n-1} \delta^{2^j}) \beta^{2^i},$$

denn

$$\begin{aligned}
x^2+x+\beta &= \left(\sum_{i=0}^{n-2}(\sum_{j=i+1}^{n-1}\delta^{2^j})\beta^{2^i}\right)^2 + \sum_{i=0}^{n-2}(\sum_{j=i+1}^{n-1}\delta^{2^j})\beta^{2^i}+\beta \\
&= \sum_{i=0}^{n-2}(\sum_{j=i+1}^{n-1}\delta^{2^{j+1}})\beta^{2^{i+1}} + \sum_{i=0}^{n-2}(\sum_{j=i+1}^{n-1}\delta^{2^j})\beta^{2^i}+\beta \\
&= (\sum_{j=1}^{n-1}\delta^{2^{j+1}})\beta^2 + (\sum_{j=2}^{n-1}\delta^{2^{j+1}})\beta^4 + \ldots + (\delta^{2^n})\beta^{2^{n-1}} \\
&\quad +(\sum_{j=1}^{n-1}\delta^{2^j})\beta + (\sum_{j=2}^{n-1}\delta^{2^j})\beta^2 + \ldots + (\delta^{2^{n-1}})\beta^{2^{n-2}} + \beta \\
&= (\sum_{j=1}^{n-1}\delta^{2^j})\beta + (\sum_{j=1}^{n-1}\delta^{2^{j+1}} + \sum_{j=2}^{n-1}\delta^{2^j})\beta^2 + \\
&\quad \ldots + (\sum_{j=n-2}^{n-1}\delta^{2^{j+1}} + \delta^{2^{n-1}})\beta^{2^{n-2}} + \delta^{2^n}\beta^{2^{n-1}} + \beta \\
&= (\mathrm{Tr}_{\mathbb{K}}(\delta)+\delta)\beta + (\delta^{2^n})\beta^2 + \ldots + (\delta^{2^n})\beta^{2^{n-2}} + (\delta^{2^n})\beta^{2^{n-1}} + \beta \\
&= (1+\delta)\beta + \delta\beta^2 + \ldots + \delta\beta^{2^{n-1}} + \beta \\
&= \delta(\beta+\beta^2+\ldots+\beta^{2^{n-1}}) + 2\beta \\
&= \delta(\mathrm{Tr}_{\mathbb{K}}(\beta)) = 0.
\end{aligned}$$

Da δ zufällig ermittelt wird, handelt es sich hier wieder um einen probabilistischen Algorithmus, dem man sofort ansieht, dass er effizient ist. Er liefert wie im Fall $p > 3$ immer das korrekte Ergebnis. □

10.3.8 Aufgabe Zeigen Sie, dass für eine Lösung $x \in \mathbb{F}_{2^n}$ von Gleichung (10.2) immer auch $x+1$ eine Lösung ist.

10.3.9 Beispiel 1. Sei $\mathbb{K} = \mathbb{F}_{2^3} = \mathbb{F}_8 = \mathbb{F}_2[T]/(T^3+T+1)$. Sei $\alpha = [T]$. Gesucht ist eine Lösung der Gleichung

$$x^2 + x + \alpha^2 = 0.$$

Es gilt $\mathrm{Tr}_{\mathbb{F}_8}(\alpha^2) = \alpha^2+\alpha^4+\alpha^8 = 0$, die Gleichung ist also lösbar. Setze $x = \tau(\alpha^2) = \alpha^2+\alpha^8 = \alpha^2+\alpha$. Dann ist tatsächlich $(\alpha^2+\alpha)^2+(\alpha^2+\alpha)+\alpha^2 = 0$. Die zweite Lösung ist dann $\alpha^2+\alpha+1$.

2. Sei $\mathbb{K} = \mathbb{F}_{2^4} = \mathbb{F}_{16} = \mathbb{F}_2[T]/(T^4+T+1)$. Sei $\alpha = [T]$. Gesucht ist eine Lösung der Gleichung
$$x^2 + x + \alpha^2 = 0.$$
Es gilt $\mathrm{Tr}_{\mathbb{F}_{16}}(\alpha^2) = \alpha^2 + \alpha^4 + \alpha^8 + \alpha^{16} = 0$, die Gleichung ist also lösbar. Zur Lösung wird ein Element $\delta \in \mathbb{F}_{16}$ mit $\mathrm{Tr}_{\mathbb{F}_{16}}(\delta) = 1$ benötigt. Da $\mathrm{Tr}_{\mathbb{F}_{16}}(\alpha) = 0$ gilt, probieren wir $\delta = \alpha^3$ und stellen fest, dass $\mathrm{Tr}_{\mathbb{F}_{16}}(\alpha^3) = 1$ gilt. Setze also
$$x = \sum_{i=0}^{2}\Big(\sum_{j=i+1}^{3} (\alpha^3)^{2^j}\Big)(\alpha^2)^{2^i} = \alpha^3 + 1.$$
Tatsächlich gilt dann $(\alpha^3+1)^2 + (\alpha^3+1) + \alpha^2 = 0$.

10.3.2 Punkte auf einer Kurve

Beim Diffie-Hellman- und beim ElGamal-Verfahren werden nicht nur eine elliptische Kurve sondern auch ein Punkt auf dieser Kurve bekannt gegeben. Man sollte also in der Lage sein, zu einer vorgegebenen elliptischen Kurve einen Punkt auf der Kurve zu finden. Da kein effizienter deterministischer Algorithmus bekannt ist, um einen Punkt auf einer elliptischen Kurve zu finden, geht man einfach folgendermaßen vor: Sei $E(a, b, \mathbb{K})$ eine elliptische Kurve mit $\mathbb{K} = \mathbb{F}_p$ und $p > 3$ oder $\mathbb{K} = \mathbb{F}_{2^n}$. Man wählt zufällig ein $x \in \mathbb{K}$ und berechnet $\alpha = x^3 + ax + b$, falls $\mathrm{char}(\mathbb{K}) > 3$ gilt und $\alpha = x^3 + ax^2 + b$, falls $\mathrm{char}(\mathbb{K}) = 2$ gilt. Ist $\mathrm{char}(\mathbb{K}) > 3$, versucht man nun, die Gleichung $y^2 = \alpha$ mit den Methoden aus Abschnitt 10.3.1 zu lösen. Ist $\mathrm{char}(\mathbb{K}) = 2$, versucht man, $y^2 + xy + \alpha = 0$ zu lösen. In beiden Fällen ist die Wahrscheinlichkeit ungefähr $\frac{1}{2}$, dass die Gleichung eine Lösung hat (das werden wir aber nicht beweisen!). Gibt es eine Lösung, dann ist $(x, y) \in E(a, b, \mathbb{K})$ ein Punkt der Kurve. Gibt es keine Lösung, probiert man den nächsten x-Wert aus. Nach k Versuchen ist die Wahrscheinlichkeit, dass man einen Punkt auf der Kurve gefunden hat, schon $1 - \frac{1}{2^k}$ (ungefähr jedenfalls).

10.3.3 Nachrichten und Punkte

Schickt man Nachrichten (oder Schlüssel) mit Kryptosystemen, die auf elliptischen Kurven basieren, so schickt man sich Punkte auf elliptischen Kurven zu. Es muss also vorher geklärt sein, wie man zu einer Nachricht m, also zum Beispiel zu einer Zahl $m \in \mathbb{Z}$, einen Punkt P_m auf der elliptischen Kurve so bestimmt, dass der Empfänger aus dem Punkt P_m wieder die Nachricht m ableiten kann.

Das Verfahren, das wir hier vorstellen, ist wieder ein probabilistisches. Man legt hier vorher eine Irrtumswahrscheinlichkeit fest, also ein $\epsilon > 0, \epsilon \in \mathbb{R}$, so dass mit Wahrscheinlichkeit höchstens ϵ kein Punkt P_m gefunden wird, der zu m gehört. Genauer gesagt wird ein $\kappa \in \mathbb{N}$ gewählt, so dass die Irrtumswahrscheinlichkeit $\frac{1}{2^\kappa}$ ist. Normalerweise wählt man κ zwischen 30 und 50. Es wird angenommen, dass die Nachrichten natürliche Zahlen m mit $0 \leq m < M$ sind (zum Beispiel $M = 26$, wenn A,...,Z mit 0,...,25 identifiziert werden). Damit das Verfahren funktioniert, sollte der Körper $\mathbb{K}$ mehr als κM Elemente haben. Weiterhin benötigt man eine injektive Abbildung φ von der Menge aller natürlichen Zahlen mit $0 \leq n \leq \kappa M$ nach $\mathbb{K}$. Wenn wir annehmen, dass $\mathbb{K} = \mathbb{F}_{2^n}$ für ein $n \in \mathbb{N}$ gilt und gegeben ist durch eine Basis $(v_0, \ldots, v_{n-1})$ über $\mathbb{F}_2$, dann können wir beispielsweise φ folgendermaßen definieren: Sei $m \in \mathbb{N}$ mit $0 \leq m < 2^n$. Dann hat m die Binärdarstellung $(\alpha_{n-1} \ldots \alpha_0)_2$ mit $\alpha_i \in \{0, 1\}$ für $0 \leq i \leq n-1$. Wir definieren $\varphi(m) = \sum_{i=0}^{n-1} \alpha_i v_i$. Da $(v_0, \ldots, v_{n-1})$ eine Basis ist, ist diese Abbildung injektiv (und sogar bijektiv).

Sei nun m mit $0 \leq m < M$ eine Nachricht. Für jedes $j \in \mathbb{N}$ mit $1 \leq j \leq \kappa$ gibt es dann ein $x \in \mathbb{K}$ mit $x = \varphi(m\kappa + j)$. Für ein solches x wird nun $\alpha = x^3 + ax + b$ berechnet, falls $\mathrm{char}(\mathbb{K}) > 3$ ist, und $\alpha = x^3 + ax^2 + b$, falls $\mathrm{char}(\mathbb{K}) = 2$ gilt. Anschließend wird die quadratische Gleichung $y^2 = \alpha$ gelöst, falls $\mathrm{char}(\mathbb{K}) > 3$ ist, und $y^2 + xy + \alpha = 0$, falls $\mathrm{char}(\mathbb{K}) = 2$ gilt. Ist die Gleichung lösbar, ist ein Punkt $P_m = (x, y)$ gefunden, wenn nicht, und wenn $j < \kappa$ ist, wird j um eins erhöht und mit $\varphi(m\kappa + (j+1))$ weiter gerechnet. In jedem Schritt ist die Wahrscheinlichkeit, einen Punkt P_m zu finden, ungefähr $\frac{1}{2}$ (auch das werden wir nicht beweisen). Insgesamt ist die Wahrscheinlichkeit, P_m zu finden, also (ungefähr) $1 - \frac{1}{2^k}$.

Bekommt der Empfänger $P_m = (x, y)$ geschickt, kann er m berechnen, indem er das Urbild von x unter φ berechnet. Das ist von der Form $a = m\kappa + j$ für ein $1 \leq j \leq \kappa$. Berechnet man nun

$$[\frac{a-1}{\kappa}] = [\frac{m\kappa + j - 1}{\kappa}] = [m + \frac{j-1}{\kappa}],$$

dann ist $0 \leq \frac{j-1}{\kappa} < 1$, also $[\frac{a-1}{\kappa}] = m$.

10.3.10 Beispiel Seien $\mathbb{K} = \mathbb{F}_{521}$ und $a = 0$, $b = 1$, das heißt $E(a, b, \mathbb{K})$ ist die Menge aller Punkte (x, y) mit $x, y \in \mathbb{F}_{521}$ und $y^2 = x^3 + 1$ zusammen mit dem Punkt $\mathcal{O}$. Weiter seien $M = 26$ und $\kappa = 20$. Es wird also mit einer Wahrscheinlichkeit von $1 - \frac{1}{2^{20}} \sim 0,999999$ ein Punkt P_m zu einer Nachricht gefunden. Es soll die Nachricht $m = 11$ verschickt werden (wenn zum Beispiel A mit 0, B mit 1, C mit 2 und so weiter identifiziert wird, ist die Nachricht L). Die Abbildung φ ist in diesem

Beispiel ganz einfach:

$$\begin{aligned} \varphi : \{0, \ldots, 520\} &\longrightarrow \mathbb{F}_{521} \\ a &\mapsto a \bmod 521. \end{aligned}$$

Es ist nun also $m\kappa = 220$. Zuerst wird $j = 1$ gesetzt. Dann ist $m\kappa + j = 221$, und es gilt

$$(221)^3 + 1 = 305 \bmod 521.$$

Das Legendre-Symbol ist $(\frac{305}{521}) = -1$. Die Gleichung $y^2 = 305$ ist in $\mathbb{F}_{521}$ also nicht lösbar. Deshalb setze $j = 2$. Nun ist $m\kappa + j = 222$, und es gilt $(222)^3 + 1 \equiv 49 (\mathrm{mod} 521)$. Natürlich gilt $(\frac{49}{521}) = 1$, denn $49 = 7^2$. Das heißt, eine Lösung für $y^2 = 49$ ist schon gefunden. Wir setzen $P_m = (222, 7)$. Der Empfänger entschlüsselt nun $P_m = (222, 7)$ und berechnet $m = [\frac{221}{20}] = [11 + \frac{1}{20}] = 11$.

10.3.4 Auswahl der Kurve

Zu guter Letzt bleibt noch die Frage zu klären, wie man sich eine elliptische Kurve auswählen sollte. Dabei gibt es verschiedene Methoden. Es kommt natürlich darauf an, welches Verfahren durchgeführt werden soll. Bei dem Verfahren von Massey-Omura muss zum Beispiel die Anzahl N der Punkte auf der Kurve bekannt sein. Das ist bei den beiden anderen vorgestellten Verfahren nicht der Fall. Dort reicht es, wenn die von dem Punkt P erzeugte Gruppe möglichst groß ist. Aber natürlich hätte man auch hier lieber die Gewissheit über die Größe der von P erzeugten Gruppe.

Da das Verfahren von Schoof, mit dem die Anzahl N der Punkte einer elliptischen Kurve bestimmt werden kann, deterministisch und polynomial ist, kann man einfach eine zufällig erzeugte elliptische Kurve nehmen und die Anzahl N der Punkte der Kurve berechnen. Wichtig für die Sicherheit des auf der Kurve basierenden Kryptosystems ist, dass N mindestens einen „großen“ Primteiler hat. Wenn N nämlich nur kleine Primteiler hat, dann ist der diskrete Logarithmus in der zugehörigen abelschen Gruppe relativ leicht zu berechnen.

Auch einen Punkt P auf der elliptischen Kurve kann man finden, wie Sie in Abschnitt 10.3.2 gesehen haben. Es geht aber auch so: Es werden zufällig $a, x, y \in \mathbb{K}$ gewählt. Dann wird

$$b = \begin{cases} y^2 - x^3 - ax, & \text{falls } \mathrm{char}(\mathbb{K}) > 3 \text{ gilt} \\ y^2 + xy + ax^2, & \text{falls } \mathrm{char}(\mathbb{K}) = 2 \text{ gilt} \end{cases}$$

gesetzt und es wird überprüft, ob $4a^3 + 27b^2 \neq 0$ beziehungsweise $b \neq 0$ gilt. Falls ja, dann ist (x, y) ein Punkt auf der Kurve $E(a, b, \mathbb{K})$. Doch davon kennt man leider

noch nicht die Ordnung des Punktes. Am einfachsten ist es, wenn die Ordnung der elliptischen Kurve eine Primzahl ist, denn dann ist jeder Punkt, der nicht $\mathcal{O}$ ist, ein Erzeuger der Gruppe.

Da es auch aus Sicherheitsgründen gut ist, wenn die Gruppenordnung eine Primzahl ist (s.o.), ist eine Möglichkeit, eine passende Kurve zu finden, zufällig Kurven zu erzeugen (mit oder ohne zugehörigem Punkt), bis man eine findet, deren Ordnung eine Primzahl ist. Es gibt eine Liste von Anforderungen an „sichere“ elliptische Kurven, siehe IEEE P1363. Wenn man nicht unbedingt darauf besteht, dass die Ordnung der Kurve eine Primzahl ist (eine solche Kurve genügt natürlich diesen Anforderungen), kann man so lange suchen, bis man eine Kurve gefunden hat, die alle Anforderungen der Liste erfüllt. Es sollte dabei bemerkt werden, dass in polynomialer Zeit überprüft werden kann, ob eine Kurve zulässig ist. Interessierte können sich in der Kurvenfabrik unter

`http://www.kurvenfabrik.de`

ihre eigene, sichere elliptische Kurve bestellen, die nach dieser Methode erzeugt wird. Das Problem bei dieser Methode ist der Algorithmus von Schoof, oder Varianten davon, der für große elliptische Kurven immer noch sehr viel Rechenaufwand benötigt.

Es gibt auch eine Methode, bei der man gleich bei der Erzeugung der elliptischen Kurve die Ordnung der zugehörigen abelschen Gruppe festlegen kann. Diese Methode soll hier aber nicht diskutiert werden, denn elliptische Kurven, die mit dieser Methode erzeugt werden, sind für kryptografische Zwecke nicht geeignet.

10.3.5 Vor- und Nachteile

Auf den ersten Blick sehen die Kryptosysteme über den elliptischen Kurven sehr viel komplizierter aus als die über den endlichen Körpern. Das sind sie natürlich auch, denn es steckt ja sehr viel mehr Mathematik dahinter. Dafür scheint aber das diskreter-Logarithmus-Problem über den elliptischen Kurven sehr viel schwieriger zu sein. Und das hat den Vorteil, dass man die Gruppengröße sehr viel kleiner wählen kann als über endlichen Körpern. So ist man bei den Kryptosystemen über endlichen Körpern gezwungen, die Körpergröße zwischen 2^{1024} und 2^{4096} zu wählen, während man bei den elliptischen Kurven für die gleiche Sicherheit nur Körper (und damit auch Gruppengrößen) mit zwischen 2^{173} und 2^{313} Elementen benötigt. Die sehr viel kürzere Länge der Gruppenelemente (auch Schlüssellänge genannt) sorgt auch dafür, dass die Addition von zwei Punkten schneller ist als bei den Kryptosystemen über endlichen Körpern, obwohl die Operation an sich

komplizierter ist. Die geringere Schlüssellänge ist ebenfalls ein Vorteil, wenn der Speicherplatz begrenzt ist, zum Beispiel beim Einsatz von Smartcards.

Außerdem gibt es viele verschiedene elliptische Kurven über einem festen endlichen Körper, so dass man auch einen Körper fest wählen kann und die Körperarithmetik in Hardware zur Verfügung stellen kann, was natürlich wesentlich schneller ist.

Lösungen der Aufgaben

Lösungen der Aufgaben in Kapitel 10

Aufgabe 10.1.4

Behauptung Für $(x, y) \in E(a, b, \mathbb{K})$ mit $\mathbb{K} = \mathbb{R}$ oder $\text{char}(\mathbb{K}) > 3$ gilt immer $(x, -y) \in E(a, b, \mathbb{K})$.

Beweis: Sei $(x, y) \in E(a, b, \mathbb{K})$, das heißt, $y^2 = x^3 + ax + b$. Dann folgt $(-y)^2 = y^2 = x^3 + ax + b$, also $(x, -y) \in E(a, b, \mathbb{K})$. □

Aufgabe 10.1.6 Seien $P = (x_1, y_1), Q = (x_2, y_2) \in E(a, b, \mathbb{K})$, wobei $x_1 \neq x_2$ gelte. G sei die Menge aller Punkte (x, y) mit $x, y \in \mathbb{K}$, die die Gleichung

$$y = (\frac{y_2 - y_1}{x_2 - x_1})x + \frac{y_1x_2 - x_1y_2}{x_2 - x_1}$$

erfüllen.

Behauptung P und Q liegen auf der Geraden G.

Beweis: Es gilt

$$\begin{aligned} \frac{y_2 - y_1}{x_2 - x_1}x_1 + \frac{y_1x_2 - x_1y_2}{x_2 - x_1} &= \frac{y_2x_1 - y_1x_1 + y_1x_2 - x_1y_2}{x_2 - x_1} \\ &= y_1(\frac{x_2 - x_1}{x_2 - x_1}) = y_1, \end{aligned}$$

also gilt $P \in G$. Weiter gilt

$$\begin{aligned} \frac{y_2 - y_1}{x_2 - x_1}x_2 - \frac{y_1x_2 - x_1y_2}{x_2 - x_1} &= \frac{y_2x_2 - y_1x_2 + y_1x_2 - x_1y_2}{x_2 - x_1} \\ &= y_2(\frac{x_2 - x_1}{x_2 - x_1}) = y_2. \end{aligned}$$

Also ist auch $Q \in G$. □

Aufgabe 10.1.10 Sei $P = (x_1, y_1) \in E(a, b, \mathbb{K})$ mit $y_1 \neq 0$. Sei T die Menge aller (x, y) mit $x, y \in \mathbb{K}$ und

$$y = \frac{3x_1^2 + a}{2y_1}x - \frac{3x_1^2 + a}{2y_1}x_1 + y_1.$$

Behauptung $P \in T$.

Beweis: Es gilt $\frac{3x_1^2+a}{2y_1}x_1 - \frac{3x_1^2+a}{2y_1}x_1 + y_1 = y_1$, also $P = (x_1, y_1) \in T$. □

Aufgabe 10.1.11 Sei

$$f(x) = x^3 - (\frac{3x_1^2 + a}{2y_1})^2x^2 + (a - 2\frac{3x_1^2 + a}{2y_1}(-\frac{3x_1^2 + a}{2y_1}x_1 + y_1))x + (b - (-\frac{3x_1^2 + a}{2y_1}x_1 + y_1)^2).$$

Behauptung x_1 ist eine doppelte Nullstelle von f.

Beweis: Nach Konstruktion von f ist x_1 eine Nullstelle von f. Wir müssen also nur noch zeigen, dass x_1 auch eine Nullstelle von f' ist. Es gilt

$$f'(x) = 3x^2 - 2(\frac{3x_1^2 + a}{2y_1})^2x + (a - 2\frac{3x_1^2 + a}{2y_1}(-\frac{3x_1^2 + a}{2y_1}x_1 + y_1)),$$

also

$$\begin{aligned} f'(x_1) &= 3x_1^2 - 2(\frac{3x_1^2 + a}{2y_1})^2x_1 + (a - 2\frac{3x_1^2 + a}{2y_1}(-\frac{3x_1^2 + a}{2y_1}x_1 + y_1)) \\ &= 3x_1^2 + a - 2\frac{(3x_1^2 + a)^2}{4y_1^2}x_1 + 2\frac{(3x_1^2 + a)^2}{4y_1^2}x_1 - 2\frac{3x_1^2 + a}{2y_1}y_1 \\ &= 3x_1^2 + a - 3x_1^2 - a \\ &= 0. \end{aligned}$$

□

Aufgabe 10.1.15 Berechnen Sie alle Punkte von $E(1, 0, \mathbb{F}_7)$ und bestimmen Sie $(1, 3) + (1, 4)$, $(1, 3) + (3, 3)$ und $2(1, 3)$.

Es gilt $4 \cdot 1^3 + 27 \cdot 0^2 \not\equiv 0 (\mathrm{mod} 7)$ und

$$E(1, 0, \mathbb{F}_7) = \{(x, y) \mid y^2 = x^3 + x\} \cup \{\mathcal{O}\}.$$

Wir probieren nun der Reihe nach alle Elemente von $\mathbb{F}_7$ für x aus und rechnen nach, ob es einen passenden y-Wert gibt.

$$\begin{aligned}
x = 0 &: y^2 = 0, \text{ also } y = 0\\
x = 1 &: y^2 = 2, \text{ also } y = 3 \text{ oder } y = 4\\
x = 2 &: y^2 = 3, \text{ diese Gleichung hat in } \mathbb{F}_7 \text{ keine Lösung}\\
x = 3 &: y^2 = 2, \text{ also } y = 3 \text{ oder } y = 4\\
x = 4 &: y^2 = 5, \text{ diese Gleichung hat in } \mathbb{F}_7 \text{ keine Lösung}\\
x = 5 &: y^2 = 4, \text{ also } y = 2 \text{ oder } y = 5\\
x = 6 &: y^2 = 5, \text{diese Gleichung hat in } \mathbb{F}_7 \text{ keine Lösung.}
\end{aligned}$$

Also gilt

$$E(1, 0, \mathbb{F}_7) = \{(0,0), (1,3), (1,4), (3,3), (3,4), (5,2), (5,5), \mathcal{O}\}.$$

Weiter ist $(1,3) + (1,4) = \mathcal{O}$, denn $(1,4) = -(1,3)$.

Außerdem ist $(1,3) + (3,3) = (x_3, y_3)$ mit $x_3 = (\frac{3-3}{3-1})^2 - 1 - 3 = 3$ und $y_3 = \frac{3-3}{3-1}(1-3) - 3 = 4$ in $\mathbb{F}_7$. Also $(1,3) + (3,3) = (3,4)$.

Es ist $2(1,3) = (x_3, y_3)$ mit $x_3 = (\frac{3+1}{6})^2 - 2 = 2 - 2 = 0$ und $y_3 = \frac{3+1}{6}(1-0) - 3 = -4 - 3 = 0$, also $2(1,3) = (0,0)$. □

Aufgabe 10.1.23 Berechnen Sie alle Punkte von $E(1, \alpha, \mathbb{F}_4)$, wobei $\mathbb{F}_4 = \mathbb{F}_2[T]/(T^2 + T + 1)$ und $\alpha = [T]$ gilt, und berechnen Sie $(0, \alpha + 1) + (\alpha, \alpha)$ und $2(\alpha, \alpha)$.

Es gilt

$$E(1, \alpha, \mathbb{F}_4) = \{(x, y) \mid y^2 + xy = x^3 + x^2 + \alpha\} \cup \{\mathcal{O}\}.$$

Wir probieren nun wieder der Reihe nach alle Elemente aus $\mathbb{F}_4$ für x aus und rechnen nach, ob es einen passenden y-Wert gibt.

$$\begin{aligned}
x = 0 &: y^2 = \alpha, \text{ also } y = \alpha + 1\\
x = 1 &: y^2 + y = \alpha, \text{ diese Gleichung hat in } \mathbb{F}_4 \text{ keine Lösung}\\
x = \alpha &: y^2 + \alpha y = 0, \text{ also } y = 0 \text{ oder } y = \alpha\\
x = \alpha + 1 &: y^2 + (\alpha + 1)y = 1, \text{ diese Gleichung hat in } \mathbb{F}_4 \text{ keine Lösung.}
\end{aligned}$$

Also gilt

$$E(1, \alpha, \mathbb{F}_4) = \{(0, \alpha + 1), (\alpha, 0), (\alpha, \alpha), \mathcal{O}\}.$$

Weiter ist $(0, \alpha + 1) + (\alpha, \alpha) = (x_3, y_3)$ mit $x_3 = (\frac{1}{\alpha})^2 + \frac{1}{\alpha} + 1 + 0 + \alpha = \alpha$ und $y_3 = (\frac{1}{\alpha})(\alpha) + \alpha + 1 + \alpha = 0$. Damit ist $(0, \alpha + 1) + (\alpha, \alpha) = (\alpha, 0)$.

Es gilt $2(\alpha,\alpha) = (x_3, y_3)$ mit $x_3 = \alpha^2 + \frac{\alpha}{\alpha^2} = 0$ und $y_3 = (\frac{\alpha}{\alpha} + \alpha + 1) \cdot 0 + \alpha^2 = \alpha + 1$, also $2(\alpha,\alpha) = (0, \alpha + 1)$. □

Aufgabe 10.1.24 Sei q eine Primzahl, die größer als drei ist, oder eine Zweierpotenz, und sei N die Anzahl der Punkte einer elliptischen Kurve $E(a, b, \mathbb{F}_q)$.

Behauptung $N \leq 2q + 1$.

Beweis: Sei $(x, y) \in E(a, b, \mathbb{F}_q)$. Dann kann x genau q verschiedene Werte annehmen, und der zugehörige y-Wert ist Lösung einer quadratische Gleichung über $\mathbb{F}_q$. Also kann es zu jedem x-Wert höchstens zwei dazugehörige y-Werte geben. Das macht insgesamt höchstens $2q$ Punkte. Dazu kommt dann noch der Punkt $\mathcal{O}$, so dann wir insgesamt tatsächlich $N \leq 2q + 1$ erhalten. □

Aufgabe 10.1.26 Sei $p > 3$ eine Primzahl.

Behauptung Die Anzahl der Punkte von $E(0, 1, \mathbb{F}_p)$ ist immer gerade.

Beweis: Es gilt

$$E(0, 1, \mathbb{F}_p) = \{(x, y) \mid y^2 = x^3 + 1\} \cup \{\mathcal{O}\}.$$

Wir setzen wieder x-Werte aus $\mathbb{F}_p$ ein und berechnen die zugehörigen y-Werte. Das Polynom $x^3 + 1$ hat in $\mathbb{F}_p$ entweder eine Nullstelle ($x = -1$) oder drei Nullstellen. Setzt man nämlich $f(x) = x^3 + 1$, dann ist $f'(x) = 3x^2$, und da die einzige Nullstelle von f' keine Nullstelle von f ist, hat f keine mehrfachen Nullstellen. Ist x eine Lösung von $x^3 + 1 = 0$, dann ist $y = 0$ der zugehörige y-Wert. Ist $x^3 + 1 \neq 0$, dann gibt es für ein solches x immer entweder überhaupt keine Lösung für y oder gleich 2 Lösungen. Bisher haben wir also ungerade viele Punkte, und zusammen mit $\mathcal{O}$ erhalten wir immer gerade viele Punkte. □

Aufgaben 10.1.29

1. Bestimmen Sie die Ordnungen der Elemente in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ und in $\mathbb{Z}/8\mathbb{Z}$.

   In $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ gilt:

Element	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$	$(0,2)$	$(1,2)$	$(0,3)$	$(1,3)$
Ordnung	1	2	4	4	2	2	4	4.

   Und in $\mathbb{Z}/8\mathbb{Z}$ gilt:

Element	0	1	2	3	4	5	6	7
Ordnung	1	8	4	8	2	8	4	8.

□

2. Berechnen Sie die Struktur der Gruppe $E(0,1,\mathbb{F}_{19})$.

   Als Vorbemerkung: $0^2 = 0$, $1^2 = 1 = 18^2$, $2^2 = 4 = 17^2$, $3^2 = 9 = 16^2$, $4^2 = 16 = 15^2$, $5^2 = 6 = 14^2$, $6^2 = 17 = 13^2$, $7^2 = 11 = 12^2$, $8^2 = 7 = 11^2$, $9^2 = 5 = 10^2$ in $\mathbb{F}_{19}$.

   Nun gilt

$$E(0,1,\mathbb{F}_{19}) = \{(x,y) \mid y^2 = x^3 + 1\} \cup \{\mathcal{O}\},$$

   also

$$\begin{aligned}
x = 0 &: y^2 = 1, \text{ also } y = 1 \text{ oder } y = 18\\
x = 1 &: y^2 = 2, \text{ diese Gleichung hat keine Lösung}\\
x = 2 &: y^2 = 9, \text{ also } y = 3 \text{ oder } y = 16\\
x = 3 &: y^2 = 9, \text{ also } y = 3 \text{ oder } y = 16\\
x = 4 &: y^2 = 8, \text{ diese Gleichung hat keine Lösung}\\
x = 5 &: y^2 = 12, \text{ diese Gleichung hat keine Lösung}\\
x = 6 &: y^2 = 8, \text{ diese Gleichung hat keine Lösung}\\
x = 7 &: y^2 = 2, \text{ diese Gleichung hat keine Lösung}\\
x = 8 &: y^2 = 0, \text{ also } y = 0\\
x = 9 &: y^2 = 8, \text{ diese Gleichung hat keine Lösung}\\
x = 10 &: y^2 = 13, \text{ diese Gleichung hat keine Lösung}\\
x = 11 &: y^2 = 2, \text{ diese Gleichung hat keine Lösung}\\
x = 12 &: y^2 = 0, \text{ also } y = 0\\
x = 13 &: y^2 = 13, \text{ diese Gleichung hat keine Lösung}\\
x = 14 &: y^2 = 9, \text{ also } y = 3 \text{ oder } y = 16\\
x = 15 &: y^2 = 13, \text{ diese Gleichung hat keine Lösung}\\
x = 16 &: y^2 = 12, \text{ diese Gleichung hat keine Lösung}\\
x = 17 &: y^2 = 12, \text{ diese Gleichung hat keine Lösung}\\
x = 18 &: y^2 = 0, \text{ also } y = 0.
\end{aligned}$$

   Also gilt

$$\begin{aligned}
E(0,1,\mathbb{F}_{19}) = \{&(0,1),(0,18),(2,3),(2,16),(3,3),(3,16),(8,0),(12,0),(14,3),\\
&(14,16),(18,0),\mathcal{O}\}
\end{aligned}$$

   und diese elliptische Kurve hat 12 Elemente. Damit gilt $E(0,1,\mathbb{F}_{19}) \simeq \mathbb{Z}/12\mathbb{Z}$ oder $E(0,1,\mathbb{F}_{19}) \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$. Auf $E(0,1,\mathbb{F}_{19})$ liegen drei Punkte der

Form $(x, 0)$ für ein $x \in \mathbb{F}_{19}$. Diese Punkte haben die Ordnung 2. Da es in $\mathbb{Z}/12\mathbb{Z}$ nur ein Element der Ordnung 2 gibt, während es in $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$ drei Elemente der Ordnung zwei gibt, gilt

$$E(0, 1, \mathbb{F}_{19}) \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z}).$$

□

Aufgabe 10.2.2 Alice und Bob möchten mit dem Diffie-Hellman-Verfahren einen Schlüssel festlegen. Sie geben $E(1, 0, \mathbb{F}_7)$ und $(3, 3)$ bekannt. Alice schickt $(0, 0)$ an Bob und Bob schickt $(5, 2)$ an Alice. Was ist der Schlüssel?

Wir berechnen die Vielfachen des Punktes $(3, 3)$. Es gilt $2(3, 3) = (x_3, y_3)$ mit $x_3 = (\frac{0}{6})^2 - 6 = 1$ und $y_3 = \frac{0}{6}(3 - 1) - 3 = 4$. Also gilt $2(3, 3) = (1, 4)$. Weiter ist $3(3, 3) = (3, 3) + (1, 4) = (x_3, y_3)$ mit $x_3 = (\frac{4-3}{1-3})^2 - 1 - 3 = 2 - 1 - 3 = 5$ und $y_3 = \frac{4-3}{1-3}(3 - 5) - 3 = 1 - 3 = 5$, also $3(3, 3) = (5, 5)$. Nun ist $4(3, 3) = 2(1, 4) = 2(-(1, 3)) = -2(1, 3) = -(0, 0) = (0, 0)$, wie wir aus Aufgabe 10.1.15 wissen. Nun wissen wir schon, dass Alice $e_A = 4$ gewählt hat (oder zumindest $e_A \equiv 4 \bmod 8$). Nun gilt $5(3, 3) = (0, 0) + (3, 3) = (x_3, y_3)$ mit $x_3 = (\frac{3}{3})^2 - 0 - 3 = 5$ und $y_3 = \frac{3}{3}(0 - 5) - 0 = 2$, also $5(3, 3) = (5, 2)$, und Bob hat $e_B \equiv 5 \bmod 8$ gewählt. Der Schlüssel ist jetzt $e_A e_B(3, 3) = 20(3, 3) = 4(3, 3) = (0, 0)$, denn die Ordnung der Gruppe ist 8 (und damit natürlich eigentlich viel zu klein). □

Aufgabe 10.2.4 Stellen Sie sich vor, Sie sind Oscar und können diskrete Logarithmen in $E(a, b, \mathbb{K})$ berechnen. Wie können Sie aus $e_A P$, $e_B P$ und $e_A e_B P$ die geheime Nachricht P berechnen?

Oscar weiß, dass die zweite Information $e_A e_B P$ ein Vielfaches von $e_A P$ ist. Da er diskrete Logarithmen berechnen kann, kann er e_B berechnen. Mit dem erweiterten Euklidischen Algorithmus berechnet er nun d_B mit $e_B d_B \equiv 1 (\mathrm{mod} N)$, und dann ist $d_B e_B P = P$. □

Aufgabe 10.3.6 Sei p eine Primzahl mit $p \equiv 3 \bmod 4$, und sei $a \in \mathbb{Z}$ mit $(\frac{a}{p}) = 1$. Welche Lösung der Gleichung $x^2 \equiv a (\mathrm{mod} p)$ wird mit dem Algorithmus von Shanks berechnet? Zeigen Sie für die so berechnete Lösung x direkt, dass $x^2 \equiv a (\mathrm{mod} p)$ gilt.

Sei $p = 4k + 3$ für ein $k \in \mathbb{N}_0$. Dann ist $p - 1 = 4k + 2$, also $r = 1$ und $s = 2k + 1$. Es wird $q = a^{k+1}$ gesetzt, und mit Lemma 10.3.1 gilt dann schon

$$(\frac{q^2}{a})^{2^0} \equiv \frac{q^2}{a} \equiv 1 \bmod p.$$

Das können wir auch direkt nachrechnen:

$$q^2 \equiv a^{2k+2} \equiv a \cdot a^{2k+1} \equiv a \cdot a^{\frac{p-1}{2}} \equiv a(\frac{a}{p}) \equiv a \bmod p.$$

□

Aufgabe 10.3.8

Behauptung Für eine Lösung $x \in \mathbb{F}_{2^n}$ von Gleichung (10.2) ist immer auch $x+1$ eine Lösung.

Beweis: Ist $x^2 + x + \beta = 0$, dann folgt auch

$$(x+1)^2 + (x+1) + \beta = x^2 + 1 + x + 1 + \beta = x^2 + x + \beta = 0.$$

□

Kurseinheit 7

Gitter

Studierhinweise

Nach unserem Streifzug durch verschiedene Teilgebiete der Mathematik kommen wir in der letzten Kurseinheit wieder ganz an den Anfang dessen, was in der Mathematik gelehrt wird: zur Linearen Algebra.

Wir betrachten Basen $(a_1, \ldots, a_n)$ von $\mathbb{R}^n$ und die Menge aller ganzzahligen Linearkombinationen der Basiselemente. Sei $L = L(a_1, \ldots, a_n) = \{\sum_{i=1}^{n} \lambda_i a_i \mid \lambda_i \in \mathbb{Z}\}$. Dann wird L ein Gitter in $\mathbb{R}^n$ mit Basis $(a_1, \ldots, a_n)$ genannt. Ein schwieriges Problem, von dem man erst seit wenigen Jahren weiß, dass es NP-hart ist (das bedeutet, dass es vermutlich keine effizienten Algorithmen zur Lösung gibt – und wenn es einen gibt, dann auch für viele andere, sehr schwere Probleme), ist, einen Algorithmus anzugeben, der einen kürzesten Vektor $\neq 0$ in L findet.

Diese Tatsache macht Gitter für kryptografische Zwecke hochinteressant. Kryptosysteme, deren Sicherheit darauf beruht, dass kürzeste Vektoren in Gittern gefunden werden müssen, scheinen gegen Angriffe resistent zu sein.

Allerdings hat die Sache einen Haken. Im Jahre 1982 veröffentlichten A. K. Lenstra, H. W. Lenstra und L. Lovász einen effizienten Algorithmus – den nach den Erfindern benannten LLL-Algorithmus – der zwar nicht immer einen kürzesten Vektor in Gittern, aber immerhin einen „relativ kurzen“ Vektor in Gittern mit Basen in $\mathbb{Q}^n$ berechnet.

Der LLL-Algorithmus hat weit reichende Folgerungen in verschiedenen Teilgebieten der Mathematik, insbesondere in der Computeralgebra. Dieser Algorithmus steht im Zentrum dieser Kurseinheit.

In Abschnitt 11.1 führen wir in die Theorie ganzzahliger Gitter ein und stellen erste Abschätzungen für die Längen von Vektoren in Gittern vor.

Abschnitt 11.2 widmet sich dem LLL-Algorithmus. Vereinfacht gesagt ist der LLL-Algorithmus der Versuch, das Gram-Schmidt Orthogonalisierungsverfahren, das

Sie in der Linearen Algebra II kennen gelernt haben, für ganzzahlige Linearkombinationen von Vektoren zu kopieren.

In Abschnitt 11.3 zeigen wir, wie der LLL-Algorithmus dazu benutzt wurde, ein sehr vielversprechendes Kryptosystem zu brechen.

Kapitel 11

Gitter

11.1 Gitter und Basen

Alle in dieser Kurseinheit betrachteten Vektoren in $\mathbb{R}^n$ beziehungsweise in $\mathbb{Q}^n$ sind Spaltenvektoren. Wir betrachten $\mathbb{R}^n$ als kanonischen n-dimensionalen Euklidischen Raum. Das Skalarprodukt bezeichnen wir mit $\langle\ ,\ \rangle$, also $\langle v, w\rangle = v^T w$ für alle $v, w \in \mathbb{R}^n$. Dabei ist v^T der zu v transponierte Vektor. Für Vektoren $v \in \mathbb{R}^n$ bezeichnen wir mit $\|v\|$ die Euklidische Norm (Länge) von v, also $\|v\| = \sqrt{v^T v}$. Der Abstand zwischen Vektoren $v, w \in \mathbb{R}^n$ ist $d(v, w) = \|v - w\|$.

11.1.1 Charakterisierung von Gittern

Wir beginnen mit der Definition des zentralen Begriffes dieser Kurseinheit.

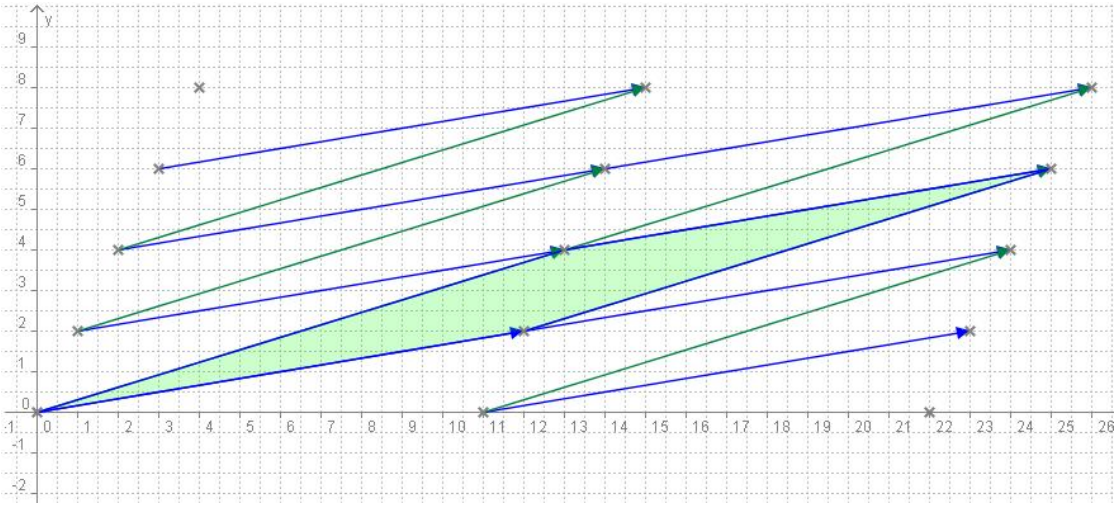
11.1.1 Definition Sei $(a_1, \ldots, a_n)$ eine Basis von $\mathbb{R}^n$. Die Menge

$$L(a_1, \ldots, a_n) = \left\{ \sum_{i=1}^{n} \lambda_i a_i \mid \lambda_i \in \mathbb{Z} \right\}$$

aller ganzahligen Linearkombinationen der Vektoren $a_1, \ldots, a_n$ wird ein **Gitter mit Basis** $(a_1, \ldots, a_n)$ genannt.

Das Gitter in $\mathbb{R}^2$ mit Basis $\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$ ist also die Menge $\mathbb{Z} \times \mathbb{Z}$.

11.1.2 Beispiel Seien $a_1 = \begin{pmatrix} 12 \\ 2 \end{pmatrix}$ und $a_2 = \begin{pmatrix} 13 \\ 4 \end{pmatrix}$. Die folgende Grafik zeigt die Punkte $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ in $L(a_1, a_2)$ mit $0 \leq x_1 \leq 26$ und $0 \leq x_2 \leq 8$. Schattiert dargestellt ist auch das Parallelogramm, das durch a_1 und a_2 aufgespannt wird.



Gitter in $\mathbb{R}^n$ sind mit der Addition von Vektoren Untergruppen von $(\mathbb{R}^n, +)$. Darüber hinaus ist ein Gitter in $\mathbb{R}^n$ eine diskrete Teilmenge von $\mathbb{R}^n$ im folgenden Sinne:

11.1.3 Definition Eine Teilmenge T eines topologischen Raumes heißt **diskret**, wenn es zu jedem $t \in T$ eine Umgebung V so gibt, dass $V \cap T = \{t\}$ ist.

Mit dieser Terminologie sind Gitter L in $\mathbb{R}^n$ also diskrete, additive Untergruppen von $\mathbb{R}^n$ mit $\langle L \rangle = \mathbb{R}^n$. Dabei bezeichnet $\langle L \rangle$ das Erzeugnis von L. Auch die Umkehrung gilt, das heißt, jede diskrete additive Untergruppe U von $\mathbb{R}^n$ mit $\langle U \rangle = \mathbb{R}^n$ ist ein Gitter. Da wir dieses Ergebnis im Folgenden aber nicht benötigen werden, verzichten wir auf einen Beweis.

11.1.2 Die Determinante eines Gitters

Gitter haben – wie Vektorräume – viele Basen. Im folgenden Abschnitt werden wir zu Gittern ganz besonders „schöne“ Basen konstruieren. Dabei wollen wir zunächst untersuchen, wie die Matrix für die Basistransformation von einer Basis eines Gitters zu einer anderen Basis des Gitters beschaffen ist. Zur Vereinfachung führen wir folgende Notation ein.

11.1.4 Notation Sei $(a_1, \ldots, a_n)$ eine Basis von $\mathbb{R}^n$. Die Matrix A, die die Vektoren $a_1, \ldots, a_n$ als Spalten enthält, wird mit $A = \big(a_1 | \cdots | a_n\big)$ bezeichnet.

11.1.5 Proposition Sei $L = L(a_1, \ldots, a_n) \subseteq \mathbb{R}^n$ ein Gitter mit Basis $(a_1, \ldots, a_n)$. Die folgenden Aussagen sind äquivalent:

(a) Die Vektoren $b_1, \ldots, b_n \in L$ bilden eine Basis von L.

(b) Es gibt eine invertierbare Matrix $U \in \mathrm{M}_{nn}(\mathbb{Z})$ mit

$$\big(b_1 | \cdots | b_n\big) = \big(a_1 | \cdots | a_n\big)\, U.$$

Beweis:

(a)⇒(b) Sei $U = (u_{ij})$ die Matrix für den Basiswechsel von $(a_1, \ldots, a_n)$ nach $(b_1, \ldots, b_n)$. Dann gilt $\big(b_1 | \cdots | b_n\big) = \big(a_1 | \cdots | a_n\big)\, U$. Es folgt $b_i = \sum_{j=1}^{n} u_{ji} a_j$ für alle $1 \leq i \leq n$. Da $b_i \in L(a_1, \ldots, a_n)$, gibt es eine Linearkombination von b_i der Vektoren $a_1, \ldots, a_n$ mit Koeffizienten in $\mathbb{Z}$. Da $(a_1, \ldots, a_n)$ eine Basis von $\mathbb{R}^n$ ist, ist diese Linearkombination eindeutig, und es folgt $u_{ij} \in \mathbb{Z}$ für alle $1 \leq i, j \leq n$.

Sei $U^{-1} = V = (v_{ij})$ die Matrix für den Basiswechsel von $(b_1, \ldots, b_n)$ nach $(a_1, \ldots, a_n)$. Dann gilt $a_i = \sum_{j=1}^{n} v_{ji} b_j$ für alle $1 \leq i \leq n$. Wie oben folgt $v_{ij} \in \mathbb{Z}$ für alle $1 \leq i, j \leq n$.

(b)⇒(a) Sei $U = (u_{ij}) \in \mathrm{M}_{nn}(\mathbb{Z})$ invertierbar mit $\big(b_1 | \cdots | b_n\big) = \big(a_1 | \cdots | a_n\big)\, U$. Dann ist $(b_1, \ldots, b_n)$ eine Basis von $\mathbb{R}^n$. Für alle $1 \leq i \leq n$ gilt $b_i = \sum_{j=1}^{n} u_{ji} a_j$, und es folgt, dass jedes Element in $L(b_1, \ldots, b_n)$ auch ein Element in $L(a_1, \ldots, a_n)$ ist. Umgekehrt, da $U^{-1} \in \mathrm{M}_{nn}(\mathbb{Z})$, folgt analog, dass jedes Element in $L(a_1, \ldots, a_n)$ auch in $L(b_1, \ldots, b_n)$ liegt. Es gilt also $L(a_1, \ldots, a_n) = L(b_1, \ldots, b_n)$.

□

Wir haben in der Linearen Algebra I gesehen, dass eine Matrix $U \in \mathrm{M}_{nn}(\mathbb{Z})$ genau dann invertierbar ist, wenn ihre Determinante 1 oder -1 ist. Mit dem Determinantenmultiplikationssatz folgt:

11.1.6 Korollar Seien $(a_1, \ldots, a_n)$ und $(b_1, \ldots, b_n)$ Basen eines Gitters L. Dann gilt

$$\det\left(a_1|\cdots|a_n\right) = \pm\det\left(b_1|\cdots|b_n\right).$$

□

Insbesondere gilt $|\det\left(a_1|\cdots|a_n\right)| = |\det\left(b_1|\cdots|b_n\right)|$ für alle Basen $(a_1, \ldots, a_n)$ und $(b_1, \ldots, b_n)$ eines Gitters L. Dies ermöglicht es uns, die Determinante eines Gitters wie folgt zu definieren:

11.1.7 Definition Sei $L = L(a_1, \ldots, a_n)$ ein Gitter in $\mathbb{R}^n$. Die **Determinante** $\det L$ von L ist definiert als $\det L = |\det\left(a_1|\cdots|a_n\right)|$.

Wir werden jetzt eine obere Schranke für die Determinante eines Gitters herleiten.

In der Linearen Algebra II haben wir mit der Gram-Schmidt-Orthonormalisierung ein Verfahren kennen gelernt, wie wir aus einer Basis von $\mathbb{R}^n$ eine Orthonormalbasis konstruieren können. In dieser Kurseinheit werden wir nicht an Orthonormalbasen interessiert sein – wohl aber an Orthogonalbasen. Auch diese können wir mit Hilfe des Verfahrens von Gram-Schmidt, das wir hier kurz wiederholen wollen, konstruieren.

Sei $(a_1, \ldots, a_n)$ eine Basis von $\mathbb{R}^n$. Wir definieren Vektoren $a_1^*, \ldots, a_n^*$ induktiv durch

$$a_i^* = a_i - \sum_{1 \le j < i} \mu_{ij} a_j^*, \text{ wobei } \mu_{ij} = \frac{\langle a_i, a_j^* \rangle}{\|a_j^*\|^2} \text{ für alle } 1 \le j < i.$$

Insbesondere ist $a_1 = a_1^*$.

11.1.8 Definition Sei $(a_1, \ldots, a_n)$ eine Basis von $\mathbb{R}^n$. Wir nennen $(a_1^*, \ldots, a_n^*)$ die **Gram-Schmidt-Orthogonalbasis** zu $(a_1, \ldots, a_n)$, und die Vektoren a_i^* zusammen mit den oben definierten μ_{ij} die **Gram-Schmidt-Orthogonalisierung** von $(a_1, \ldots, a_n)$.

Beachten Sie, dass die Gram-Schmidt-Orthogonalbasis zu einer Basis eines Gitters im Allgemeinen keine Basis des Gitters ist.

11.1.9 Aufgabe Seien $a_1 = \begin{pmatrix} 12 \\ 2 \end{pmatrix}, a_2 = \begin{pmatrix} 13 \\ 4 \end{pmatrix} \in \mathbb{R}^2$. Bestimmen Sie die Gram-Schmidt-Orthogonalisierung von (a_1, a_2). Skizzieren Sie die Vektoren a_1, a_2, a_1^* und a_2^* in der Euklidischen Ebene.

Der folgende Satz, der im Wesentlichen schon in der Linearen Algebra II bewiesen wurde, fasst die wichtigsten Eigenschaften von Orthogonalbasen zusammen.

11.1.10 Satz Sei $\mathcal{B} = (a_1, \ldots, a_n)$ eine Basis von $\mathbb{R}^n$, und sei $\mathcal{B}' = (a_1^*, \ldots, a_n^*)$ die Gram-Schmidt-Orthogonalbasis zu $\mathcal{B}$. Dann gilt:

1. $\mathcal{B}'$ ist eine Basis von $\mathbb{R}^n$.
2. $\langle a_i^*, a_j^* \rangle = 0$ für alle $1 \leq i, j \leq n$ mit $i \neq j$.
3. $\langle a_1, \ldots, a_k \rangle = \langle a_1^*, \ldots, a_k^* \rangle$ für alle $1 \leq k \leq n$.
4. Die Matrix $M = {}_{\mathcal{B}}\mathrm{M}_{\mathcal{B}'}(\mathrm{id})$ für den Basiswechsel von $\mathcal{B}$ nach $\mathcal{B}'$ ist
$$M = \begin{pmatrix} 1 & \mu_{21} & \cdots & \mu_{n1} \\ 0 & 1 & \cdots & \mu_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}, \text{ also } \left(a_1^* | \cdots | a_n^*\right) M = \left(a_1 | \cdots | a_n\right).$$
5. $\det\left(a_1 | \cdots | a_n\right) = \det\left(a_1^* | \cdots | a_n^*\right)$.
6. $\|a_i^*\| \leq \|a_i\|$ für alle $1 \leq i \leq n$.

Beweis: Die ersten drei Aussagen folgen analog zu dem Beweis in der Linearen Algebra II. Die vierte Aussage folgt unmittelbar aus der Definition der Vektoren a_i^*. Da die Matrix für den Basiswechsel von $\mathcal{B}$ nach $\mathcal{B}'$ die Determinante 1 hat, folgt die fünfte Aussage aus dem Determinantenmultiplikationssatz. Es bleibt nur noch die sechste Aussage zu beweisen. Für alle $1 \leq i \leq n$ gilt:

$$\begin{aligned} \langle a_i, a_i \rangle &= \langle a_i^* + \sum_{1 \leq j < i} \mu_{ij} a_j^*, a_i^* + \sum_{1 \leq j < i} \mu_{ij} a_j^* \rangle \\ &= \langle a_i^*, a_i^* \rangle + 2\langle a_i^*, \sum_{1 \leq j < i} \mu_{ij} a_j^* \rangle + \langle \sum_{1 \leq j < i} \mu_{ij} a_j^*, \sum_{1 \leq j < i} \mu_{ij} a_j^* \rangle \\ &\geq \langle a_i^*, a_i^* \rangle, \end{aligned}$$

denn $2\langle a_i^*, \sum_{1 \leq j < i} \mu_{ij} a_j^* \rangle = 0$, mit der zweiten Aussage, und $\langle \sum_{1 \leq j < i} \mu_{ij} a_j^*, \sum_{1 \leq j < i} \mu_{ij} a_j^* \rangle \geq 0$, da $\langle\ ,\ \rangle$ ein Skalarprodukt ist. □

Als Folgerung aus diesem Satz und der Charakterisierung der orthogonalen Matrizen in der Linearen Algebra II erhalten wir die Hadamard'sche Abschätzung, die nach dem französischen Mathematiker Jacques Salomon Hadamard (1865-1963) benannt ist.

11.1.11 Satz (Hadamard'sche Ungleichung)

Sei $A = \big(a_1|\cdots|a_n\big) \in \mathrm{M}_{nn}(\mathbb{R})$. Dann gilt $|\det(A)| \leq \prod_{i=1}^{n} \|a_i\|$. Ist $(a_1, \ldots, a_n)$ eine Orthogonalbasis, so gilt $|\det(A)| = \prod_{i=1}^{n} \|a_i\|$.

Beweis: Die Ungleichung ist sicherlich richtig, wenn A nicht invertierbar ist. Wir können also annehmen, dass die Spalten von A eine Basis von $\mathbb{R}^n$ bilden. Mit der fünften Aussage von Satz 11.1.10 gilt:

$$|\det\big(a_1|\cdots|a_n\big)| = |\det\big(a_1^*|\cdots|a_n^*\big)| = \prod_{i=1}^{n} \|a_i^*\| \cdot |\det\Big(\tfrac{1}{\|a_1^*\|}a_1^*|\cdots|\tfrac{1}{\|a_n^*\|}a_n^*\Big)|.$$

Die Matrix $\Big(\frac{1}{\|a_1^*\|}a_1^*|\cdots|\frac{1}{\|a_n^*\|}a_n^*\Big)$ ist orthogonal, denn ihre Spalten sind eine Orthonormalbasis von $\mathbb{R}^n$. Somit ist ihre Determinante 1 oder -1, wie in der Linearen Algebra II gezeigt wurde. Es folgt $|\det\big(a_1|\cdots|a_n\big)| = \prod_{i=1}^{n} \|a_i^*\|$. Mit der letzten Aussage von Satz 11.1.10 folgt die Behauptung. □

Als unmittelbare Folgerung dieses Satzes erhalten wir:

11.1.12 Korollar Sei $L(a_1, \ldots, a_n)$ ein Gitter in $\mathbb{R}^n$. Dann gilt

$$\det(L(a_1, \ldots, a_n)) \leq \prod_{i=1}^{n} \|a_i\|.$$

□

Diese obere Abschätzung der Determinante eines Gitters L hängt von der Auswahl einer Basis von L ab. Es ist ein interessantes Problem, eine Basis $(a_1, \ldots, a_n)$ von L zu bestimmen, so dass $\prod_{i=1}^{n} \|a_i\|$ minimal ist. Dieser Frage widmet sich die Mathematik schon seit Langem. Die ersten Verfahren zur Bestimmung einer Gitterbasis für $n = 2$ und $n = 3$, die aus möglichst kurzen Vektoren besteht, gehen auf Lagrange, Gauß , und Dirichlet in der Mitte des 19. Jahrhunderts zurück. Hermite untersuchte in etwa zur selben Zeit diese Frage für beliebige $n \in \mathbb{N}$. Seither haben sich viele Mathematiker mit diesem Problem beschäftigt. Genannt seien A. Korkine, G. Zolotareff, H. Minkowski und C. L. Siegel. Es ist inzwischen bekannt, dass dieses Problem in die Klasse der so genannten NP-harten Probleme gehört. Von Problemen in dieser Klasse wird vermutet, dass es keine polynomialen Algorithmen zur

Lösung gibt. Sogar noch mehr: Wenn es für ein NP-hartes Problem einen polynomialen Algorithmus zur Lösung gibt, dann auch für alle anderen Probleme in NP. In dieser Klasse liegen so bekannte Probleme wie das Handelsreisendenproblem, das Stundenplanproblem, die Hamilton-Zyklen und noch viele andere bekannte, tatsächlich auftretende Probleme.

Es dauerte jedoch lange, bis bei diesem Problem ein wirklicher Durchbruch erzielt werden konnte. Im Jahre 1982 wurde von A. K. Lenstra, H. W. Lenstra und L. Lovász [LLL] ein Verfahren zur Berechnung von Gitterbasen veröffentlicht, das in Gittern effizient eine Basis bestimmt, die zwar nicht aus den kürzest möglichen, aber immerhin aus kurzen Vektoren besteht. In der Praxis sind die Vektoren der berechneten Basis sogar meist weitaus kürzer, als sich theoretisch vorhersagen lässt. Wir werden diesen Algorithmus in Abschnitt 11.2.2 vorstellen.

11.1.3 Kurze Vektoren in Gittern

Ein weiteres Problem, das in die Klasse der NP-harten Probleme gehört, ist das „Kürzester Vektor Problem“. Hier wird nach einem Algorithmus gesucht, den kürzesten Vektor $v \neq 0$ in einem gegebenen Gitter zu bestimmen. Dass dieses Problem NP-hart ist, wurde übrigens erst 1997 von Miklos Ajtai [A] bewiesen. Somit sind Kryptosysteme, deren Sicherheit darauf beruht, dass kürzeste Vektoren in Gittern gefunden werden müssen, natürlich sehr viel versprechend. Wir werden darauf später noch einmal eingehen. Wir werden in diesem Abschnitt obere und untere Schranken für die Längen von kürzesten Vektoren in Gittern angeben und aus diesen Schranken einige zahlentheoretische Folgerungen ziehen.

11.1.13 Proposition Sei $L = L(a_1, \ldots, a_n)$ ein Gitter in $\mathbb{R}^n$, und sei $(a_1^*, \ldots, a_n^*)$ die Gram-Schmidt-Orthogonalbasis von $(a_1, \ldots, a_n)$. Dann gilt

$$\|a\| \geq \min\{\|a_1^*\|, \ldots, \|a_n^*\|\}$$

für alle $a \in L \setminus \{0\}$.

Beweis: Sei $a = \sum_{i=1}^{n} \lambda_i a_i \in L \setminus \{0\}$, und sei k der größte Index, für den $\lambda_k \neq 0$ gilt. Wir setzen $\mu_{ii} = 1$ und substituieren $\sum_{1 \leq j \leq i} \mu_{ij} a_j^*$ für a_i und erhalten

$$a = \sum_{1 \leq i \leq k} \lambda_i \sum_{1 \leq j \leq i} \mu_{ij} a_j^* = \lambda_k a_k^* + \sum_{1 \leq i < k} \nu_i a_i^*$$

für geeignete $\nu_i \in \mathbb{R}$. Dann gilt

$$\begin{aligned}
\|a\|^2 &= \langle \lambda_k a_k^* + \sum_{1\le i<k} \nu_i a_i^*, \lambda_k a_k^* + \sum_{1\le i<k} \nu_i a_i^* \rangle \\
&= \lambda_k^2 \|a_k^*\|^2 + \sum_{1\le i<k} \nu_i^2 \|a_i^*\|^2 \\
&\geq \lambda_k^2 \|a_k^*\|^2 \\
&\geq \|a_k^*\|^2 \\
&\geq \min\{\|a_1^*\|^2, \ldots, \|a_n^*\|^2\}.
\end{aligned}$$

Dabei haben wir benutzt, dass $(a_1^*, \ldots, a_n^*)$ eine Orthogonalbasis ist, und dass $\lambda_k \in \mathbb{Z}$ gilt. Es folgt $\|a\| \geq \min\{\|a_1^*\|, \ldots, \|a_n^*\|\}$, die Behauptung. □

Ein kürzester Vektor $v \neq 0$ in einem Gitter mit Basis $(a_1, \ldots, a_n)$ ist also immer mindestens so lang, wie ein kürzester Vektor in der Gram-Schmidt-Orthogonalbasis zu $(a_1, \ldots, a_n)$. Zu beachten ist allerdings, dass die Vektoren in der Gram-Schmidt-Orthogonalbasis in der Regel nicht in dem Gitter liegen.

Eine obere Schranke für die Länge eines kürzesten Vektors in einem Gitter liefert der so genannte Gittersatz von Minkowski (1864-1909). Wir formulieren den Gittersatz hier in einem Spezialfall, den wir im Folgenden benutzen werden.

11.1.14 Satz (Minkowski's Gittersatz)

Sei $\omega(n)$ das Volumen der Einheitskugel in $\mathbb{R}^n$, also $\omega(1) = 2$, $\omega(2) = \pi$ und $\omega(n) = \omega(n-2)\frac{2\pi}{n}$ für alle $n > 2$. Sei $a \neq 0$ der kürzeste Vektor in einem Gitter L in $\mathbb{R}^n$. Dann gilt

$$\|a\| \leq 2 \left(\frac{\det L}{\omega(n)} \right)^{\frac{1}{n}}.$$

Wir werden diesen Satz hier nicht beweisen, denn der Beweis greift auf analytische Methoden zurück, die wir im Weiteren nicht benötigen werden.

Obgleich der Minkowskische Gittersatz mit Argumenten der Analysis und Maßtheorie bewiesen wird, hat er sehr schöne Anwendungen in der elementaren Zahlentheorie. Mit seiner Hilfe können alte Ergebnisse, die schon Fermat, Euler und Lagrange bekannt waren, erneut elegant bewiesen werden. Wir illustrieren das an zwei Beispielen: dem Zwei-Quadrate-Satz und dem Vier-Quadrate-Satz.

Für den Zwei-Quadrate-Satz benötigen wir noch eine Vorüberlegung.

11.1.15 Lemma Sei p eine Primzahl. Genau dann gibt es ein $u \in \mathbb{Z}$ mit $u^2 \equiv -1 \,(\mathrm{mod} p)$, wenn $p = 4k + 1$ ist, für ein $k \in \mathbb{N}$.

Beweis: Die Aussage ist gerade die Aussage 3.) in Lemma 7.3.7. □

11.1.16 Satz (Zwei-Quadrate-Satz (Fermat, Euler))

Jede Primzahl der Form $p = 4k+1$, $k \in \mathbb{N}$, ist Summe von zwei Quadraten ganzer Zahlen.

Beweis: Sei $p = 4k + 1$, $k \in \mathbb{N}$, ein Primzahl, und sei $u \in \mathbb{Z}$ mit $u^2 \equiv -1 \,(\mathrm{mod} p)$.

Sei $L = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \mid y \equiv ux \,(\mathrm{mod} p) \right\}$. Dann ist L ein Gitter mit Basis $\left(\begin{pmatrix} 1 \\ u \end{pmatrix}, \begin{pmatrix} 0 \\ p \end{pmatrix} \right)$. Es folgt $\det L = p$.

Sei $\begin{pmatrix} x \\ y \end{pmatrix} \neq 0$ ein kürzester Vektor in L. Da $y \equiv ux \,(\mathrm{mod} p)$ und $u^2 \equiv -1 \,(\mathrm{mod} p)$ folgt, dass $x^2 + y^2$ durch p teilbar ist, also $x^2 + y^2 = lp$ mit $l \in \mathbb{N}$. Mit dem Gittersatz folgt

$$lp = x^2 + y^2 \leq 4 \frac{\det L}{\omega(2)} = \frac{4p}{\pi} < 2p.$$

Es folgt $l = 1$, also $p = x^2 + y^2$. □

Beachten Sie, dass der Beweis nicht konstruktiv ist. Er liefert keine Informationen darüber, wie die quadratischen Summanden bestimmt werden können.

Der Vier-Quadrate-Satz besagt, dass jede natürliche Zahl als Summe von vier Quadratzahlen geschrieben werden kann. Dabei dürfen als Summanden auch $0 = 0 \cdot 0$ auftauchen. Dabei machen wir uns zunächst klar, dass es ausreicht, diesen Satz für Primzahlen zu beweisen.

Dazu seien $x = \sum_{i=1}^{4} x_i^2$ und $y = \sum_{i=1}^{4} y_i^2$ ganze Zahlen, die Summen von vier Quadraten ganzer Zahlen sind. Dann gilt

$$\left(\sum_{i=1}^{4} x_i^2 \right) \left(\sum_{i=1}^{4} y_i^2 \right) = \left(\sum_{i=1}^{4} x_i y_i \right)^2 + u^2 + v^2 + w^2$$

wobei

$$u = -x_1 y_2 + x_2 y_1 - x_3 y_4 + x_4 y_3, \quad v = -x_1 y_3 + x_3 y_1 - x_4 y_2 + x_2 y_4$$

und

$$w = -x_1y_4 + x_4y_1 - x_2y_3 + x_3y_2.$$

Das Produkt von zwei Summen von vier Quadratzahlen ist also wieder die Summe von vier Quadratzahlen. Wenn also jede Primzahl ein Produkt von vier Quadratzahlen ist, so ist (mit Induktion nach der Anzahl der Primfaktoren von n) auch jede natürliche Zahl n eine Summe von vier Quadratzahlen.

Im Beweis des Vier-Quadrate-Satzes benötigen wir noch das folgende Lemma.

11.1.17 Lemma Sei $\mathbb{K}$ ein endlicher Körper, und seien $a, b, c \in \mathbb{K} \setminus \{0\}$. Dann gibt es $x, y \in \mathbb{K}$ mit $ax^2 + by^2 = c$.

Beweis: Seien $a, b, c \in \mathbb{K}^\times$. Sei $q = |\mathbb{K}|$. Da $\mathbb{K}^\times$ zyklisch ist, gibt es mindestens $\frac{q-1}{2}$ Elemente in $\mathbb{K}^\times$, die von der Form x^2 sind. Weiter ist $0 = 0^2$. Es gibt also mindestens $\frac{q+1}{2}$ Quadrate in $\mathbb{K}$. Es folgt

$$|\{ax^2 \mid x \in \mathbb{K}\}| \geq \frac{q+1}{2} \text{ und } |\{c - by^2 \mid y \in \mathbb{K}\}| \geq \frac{q+1}{2}.$$

Diese beiden Mengen können nicht disjunkt sein, denn anderenfalls hätte $\mathbb{K}$ mehr als q Elemente. Es gibt also ein Element $ax^2 = c - by^2$ in beiden Mengen. □

11.1.18 Satz (Vier-Quadrate-Satz (Fermat, Lagrange))

Jede natürliche Zahl ist Summe von vier Quadraten ganzer Zahlen.

Beweis: Wie wir vorher überlegt haben, reicht es, die Behauptung für Primzahlen zu beweisen. Offenbar ist $2 = 1^2 + 1^2 + 0^2 + 0^2$ Summe von vier Quadratzahlen. Sei also p eine ungerade Primzahl. Seien $u, v \in \mathbb{Z}$ mit $u^2 + v^2 + 1 = 0 \bmod p$. Solche Zahlen existieren mit dem Lemma. Wir definieren ein Gitter L durch

$$L = \left\{ \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \in \mathbb{Z}^4 \mid c \equiv ua + vb \bmod p, d \equiv ub - va \bmod p \right\}.$$

Die Nebenbedingungen implizieren (Beweis durch Nachrechnen), dass $\|x\|^2$ durch p teilbar ist, für alle $x \in L$.

Die Vektoren $\begin{pmatrix} 1 \\ 0 \\ u \\ -v \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ v \\ u \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ p \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ p \end{pmatrix}$ bilden eine Basis von L, und es gilt

$$\det L = |\det \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ -v & u & 0 & p \end{pmatrix}| = p^2.$$

Sei $\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$ der kürzeste Vektor in L. Mit dem Gittersatz gilt

$$kp = a^2 + b^2 + c^2 + d^2 \leq 4 \left(\frac{\det L}{\omega(4)} \right)^{\frac{1}{2}} = 4 \left(\frac{2p^2}{\pi^2} \right)^{\frac{1}{2}} = \frac{4\sqrt{2}}{\pi} p < 2p.$$

Es folgt $k = 1$, also $p = a^2 + b^2 + c^2 + d^2$. □

Außer diesen eher theoretischen Anwendungen des Gittersatzes werden wir später auch ganz praktische Folgerungen aus der Theorie über kurze Vektoren in Gittern kennenlernen.

11.2 Reduzierte Basen von Gittern

Wie oben bereits angesprochen, die Tatsache, dass es vermutlich keine effizienten Algorithmen gibt, die kürzeste Vektoren in Gittern finden, macht Gitter für die Entwicklung von Kryptosystemen hochinteressant.

Aber: Die Mathematik lehrt uns, dass wir vorsichtig sein müssen. Im Jahre 1982 entwickelten A.K. Lenstra, H.W.Lenstra und L. Lovász [LLL] einen Algorithmus, der in polynomialer Zeit „relativ kurze“ Vektoren in Gittern $L \subseteq \mathbb{Q}^n$ bestimmt. Wir werden diesen Algorithmus unten vorstellen. Dabei folgen wir nicht der Darstellung in [LLL], sondern der des Lehrbuchs „Modern Computer Algebra“ von J. von zur Gathen und J. Gerhard [vzGG].

Das Ergebnis von Lenstra, Lenstra und Lovász bedeutet nicht, dass ein Problem in der Klasse NP effizient gelöst werden konnte. Aber dennoch hat dieser Algorithmus, der zu Ehren der Erfinder „LLL-Algorithmus“ genannt wird, viele wichtige

Folgerungen in der reinen und der angewandten Mathematik. Eine Anwendung – das Brechen eines viel versprechenden Kryptosystems – werden wir im letzten Abschnitt vorstellen.

11.2.1 Reduzierte Basen und kurze Vektoren

Wir haben oben gesehen, dass die Länge eines kürzesten Vektors a in einem Gitter L mit Basis $(a_1, \ldots, a_n)$ immer mindestens so lang ist, wie ein Vektor in der Gram-Schmidt-Orthogonalbasis zu $(a_1, \ldots, a_n)$. Das Problem ist allerdings, dass der kürzeste Vektor in $(a_1^*, \ldots, a_n^*)$ in der Regel gar nicht in L liegt. Die Idee ist, eine „fast orthogonale“ Basis zu $(a_1, \ldots, a_n)$ zu konstruieren, die in L liegt. Dabei bedeutet „fast orthogonale“, dass die Gram-Schmidt-Orthogonalisierung durchgeführt wird, allerdings werden die auftretenden Koeffizienten zur nächstliegenden ganzen Zahl gerundet. Dazu aber mehr im folgenden Abschnitt. Wir beginnen mit einer Definition.

11.2.1 Definition Sei $(a_1, \ldots, a_n)$ eine Basis von $\mathbb{R}^n$, und sei $(a_1^*, \ldots, a_n^*)$ die zugehörige Gram-Schmidt-Orthogonalbasis. Die Basis $(a_1, \ldots, a_n)$ heißt **reduziert**, wenn $\|a_i^*\|^2 \leq 2\|a_{i+1}^*\|^2$ gilt, für alle $1 \leq i < n$.

11.2.2 Aufgabe Seien $a_1 = \begin{pmatrix} 12 \\ 2 \end{pmatrix}$, $a_2 = \begin{pmatrix} 13 \\ 4 \end{pmatrix} \in \mathbb{Z}^2$.

1. Beweisen Sie, dass die Basis (a_1, a_2) nicht reduziert ist.
2. Seien $b_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, b_2 = \begin{pmatrix} 9 \\ -4 \end{pmatrix}$. Beweisen Sie, dass auch (b_1, b_2) eine Basis von $L(a_1, a_2)$ ist.
3. Beweisen Sie, dass (b_1, b_2) eine reduzierte Basis ist.
4. Skizzieren Sie a_1, a_2, b_1, b_2 in der Euklidischen Ebene und überzeugen Sie sich davon, dass b_1 und b_2 „fast orthogonal“ sind.

11.2.3 Proposition Sei $(a_1, \ldots, a_n)$ eine reduzierte Basis eines Gitters L. Für alle $a \in L \setminus \{0\}$ gilt dann $\|a_1\| \leq 2^{\frac{n-1}{2}}\|a\|$.

Beweis: Es gilt $\|a_1\|^2 \leq \|a_1^*\|^2 \leq 2\|a_2^*\|^2 \leq \cdots \leq 2^{n-1}\|a_n^*\|^2$. Es folgt $\|a_i^*\|^2 \geq 2^{-(i-1)}\|a_1\|^2 \geq 2^{-(n-1)}\|a_1\|^2$ für alle $1 \leq i \leq n$. Da $\|a\| \geq \min\{\|a_1^*\|, \ldots, \|a_n^*\|\}$, folgt $\|a_1\| \leq 2^{\frac{n-1}{2}}\|a\|$, die Behauptung. □

Insbesondere ist also der erste Basisvektor einer reduzierten Basis eines Gitters L schlimmstenfalls um den Faktor $2^{\frac{n-1}{2}}$ größer als ein kürzester Vektor in L. Allerdings ist erst einmal gar nicht klar, dass jedes Gitter eine reduzierte Basis besitzt.

11.2.2 Der LLL-Algorithmus

Der LLL-Algorithmus berechnet eine reduzierte Basis eines Gitters L in $\mathbb{Z}^n$ aus einer beliebigen Basis von L. Auf den ersten Blick sieht die Annahme, dass alle Vektoren in L Einträge in $\mathbb{Z}$ haben, so aus, als würden wir weniger leisten, als wir versprochen hatten. Aber der LLL-Algorithmus liefert in der Tat auch reduzierte Basen von Gittern in $\mathbb{Q}^n$. Sei nämlich $L(a_1, \ldots, a_n) \subseteq \mathbb{Q}^n$ ein Gitter in $\mathbb{Q}^n$. Sei λ ein gemeinsames Vielfaches der Nenner der Einträge in den Vektoren $a_1, \ldots, a_n$. Dann sind $a'_1 = \lambda a_1, \ldots, a'_n = \lambda a_n$ Vektoren in $\mathbb{Z}^n$. Ist $(c_1, \ldots, c_n)$ eine reduzierte Basis von $L(a'_1, \ldots, a'_n)$, so ist $(\frac{1}{\lambda}c_1, \ldots, \frac{1}{\lambda}c_n)$ eine reduzierte Basis von $L(a_1, \ldots, a_n)$.

Im LLL-Algorithmus werden wir die folgende Notation verwenden:

11.2.4 Notation Für $\mu \in \mathbb{R}$ schreiben wir $\lceil \mu \rfloor = [\mu + \frac{1}{2}]$ für diejenige ganze Zahl, die am nächsten an μ liegt.

Wir stellen den LLL-Algorithmus wieder in einer vereinfachten Programmiersprache vor.

11.2.5 Algorithmus LLL-Algorithmus

Eingabe Linear unabhängige Spaltenvektoren $a_1, \ldots, a_n$ in $\mathbb{Z}^n$.

Ausgabe Eine reduzierte Basis $(b_1, \ldots, b_n)$ des Gitters $L = L(a_1, \ldots, a_n)$.

1. **for** $i = 1, \ldots, n$ **do** $b_i \leftarrow a_i$.

2. Berechne die Gram-Schmidt-Orthogonalisierung $(b_1^*, \ldots, b_n^*)$ und

$$M = \begin{pmatrix} 1 & \mu_{21} & \cdots & \mu_{n1} \\ 0 & 1 & \cdots & \mu_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

3. $i \leftarrow 2$

4. **while** $i \leq n$ **do**

5. **for** $j = i - 1, \ldots, 1$ **do**

$b_i \leftarrow b_i - \lceil \mu_{ij} \rfloor b_j$ und aktualisiere die Gram-Schmidt-Orthogonalisierung

6. **if** $i > 1$ und $\|b_{i-1}^*\|^2 > 2\|b_i^*\|^2$

then tausche b_i und b_{i-1}, aktualisiere die Gram-Schmidt-Orthogonalisierung,

$i \leftarrow i - 1$

else $i \leftarrow i + 1$

7. **übergebe** $b_1, \ldots, b_n$

Gehen wir das noch einmal durch. Zunächst wird im Schritt 2 die Gram-Schmidt-Orthogonalisierung der Eingangsvektoren berechnet. Danach durchlaufen wir nur noch die **while**-Schleife, die bei Schritt 4 beginnt und bei Schritt 6 endet, um dann, mit einem neuen i, wieder bei Schritt 4 einzusteigen. Der Schritt 5 ist ein Ersetzungsschritt. Hier wird b_i ein oder mehrere Male (wie oft, sagt die Bedingung $j = i - 1, \ldots, 1$) durch einen anderen Vektor ersetzt, wobei jedes Mal die Gram-Schmidt-Orthogonalisierung neu zu berechnen ist. Ist Schritt 5 abgearbeitet, so wenden wir uns Schritt 6 zu. In diesem Schritt gibt es zwei Möglichkeiten. Entweder wir vertauschen zwei Vektoren, berechnen die zugehörige Gram-Schmidt-Orthogonalisierung und setzen i auf $i - 1$, oder wir tun gar nichts, und setzen i auf $i + 1$. Dann geht es weiter mit Schritt 4. Die bis dahin berechneten Vektoren sind die $b_1, \ldots, b_n$ mit denen wir weiter rechnen. Diese Vektoren und das neu bestimmte i werden an Schritt 4 zurückgegeben, und das Ganze beginnt von vorne.

Der Algorithmus bricht ab, wenn wir die **while**-Schleife nicht mehr durchlaufen können, das heißt, wenn das i im vorherigen Durchlauf der Schleife n war und im Schritt 6 der Schleife auf $n + 1$ gesetzt wurde.

Es ist zu diesem Zeitpunkt überhaupt nicht klar, dass der Algorithmus jemals abbricht. Da wir i in Schritt 6 sowohl um 1 rauf als auch runter setzen können, ist nicht offensichtlich, dass wir nicht in eine Endlosschleife gelaufen sind. Und in der Tat, ein wichtiger Schritt wird sein, zu zeigen, dass uns die Endlosschleife erspart bleibt.

Bevor wir beweisen, dass der LLL-Algorithmus wirklich in endlicher Zeit eine reduzierte Basis berechnet, werden wir explizit ein Beispiel durchführen, in dem jeder der möglichen Schritte des Algorithmus' vorkommt.

11.2.6 Beispiel

Eingabe: $a_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$, $a_2 = \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix}$, $a_3 = \begin{pmatrix} 3 \\ 5 \\ 6 \end{pmatrix}$.

1. Sei $(b_1, b_2, b_3) = \left(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \\ 6 \end{pmatrix} \right)$.

2. Wir berechnen die Gram-Schmidt-Orthogonalisierung dieser Basis.

$b_1^* = b_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$. Es ist $\|b_1^*\|^2 = 3$.

$$\mu_{21} = \frac{\langle b_2, b_1^* \rangle}{\|b_1^*\|^2} = \frac{\left\langle \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle}{\left\| \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\|^2} = \frac{1}{3}.$$

$b_2^* = b_2 - \mu_{21} b_1^* = \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix} - \frac{1}{3} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{3} \begin{pmatrix} -4 \\ -1 \\ 5 \end{pmatrix}$. Es ist $\|b_2^*\|^2 = \frac{14}{3}$.

$$\mu_{31} = \frac{\langle b_3, b_1^* \rangle}{\|b_1^*\|^2} = \frac{\left\langle \begin{pmatrix} 3 \\ 5 \\ 6 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle}{\left\| \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\|^2} = \frac{14}{3}.$$

$$\mu_{32} = \frac{\langle b_3, b_2^* \rangle}{\|b_2^*\|^2} = \frac{\left\langle \begin{pmatrix} 3 \\ 5 \\ 6 \end{pmatrix}, \frac{1}{3} \begin{pmatrix} -4 \\ -1 \\ 5 \end{pmatrix} \right\rangle}{\left\| \frac{1}{3} \begin{pmatrix} -4 \\ -1 \\ 5 \end{pmatrix} \right\|^2} = \frac{13}{14}.$$

$b_3^* = b_3 - \mu_{31} b_1^* - \mu_{32} b_2^* = \begin{pmatrix} 3 \\ 5 \\ 6 \end{pmatrix} - \frac{14}{3} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} - \frac{13}{14} \cdot \frac{1}{3} \begin{pmatrix} -4 \\ -1 \\ 5 \end{pmatrix} = \frac{3}{14} \begin{pmatrix} -2 \\ 3 \\ -1 \end{pmatrix}$. Es ist $\|b_3^*\|^2 = \frac{9}{14}$.

Die Gram-Schmidt-Orthogonalisierung ist damit

$$\left(b_1^* = \begin{pmatrix}1\\1\\1\end{pmatrix}, b_2^* = \frac{1}{3}\begin{pmatrix}-4\\-1\\5\end{pmatrix}, b_3^* = \frac{3}{14}\begin{pmatrix}-2\\3\\-1\end{pmatrix}\right)$$

und

$$M = \begin{pmatrix}1 & \mu_{21} & \mu_{31}\\0 & 1 & \mu_{32}\\0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & \frac{1}{3} & \frac{14}{3}\\0 & 1 & \frac{13}{14}\\0 & 0 & 1\end{pmatrix}.$$

3. Die Initialisierung ist $i \leftarrow 2$, also $i = 2$.

4. Es ist $i = 2 \leq 3$. Wir durchlaufen die **while**-Schleife:

5. **for** $j = i - 1 = 1$ **do**

$$b_2 \leftarrow b_2 - \lceil \mu_{21} \rfloor b_1 = \begin{pmatrix}-1\\0\\2\end{pmatrix} - \left\lceil \frac{1}{3} \right\rfloor \begin{pmatrix}1\\1\\1\end{pmatrix} = b_2.$$

Die Gram-Schmidt-Orthogonalisierung von (b_1, b_2, b_3) ist die, die wir oben ausgerechnet haben, also

$$\left(b_1^* = \begin{pmatrix}1\\1\\1\end{pmatrix}, b_2^* = \frac{1}{3}\begin{pmatrix}-4\\-1\\5\end{pmatrix}, b_3^* = \frac{3}{14}\begin{pmatrix}-2\\3\\-1\end{pmatrix}\right)$$

und

$$M = \begin{pmatrix}1 & \mu_{21} & \mu_{31}\\0 & 1 & \mu_{32}\\0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & \frac{1}{3} & \frac{14}{3}\\0 & 1 & \frac{13}{14}\\0 & 0 & 1\end{pmatrix}.$$

6. Es sind $2 > 1$, $\|b_1^*\|^2 = 3$ und $\|b_2^*\|^2 = \frac{14}{3}$. Somit gilt $\|b_1^*\|^2 < 2\|b_2^*\|^2$. Wir setzen $i \leftarrow i + 1 = 3$.

4. Es ist $i = 3 \leq 3$. Wir durchlaufen die **while**-Schleife:

5. $j = 2$:

$$b_3 \leftarrow b_3 - \lceil \mu_{32} \rfloor b_2 = \begin{pmatrix}3\\5\\6\end{pmatrix} - \left\lceil \frac{13}{14} \right\rfloor \begin{pmatrix}-1\\0\\2\end{pmatrix} = \begin{pmatrix}4\\5\\4\end{pmatrix}.$$

Somit erhalten wir $\left(b_1 = \begin{pmatrix}1\\1\\1\end{pmatrix}, b_2 = \begin{pmatrix}-1\\0\\2\end{pmatrix} b_3 = \begin{pmatrix}4\\5\\4\end{pmatrix}\right)$.

Wir berechnen die Gram-Schmidt-Orthogonalisierung:

$b_1^* = \begin{pmatrix}1\\1\\1\end{pmatrix}$, $\mu_{21} = \frac{1}{3}$ und $b_2^* = \frac{1}{3}\begin{pmatrix}-4\\-1\\5\end{pmatrix}$, wie gehabt. Es sind

$$\mu_{31} = \frac{\left\langle \begin{pmatrix}4\\5\\4\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix} \right\rangle}{\left\| \begin{pmatrix}1\\1\\1\end{pmatrix} \right\|^2} = \frac{13}{3} \text{ und } \mu_{32} = \frac{\left\langle \begin{pmatrix}4\\5\\4\end{pmatrix}, \frac{1}{3}\begin{pmatrix}-4\\-1\\5\end{pmatrix} \right\rangle}{\left\| \frac{1}{3}\begin{pmatrix}-4\\-1\\5\end{pmatrix} \right\|^2} = -\frac{1}{14},$$

also

$$b_3^* = b_3 - \mu_{31}b_1^* - \mu_{32}b_2^* = \begin{pmatrix}4\\5\\4\end{pmatrix} - \frac{13}{3}\begin{pmatrix}1\\1\\1\end{pmatrix} + \frac{1}{14}\cdot\frac{1}{3}\begin{pmatrix}-4\\-1\\5\end{pmatrix} = \frac{3}{14}\begin{pmatrix}-2\\3\\-1\end{pmatrix}.$$

Es ist $\|b_3^*\|^2 = \frac{9}{14}$.

Die Gram-Schmidt-Orthogonalisierung ist somit

$$\left(b_1^* = \begin{pmatrix}1\\1\\1\end{pmatrix}, b_2^* = \frac{1}{3}\begin{pmatrix}-4\\-1\\5\end{pmatrix}, b_3^* = \frac{3}{14}\begin{pmatrix}-2\\3\\-1\end{pmatrix} \right)$$

und

$$M = \begin{pmatrix}1 & \mu_{21} & \mu_{31}\\0 & 1 & \mu_{32}\\0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & \frac{1}{3} & \frac{13}{3}\\0 & 1 & -\frac{1}{14}\\0 & 0 & 1\end{pmatrix}.$$

5. $j = 1$:

$b_3 \leftarrow b_3 - \lceil \mu_{31} \rfloor b_1 = \begin{pmatrix}4\\5\\4\end{pmatrix} - 4\begin{pmatrix}1\\1\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\end{pmatrix}$.

Die neue Basis ist dann $\left(\begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}-1\\0\\2\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix} \right)$. Wir bestimmen deren Gram-Schmidt-Orthogonalisierung.

Es sind $b_1^* = \begin{pmatrix}1\\1\\1\end{pmatrix}$, $\mu_{21} = \frac{1}{3}$ und $b_2^* = \frac{1}{3}\begin{pmatrix}-4\\-1\\5\end{pmatrix}$, wie gehabt. Es sind

$$\mu_{31} = \frac{\left\langle \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix} \right\rangle}{\left\| \begin{pmatrix}1\\1\\1\end{pmatrix} \right\|^2} = \frac{1}{3} \text{ und } \mu_{32} = \frac{\left\langle \begin{pmatrix}0\\1\\0\end{pmatrix}, \frac{1}{3}\begin{pmatrix}-4\\-1\\5\end{pmatrix} \right\rangle}{\left\| \frac{1}{3}\begin{pmatrix}-4\\-1\\5\end{pmatrix} \right\|^2} = -\frac{1}{14}.$$

Es folgt

$$b_3^* = b_3 - \mu_{31}b_1^* - \mu_{32}b_2^* = \begin{pmatrix}0\\1\\0\end{pmatrix} - \frac{1}{3}\begin{pmatrix}1\\1\\1\end{pmatrix} + \frac{1}{14}\cdot\frac{1}{3}\begin{pmatrix}-4\\-1\\5\end{pmatrix} = \frac{3}{14}\begin{pmatrix}-2\\3\\-1\end{pmatrix}.$$

Es ist $\|b_3^*\|^2 = \frac{9}{14}$. Die Gram-Schmidt-Orthogonalisierung ist damit

$$\left(b_1^* = \begin{pmatrix}1\\1\\1\end{pmatrix}, b_2^* = \frac{1}{3}\begin{pmatrix}-4\\-1\\5\end{pmatrix}, b_3^* = \frac{3}{14}\begin{pmatrix}-2\\3\\-1\end{pmatrix} \right)$$

und

$$M = \begin{pmatrix}1 & \mu_{21} & \mu_{31}\\0 & 1 & \mu_{32}\\0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & \frac{1}{3} & \frac{1}{3}\\0 & 1 & -\frac{1}{14}\\0 & 0 & 1\end{pmatrix}.$$

6. Es sind $i = 3 > 1$, $\|b_2^*\|^2 = \frac{14}{3}$ und $\|b_3^*\|^2 = \frac{9}{14}$. Es folgt $\|b_2^*\|^2 > 2\|b_3^*\|^2$, und jetzt müssen wir b_2 und b_3 vertauschen. Unsere neue Basis ist somit

$$\left(b_1 = \begin{pmatrix}1\\1\\1\end{pmatrix}, b_2 = \begin{pmatrix}0\\1\\0\end{pmatrix}, b_3 = \begin{pmatrix}-1\\0\\2\end{pmatrix} \right).$$

Wir berechnen die Gram-Schmidt-Orthogonalisierung.

$$b_1^* = \begin{pmatrix}1\\1\\1\end{pmatrix}, \mu_{21} = \frac{\left\langle \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix} \right\rangle}{\left\| \begin{pmatrix}1\\1\\1\end{pmatrix} \right\|^2} = \frac{1}{3}, \text{ und } b_2^* = \begin{pmatrix}0\\1\\0\end{pmatrix} - \frac{1}{3}\begin{pmatrix}1\\1\\1\end{pmatrix} = \frac{1}{3}\begin{pmatrix}-1\\2\\-1\end{pmatrix}.$$

Weiter sind

$$\mu_{31} = \frac{\left\langle \begin{pmatrix}-1\\0\\2\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix} \right\rangle}{\left\| \begin{pmatrix}1\\1\\1\end{pmatrix} \right\|^2} = \frac{1}{3} \text{ und } \mu_{32} = \frac{\left\langle \begin{pmatrix}-1\\0\\2\end{pmatrix}, \frac{1}{3}\begin{pmatrix}-1\\2\\-1\end{pmatrix} \right\rangle}{\left\| \frac{1}{3}\begin{pmatrix}-1\\2\\-1\end{pmatrix} \right\|^2} = -\frac{1}{2}.$$

Es folgt

$$b_3^* = \begin{pmatrix}-1\\0\\2\end{pmatrix} - \frac{1}{3}\begin{pmatrix}1\\1\\1\end{pmatrix} + \frac{1}{2}\cdot\frac{1}{3}\begin{pmatrix}-1\\2\\-1\end{pmatrix} = \frac{3}{2}\begin{pmatrix}-1\\0\\1\end{pmatrix}.$$

Es ist $\|b_3^*\|^2 = \frac{9}{2}$.

Die Gram-Schmidt-Orthogonalisierung ist somit:

$$\left(b_1^* = \begin{pmatrix}1\\1\\1\end{pmatrix}, b_2^* = \frac{1}{3}\begin{pmatrix}-1\\2\\-1\end{pmatrix}, b_3^* = \frac{3}{2}\begin{pmatrix}-1\\0\\1\end{pmatrix} \right)$$

und

$$M = \begin{pmatrix}1 & \mu_{21} & \mu_{31}\\0 & 1 & \mu_{32}\\0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & \frac{1}{3} & \frac{1}{3}\\0 & 1 & -\frac{1}{2}\\0 & 0 & 1\end{pmatrix}.$$

Es wird i auf 2 gesetzt.

4. Es ist $i = 2 \leq 3$. Wir durchlaufen die **while**-Schleife:

5. **for** $j = i - 1 = 1$ **do**

$b_2 \leftarrow b_2 - \lceil \mu_{21} \rfloor b_1 = \begin{pmatrix}0\\1\\0\end{pmatrix}$. Die Gram-Schmidt-Orthogonalisierung von (b_1, b_2, b_3) ist die, die wir oben ausgerechnet haben.

6. Es ist $i = 2 > 1$, und $\|b_1^*\|^2 = 3$, und $\|b_2^*\|^2 = \frac{2}{3}$. Es folgt $\|b_1^*\|^2 > 2\|b_2^*\|^2$, und wieder müssen wir tauschen. Die neue Basis ist

$$\left(b_1 = \begin{pmatrix}0\\1\\0\end{pmatrix}, b_2 = \begin{pmatrix}1\\1\\1\end{pmatrix}, b_3 = \begin{pmatrix}-1\\0\\2\end{pmatrix} \right).$$

Wir bestimmen die zugehörige Gram-Schmidt-Orthogonalisierung.

$b_1^* = \begin{pmatrix}0\\1\\0\end{pmatrix}$, $\mu_{21} = \dfrac{\left\langle \begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix} \right\rangle}{\left\| \begin{pmatrix}0\\1\\0\end{pmatrix} \right\|^2} = 1$, und $b_2^* = \begin{pmatrix}1\\1\\1\end{pmatrix} - \begin{pmatrix}0\\1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\1\end{pmatrix}$. Weiter sind

$$\mu_{31} = \frac{\left\langle \begin{pmatrix}-1\\0\\2\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix} \right\rangle}{\left\| \begin{pmatrix}0\\1\\0\end{pmatrix} \right\|^2} = 0 \text{ und } \mu_{32} = \frac{\left\langle \begin{pmatrix}-1\\0\\2\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix} \right\rangle}{\left\| \begin{pmatrix}1\\0\\1\end{pmatrix} \right\|^2} = \frac{1}{2}.$$

Es folgt $b_3^* = \begin{pmatrix}-1\\0\\2\end{pmatrix} - \frac{1}{2}\begin{pmatrix}1\\0\\1\end{pmatrix} = \frac{3}{2}\begin{pmatrix}-1\\0\\1\end{pmatrix}$. Die Gram-Schmidt-Orthogonalisierung ist damit

$$\left(b_1^* = \begin{pmatrix}0\\1\\0\end{pmatrix}, b_2^* = \begin{pmatrix}1\\0\\1\end{pmatrix}, b_3^* = \frac{3}{2}\begin{pmatrix}-1\\0\\1\end{pmatrix} \right)$$

und

$$M = \begin{pmatrix}1 & \mu_{21} & \mu_{31}\\0 & 1 & \mu_{32}\\0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 1 & 0\\0 & 1 & \frac{1}{2}\\0 & 0 & 1\end{pmatrix}.$$

Jetzt wird i auf 1 gesetzt.

4. Es ist $i = 1 \leq 3$. Wir durchlaufen die **while**-Schleife:

5. **for** $j = i - 1 = 0$ **do**
Wir können keinen Vektor ersetzen und gehen zu Schritt 6.

6. Da $i = 1$, müssen wir die **else**-Option dieses Schrittes wählen. Wir setzen also $i = 2$.

4. Es ist $i = 2 \leq 3$. Wir durchlaufen die **while**-Schleife:

5. **for** $j = i - 1 = 1$ **do**

$$b_2 \leftarrow b_2 - \lceil \mu_{21} \rfloor b_1 = \begin{pmatrix}1\\1\\1\end{pmatrix} - \begin{pmatrix}0\\1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\1\end{pmatrix}.$$

Wir berechnen die zugehörige Gram-Schmidt-Orthogonalisierung:

$b_1^* = \begin{pmatrix}0\\1\\0\end{pmatrix}$, $\mu_{21} = \dfrac{\left\langle \begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix} \right\rangle}{\left\| \begin{pmatrix}0\\1\\0\end{pmatrix} \right\|^2} = 0$, und $b_2^* = \begin{pmatrix}1\\0\\1\end{pmatrix}$. Weiter sind

$$\mu_{31} = \frac{\left\langle \begin{pmatrix}-1\\0\\2\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix} \right\rangle}{\left\| \begin{pmatrix}0\\1\\0\end{pmatrix} \right\|^2} = 0 \text{ und } \mu_{32} = \frac{\left\langle \begin{pmatrix}-1\\0\\2\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix} \right\rangle}{\left\| \begin{pmatrix}1\\0\\1\end{pmatrix} \right\|^2} = \frac{1}{2}.$$

Es folgt $b_3^* = \begin{pmatrix}-1\\0\\2\end{pmatrix} - \frac{1}{2}\begin{pmatrix}1\\0\\1\end{pmatrix} = \frac{3}{2}\begin{pmatrix}-1\\0\\1\end{pmatrix}$. Die Gram-Schmidt-Orthogonalisierung ist damit

$$\left(\begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix}, \frac{3}{2}\begin{pmatrix}-1\\0\\1\end{pmatrix} \right)$$

und

$$M = \begin{pmatrix}1 & \mu_{21} & \mu_{31}\\ 0 & 1 & \mu_{32}\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & \frac{1}{2}\\ 0 & 0 & 1\end{pmatrix}.$$

6. Es ist $i = 2 > 1$ und $\|b_1^*\|^2 = 1 \leq 2\|b_2^*\|^2 = 4$, und wir setzen $i = 3$.

4. Es ist $i = 3 \leq 3$. Wir durchlaufen die **while**-Schleife:

5. $j = 2$

$$b_3 \leftarrow b_3 - \lceil \mu_{32} \rfloor b_2 = \begin{pmatrix}-1\\0\\2\end{pmatrix} - \begin{pmatrix}1\\0\\1\end{pmatrix} = \begin{pmatrix}-2\\0\\1\end{pmatrix}$$

Es sind $\mu_{21} = 0$, $\mu_{31} = 0$ und $\mu_{32} = -\frac{1}{2}$. Die Gram-Schmidt-Orthogonalisierung ist somit

$$\left(\begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix}, \frac{3}{2}\begin{pmatrix}-1\\0\\1\end{pmatrix} \right)$$

und

$$M = \begin{pmatrix} 1 & \mu_{21} & \mu_{31} \\ 0 & 1 & \mu_{32} \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -\frac{1}{2} \\ 0 & 0 & 1 \end{pmatrix}.$$

5. $j = 1$:
$b_3 \leftarrow b_3 - \lceil \mu_{31} \rfloor b_2 = b_3$. Die Gram-Schmidt-Orthogonalisierung bleibt unverändert.

6. Es ist $\|b_2^*\|^2 = 2 < 2\|b_3^*\|^2 = 9$. Wir setzen $i = 4$, und die **while**-Schleife lässt sich nicht erneut durchführen.

7. $\left(\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -2 \\ 0 \\ 1 \end{pmatrix} \right)$, eine reduzierte Basis von $L(a_1, a_2, a_3)$.

Wir werden zuerst zeigen, dass der LLL-Algorithmus eine reduzierte Basis liefert, sofern er abbricht.

Dazu erinnern wir an das orthogonale Komplement zu einem Unterraum:

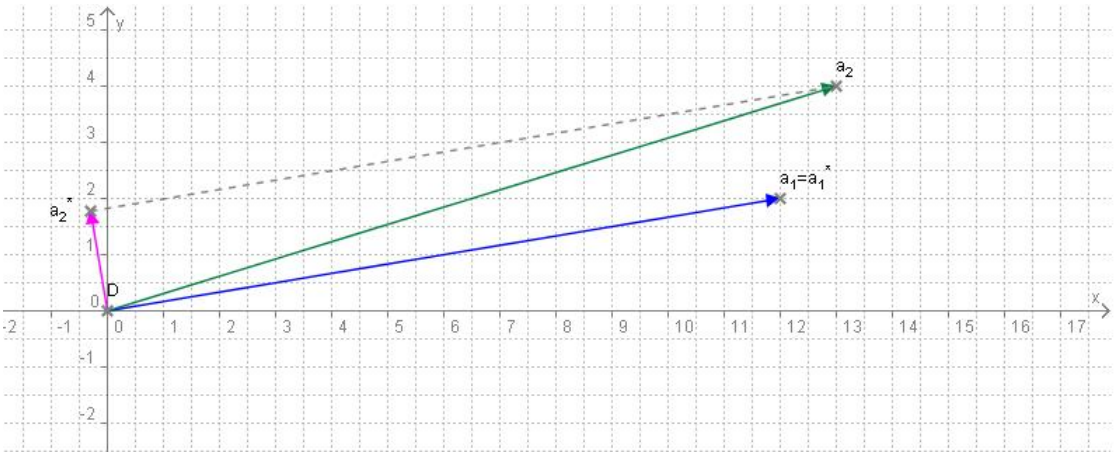
11.2.7 Definition Sei U ein Unterraum von $\mathbb{R}^n$. Das **orthogonale Komplement** $U^\perp$ zu U ist der Vektorraum $U^\perp = \{v \in \mathbb{R}^n \mid \langle v, u \rangle = 0 \text{ für alle } u \in U\}$.

Wir haben in der Linearen Algebra II gesehen, dass $U^\perp$ in der Tat ein Vektorraum ist, und es gilt $\mathbb{R}^n = U \oplus U^\perp$. Für alle $v \in \mathbb{R}^n$ gibt es dann eindeutig bestimmte $u \in U$ und $u' \in U^\perp$ mit $v = u + u'$. Die lineare Abbildung $\pi : \mathbb{R}^n \to \mathbb{R}^n$ mit $\pi(v) = \pi(u + u') = u'$ für alle $v = u + u'$, $u \in U$, $u' \in U^\perp$, wird die **orthogonale Projektion** von $\mathbb{R}^n$ auf $U^\perp$ genannt. Mit unseren Vorüberlegungen gilt:

11.2.8 Lemma Sei $(b_1, \ldots, b_n)$ eine Basis von $\mathbb{R}^n$. Für alle $1 \leq i \leq n$ sei $U_{i-1} = \langle b_1, \ldots, b_{i-1} \rangle$. Dann gilt $\pi_{i-1}(b_i) = b_i^*$, wobei π_{i-1} die orthogonale Projektion von $\mathbb{R}^n$ auf $U_{i-1}^\perp$ ist.

Beweis: Es ist $\langle b_1, \ldots, b_{i-1} \rangle = \langle b_1^*, \ldots, b_{i-1}^* \rangle$. Weiter gilt $b_i = \sum_{j=1}^{i-1} \mu_{ij} b_j^* + b_i^*$, und $b_i^* \in U_{i-1}^\perp$. Es folgt $\pi_{i-1}(b_i) = \pi_{i-1}\left(\sum_{j=1}^{i-1} \mu_{ij} b_j^* + b_i^* \right) = b_i^*$, die Behauptung. □

11.2.9 Beispiel Wir hatten in Aufgabe 11.1.9 die Gram-Schmidt Orthogonalbasis (a_1^*, a_2^*) zu (a_1, a_2) mit $a_1 = \begin{pmatrix}12\\2\end{pmatrix}$ und $a_2 = \begin{pmatrix}13\\4\end{pmatrix}$ berechnet und die Vektoren in der Euklidischen Ebene skizziert. Die Vektoren a_1, a_2, a_1^* und a_2^* sind



Der Vektor a_2^* ist die Projektion von a_2 auf das orthogonale Komplement des durch a_1 erzeugten Unterraums von $\mathbb{R}^2$.

Dieses Lemma impliziert:

11.2.10 Lemma Sei $(b_1, \ldots, b_n)$ eine Basis von $\mathbb{R}^n$, und sei $a \in \mathbb{Z}$. Sei $\widetilde{b_i} = b_i - ab_j$ für ein $1 \leq j < i \leq n$. Dann ist $(b_1, \ldots, b_{i-1}, \widetilde{b_i}, b_{i+1}, \ldots, b_n)$ eine Basis von $\mathbb{R}^n$, und $\widetilde{b_i}^* = b_i^*$.

Beweis: Dass $(b_1, \ldots, b_{i-1}, \widetilde{b_i}, b_{i+1}, \ldots, b_n)$ eine Basis von $\mathbb{R}^n$ ist, ist eine Routineaufgabe.

Sei π_{i-1} die orthogonale Projektion von $\mathbb{R}^n$ auf $U_{i-1}^{\perp}$. Dann gilt

$$\widetilde{b_i}^* = \pi_{i-1}(\widetilde{b_i}) = \pi_{i-1}(b_i - ab_j) = \pi_{i-1}(b_i) = b_i^*,$$

die Behauptung. □

Mit dieser Notation folgt:

11.2.11 Lemma Die Gram-Schmidt-Orthogonalbasen zu den Basen $(b_1, \ldots, b_n)$ und $(b_1, \ldots, b_{i-1}, \widetilde{b_i}, b_{i+1}, \ldots, b_n)$ stimmen überein. □

11.2.12 Aufgabe Überzeugen Sie sich in dem Beispiel 11.2.6 oben davon, dass sich die Gram-Schmidt-Orthogonalbasen nicht ändern, wenn wir den Schritt 5. des LLL-Algorithmus durchlaufen.

11.2.13 Proposition Zu Beginn von Schritt 4. des LLL-Algorithmus gilt die Abschätzung $\|b_{k-1}^*\|^2 \leq 2\|b_k^*\|^2$ für alle $1 < k < i$.

Beweis: Zu Beginn des LLL-Algorithmus ist $i = 2$ bei Schritt 4. Dann ist diese Aussage leer, also wahr. Wir können also annehmen, dass die Aussage zu Beginn von Schritt 4. gilt. Wir müssen zeigen, dass sie auch nach Beendigung von Schritt 6. gilt. Schritt 5. ändert die Abschätzung nicht, denn die Orthogonalbasen ändern sich mit Lemma 11.2.11 nicht. Wenn in Schritt 6. der Index i auf $i+1$ gesetzt wird, so gilt entweder $\|b_{i-1}^*\|^2 \leq 2\|b_i^*\|$, und dann folgt, dass die behaupteten Ungleichungen bei dem folgenden Schritt 4. gelten. Die andere Möglichkeit ist, dass i auf 2 gesetzt wird, und dann gilt die Abschätzung bei dem folgenden Schritt 4. wie oben aus trivialen Gründen. Wird der Index i in Schritt 6. auf $i-1$ gesetzt, so ändern sich $b_1^*, \ldots, b_{i-2}^*$ nicht, und die Ungleichungen gelten, da sie vor Schritt 6. galten. □

Es folgt der erste Schritt im Beweis, dass der LLL-Algorithmus eine reduzierte Basis liefert.

11.2.14 Korollar Wenn der LLL-Algorithmus abbricht, so ist die Ausgabe $(b_1, \ldots, b_n)$ eine reduzierte Basis des Gitters $L(a_1, \ldots, a_n)$.

Beweis: Da die b_i, $1 \leq i \leq n$, ganzzahlige Linearkombinationen der $a_1, \ldots, a_n$ sind, liegen sie in $L(a_1, \ldots, a_n)$. Wenn der LLL-Algorithmus abbricht, so gilt $i = n+1$. Mit der Proposition 11.2.13 folgt die Behauptung. □

Wir werden den Rest des Abschnitts darauf verwenden, zu beweisen, dass der LLL-Algorithmus wirklich abbricht.

Dazu betrachten wir für alle $1 \leq k \leq n$ die Matrizen $B_k = \big(b_1|\cdots|b_k\big) \in \mathrm{M}_{nk}(\mathbb{Z})$. Dann gilt $B_k^T B_k = \big(\langle b_j, b_l\rangle\big)_{1\leq j,l\leq k} \in \mathrm{M}_{kk}(\mathbb{Z})$. Sei $d_k = \det(B_k^T B_k)$. Da $B_k^T B_k$ eine Matrix über $\mathbb{Z}$ ist, folgt, dass d_k eine ganze Zahl ist. Die Zahl d_k wird die **Gram'sche Determinante** zu $b_1, \ldots, b_k$ genannt. Das folgende Lemma gibt eine Interpretation der Gram'schen Determinante im Zusammenhang mit der Orthogonalbasis von $(b_1, \ldots, b_n)$.

11.2.15 Lemma Für alle $1 \leq k \leq n$ gilt $d_k = \prod_{l=1}^{k} \|b_l^*\|^2 > 0$.

Beweis: Sei $M = \begin{pmatrix} 1 & \mu_{21} & \cdots & \mu_{n1} \\ 0 & 1 & \cdots & \mu_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$, und sei $M_k = \begin{pmatrix} 1 & \mu_{21} & \cdots & \mu_{k1} \\ 0 & 1 & \cdots & \mu_{k2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ die

linke obere $k \times k$-Teilmatrix der Matrix M für den Basiswechsel von $(b_1, \ldots, b_n)$ nach $(b_1^*, \ldots, b_n^*)$.

Sei $B_k^* = \left(b_1^* | \cdots | b_k^*\right)$. Dann gelten $B_k^{*T} B_k^* = \begin{pmatrix} \|b_1^*\|^2 & & 0 \\ & \ddots & \\ 0 & & \|b_k^*\|^2 \end{pmatrix}$ und $B_k^* M_k = B_k$. Es folgt

$$\begin{aligned} d_k &= \det(B_k^T B_k) \\ &= \det((B_k^* M_k)^T (B_k^* M_k)) \\ &= \det(M_k^T B_k^{*T} B_k^* M_k) \\ &= \det(B_k^{*T} B_k^*), \text{ denn } \det(M_k^T) = 1 = \det(M_k) \\ &= \prod_{l=1}^{k} \|b_l^*\|^2. \end{aligned}$$

□

Als Folgerung aus diesem Lemma und aus Lemma 11.2.11 erhalten wir:

11.2.16 Bemerkung Die Gram'sche Determinate d_k ändert sich nicht, wenn Schritt 5. des LLL-Algorithmus durchlaufen wird. □

Wir werden jetzt untersuchen, wie sich die Gram'sche Determinante ändert, wenn wir in Schritt 6 zwei Vektoren vertauschen.

11.2.17 Lemma Angenommen, b_i und b_{i-1} werden in Schritt 6 vertauscht. Wir bezeichnen mit c_k und c_k^* die Basisvektoren der Basis beziehungsweise deren Gram-Schmidt-Orthogonalbasis nach der Vertauschung, also $c_k = b_k$ für alle $k \notin \{i-1, i\}$, $c_{i-1} = b_i$ und $c_i = b_{i-1}$. Dann gilt:

1. $c_k^* = b_k^*$ für alle $k \notin \{i-1, i\}$.
2. $\|c_{i-1}^*\|^2 < \frac{3}{4}\|b_{i-1}^*\|^2$.
3. $\|c_i^*\|^2 \leq \|b_{i-1}^*\|^2$.

Beweis:

1. Für alle $k \notin \{i-1, i\}$ gilt $c_k^* = \pi_{k-1}(c_k) = \pi_{k-1}(b_k) = b_k^*$. Dabei bezeichnet π_{k-1} die orthogonale Projektion auf $\langle b_1, \ldots, b_{k-1}\rangle^\perp$.

2. Es gilt
$$\begin{aligned} c_{i-1}^* &= \pi_{i-2}(c_{i-1}) \\ &= \pi_{i-2}(b_i) \\ &= \pi_{i-2}\left(b_i^* + \mu_{i,i-1}b_{i-1}^* + \sum_{j=1}^{i-2}\mu_{ij}b_j^*\right) \\ &= b_i^* + \mu_{i,i-1}b_{i-1}^*, \end{aligned}$$
denn $b_i^* + \mu_{i,i-1}b_{i-1}^* \in \langle b_1, \ldots, b_{i-2}\rangle^\perp = \langle b_1^*, \ldots, b_{i-2}^*\rangle^\perp$ und $\sum_{j=1}^{i-2}\mu_{ij}b_j^* \in \langle b_1, \ldots, b_{i-2}\rangle = \langle b_1^*, \ldots, b_{i-2}^*\rangle$. Es folgt
$$\|c_{i-1}^*\|^2 = \|b_i^*\|^2 + \mu_{i,i-1}^2\|b_{i-1}^*\|^2 < \frac{1}{2}\|b_{i-1}^*\|^2 + \mu_{i,i-1}^2\|b_{i-1}^*\|^2,$$
denn $\|b_i^*\|^2 < \frac{1}{2}\|b_{i-1}^*\|^2$, da b_i und b_{i-1} vertauscht werden. Im Schritt 5. wurde b_i auf $b_i - \lceil\mu_{i,i-1}^{\text{alt}}\rfloor b_{i-1}$ gesetzt. Es folgt
$$\begin{aligned} |\mu_{i,i-1}| &= |\frac{\langle b_i - \lceil\mu_{i,i-1}^{\text{alt}}\rfloor b_{i-1}, b_{i-1}^*\rangle}{\langle b_{i-1}^*, b_{i-1}^*\rangle}| \\ &= |\frac{\langle b_i, b_{i-1}^*\rangle}{\langle b_{i-1}^*, b_{i-1}^*\rangle} - \lceil\mu_{i,i-1}^{\text{alt}}\rfloor\frac{\langle b_{i-1}, b_{i-1}^*\rangle}{\langle b_{i-1}^*, b_{i-1}^*\rangle}| \\ &= |\mu_{i,i-1}^{\text{alt}} - \lceil\mu_{i,i-1}^{\text{alt}}\rfloor| \\ &\leq \frac{1}{2}. \end{aligned}$$
Somit gilt
$$\|c_{i-1}^*\|^2 < \frac{1}{2}\|b_{i-1}^*\|^2 + \frac{1}{4}\|b_{i-1}^*\|^2 = \frac{3}{4}\|b_{i-1}^*\|^2.$$

3. Sei $u = \sum_{j=1}^{i-2}\mu_{i-1,j}b_j^*$. Es gilt $c_i = b_{i-1} = b_{i-1}^* + u$. Sei π die orthogonale Projektion von $\mathbb{R}^n$ auf $\langle b_1, \ldots, b_{i-2}, b_i\rangle^\perp$. Dann gilt $c_i^* = \pi(c_i) = \pi(b_{i-1}) = \pi(b_{i-1}^* + u) = \pi(b_{i-1}^*)$. Es folgt $\|c_i^*\|^2 = \|\pi(b_{i-1}^*)\|^2 \leq \|b_{i-1}^*\|^2$.

□

Wir benutzen dieses Lemma, um die Gram'schen Determinanten bei Schritt 6 des LLL-Algorithmus abzuschätzen.

11.2.18 Lemma Angenommen, b_{i-1} und b_i werden in Schritt 6 des LLL-Algorithmus vertauscht. Wir bezeichnen mit $\widetilde{d_k}$ die Gram'schen Determinanten nach Austausch von b_{i-1} und b_i. Dann gilt:

1. $d_k = \widetilde{d_k}$ für alle $k \neq i-1$.
2. $\widetilde{d_{i-1}} \leq \frac{3}{4} d_{i-1}$.

Beweis:

1. Die Gram'sche Determinante nach dem Austausch unterscheidet sich von der vor dem Austausch dadurch, dass die $(i-1)$-te und die i-te Zeile und die $(i-1)$-te und die i-te Spalte vertauscht werden. Damit ändert sich die Gram'sche Determinante um den Faktor $(-1)^2$, also gar nicht.
2. Mit Lemma 11.2.15 gilt $d_{i-1} = \prod_{l=1}^{i-1} \|b_l^*\|^2$, und mit der zweiten Aussage von Lemma 11.2.17 folgt $\widetilde{d_{i-1}} \leq \frac{3}{4} d_{i-1}$.

□

Jetzt haben wir alle Zutaten zusammen, um das Hauptergebnis dieses Abschnitts zu beweisen.

11.2.19 Satz Der LLL-Algorithmus berechnet nach endlich vielen Schritte eine reduzierte Basis eines Gitters $L(a_1, \ldots, a_n)$ in $\mathbb{Z}^n$.

Beweis: Wir haben in Korollar 11.2.14 gezeigt, dass der Algorithmus eine reduzierte Basis liefert, wenn er abbricht. Wir definieren nun $D = \prod_{i=1}^{n-1} d_i$. Zu Beginn des Algorithmus ist

$$\begin{aligned} D &= \|a_1^*\|^{2(n-1)} \|a_2^*\|^{2(n-2)} \cdots \|a_{n-1}^*\|^2 \\ &\leq \|a_1\|^{2(n-1)} \|a_2\|^{2(n-2)} \cdots \|a_{n-1}\|^2 \\ &\leq A^{n(n-1)}, \end{aligned}$$

wobei A die maximale Länge der Vektoren $a_1, \ldots, a_n$ bezeichnet. Das erste Ungleichheitszeichen folgt aus Satz 11.1.10. Immer gilt $D \in \mathbb{N}$, denn mit Lemma 11.2.15 gilt $D > 0$, und als Produkt Gram'scher Determinanten ist D eine ganze Zahl. Die Zahl D ändert sich nicht, wenn der Schritt 5 des Algorithmus durchlaufen wird, wie wir in Bemerkung 11.2.16 gesehen haben. Sie ändert sich auch nicht, wenn wir in Schritt 6 den Index i erhöhen. Sie verringert sich um mindestens den Faktor $\frac{3}{4}$, wenn wir in Schritt 6 zwei Vektoren vertauschen. Wir können also nur endlich viele Vertauschungsschritte durchführen. Es folgt, dass i in Schritt 6 nach endlich vielen Schritten auf $n+1$ gesetzt wird, und dass der Algorithmus abbricht. □

Wir haben zu Beginn des Abschnittes 11.2.2 gesehen, dass es ausreicht, diese Behauptung für Gitter in $\mathbb{Z}^n$ zu beweisen.

In dem Beweisschritt, dass der LLL-Algorithmus abbricht, haben wir das erste Mal benötigt, dass das betrachtete Gitter in $\mathbb{Q}^n$ und nicht in $\mathbb{R}^n$ liegt. Wir brauchten, dass die Zahlen D in $\mathbb{N}$ liegen, um argumentieren zu können, dass dann eine absteigende Folge natürlicher Zahlen abbrechen muss.

11.2.20 Aufgabe Berechnen Sie die Zahlen D in dem Beispiel 11.2.6.

Eine genaue Komplexitätsanalyse können Sie beispielsweise in [vzGG] nachlesen. Dort wird gezeigt, dass der LLL-Algorithmus $\mathcal{O}(n^4 \log A)$ Operationen in $\mathbb{Z}$ auf Zahlen der Länge $\mathcal{O}(n \log A)$ benötigt. Dabei bezeichnet A die maximale Länge der Vektoren $a_1, \ldots, a_n$ des Gitters $L(a_1, \ldots, a_n)$.

11.3 Das Knapsack-Kryptosystem

„Knapsack“ ist englisch und bedeutet Rucksack. Das Bild, das die Erfinder Merkle und Hellman des Knapsack-Kryptosystems bei der Namensgebung vor Augen hatten, ist das folgende: Nehmen wir an, wir hätten einen Rucksack und verschiedene Gegenstände, von denen wir einige in den Rucksack stopfen können. Können wir aus den Gegenständen so auswählen, dass der Rucksack optimal gefüllt wird, dass also gar nichts weiter reinpasst?

Da wir hier aber keinen Campingurlaub planen, sondern Mathematik machen, werden wir präziser und beginnen mit der formalen Problemstellung:

11.3.1 Problem Seien $a_0, \ldots, a_n, s \in \mathbb{N}$ gegeben. Gibt es $x_1, \ldots, x_n \in \{0, 1\}$ mit

$$\sum_{i=0}^{n} a_i x_i = s?$$

11.3.2 Beispiel Gibt es $x_0 \ldots, x_5 \in \{0, 1\}$ mit $366x_0 + 385x_1 + 392x_2 + 401x_3 + 422x_4 + 437x_5 = 1215$?

Das Problem wird **Teilmengen-Summen-Problem** genannt, und es ist bekannt, dass es NP-hart ist, und es wird vermutet, dass es keine effizienten Algorithmen zur Lösung gibt.

Nachdem Diffie und Hellman im Jahre 1976 in [DH] Public-Key-Kryptografie erfanden, schlugen Merkle und Hellman 1978 in [MH] ein Public-Key-Kryptosystem vor, das auf dem Teilmengen-Summen-Problem aufbaut – das so genannte Knapsack-Kryptosystem. Die Rechnungen in diesem System waren weitaus weniger aufwändig als im RSA-System oder anderen bis dahin bekannten Public-Key-Kryptosystemen, und das versprach dem Knapsack-Kryptosystem eine große Zukunft. Verschiedene weitere Systeme, die auf dem Knapsack-Kryptosystem aufbauten, wurden vorgeschlagen. Aber es kam anders – all diese Kryptosysteme fielen wie ein Kartenhaus zusammen. Im Jahre 1984 wurde das Knapsack-Kryptosystem von Adi Shamir in [S] gebrochen – möglich wurde dies durch den LLL-Algorithmus.

11.3.1 Beschreibung des Kryptosystems

Beginnen wir mit einem kleinen Beispiel.

11.3.3 Beispiel Seien $a_0 = 1, a_1 = 2, a_2 = 4, a_3 = 7$ und $a_4 = 9$. Sei $s = 11$. Dann ist $(x_0, x_1, x_2, x_2, x_4) = (0, 0, 1, 1, 0)$ eine Lösung des Teilmengen-Summen-Problems $\sum_{i=0}^{4} a_i x_i = 11$, denn $0 \cdot a_1 + 0 \cdot a_2 + 1 \cdot a_3 + 1 \cdot a_4 + 0 \cdot a_5 = 4 + 7 = 11$. Auch $(0, 1, 0, 0, 1)$ ist eine Lösung, denn $2 + 9 = 11$. Wir sehen also:

11.3.4 Bemerkung Wenn es eine Lösung eines Teilmengen-Summen-Problems gibt, so ist diese Lösung in der Regel nicht eindeutig. □

11.3.5 Definition Wir nennen eine Folge $(a_0, \ldots, a_n)$ von natürlichen Zahlen **superaufsteigend**, wenn $a_i > \sum_{j=0}^{i-1} a_j$ für alle $1 \leq i \leq n$ gilt.

11.3.6 Beispiel Die Folge $(2, 3, 7, 15, 31)$ ist superaufsteigend.

Ein Teilmengen-Summen-Problem mit superaufsteigender Zahlenfolge ist leicht zu lösen: Sei $(a_0, \ldots, a_n)$ superaufsteigend, und sei $s \in \mathbb{N}$. Wähle das größte a_i mit $a_i \leq s$ und wir merken uns $x_i = 1$. Wir wählen nun das größte a_j mit $a_j \leq s - a_i$ und merken uns $x_j = 1$. Dann wählen wir das größte a_k mit $a_k \leq s - a_i - a_j$ und merken uns $x_k = 1$. Dieses Verfahren iterieren wir, und wir erhalten auf diese Weise eine Teilmenge von $\{a_0, \ldots, a_n\}$, deren Summe s ist, oder wir kommen bei einer Zahl an, die kleiner als a_0 ist. In diesem Fall hat das Teilmengen-Summen-Problem keine Lösung.

11.3.7 Aufgabe Sei $(a_0, \ldots, a_n)$ superaufsteigend, und sei $s \in \mathbb{N}$. Beweisen Sie: Wenn das Teilmengen-Summen-Problem $\sum_{i=0}^{n} a_i x_i = s$ eine Lösung hat, so ist diese Lösung eindeutig bestimmt.

Diese Überlegungen liegen dem Knapsack-Kryptosystem zu Grunde.

Erzeugung des öffentlichen Schlüssels: Alice wählt ein superaufsteigendes n-Tupel natürlicher Zahlen $(a_0, \ldots, a_{n-1})$, eine natürliche Zahl $m > \sum_{i=0}^{n-1} a_i$ und eine zu m teilerfremde Zahl a. Dann berechnet sie ein $b \in \mathbb{Z}/m\mathbb{Z}$ mit $ab \equiv 1 \bmod m$.

Die Daten: $(a_0, \ldots, a_{n-1})$, m, a und b hält sie geheim.

Sie bildet nun die Folge $(aa_0 \bmod m, \ldots, aa_{n-1} \bmod m) = (w_0, \ldots, w_{n-1})$. Diese Folge ist in der Regel nicht mehr superaufsteigend.

Der öffentliche Schlüssel: Als öffentlichen Schlüssel gibt Alice $(w_0, \ldots, w_{n-1})$ bekannt.

Chiffrieren: Die Nachrichten, die Bob übermitteln möchte, sind n-Bit Zahlen. Will Bob die Nachricht $(x_{n-1} \ldots x_0)$ mit $x_i \in \{0, 1\}$ für alle $0 \leq i \leq n-1$ übermitteln, so bildet er

$$s = \sum_{i=0}^{n-1} x_i w_i.$$

Diese Zahl übermittelt er Alice.

Dechiffrieren: Alice bildet in $\mathbb{Z}/m\mathbb{Z}$

$$bs = b \sum_{i=0}^{n-1} x_i w_i = b \sum_{i=0}^{n-1} x_i a a_i = \sum_{i=0}^{n-1} x_i b a a_i = \sum_{i=0}^{n-1} x_i a_i.$$

Sie ist jetzt gefordert, ein Teilmengen-Summen-Problem mit superaufsteigender Folge zu berechnen. Wie wir oben gesehen haben, kann sie dies leicht lösen.

Die vermeintliche Sicherheit des Knapsack-Kryptosystems liegt darin begründet, dass Oskar mit einem Teilmengen-Summen-Problem konfrontiert ist, das auf einer Zahlenfolge basiert, die nicht superaufsteigend ist. Auf den ersten Blick sieht es so aus, als müsse er ein Problem in der Klasse NP knacken. Es geht aber anders, wie wir jetzt sehen werden.

11.3.2 Knapsack und kurze Vektoren

Um das Knapsack-Kryptosystem zu knacken, muss kein Teilmengen-Summen-Problem gelöst werden, wie Adi Shamir 1984 in [S] feststellte.

Nehmen wir an, wir suchen $x_1 \ldots, x_n \in \{0, 1\}$, für die die Gleichung

$$s = \sum_{i=1}^{n} a_i x_i, \text{ mit } a_i \in \mathbb{N} \text{ für alle } 1 \leq i \leq n$$

erfüllt ist. Wir können annehmen, dass die a_i sehr große Zahlen sind, denn wären die a_i klein, dann könnte man das Kryptosystem auch durch Ausprobieren brechen. Wir bilden das Gitter $L(b_1, \ldots, b_{n+1})$, dessen Basis $b_1, \ldots, b_{n+1}$ die Spalten der folgenden Matrix sind:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ -a_1 & -a_2 & \cdots & -a_n & s \end{pmatrix}$$

Angenommen, wir haben $x_1 \ldots, x_n \in \{0, 1\}$ gefunden, für die $-\sum_{i=1}^{n} a_i x_i + s = 0$ gilt. Dann ist

$$\sum_{i=1}^{n} x_i b_i + b_{n+1} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \\ 0 \end{pmatrix}$$

ein Vektor in $L(b_1, \ldots, b_{n+1})$, der sehr kurz ist, denn seine Länge ist maximal $\sqrt{n}$. Um das Knapsack-Kryptosystem zu brechen, berechnen wir mit dem LLL-Algorithmus eine reduzierte Basis von $L(b_1, \ldots, b_{n+1})$ und hoffen, dass der erste

Vektor der reduzierten Basis der Vektor $\begin{pmatrix} x_1 \\ \vdots \\ x_n \\ 0 \end{pmatrix}$ ist. Und das ist so oft der Fall, dass das Knapsack-Kryptosystem als nicht sicher verworfen wurde.

Lösungen der Aufgaben

Lösungen der Aufgaben in Kapitel 11

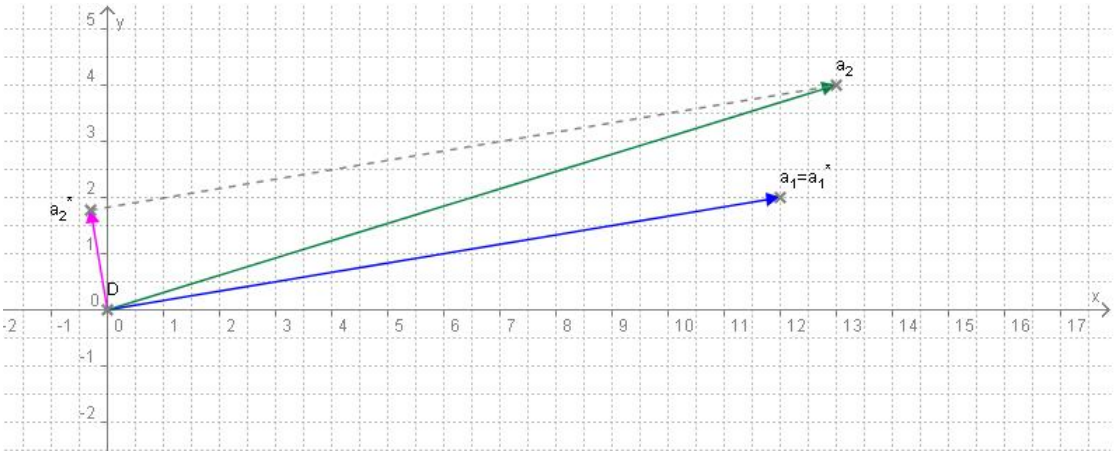
Aufgabe 11.1.9

Seien $a_1 = \begin{pmatrix}12\\2\end{pmatrix}, a_2 = \begin{pmatrix}13\\4\end{pmatrix} \in \mathbb{R}^2$. Wir suchen die Gram-Schmidt-Orthogonalisierung von (a_1, a_2).

Es ist $a_1 = a_1^* = \begin{pmatrix}12\\2\end{pmatrix}$. Weiter ist

$$a_2^* = a_2 - \mu_{21} a_1^* = \begin{pmatrix}13\\4\end{pmatrix} - \frac{\langle a_2, a_1^*\rangle}{\|a_1^*\|^2}\begin{pmatrix}12\\2\end{pmatrix} = \begin{pmatrix}13\\4\end{pmatrix} - \frac{41}{37}\begin{pmatrix}12\\2\end{pmatrix} = \begin{pmatrix}-\frac{11}{37}\\\frac{66}{37}\end{pmatrix}.$$

Die Vektoren a_1, a_2, a_1^* und a_2^* sind



Der Vektor a_2^* ist die Projektion von a_2 auf das orthogonale Komplement des durch a_1 erzeugten Unterraums von $\mathbb{R}^2$. □

Aufgabe 11.2.2

1. Wir wissen bereits, dass $a_1^* = \begin{pmatrix} 12 \\ 2 \end{pmatrix}$ und $a_2^* = \begin{pmatrix} -\frac{11}{37} \\ \frac{66}{37} \end{pmatrix}$ gilt. Es ist $\|a_1^*\|^2 = 148$. Ferner ist $\|a_2\|^2 = \frac{4477}{1369} \leq 4$, also $\|a_1^*\|^2 > 2\|a_2^*\|^2$. Es folgt, dass (a_1, a_2) nicht reduziert ist. □

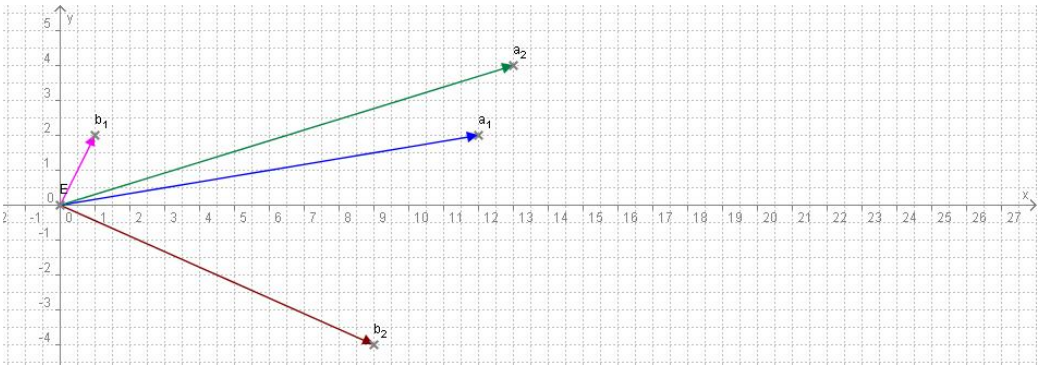
2. Es gilt $b_1 = -a_1 + a_2$ und $b_2 = 4a_1 - 3a_2$. Die Matrix für den Basiswechsel von (a_1, a_2) nach (b_1, b_2) ist somit $U = \begin{pmatrix} -1 & 4 \\ 1 & -3 \end{pmatrix}$. Diese Matrix liegt in $\mathrm{M}_{22}(\mathbb{Z})$ und ist invertierbar, und es folgt, dass (b_1, b_2) eine Basis von $L(a_1, a_2)$ ist.□.

3. Wir berechnen die Gram-Schmidt Orthogonalbasis von (b_1, b_2). Es ist $b_1 = b_1^*$. Weiter ist

$$b_2^* = b_2 - \frac{\langle b_2, b_1^* \rangle}{\|b_1^*\|^2} b_1^* = \begin{pmatrix} 9 \\ -4 \end{pmatrix} - \frac{1}{5} \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \frac{22}{5} \begin{pmatrix} 2 \\ -1 \end{pmatrix}.$$

   Es ist $\|b_1^*\|^2 = 5$ und $\|b_2^*\|^2 = \frac{484}{5}$. Offenbar gilt $\|b_1^*\|^2 \leq 2\|b_2^*\|$, und es folgt, dass (b_1, b_2) eine reduzierte Basis von $L(a_1, a_2)$ ist. □

4. Die folgende Skizze zeigt die Vektoren a_1, a_2, b_1 und b_2. Die Vektoren b_1 und b_2 sind nicht wirklich orthogonal, denn $\langle b_1, b_2 \rangle = 1 \neq 0$.



Aufgabe 11.2.12 Ohne Lösung

Aufgabe 11.2.20

Zu Beginn des Algorithmus' sind $b_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$, $b_2 = \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix}$ und $b_3 = \begin{pmatrix} 3 \\ 5 \\ 6 \end{pmatrix}$. Es sind

$$\begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \end{pmatrix}, \text{ also } d_1 = 3$$

und

$$\begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 0 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 5 \end{pmatrix}, \text{ also } d_2 = 14.$$

Es folgt, dass D zu Beginn des Algorithmus $3 \cdot 14 = 42$ ist.

Wir haben gesehen, dass D sich nicht ändert, wenn Schritt 5 des Algorithmus' durchgeführt wird, oder wenn in Schritt 6 der der Index erhöht wird.

Die erste Vertauschung geschieht beim Übergang der Basis

$$\left(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right)$$

zur Basis

$$\left(b_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, b_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, b_3 = \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix} \right).$$

Dann gilt $d_1 = 3$ und $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}$, also $d_2 = 2$. Es folgt $D = 6$.

Die nächste Vertauschung findet statt beim Übergang der Basis

$$\left(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix} \right).$$

zur Basis

$$\left(b_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, b_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, b_3 = \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix} \right).$$

Dann gilt $d_1 = 1$ und $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}$, also $d_2 = 2$. Es folgt $D = 2$.

Weitere Vertauschungen finden beim Durchführen des LLL-Algorithmus nicht mehr statt, das heißt, bis zum Abbruch bleibt $D = 2$. □

Aufgabe 11.3.7

Sei $(a_0, \ldots, a_n)$ eine superaufsteigende Folge. Sei $s \in \mathbb{N}$ mit $s = \sum_{i=0}^{n} a_i x_i$ und $s = \sum_{i=0}^{n} a_i y_i$ und $x_i, y_j \in \{0, 1\}$ für alle $0 \leq i, j \leq n$. Es folgt $0 = \sum_{i=0}^{n} a_i(x_i - y_i)$ mit $x_i - y_i \in \{-1, 0, 1\}$.

Sei k maximal, so dass $x_k - y_k \neq 0$ ist. Dann gilt $(y_k - x_k)a_k = \sum_{i=0}^{k-1}(x_i - y_i)a_i$. Wir nehmen auf beiden Seiten dieser Gleichung die Beträge und erhalten $a_k = \left|\sum_{i=0}^{k-1}(x_i - y_i)a_i\right| \leq \sum_{i=0}^{k-1} a_i$. Dies ist ein Widerspruch zur Annahme, dass $(a_0, \ldots, a_n)$ superaufsteigend ist. Somit gilt $x_i = y_i$ für alle $0 \leq i \leq n$. □

Anhang

Literaturverzeichnis

[A] M. Ajtai: *The Shortest Vector Problem in L_2 is NP-hard for Randomized Reductions*, Electronic Colloquium on Computational Complexity TR97-047.

[AGP] W.R. Alford, A. Granville, C. Pommerance: *There are infinitely many Carmichael numbers*, Annals of Mathematics **140**, 703-722 (1994).

[AKS] M. Agrawal, N. Kayal, N. Saxena: *PRIMES is in P*, Annals of Mathematics 160(2), 781-793.
siehe auch: `http://www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf`

[Ba] F. L. Bauer: *Entzifferte Geheimnisse, Methoden und Maxime der Kryptologie*, 2. Auflage, Springer Verlag, Berlin, Heidelberg, New York (1997).

[Beu] A. Beutelspacher: *Kryptologie*, 5. Auflage, Vieweg Verlag, Braunschweig, Wiesbaden (1996).

[Bu] J. Buchmann: *Einführung in die Kryptographie*, Springer Verlag, Berlin, Heidelberg, New York (1999).

[DH] W. Diffie, M. E. Hellman: *New directions in cryptography*, IEEE Transactions on Information Theory, **IT-22**(6), 644-654.

[vzGG] J. von zur Gathen, J. Gerhard: *Modern Computer Algebra*, Cambridge University Press, Cambridge (1999).

[Kn] A.W. Knapp: *Elliptic Curves*, Mathematical Notes (40), Princeton University Press (1992).

[K] N. Koblitz: *A course in number theory and cryptography*, 2. Auflage, Springer Verlag, Berlin, Heidelberg, New York (1994).

[KR] R. Kumanduri, C. Romero: *Number Theory With Computer Applications*, Prentice Hall, Upper Saddle River (1998).

[LLL] A. K. Lenstra, H. W. Lenstra, L. Lovász: *Factoring Polynomials with Rational Coefficients*, Mathematische Annalen **261**, 515-534.

[MH] R. C. Merkle, M. E. Hellman: *Hiding information and signiatures in trapdoor knapsacks*, IEEE Transactions on Information Theory, **IT-24**(5), 525-530.

[Ra] M.O. Rabin: *Probabilistic Algorithms for Testing Primality*, Journal of Number Theory **12**, 128-138 (1980).

[RSA] R. L. Rivest, A. Shamir, L. M. Adleman: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM **21**(2), 120-126 (1978).

[Sch] R. Schoof: *Counting points on elliptic curves over finite fields*, J. Théorie des Nombres de Bordeaux, **7**, 219-254(1995).

[S] A. Shamir: *A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem*, IEEE Transactions on Information Theory, **IT-30**(5), 699-704.

[Si1] S. Singh: *Fermats letzter Satz*, Deutscher Taschenbuch Verlag, München (2000).

[Si2] S. Singh: *Geheime Botschaften*, Carl Hanser Verlag, München, Wien (2000).

[Sil] J.H. Silverman: *The Arithmetic of Elliptic Curves*, Springer Verlag, Berlin, Heidelberg, New York (1986).

[St] D. R. Stinson: *Cryptography, Theory and Practice*, CRC-Press, Boca Raton, New York, London, Tokyo (1995).

[Su] Suetonius Tranquillus: *De vita Caesarum Libri VIII*, (Bibliotheca Scriptorum Graecorum et Romanorum Teubneriania), Teubner Verlag, Stuttgart (1978).

Index

Symbolverzeichnis

$\langle a \rangle$ von a erzeugte Untergruppe, 84

$\left(a_1|\cdots|a_n\right)$ Matrix mit Spalten $a_1, \ldots, a_n$, 341

$(a_1^*, \ldots, a_n^*)$ Gram-Schmidt-Orthogonalbasis, 342

A^{Ad} Adjunkte, 59

$[\alpha]$ Gaußklammer, 192

$\alpha(\lambda)$ Vielfachheit einer Nullstelle, 163

$a \bmod m$ Rest von a durch m, 18

$(\frac{a}{n})$ Jacobi-Symbol, 222

$(\frac{a}{p})$ Legendre-Symbol, 220

C_a Konjugationsklasse, 105

$C(G)$ Zentrum, 106

$\mathrm{char}(R)$ Charakteristik, 152

C_∞ unendliche zyklische Gruppe, 108

C_n endliche zyklische Gruppe, 108

$\det L$ Determinante eines Gitters, 342

d_k Gram'sche Determinante, 362

$(d_{k-1} \ldots d_0)_b$ Zahl zur Basis b, 67

DLP Diskreter-Logarithmus-Problem, 311

$d(v, w)$ Abstand von v und w, 339

$E(a, b, \mathbb{K})$ elliptische Kurve, 298

$E^{(n)}$ n-te Einheitswurzeln, 269

f' Ableitung, 163

f_a innerer Automorphismus, 104

$\mathbb{F}_q$ endlicher Körper, 267

ggT größter gemeinsamer Teiler, 24, 160

$[G : H]$ Index einer Untergruppe, 87

$\mathrm{Gl}_m(R)$ invertierbare Matrizen, 59

G/S Faktorgruppe, 101

$H < G$ Untergruppe, 82

I_m Einheitsmatrix, 59

$I \lhd R$ Ideal, 137

$\simeq$ isomorph, 141

$I(x)$ Friedmanscher Koinzidenzindex, 55

$\mathbb{K}(a_1, \ldots, a_n)$ $\mathbb{K}$ adjungiert $a_1, \ldots, a_n$, 257

kgV kleinstes gemeinsames Vielfaches, 110, 161

$\mathbb{K}^{(n)}$ n-ter Kreisteilungskörper, 269

$\equiv$ kongruent, 18, 138

$L(a_1, \ldots, a_n)$ Gitter, 339

L_H Rechtskongruenz, 86

$\mathbb{L} : \mathbb{K}$ Körpererweiterung, 251

$[\mathbb{L} : \mathbb{K}]$ Grad einer Körpererweiterung, 253

$\mathrm{M}_{mm}(R)$ Matrizenring, 59

$\lceil \mu \rfloor$ modifizierte Gaußklammer, 351

$\binom{n}{k}$ Binomialkoeffizient, 54

$N(S)$ Normalisator, 104

$\mathcal{O}$ $\mathcal{O}$-Notation, 195

$\mathcal{O}$ Punkt bei Unendlich, 298

$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ Kryptosystem, 11

φ Eulersche φ-Funktion, 90

$P(R)$ Primring, 150

Q_n n-tes Kreisteilungspolynom, 271

R_H Linkskongruenz, 86

R/I Faktorring, 140

$R^\times$ Einheitengruppe, 89

$S \lhd G$ Normalteiler, 100

sgn Signatur, 83

$\langle\, , \rangle$ Skalarprodukt, 339

$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha)$ Spur, 274

$U^\perp$ orthogonales Komplement, 360

$\|v\|$ Norm, 339

$w_p(c)$ Exponent in der Primzahlzerlegung, 110