A Anhang

In diesem Anhang werden einige grundlegende Begriffe aufgelistet, die im Buch verwendet werden, ohne sie dort explizit über Definitionen einzuführen.

A.1 Zahlenmengen

Folgende Bezeichnungen für Zahlenmengen werden verwendet:

$\mathbb{N} = \{1, 2, 3, \ldots\}$	natürliche Zahlen
$\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$	natürliche Zahlen einschließlich 0
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$	ganze Zahlen
$\mathbb{G} = \{\ldots - 4, -2, 0, 2, 4, \ldots\}$	gerade Zahlen
$\mathbb{G}_+ = \{0, 2, 4, \ldots\}$	positive gerade Zahlen
$\mathbb{G}_- = \{-2, -4, -6, \ldots\}$	negative gerade Zahlen
$\mathbb{U} = \{\ldots - 3, -1, 1, 3, \ldots\}$	ungerade Zahlen
$\mathbb{U}_+ = \{1, 3, 5, \ldots\}$	positive ungerade Zahlen
$\mathbb{U}_- = \{-1, -3, -5, \ldots\}$	negative ungerade Zahlen
$\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z},\, q \in \mathbb{N} \right\}$	rationale Zahlen
$\mathbb{R} =$ Menge der reellen Zahlen	
$\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$	reelle Zahlen gößer 0
$\mathbb{C} = \left\{ a + bi \mid a, b \in \mathbb{R},\, i^2 = -1 \right\}$	komplexe Zahlen

A.2 Alphabete, Wörter, Sprachen

Alphabet

Ein *Alphabet* ist eine endliche Menge von Symbolen, die im Allgemeinen mit Σ bezeichnet wird. Aus den Symbolen (Buchstaben) können Wörter gebildet werden. Die Menge aller Wörter über Σ wird mit Σ^* bezeichnet. Σ^* kann wie folgt rekursiv festgelegt werden:

Leeres Wort

(1) Das *leere Wort*, welches wir mit ε bezeichnen, ist ein Wort über Σ: $\varepsilon \in \Sigma^*$,

(2) jeder Buchstabe aus Σ ist ein Wort: ist $a \in \Sigma$, dann ist auch $a \in \Sigma^*$,

(3) werden zwei Wörter aus Σ^* hintereinander geschrieben (*konkateniert*), dann ergibt sich wieder ein Wort: ist $v, w \in \Sigma^*$, dann ist auch $v \circ w = vw \in \Sigma^*$,

K.-U. Witt, *Algebraische und zahlentheoretische Grundlagen für die Informatik*,
DOI 10.1007/978-3-658-04075-8, © Springer Fachmedien Wiesbaden 2014

(4) Σ^* ist die kleinste Menge von endlichen Buchstabenfolgen, die mit den Regeln (1) – (3) gebildet werden können.

Es gilt z.B.:

- Ist $\Sigma = \emptyset$, dann ist $\Sigma^* = \{\varepsilon\}$;
- ist $\Sigma^* = \{a\}$, dann ist $\Sigma^* = \{\varepsilon, a, aa, aaa, \ldots\}$;
- ist $\Sigma^* = \{a, b\}$, dann ist

$$\Sigma^* = \{\varepsilon, a, b, aa, ab, ba, bb, aaa, aab, aba, abb, baa, bab, bba, bbb, \ldots\}$$

Eine Menge $L \subseteq \Sigma^*$ heißt (*formale*) *Sprache über* Σ. die Sprache

$$L = \left\{\varepsilon, ab, a^2b^2, \ldots\right\} = \left\{a^n b^n \mid n \in \mathbb{N}_0\right\}$$

enthält besipielsweise alle Wörter über dem Alphabet $\Sigma = \{a, b\}$, deren Wörten aus eine Folge von a's gefolgt von einer gleich langen Folge von b's bestehen.

A.3 Relationen und Funktionen

Sind A und B Mengen, dann heißt $R \subseteq A \times B = \{(a, b) \mid a \in A,\, b \in B\}$ eine *Relation* zwischen A und B; ist $A = B$, dann heißt R *homogen* und A *Grundmenge* von R. Anstelle von $(a, b) \in R$ schreibt man auch aRb. Gilt für eine homogene Relation $R \subseteq A \times A$, dass aRa gilt für alle $a \in A$, dann heißt R *reflexiv*. Folgt aus aRb, dass dann auch bRa gilt, dann heißt R *symmetrisch*. Folgt aus aRb und bRc, dass dann auch aRc gilt, dann heißt R *transitiv*. Eine reflexive, symmetrische und transitive Relation heißt *Äquivalenzrelation*. Für eine Äquivalenzrelation R über der Grundmenge A heißt $[a]_R = \{b \in A \mid aRb\}$ *Äquivalenzklasse* von R mit dem *Repräsentanten* a.

Eine Äquivalenzklasse ist niemals leer, denn wegen der Reflexivität gilt $a \in [a]_R$ für alle $a \in A$, und eine Äquivalenzklasse ist unabhängig von ihrem Repräsentanten, denn für jedes $b \in [a]_R$ gilt $[a]_R = [b]_R$. Des Weiteren gilt für $a, b \in A$ entweder $[a]_R = [b]_R$ oder $[a]_R \cap [b]_R = \emptyset$; Äquivalenzklassen mit verschiedenen Repräsentanten sind also entweder gleich oder disjunkt. Die Vereinigung aller Äquivalenzklassen ergibt die Grundmenge: $\bigcup_{a \in A} [a]_R = A$. Eine Äquivalenzrelation *partitioniert* also die Grundmenge vollständig in nicht leere, disjunkte Teilmengen, den Äquivalenzklassen. Umgekehrt legt jede vollständige *Partition* einer Menge A in nichtleere, disjunkte Teilmengen eine Äquivalenrelation über der Grundmenge A fest.

Eine Relation $R \subseteq A \times B$ heißt *rechtseindeutig* genau dann, wenn aus aRb und aRc folgt, dass $b = c$ ist. Rechtseindeutige Relationen heißen *Funktionen* oder *Abbildungen*. Funktionen werden im Allgemeinen mit f bezeichnet, und anstelle

von $f \subseteq A \times B$ schreibt man $f : A \to B$ und anstelle von xfy schreibt man $f(x) = y$. x heißt *Argument* von f, y heißt *Wert* oder *Bild* von x unter f. Gibt es zu einem $x \in A$ kein $y \in B$ mit $f(x) = y$, dann ist f für das Argument x nicht definiert, was auch mit $f(x) = \perp$ notiert wird.

A heißt *Ausgangsmenge* und B *Zielmenge* von f. Die Menge $Def(f) = \{x \in A \mid \text{es existiert ein } y \in B \text{ mit } f(x) = y\}$ heißt *Definitionsbereich* von f, und $W(f) = \{y \in B \mid \text{es existiert ein } x \in A \text{ mit } f(x) = y\}$ heißt *Wertebereich* von f. Für $C \subseteq A$ heißt $f(C) = \{f(x) \mid x \in C\}$ *Bildmenge* von C unter f, und für $D \subseteq B$ heißt $f^{-1}(D) = \{x \in A \mid f(x) \in D\}$ *Urbildmenge* von D unter f. Die Menge $graph(f) = \{(x, y) \in A \times B \mid f(x) = y\} = Def(f) \times W(f)$ heißt *Graph* von f.

Sei $f : A \to B$ eine Funktion: Ist für alle $x, y \in A$ mit $x \neq y$ auch $f(x) \neq y$, dann heißt f *injektiv* oder auch *linkseindeutig*. Gilt $Def(f) = A$, dann heißt f *total*, gilt $W(f) = B$, dann heißt f *surjektiv*. Ist eine Funktion total, injektiv und surjektiv, dann heißt sie *bijektiv* oder auch *eineindeutig*.

Zwei Mengen A und B heißen *gleichmächtig* genau dann, wenn eine bijektive Funktion $f : A \to B$ existiert; man schreibt dann $|A| = |B|$. Hat eine Menge A endlich viele Elemente, dann schreibt man $|A| < \infty$, hat sie n Elemente, so schreibt man $|A| = n$, hat sie unendlich viele Elemente, so schreibt man $|A| = \infty$.

Die Menge $\mathcal{P}(A) = \{M \mid M \subseteq A\}$ aller Teilmengen von A heißt *Potenzmenge* von A. Eine andere Schreibweise für $\mathcal{P}(A)$ ist 2^A. Mit B^A bezeichnet man die Menge aller totalen Funktionen von A nach B.

A.4 Spezielle Funktionen sowie Summen und Produkte

Die Funktion $\lceil \cdot \rceil : \mathbb{R} \to \mathbb{R}$ definiert durch

$$\lceil x \rceil = \min \{y \in \mathbb{Z} \mid x \leq y\}$$

heißt *obere Gaussklammer*, die Funktion $\lfloor \cdot \rfloor : \mathbb{R} \to \mathbb{R}$ definiert durch

Obere Gaussklammer

$$\lfloor x \rfloor = \max \{y \in \mathbb{Z} \mid y \leq x\}$$

heißt *untere Gaussklammer*. Es gilt z.B. $\lceil 2.3 \rceil = 3$, $\lceil -2.3 \rceil = -2$, $\lfloor 3.7 \rfloor = 3$ und $\lfloor -3.7 \rfloor = -4$.

Untere Gaussklammer

Zur kompakten Beschreibung von Summen und Produkten benutzen wir die Symbole $\sum$ und $\prod$: Für reelle (komplexe) Zahlen a_i und $m, n \in \mathbb{Z}$ mit $m \leq n$

gilt

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + a_{m+2} + \ldots + a_n$$

$$\sum_{k=m}^{\infty} a_k = \sum_{k\geq m} a_k = a_m + a_{m+1} + a_{m+2} + \ldots$$

$$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot a_{m+2} \cdot \ldots \cdot a_n$$

$$\prod_{k=m}^{\infty} a_k = \prod_{i\geq m} a_k = a_m \cdot a_{m+1} \cdot a_{m+2} \cdot \ldots$$

Die endlichen Summen (analog Produkte) können auch rückwärts berechnet werden:

$$\sum_{k=m}^{n} a_k = \sum_{k=0}^{n-m} a_{n-k}$$

Indexverschiebung

Beim Rechnen mit solchen Summen und Produkten sind oft so genannte *Indexverschiebungen* hilfreich: Sei $i \in \mathbb{N}_0$, dann gilt für Summen (analog für Produkte):

$$\sum_{k=m}^{n} a_k = \sum_{k=m+i}^{n+i} a_{k-i} = \sum_{k=m-i}^{n-i} a_{k+i}$$

$$\sum_{k\geq m} a_k = \sum_{k\geq m+i} a_{k-i} = \sum_{k\geq m-i} a_{k+i}$$

Speziell für $i = m$ gilt

$$\sum_{k=m}^{n} a_k = \sum_{k=0}^{n-m} a_{k+m}$$

$$\sum_{k\geq m} a_k = \sum_{k\geq 0} a_{k+m}$$

Fakultät

Für $n \in \mathbb{N}$ heißt das Produkt der ersten n Zahlen

$$1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n = \prod_{k=1}^{n} k$$

Fakultät von n. Diese Funktion wird kurz mit $n!$ notiert. Es ist sinnvoll, $0! = 1$ zu setzen. Damit erhält man folgende rekursive Definition der Fakultätsfunktion:

$$n! = \begin{cases} 1, & n = 0 \\ (n-1)! \cdot n, & n \geq 1 \end{cases}$$

A.5 Vektorräume

Vektorraum

Sei $\mathcal{V}$ eine additive abelsche Gruppe und $\mathcal{K}$ ein Körper sowie $* : \mathcal{K} \times \mathcal{V} \to \mathcal{V}$ eine Verknüpfung, die folgende Eigenschaften erfüllt:

$$\begin{array}{rl} 1 * \mathbf{x} = \mathbf{x} & \text{für alle } \mathbf{x} \in \mathcal{V} \\ \alpha * (\mathbf{x} + \mathbf{y}) = \alpha * \mathbf{x} + \alpha * \mathbf{y} & \text{für alle } \mathbf{x}, \mathbf{y} \in \mathcal{V}, \alpha \in \mathcal{K} \\ (\alpha + \beta) * \mathbf{x} = \alpha * \mathbf{x} + \beta * \mathbf{y} & \text{für alle } \mathbf{x} \in \mathcal{V}, \alpha, \beta \in \mathcal{K} \\ (\alpha \cdot \beta) * \mathbf{x} = \alpha * (\beta * \mathbf{x}) & \text{für alle } \mathbf{x} \in \mathcal{V}, \alpha, \beta \in \mathcal{K} \end{array}$$

Dann heißt $\mathcal{V}$ ein *Vektorraum* über $\mathcal{K}$.

Sei $\mathcal{K}$ ein Körper. Dann bildet $\mathcal{K}^n$ für alle $n \in \mathbb{N}$ einen Vektorraum über $\mathcal{K}$, wenn die Addition $\mathbf{x} + \mathbf{y}$ von $\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{K}^n$ und $\mathbf{y} = (y_1, \ldots, y_n) \in \mathcal{K}^n$ komponentenweise definiert ist durch

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1, \ldots, x_n + y_n)$$

und die skalare Multiplikation $\alpha * \mathbf{x}$ mit $\alpha \in \mathcal{K}$ ebenfalls komponentenweise definiert ist durch

$$\alpha * \mathbf{x} = (\alpha \cdot x_1, \ldots, \alpha \cdot x_n)$$

Sei Sei $\mathcal{A} = \{\mathbf{a_1}, \ldots, \mathbf{a_n}\} \subseteq \mathcal{V}$, dann bildet

$$Span_{\mathcal{A}} = \{\alpha_1 \mathbf{a_1} + \ldots + \alpha_n \mathbf{a_n} \mid \alpha_i \in \mathcal{K}\}$$

einen Unterraum von $\mathcal{V}$, den von $\mathcal{A}$ *aufgespannten Unterraum*. Sei $\mathcal{B} \subseteq \mathcal{V}$ mit $Span_{\mathcal{B}} = \mathcal{V}$ und gilt $Span_{\mathcal{B}-\{\mathbf{b}\}} \subset \mathcal{V}$ für alle $\mathbf{b} \in \mathcal{B}$, dann bildet $\mathcal{B}$ eine *Basis* für $\mathcal{V}$. Sind $\mathcal{B}_1$ und $\mathcal{B}_2$ zwei endliche Basen für $\mathcal{V}$, dann gilt $|\mathcal{B}_1| = |\mathcal{B}_2|$. Ist $\mathcal{B}$ eine Basis für $\mathcal{V}$ und $|\mathcal{B}| = n$, dann heißt $\dim(\mathcal{V}) = n$ die *Dimension* von $\mathcal{V}$.

Basis

Dimension

Sei $\mathcal{K}$ ein Körper. Jede Menge von n Vektoren

$$\mathbf{e_i} = (x_{i1}, \ldots, x_{in}) \in \mathcal{K}^n,\ 1 \leq i \leq n,\ n \geq 1$$

definiert durch $x_{ij} = 0$ für $1 \leq j \leq n$, $j \neq i$ und $x_{ii} \in \mathcal{K}^*$ bildet eine Basis für $\mathcal{K}^n$. Es gilt also $\dim(\mathcal{K}^n) = n$. Für jeden Vektor $\mathbf{y} = (y_1, \ldots y_n) \in \mathcal{K}^n$ gibt es Skalare $\alpha_i = y_i \cdot x_i^{-1} \in \mathcal{K}$, $1 \leq i \leq n$, mit

$$\mathbf{y} = (y_1, \ldots, y_n) = \sum_{i=1}^{n} \alpha_i \mathbf{e_i}$$

Lösungen zu den Aufgaben

Aufgabe 1.2

(1) Es gibt ein q mit $a = m \cdot q + b$, und es gibt ein r mit $m = k \cdot r$. Es folgt $a = k \cdot (r \cdot q) + b$, woraus die Behauptung $a = b\,(k)$ folgt.

(2) Es gibt ein q mit $2^m = m \cdot q + 2$. Es folgt, dass $q \in \mathbb{G}_+$ sein muss, da $2^m, 2 \in \mathbb{G}_+$ und $m \in \mathbb{U}_+$ ist. Es gibt also ein r mit $q = 2 \cdot r$. Damit erhalten wir $2^m = 2m \cdot r + 2$, woraus die Behauptung $2^m = 2\,(2m)$ folgt.

(3) Es gilt die binomische Formel

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} \tag{E.1}$$

Dabei gilt

$$\binom{p}{0} = \binom{p}{p} = 1 \tag{E.2}$$

sowie

$$\binom{p}{1} = \binom{p}{p-1} = p = 0\,(p) \tag{E.3}$$

Wir betrachten

$$\binom{p}{k} \text{ für } 2 \leq k \leq p-2$$

Es gilt

$$\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1} = p \cdot \frac{\binom{p-1}{k-1}}{k} \tag{E.4}$$

Da $\binom{p}{k}$ eine ganze Zahl ist, ist auch $\frac{p}{k}\binom{p-1}{k-1}$ eine ganze Zahl. Da p prim ist, ist k kein Teiler von p für $2 \leq k \leq p-2$, d.h. k muss ein Teiler von $\binom{p-1}{k-1}$ sein. Sei also

$$\frac{\binom{p-1}{k-1}}{k} = q$$

Damit gilt mit (E.4)

$$\binom{p}{k} = p \cdot q$$

woraus folgt, dass $p|\binom{p}{k}$ gilt und damit $\binom{p}{k} = 0\,(p)$ für $2 \leq k \leq p-2$. Deswegen sowie wegen (E.2) und (E.3) fallen in der Summe (E.1), wenn modulo p gerechnet wird, alle Summanden bis auf den ersten und letzten weg, womit die Behauptung gezeigt ist.

(4) Für $\ell = 2$ gilt die Behauptung offensichtlich. Sei also $\ell \geq 3$.

Wir zeigen zunächst mit vollständiger Induktion, dass es zu jedem $\ell \geq 3$ ein $b \in \mathbb{Z}$ gibt mit

$$(1+ap)^{p^{\ell-3}} = 1 + ap^{\ell-2} + bp^{\ell-1} \tag{E.5}$$

Für $\ell = 3$ gilt die Behauptung offensichtlich (wähle $b = 0$). Mit Verwendung der Induktionsannahme und mithilfe der binomischen Formel erhalten wir

$$\begin{aligned}
&(1+ap)^{p^{\ell-2}} \\
&= \left((1+ap)^{p^{\ell-3}}\right)^p && \text{Potenzrechengesetz} \\
&= \left(1 + ap^{\ell-2} + bp^{\ell-1}\right)^p && \text{Induktionsannahme} \\
&= \sum_{k=0}^{p} \binom{p}{k} \left((a+bp)p^{\ell-2}\right)^k && \text{binomische Formel} \\
&= 1 + p(a+bp)p^{\ell-2} + \sum_{k=2}^{p} \binom{p}{k} \left((a+bp)p^{\ell-2}\right)^k \\
&= 1 + ap^{\ell-1} + bp^{\ell} + \sum_{k=2}^{p} \binom{p}{k} \left((a+bp)p^{\ell-2}\right)^k
\end{aligned}$$

Die Summanden ab $k = 2$ enthalten wegen den Voraussetzungen $p,\ell \geq 3$ alle den Faktor p^{ℓ}. Somit gibt es eine Zahl $b' \in \mathbb{Z}$ mit

$$(1+ap)^{p^{\ell-2}} = 1 + ap^{\ell-1} + b'p^{\ell}$$

womit der Induktionsschritt gezeigt ist.

Wir kehren zur Aufgabe zurück und zeigen die Behauptung mithilfe von (E.5) und der binomischen Formel:

$$\begin{aligned}
(1+ap)^{p^{\ell-2}} &= \left((1+ap)^{p^{\ell-3}}\right)^p && \text{Potenzrechengesetz} \\
&= \left(1 + ap^{\ell-2} + bp^{\ell-1}\right)^p && \text{wegen (E.5)} \\
&= \sum_{k=0}^{p} \binom{p}{k} \left((a+bp)p^{\ell-2}\right)^k && \text{binomische Formel} \\
&= 1 + p(a+bp)p^{\ell-2} + \sum_{k=2}^{p-1} \binom{p}{k} \left((a+bp)p^{\ell-2}\right)^k + (a+bp)^p p^{(\ell-2)p} \\
&\in 1 + p(a+bp)p^{\ell-2} + p^{\ell}\mathbb{Z} + (a+bp)^p p^{(\ell-2)p}
\end{aligned}$$

wobei wir hier wie oben in der Induktion feststellen, dass die Summanden für $2 \leq k \leq p-1$ alle den Faktor p^{ℓ} enthalten. Des Weiteren gilt wegen $p,\ell \geq 3$:

$p^\ell | p^{(\ell-2)p}$. Wenn wir nun modulo p^ℓ rechnen erhalten wir

$$(1+ap)^{p^{\ell-2}} = 1 + p(a+bp)p^{\ell-2} = 1 + ap^{\ell-1} + bp^\ell = 1 + ap^{\ell-1} \; (p^\ell)$$

womit die Behauptung gezeigt ist.

(5) Hier ist die Behauptung für $\ell = 3$ offensichtlich; sei also $\ell \geq 4$. Mit einer Induktion analog zu der in (5) kann man zeigen, dass es für alle $\ell \geq 4$ und $a \in \mathbb{Z}$ ein $b \in \mathbb{Z}$ gibt mit

$$(1+4a)^{2^{\ell-4}} = 1 + 2^{\ell-2}a + 2^{\ell-1}b$$

Damit ergibt sich

$$\begin{aligned}(1+4a)^{2^{\ell-3}} &= \left((1+4a)^{2^{\ell-4}}\right)^2 \\ &= \left(1 + 2^{\ell-2}a + 2^{\ell-1}b\right)^2 \\ &= 1 + 2^{\ell-1}(a+2b) + 2^{2\ell-4}(a+2b)^2 \end{aligned} \tag{E.6}$$

Wegen der Voraussetzung $\ell \geq 4$ ist $\ell \leq 2\ell - 4$ und deswegen $2^\ell | 2^{2\ell-4}$. Damit ergibt aus (E.6) modulo 2 gerechnet

$$(1+4a)^{2^{\ell-3}} = 1 + 2^{\ell-1}(a+2b) = 1 + 2^{\ell-1}a + 2^\ell b = 1 + 2^{\ell-1}a \; (2^\ell)$$

und damit die Behauptung.

(6) Wir dividieren $a^n - b^n$ durch $a - b$ und erhalten im ersten Schritt

$$a^n - b^n = (a-b) \cdot a^{n-1} + a^{n-1}b - b^n$$

Wir fahren fort mit der Division des Restes

$$a^{n-1}b - b^n = (a-b) \cdot a^{n-2}b + a^{n-2}b^2 - b^n$$

usw. Letztendlich landen wir bei der vorletzten Divison

$$a^2 b^{n-2} - b^n = (a-b) \cdot ab^{n-2} + ab^{n-1} - b^n$$

und dann bei der letzten

$$ab^{n-1} - b^n = (a-b) \cdot b^{n-1}$$

bei der kein Rest mehr entsteht. Wir sammeln die Quotienten auf und erhalten insgesamt

$$a^n - b^n = (a-b) \cdot (a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}) = (a-b) \cdot \sum_{i=1}^{n} a^{n-i}b^{i-1}$$

Wir führen eine Probe durch

$$\begin{aligned}
(a-b)\cdot\sum_{i=1}^{n}a^{n-i}b^{i-1} &= a\cdot\sum_{i=1}^{n}a^{n-i}b^{i-1}-b\cdot\sum_{i=1}^{n}a^{n-i}b^{i-1}\\
&=\sum_{i=1}^{n}a^{n+1-i}b^{i-1}-\sum_{i=1}^{n}a^{n-i}b^{i}\\
&=a^{n}+\sum_{i=2}^{n}a^{n+1-i}b^{i-1}-\sum_{i=1}^{n-1}a^{n-i}b^{i}-b^{n}\\
&=a^{n}+\sum_{i=1}^{n-1}a^{n+1-(i+1)}b^{i+1-1}-\sum_{i=1}^{n-1}a^{n-i}b^{i}-b^{n}\\
&=a^{n}+\sum_{i=1}^{n-1}a^{n-i}b^{i}-\sum_{i=1}^{n-1}a^{n-i}b^{i}-b^{n}\\
&=a^{n}-b^{n}
\end{aligned}$$

und erhalten das Ergebnis bestätigt. Damit ist die Behauptung gezeigt.

Aufgabe 1.3

Wir nehmen an, es gebe zu $a, b \in \mathbb{Z}$ zwei größte gemeinsame Teiler $t, t' \in \mathbb{N}_0$. Dann folgt aus der Definition, dass $t|t'$ und dass $t'|t$ gelten. Mit Korollar 1.2 i) folgt, da $t, t' \in \mathbb{N}_0$ ist, dass $t = t'$ sein muss.

Aufgabe 1.5

Wir nehmen an, es sei $(a, k) = t > 1$. Es folgt $t|a$ sowie $t|k$, d.h. es gibt q und p mit $a = q \cdot t$ bzw. $k = p \cdot t$. Des Weiteren gibt es ein r mit $m = r \cdot k$. Durch Einsetzen erhalten wir $m = r \cdot p \cdot t$. Das heißt neben $t|a$ gilt auch $t|m$. Es folgt: t ist ein gemeinsamer Teiler von a und b, also gilt $(a, m) \geq t > 1$, was ein Widerspruch zur Voraussetzung $(a, m) = 1$ ist.

Aufgabe 1.6

a) Es gilt

$$\alpha_i = \alpha_1 \cdot 0 + \ldots + \alpha_{i-1} \cdot 0 + \alpha_i \cdot 1 + \alpha_{i+1} \cdot 0 + \ldots + \alpha_k \cdot 0$$

b) Es gilt:

$$\begin{aligned}
6\mathbb{Z} + 9\mathbb{Z} &= \{0, 3, -3, 6, -6, , 9, -9, 12, -12, \ldots\} = (6, 9)\mathbb{Z}\\
3\mathbb{Z} + 4\mathbb{Z} &= \{0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots\} = (3, 4)\mathbb{Z} = \mathbb{Z}\\
5\mathbb{Z} + 8\mathbb{Z} &= \{0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots\} = (5, 8)\mathbb{Z} = \mathbb{Z}
\end{aligned}$$

Generelle Vermutung: $a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}$.

Aufgabe 1.9

(1) Wir müssen die Anzahl der Primzahlen im Intervall $\left[2^{k-1}, 2^k\right]$ abschätzen. Mit dem Primzahlsatz erhalten wir

$$\begin{aligned}\pi\left(2^k\right) - \pi\left(2^{k-1}\right) &\approx \frac{2^k}{k \cdot \ln 2} - \frac{2^{k-1}}{(k-1) \cdot \ln 2} \\ &= \frac{2^{k-1}}{\ln 2} \cdot \frac{k-2}{k(k-1)} \\ &= \frac{1}{2} \cdot \frac{2^k}{k \ln 2} \cdot \frac{k-2}{k-1} \\ &\approx \frac{1}{2} \cdot \pi\left(2^k\right)\end{aligned}$$

(2) Die Wahrscheinlichkeit ist

$$\frac{\pi\left(2^k\right) - \pi\left(2^{k-1}\right)}{2^{k-1}} \approx \frac{\pi\left(2^k\right)}{2^k} \approx \frac{2^k}{2^k \cdot k \cdot \ln 2} \approx \frac{1.44}{k}$$

Für $k = 128$ ergibt sich die Wahrscheinlichkeit 0.01125, für $k = 512$ ergibt sich 0.0028125.

Aufgabe 1.11

Es ist

$$a = \prod_{p \in \mathbb{P}} p^{\pi_a(p)} \text{ und } b = \prod_{p \in \mathbb{P}} p^{\pi_b(p)} \tag{E.7}$$

Es sei

$$t = \prod_{p \in \mathbb{P}} p^{\min\{\pi_a(p), \pi_b(p)\}}$$

Aus diesen Darstellungen ist ersichtlich, dass $t|a$ und $t|b$ gilt, denn es ist sowohl $\min\{\pi_a(p), \pi_b(p)\} \leq \pi_a(p)$ als auch $\min\{\pi_a(p), \pi_b(p)\} \leq \pi_b(p)$; t ist also ein gemeinsamer Teiler von a und b.

Sei nun t' eine weiterer Teiler von a und b und

$$t' = \prod_{p \in \mathbb{P}} p^{\pi_{t'}(p)}$$

dessen Faktorisierung. Dann muss $p^{\pi_{t'}(p)} \leq \min\{\pi_a(p), \pi_b(p)\}$ für alle $p \in \mathbb{P}$ gelten. Hieraus folgt, dass $t'|t$ gilt. Insgesamt folgt $t = (a, b)$.

Es sei

$$c = \prod_{p \in \mathbb{P}} p^{\max\{\pi_a(p), \pi_b(p)\}} \tag{E.8}$$

Aus dieser Darstellung und den Darstellungen von a und b in (E.7) ist ersichtlich, dass sowohl $a|c$ als auch dass $b|c$ gilt, denn es ist $\pi_a(p) \leq \max\{\pi_a(p), \pi_b(p)\}$ als auch $\pi_b(p) \leq \max\{\pi_a(p), \pi_b(p)\}$; c ist also ein gemeinsames Vielfaches von a und b.

Aus (E.8) folgt

$$\pi_c(p) = \max\{\pi_a(p), \pi_b(p)\} \tag{E.9}$$

Sei nun c' ein weiteres Vielfaches von a und b mit

$$c' = \prod_{p \in \mathbb{P}} p^{\pi_{c'}(p)}$$

Da $a|c'$ und $b|c'$ gilt, folgt, dass $\pi_a(p) \leq \pi_{c'}(p)$ und $\pi_b(p) \leq \pi_{c'}(p)$ und damit dass $\max\{\pi_a(p), \pi_b(p)\} \leq \pi_{c'}(p)$ ist. Hieraus folgt mit (E.9) $\pi_c(p) \leq \pi_{c'}(p)$ und damit $c|c'$ und damit $c \leq c'$. Es folgt insgesamt, dass $c = [a, b]$ ist.

Aufgabe 1.12

(1) Für $a, b \in \{0, 1\}$ lässt sich die Gleichung nachrechnen. Für $a, b \geq 2$ folgt mit Satz 1.15:

$$\begin{aligned}
(a, b) \cdot [a, b] &= \prod_{p \in \mathbb{P}} p^{\min\{\pi_a(p), \pi_b(p)\}} \cdot \prod_{p \in \mathbb{P}} p^{\max\{\pi_a(p), \pi_b(p)\}} \\
&= \prod_{p \in \mathbb{P}} p^{\pi_a(p) + \pi_b(p)} \\
&= \prod_{p \in \mathbb{P}} p^{\pi_a(p)} \cdot p^{\pi_b(p)} \\
&= \prod_{p \in \mathbb{P}} p^{\pi_a(p)} \cdot \prod_{p \in \mathbb{P}} p^{\pi_b(p)} \\
&= a \cdot b
\end{aligned}$$

(2) Folgt unmittelbar aus Satz 1.16, da $(a, b) = 1$ vorausgesetzt ist.

Aufgabe 2.4

Alle Strukturen sind assoziativ, denn Addition und Multiplikation von ganzen Zahlen sind – auch modulo gerechnet – assoziativ, und Vereinigung und Durchschnitt von Mengen sind ebenfalls assoziative Verknüpfungen.

Alle Strukturen besitzen ein Einselement. Bei den additiven Strukturen ist das die 0, bei den multiplikativen ist das die 1. Bei der Vereinigung von Mengen ist die leere Menge $\emptyset$ das Einselement, und beim Durchschnitt von Mengen ist die gesamte Menge $M = \{a, b\}$ das Einselement.

Bei der Addition modulo 2 sind die beiden Elemente selbstinvers; bei der Multiplikation modulo 2 ist 1 zu sich selbstinvers, die 0 besitzt kein Inverses. Bei der

Addition modulo 5 ist das Element a invers zu $5-a$, denn $a+(5-a)=5=0$ modulo 5 gerechnet. Bei der Multiplikation modulo 5 sind die Elemente 1 und 4 selbstinvers, und 2 und 3 sind invers zueinander, d.h. es ist $2^{-1}=3$ und $3^{-1}=2$, denn es gilt $2\cdot 3=3\cdot 2=1$. Die Zahl 0 besitzt keine Inverses modulo 5. Bei der Vereinigung und dem Durchschitt besitzen nur die beiden Einselemente $\emptyset$ bzw. M ein Inverses, sie sind selbstinvers. Alle anderen Elemente sind nicht invertierbar.

Alle Strukturen sind kommutativ.

Aufgabe 2.5

Die additive Struktur modulo 2 in Abbildung 7 bildet eine abelsche Gruppe der Ordnung 2; 0 ist das Einselement, 1 ist selbtsinvers und hat die Ordnung 2.

Die multiplikative Struktur in dieser Abbildung bildet ein kommutatives Monoid mit dem Einselement 1. Entfernt man die 0, die kein Inverses besitzt, bleibt eine Gruppe übrig, die nur aus dem Einselement besteht.

Die additive Struktur modulo 5 in Abbildung 8 bildet eine abelsche Gruppe der Ordnung 5. 0 ist das Einselement, und a ist modulo 5 invers zu $5-a$. In Beispiel 2.1 f) haben wir bereits festgestellt, dass alle Elemente außer der 0 Ordnung 5 haben.

Die multiplikative Struktur in Abbildung 8 bildet eine abelsche Gruppe der Ordnung 4. 1 ist das Einselement, 1 und 4 sind selbstinvers, und 2 und 3 sind invers zueinander. 2 hat die Ordnung 4, denn 4 ist die kleinste Zahl, so dass $2^4=1$ modulo 5 ist. 3 hat ebenfalls die Ordnung 4, und 4 hat die Ordnung 2 (ist ja selbstinvers).

Die beiden Strukturen in Abbildung 9 bilden kommutative Monoide. Die leere Menge $\emptyset$ bzw. die Ausgangsmenge M sind die Einselemente. Außer diesen sind alle anderen Elemente nicht invertierbar.

Aufgabe 2.6

Verknüpfungstafel:

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Die Struktur ist offensichtlich abgeschlossen, die Multiplikation ist assoziativ und kommutativ, 1 ist das Einselement. Jedes Element besitzt ein Inverses: $1^{-1}=1, 2^{-1}=4, 3^{-1}=5, 4^{-1}=2, 5^{-1}=3, 6^{-1}=6$. Die Struktur bildet eine abelsche Gruppe der Ordnung 6.

Die Elementordnungen sind: $ord(1)=1$, $ord(2)=3$, $ord(3)=6$, $ord(4)=2$, $ord(5)=6$, $ord(6)=1$.

$\{1, 6\}$ bildet die einzige zweielementige Untergruppe, und $\{1, 2, 4\}$ ist die einzige dreielementige Untergruppe.

Aufgabe 2.7

Verknüpfungstafel:

$\circ$	*id*	*nid*	*rez*	*nrez*
id	*id*	*nid*	*rez*	*nrez*
nid	*nid*	*id*	*nrez*	*rez*
rez	*rez*	*nrez*	*id*	*nid*
nrez	*nrez*	*rez*	*nid*	*id*

Die Komposition von Funktionen ist generell assoziativ, und die Identität ist generell das Einselement dieser Verknüpfung. Aus der Tabelle ist ersichtlich („Symmetrie bezüglich der Hauptdiagonale“), dass die Struktur kommutativ ist. Aus der Tabelle ist ebenfalls ersichtlich, dass alle Elemente zu sich selbst invers sind. Diese Struktur bildet also eine abelsche Gruppe der Ordnung 4. Weil alle Elemente selbstinvers sind, gilt für alle $f \in \{nid, rez, nrez\}$ $f^2 = id$, d.h. alle Elemente außer dem Einselement id, welches natürlich die Ordnung 1 hat, haben die Ordnung 2.

Aufgabe 2.8

Die Operation ist abgeschlossen auf $\mathbb{R}$, denn für alle $a, b \in \mathbb{R}$ gilt $a * b = \sqrt[3]{a^3 + b^3} \in \mathbb{R}$.

Es gilt $a * b = \sqrt[3]{a^3 + b^3} = \sqrt[3]{b^3 + a^3} = b * a$, also ist $*$ kommutativ.

Weiterhin gilt:

$$\begin{aligned} a * (b * c) &= \sqrt[3]{a^3 + (\sqrt[3]{b^3 + c^3})^3} \\ &= \sqrt[3]{a^3 + b^3 + c^3} \\ &= \sqrt[3]{(\sqrt[3]{a^3 + b^3})^3 + c^3} = (a * b) * c \end{aligned}$$

Also ist $*$ assoziativ.

0 ist das neutrale Element dieser Struktur:

$$a * 0 = \sqrt[3]{a^3 + 0^3} = \sqrt[3]{a^3} = a = \sqrt[3]{0 + a^3} = \sqrt[3]{0^3 + a^3} = 0 * a$$

Zu a ist $-a$ invers, denn es gilt

$$a * -a = \sqrt[3]{a^3 + (-a)^3} = \sqrt[3]{a^3 - a^3} = \sqrt[3]{0} = 0$$

Aufgabe 2.9

(1) Wir zeigen zunächst die Abgeschlossenheit. Dazu müssen wir zeigen, dass $(a, b, c, d) * (e, f, g, h) \in \mathbb{Z}^{4,1}$, d.h. dass $(ae + bg, af + bh, ce + dg, cf + dh) \in \mathbb{Z}^{4,1}$

ist. Das gilt gemäß der Definition von $\mathbb{Z}^{4,1}$ genau dann, wenn $(ae+bg)(cf+dh)-(af+bh)(ce+dg)=1$ ist. Wir rechnen nach:

$$\begin{aligned}(ae+bg)(cf+dh)-(af+bh)(ce+dg) &= acef+adeh+bcfg+bdgh\\ &\quad -acef-adfg-bceh-bdgh\\ &= (ad-bc)eh+(ad-bc)(-fg)\\ &= (ad-bc)\cdot(eh-fg)\\ &= 1\end{aligned}$$

Die letzte Gleichung folgt, weil $(a,b,c,d),(e,f,g,h)\in\mathbb{Z}^{4,1}$ und damit $ad-bc=1$ und $eh-fg=1$ ist.

Jetzt rechnen wir nach, dass die Assoziativität

$$(a,b,c,d)*((ef,g,h)*(i,j,k,l))=((a,,c,d)*(e,f,g,h))*(i,j,k,l) \tag{E.10}$$

gilt: Einerseits erhalten wir

$$\begin{aligned}(a,b,c,d)*((ef,g,h)*(i,j,k,l)) &= (a,b,c,d)*\\ &\quad (ei+fk,\\ &\quad ej+fl,\\ &\quad gi+hk,\\ &\quad gj+hl)\\ &= (aei+afk+bgi+bhk,\\ &\quad aej+afl+bgi+bhl,\\ &\quad cei+cfk+dgi+dhk,\\ &\quad cej+cfl+dgj+dhl)\end{aligned} \tag{E.11}$$

und andererseits

$$\begin{aligned}((a,,c,d)*(e,f,g,h))*(i,j,k,l) &= (ae+bg,\\ &\quad af+bh,\\ &\quad ce+dg,\\ &\quad cf+dh)*(i,j,k,l)\\ &= (aei+bgi+afk+bhk,\\ &\quad aej+bgj+afl+bhl,\\ &\quad cei+dgi+cfk+dhk,\\ &\quad cej+dgj+cfl+dhl)\end{aligned} \tag{E.12}$$

Durch Vergleich von (E.11) und (E.12) stellen wir fest, dass (E.10) gilt.

Wir bestimmen nun das Einselement, d.h. wir suchen ein Element $(e,f,g,h)\in\mathbb{Z}^4$ mit $eh-fg=1$ und $(a,b,c,d)*(e,f,g,h)=(a,b,c,d)$, also mit $(ae+$

$bg, af+bh, ce+dg, cf+dh) = (a,b,c,d)$ für alle $(a,b,c,d) \in \mathbb{Z}^4$ mit $ad-bc = 1$. Wir suchen also $e,f,g,h \in \mathbb{Z}$ mit

$$ae + bg = a \tag{E.13}$$
$$af + bh = b \tag{E.14}$$
$$ce + dg = c \tag{E.15}$$
$$cf + dh = d \tag{E.16}$$

Die Gleichungen (E.13) und (E.15) sind erfüllt für $e = 1$ und $g = 0$, und die Gleichungen (E.14) und (E.16) sind erfüllt für $f = 0$ und $h = 1$. Für das Element $(e,f,g,h) = (1,0,0,1)$ gilt einerseits $eh - fg = 1$, es ist also $(1,0,0,1) \in \mathbb{Z}^{4,1}$, und andererseits gilt $(a,b,c,d) * (1,0,0,1) = (a\cdot 1 + b\cdot 0, a\cdot 0 + b\cdot 1, c\cdot 1 + d\cdot 0, c\cdot 0 + d\cdot 1) = (a,b,c,d)$. Insgesamt folgt, dass $(1,0,0,1)$ das Einselement von $\mathcal{SL}_2(\mathbb{Z})$ ist.

Jetzt müssen wir noch zeigen, dass zu jedem Element $(a,b,c,d) \in \mathbb{Z}^{4,1}$ ein Element $(e,f,g,h) \in \mathbb{Z}^{4,1}$ existiert mit $(a,b,c,d) * (e,f,g,h) = (1,0,0,1)$. Wir suchen also $e,f,g,h \in \mathbb{Z}$ mit

$$ae + bg = 1 \tag{E.17}$$
$$af + bh = 0 \tag{E.18}$$
$$ce + dg = 0 \tag{E.19}$$
$$cf + dh = 1 \tag{E.20}$$

Wenn wir berücksichtigen, dass $ad - bc = 1$ ist, werden die Gleichungen (E.17) und (E.19) für $e = d$ und $g = -c$ erfüllt, und die Gleichungen (E.18) und (E.20) werden für $f = -b$ und $h = a$ erfüllt. Wir erhalten also $(e,f,g,h) = (d,-b,-c,a)$. Für dieses Element gilt $eh - gf = da - (-b)(-c) = ad - bc = 1$ und $(a,b,c,d) * (e,f,g,h) = (a,b,c,d) * (d,-b,-c,a) = (ad-bc, -ab+ab, cd-dc, -bc+da) = (1,0,0,1)$. Es folgt also zusammengefasst

$$(a,b,c,d)^{-1} = (d,-b,-c,a)$$

$\mathcal{SL}_2(\mathbb{Z})$ bildet also eine Gruppe. Diese Gruppe ist nicht abelsch. Dazu betrachten wir folgendes Beispiel: Für $(1,1,1,2), (2,3,1,2) \in \mathcal{SL}_2(\mathbb{Z})$ gilt

$$(1,1,1,2) * (2,3,1,2) = (3,5,4,7) \neq (5,8,3,5) = (2,3,1,2) * (1,1,1,2)$$

(2) Wir zeigen mit vollständiger Induktion, dass $\mathbf{a}^n = (1,n,0,1)$ für alle $n \in \mathbb{N}$ gilt: Für $n = 1$ gilt die Behauptung offensichtlich. Wir berechnen $\mathbf{a}^{n+1}$ mithilfe von $\mathbf{a}^n = (1,n,0,1)$:

$$\begin{aligned}
\mathbf{a}^{n+1} &= \mathbf{a}^n * \mathbf{a} \\
&= (1,n,0,1) * (1,1,0,1) \\
&= (1\cdot 1 + n\cdot 0, 1\cdot 1 + n\cdot 1, 0\cdot 1 + 1\cdot 0, 0\cdot 1 + 1\cdot 1) \\
&= (1, n+1, 0, 1)
\end{aligned}$$

womit die Induktionsbehauptung gezeigt ist. Es folgt: $\mathbf{a}$ hat unendliche Ordnung.

(2) Es gilt

$$\begin{aligned}\mathbf{b}^4 &= (0,1,-1,0)^4\\ &= (0,1,-1,0)^2 * (0,1,-1,0)^2\\ &= (-1,0,0,-1) * (-1,0,0,1)\\ &= (1,0,0,1)\end{aligned}$$

und damit $ord_{\mathcal{SL}_2(\mathbb{Z})}(0,1,-1,0) = 4$.

Es gilt

$$\begin{aligned}\mathbf{c}^6 &= (0,-1,1,1)^6\\ &= (0,-1,1,1)^2 * (0,-1,1,1)^2 * (0,-1,1,1)^2\\ &= (-1,-1,1,0) * (-1,-1,1,0) * (-1,-1,1,0)\\ &= (0,1,-1,-1) * (-1,-1,1,0)\\ &= (1,0,0,1)\end{aligned}$$

und damit $ord_{\mathcal{SL}_2(\mathbb{Z})}(0,-1,1,1) = 6$.

Aufgabe 2.10

a) Es gilt z.B. $\{a\} \cup \{a,b\} = \{b\} \cup \{a,b\}$, es ist aber $\{a\} \neq \{b\}$. Analog gilt $\emptyset \cap \{a\} = \emptyset \cap \{b\}$ und $\{a\} \neq \{b\}$.

b) Wir betrachten die Verknüfungstafel der Gruppe $\mathcal{G} = (\{a_1, \ldots, a_n\}, *)$, dabei seien die Elemente in der Reihenfolge, wie sie in der Verknüpfungstafel aufgeführt sind, indiziert. Wir stellen die Überlegungen für die i Zeile an, für Spalten sind sie vollkommen analog.

Wir nehmen an, dass in der Zeile i in den Spalten r und s mit $r \neq s$ dasselbe Element steht. Das bedeutet, dass $a_i * a_r = a_i * a_s$ ist, woraus mit der Kürzungsregel $a_r = a_s$ folgt, ein Widerspruch zur Voraussetzung $r \neq s$.

In der Zeile i wird das Element a_i mit jedem a_j, $1 \leq i \leq n$, verknüpft; in der i-ten Zeile stehen also die Elemente der Menge $a_i * \mathcal{G} = \{a_i * a_1, a_1 * a_2, \ldots, a_i * a_n\}$. Offensichtlich kann diese Menge nicht mehr als n Elemente haben, d.h. es ist $|a_i * \mathcal{G}| \leq n$. Wegen der obigen Überlegung sind alle Elmente diese Menge aber verschieden voneinander, d.h. in der i-ten Zeile treten alle n Elemente von $\mathcal{G}$ auf: $a_i * \mathcal{G} = \mathcal{G}$.

c) Es gilt

$$\begin{aligned}a * b &= (a * b)^{-1} && \text{weil alle Elemente selbstinvers sind, also auch } a * b\\ &= b^{-1} * a^{-1} && \text{wegen Satz 2.1 e)}\\ &= b * a && \text{weil alle Elemente, also auch } a \text{ und } b, \text{ selbstinvers sind}\end{aligned}$$

Aufgabe 2.11

Es sei $\mathcal{G}_1 = (\mathbb{Z}_2, +)$ die additive Gruppe modulo 2 und $\mathcal{G}_2 = (\mathbb{Z}_5^*, \cdot)$ die multiplikative Gruppe modulo 5, dann ist die Verknüpfungstafel von $\mathcal{G}_1 \times \mathcal{G}_2 = (\mathbb{Z}_2 \times \mathbb{Z}_5^*, *)$ gegeben durch:

$*$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,4)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,4)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,4)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,4)$
$(0,2)$	$(0,2)$	$(0,4)$	$(0,1)$	$(0,3)$	$(1,2)$	$(1,4)$	$(1,1)$	$(1,3)$
$(0,3)$	$(0,3)$	$(0,1)$	$(0,4)$	$(0,2)$	$(1,3)$	$(1,1)$	$(1,4)$	$(1,2)$
$(0,4)$	$(0,4)$	$(0,3)$	$(0,2)$	$(0,1)$	$(1,4)$	$(1,3)$	$(1,2)$	$(1,1)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,4)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,4)$
$(1,2)$	$(1,2)$	$(1,4)$	$(1,1)$	$(1,3)$	$(0,2)$	$(0,4)$	$(0,1)$	$(0,3)$
$(1,3)$	$(1,3)$	$(1,1)$	$(1,4)$	$(1,2)$	$(0,3)$	$(0,1)$	$(0,4)$	$(0,2)$
$(1,4)$	$(1,4)$	$(1,3)$	$(1,2)$	$(1,1)$	$(0,4)$	$(0,3)$	$(0,2)$	$(0,1)$

Das Einselement ist $(0,1)$, und die Inversen sind: $(0,1)^{-1} = (0,1)$, $(0,2)^{-1} = (0,3)$, $(0,3)^{-1} = (0,2)$, $(0,4)^{-1} = (0,4)$, $(1,1)^{-1} = (1,1)$, $(1,2)^{-1} = (1,3)$, $(1,3)^{-1} = (1,2)$, $(1,4)^{-1} = (1,4)$.

Aufgabe 2.13

Zeige: $a, b \in U_1 \cap U_2$ genau dann, wenn $a^{-1} * b \in U_1 \cap U_2$ ist.

$$\begin{aligned} a, b \in U_1 \cap U_2 \quad & \text{genau dann, wenn} \quad a, b \in U_1 \wedge a, b \in U_2 \\ & \text{genau dann, wenn} \quad a^{-1} * b \in U_1 \wedge a^{-1} * b \in U_2 \\ & \text{genau dann, wenn} \quad a^{-1} * b \in U_1 \cap U_2 \end{aligned}$$

Aufgabe 2.14

(1) Wir benutzen Satz 2.5 b) und zeigen, dass für $a, b \in m\mathbb{Z}$ auch $a - b \in m\mathbb{Z}$ ist. Zu $a, b \in m\mathbb{Z}$ gibt es $x_a, x_b \in \mathbb{Z}$ mit $a = m \cdot x_a$ bzw. $b = m \cdot x_b$. Damit gilt $a - b = m \cdot x_a - m \cdot x_b = m \cdot (x_a - x_b) \in m\mathbb{Z}$, da für $x_a, x_b \in \mathbb{Z}$ auch $x_a - x_b \in \mathbb{Z}$ ist.

(2) Wir verwenden Satz 2.5 b) und zeigen, dass für $a, b \in \mathcal{G}_U$ gilt: $a * b^{-1} \in \mathcal{G}_U$.

Sei also $a, b \in \mathcal{G}_U$, mit $ord_{\mathcal{G}}(a) = r$, d.h. es ist $r \in \mathbb{U}_+$, bzw. mit $ord_{\mathcal{G}}(b) = s$, d.h. es ist $s \in \mathbb{U}_+$. Es gilt $r \cdot s \in \mathbb{U}_+$. Des Weiteren gilt, da $\mathcal{G}$ abelsch ist,

$$\left(a * b^{-1}\right)^{r \cdot s} = \left(a^r\right)^s * \left(b^s\right)^{-r} = e^s * e^{-r} = e$$

Mithilfe von Satz 2.2 b) folgt

$$ord_{\mathcal{G}}(a * b^{-1}) \mid r \cdot s$$

Da $r \cdot s \in \mathbb{U}_+$ ist, muss ebenso $ord_{\mathcal{G}}(a * b^{-1}) \in \mathbb{U}_+$ sein. Damit gilt, dass $a * b^{-1} \in \mathcal{G}_U$ ist, was zu zeigen war.

Aufgabe 2.15

(1) Es gilt $e \in \mathcal{I}(\mathcal{G})$.

(2) Ist m gerade, dann gilt $2x = 0$ genau dann, wenn $x = 0$ oder $x = \frac{m}{2}$ ist. Ist m ungerade, dann gilt $2x = 0$ genau dann, wenn $x = 0$ ist. Somit gilt

$$\mathcal{I}(\mathcal{Z}_m) = \begin{cases} \{0, \frac{m}{2}\}, & m \text{ gerade} \\ \{0\}, & m \text{ ungerade} \end{cases}$$

(3) Es gilt $1, m-1 \in \mathbb{Z}_m^*$ (und $1 \neq m-1$) für alle $m \geq 3$.

(4) Sei $a, b \in \mathcal{I}(\mathcal{G})$, dann ist $a^2 = e$ und $b^2 = e$. Es folgt mit der Kommutativität

$$\left(a * b^{-1}\right)^2 = a^2 * \left(b^{-1}\right)^2 = a^2 * \left(b^2\right)^{-1} = e * e^{-1} = e$$

Also ist $\left(a * b^{-1}\right)^2 \in \mathcal{I}(\mathcal{G})$, womit mit Satz 2.5 b) die Behauptung folgt.

Aufgabe 2.16

(1) gilt offensichtlich.

(2) gilt, da $e \in \mathcal{C}(\mathcal{G})$ ist.

(3) Es sei $a, b \in \mathcal{C}(\mathcal{G})$, dann gilt

$$x * a = a * x \text{ für alle } x \in \mathcal{G} \tag{E.21}$$
$$x * b = b * x \text{ für alle } x \in \mathcal{G} \tag{E.22}$$

Des Weiteren gilt mit diesen Gleichungen:

$$\begin{aligned} x * a = a * x \quad &\text{gdw. } (x * a)^{-1} = (a * x)^{-1} \\ &\text{gdw. } a^{-1} * x^{-1} = x^{-1} * a^{-1} \\ &\text{gdw. } x * \left(a^{-1} * x^{-1}\right) * (x * b) = x * \left(x^{-1} * a^{-1}\right) * (b * x) \\ &\text{gdw. } x * \left(a^{-1} * b\right) = \left(a^{-1} * b\right) * x \\ &\text{gdw. } a^{-1} * b \in \mathcal{C}(\mathcal{G}) \end{aligned}$$

Für $a, b \in \mathcal{C}(\mathcal{G})$ folgt also $a^{-1} * b \in \mathcal{C}(\mathcal{G})$, woraus mit Satz 2.5 a) die Behauptung folgt.

Aufgabe 2.17

(1) Wir zeigen (i) $\mathcal{G}_U * \mathcal{G}_U \subseteq \mathcal{G}_U$ und (ii) $\mathcal{G} \subseteq \mathcal{G}_U * \mathcal{G}_U$, womit die Behauptung gezeigt ist.

Zu (i): Sei $a \in \mathcal{G}_U * \mathcal{G}_U$, dann gibt es $b, c \in \mathcal{G}_U$ mit $a = b * c$. Da $\mathcal{G}_U$ abgeschlossen ist, ist $b * c \in \mathcal{G}_U$ und damit $a \in \mathcal{G}_U$, womit $\mathcal{G}_U * \mathcal{G}_U \subseteq \mathcal{G}_U$ gezeigt ist.

Zu (ii): Es gilt $\mathcal{G}_U = e * \mathcal{G}_U \subseteq \mathcal{G}_U * \mathcal{G}_U$.

(2) Diese Behauptung folgt unmittelbar aus der Abgeschlossenheit der Untergruppe $\mathcal{G}_U$ gegenüber Inversenbildung: Es gilt

$$a \in \mathcal{G}_U^{-1} \text{ gdw. } a^{-1} \in \mathcal{G}_U \text{ gdw. } a \in \mathcal{G}_U$$

(3) folgt unmittelbar aus (1) und (2): $\mathcal{G}_U * \mathcal{G}_U^{-1} = \mathcal{G}_U * \mathcal{G}_U = \mathcal{G}_U$.

(4) Es gilt

$$\begin{aligned}
a * \mathcal{G}_U * a^{-1} &= a * \mathcal{G}_U * \mathcal{G}_U^{-1} * a^{-1} && \text{wegen (3)} \\
&= a * \mathcal{G}_U * (\, a * \mathcal{G}_U \,)^{-1} && \text{wegen Satz 2.1 e)} \\
&= b * \mathcal{G}_U * (\, b * \mathcal{G}_U \,)^{-1} && \text{wegen Voraussetzung} \\
&= b * \mathcal{G}_U * \mathcal{G}_U^{-1} * b^{-1} && \text{wegen Satz 2.1 e)} \\
&= b * \mathcal{G}_U * b^{-1} && \text{wegen (3)}
\end{aligned}$$

Aufgabe 2.18

(1) Es gilt:

$$\begin{aligned}
&\langle\, 1 \,\rangle = \{1\} \\
&\langle\, 2 \,\rangle = \{1, 2, 4\} \\
&\langle\, 3 \,\rangle = \{1, 3, 2, 6, 4, 5\} = \mathbb{Z}_7^* \\
&\langle\, 4 \,\rangle = \{1, 4, 2\} = \langle\, 2 \,\rangle \\
&\langle\, 5 \,\rangle = \{1, 5, 4, 6, 2, 3\} = \mathbb{Z}_7^* \\
&\langle\, 6 \,\rangle = \{1, 6\}
\end{aligned}$$

Die Gruppe $\mathbb{Z}_7^*$ ist zyklisch; sie besitzt die Generatoren 3 und 5.

(2) Die Elemente von $\mathbb{Z}_2 \times \mathbb{Z}_{2^k}$ haben die Gestalt (a, b) mit $a \in \{0, 1\}$ und $0 \leq b \leq 2^k - 1$. Von einem Element $(0, b)$, $b \neq 0$, kann kein Element $(1, b')$ durch fortgesetzte Addition erreicht werden, d.h. es gibt kein $n \in \mathbb{N}$ mit $n \cdot (0, b) = (1, b')$, weil $n \cdot 0 = 0$ ist. Die Elemente $(0, b)$ können also keine Erzeuger sein.

Betrachten wir nun Elemente der Art $(1, b)$ als potenzielle Erzeuger. Diese müssten u.a. alle Elemente der Art $(0, b')$ durch fortgesetzte Addition erzeugen, d.h. es muss ein $n \in \mathbb{N}$ geben mit $n \cdot (1, b) = (0, b')$. Es folgt, dass n gerade sein muss, damit $n \cdot 1 = 0$ ist. Daraus folgt, dass $b' = n \cdot b$ ebenfalls gerade ist. Das bedeutet, dass Element der Art $(0, b')$ mit b' ungerade nicht von Elementen der Art $(1, b)$ erzeugt werden können.

Damit ist insgesamt die Behauptung gezeigt.

Aufgabe 2.21

Es ist (siehe oben) $\langle 2 \rangle = \{1, 2, 4\}$; damit ergibt sich:

$$\begin{aligned}
1 \cdot \langle 2 \rangle &= \{1, 2, 4\} = \langle 2 \rangle \\
2 \cdot \langle 2 \rangle &= \{1, 2, 4\} = \langle 2 \rangle \\
3 \cdot \langle 2 \rangle &= \{3, 5, 6\} \\
4 \cdot \langle 2 \rangle &= \{1, 2, 4\} = \langle 2 \rangle \\
5 \cdot \langle 2 \rangle &= \{3, 5, 6\} \\
6 \cdot \langle 2 \rangle &= \{3, 5, 6\}
\end{aligned}$$

Des Weiteren gilt $\mathbb{Z}_7^*/\langle 2 \rangle = \{\{1, 2, 4\}, \{3, 5, 6\}\} = \langle 2 \rangle \backslash \mathbb{Z}_7^*$.

Aufgabe 2.22

Die Abbildung φ_a ist offensichtlich total definiert. Sie ist injektiv. Denn, wenn wir annehmen, dass $\varphi_a(x) = \varphi_a(y)$ für $x \neq y$ ist, folgt $ax = ay$ und daraus mit der Kürzungsregel $x = y$, ein Widerspruch zur Voraussetzung $x \neq y$. Um die Surjektivität zu zeigen, müssen wir zu jedem $y \in aU$ ein $x \in U$ angeben mit $\varphi_a(x) = y$. Sei also $y \in aU$, d.h. es gibt ein $u \in U$ mit $y = a * u$. Wir wählen jetzt $x = u$, dann gilt $\varphi_a(x) = \varphi_a(u) = a * u = y$.

φ_a ist also total, injektiv und surjektiv und damit bijektiv.

Aufgabe 2.23

Die Verknüpfungstafel für die Faktorgruppe $\mathbb{Z}_7^*/\langle 2 \rangle$ ist:

$*_{\langle 2 \rangle}$	$\{1, 2, 4\}$	$\{3, 5, 6\}$
$\{1, 2, 4\}$	$\{1, 2, 4\}$	$\{3, 5, 6\}$
$\{3, 5, 6\}$	$\{3, 5, 6\}$	$\{1, 2, 4\}$

Aufgabe 2.23

(1) Es ist:

$$\begin{aligned}
\mathbb{Z}_2^* &= \{1\} \\
\mathbb{Z}_3^* &= \{1, 2\} \\
\mathbb{Z}_4^* &= \{1, 3\} \\
\mathbb{Z}_5^* &= \{1, 2, 3, 4, 5\} \\
\mathbb{Z}_6^* &= \{1, 5\} \\
\mathbb{Z}_7^* &= \{1, 2, 3, 4, 5, 6\} \\
\mathbb{Z}_8^* &= \{1, 3, 5, 7\}
\end{aligned}$$

(2) 1 ist als Einselement immer zu sich selbstinvers. Das Gleiche gilt für $-1 = m-1\,(m)$, denn es ist: $(-1) \cdot (-1) = (m-1) \cdot (m-1) = m^2 - 2m + 1 = 1\,(m)$.

(3) Alle diese Strukturen sind abelsche Gruppen.

Aufgabe 2.24

Eine Gruppe mit zwei Elementen e und a, von denen eines das Einselment sein muss, kann nur folgende Verknüpfungstafel besitzen (dabei sei e das Einselement):

$*$	e	a
e	e	a
a	a	e

Die erste Zeile und die erste Spalte sind klar, weil e Einselement ist, und es muss $a * a = e$ sein, sonst wäre a nicht invertierbar. Abgesehen von der Benennung der Elemente gibt es also genau eine Gruppe mit zwei Elementen (siehe auch Abbildung 7).

Wir betrachten nun Möglichkeiten für Gruppen mit drei Elementen e (Einselement), a und b. Da e Einselement ist, sind die erste Zeile und die erste Spalte der Verknüpfungstabelle festgelegt:

$*$	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

Es gibt zwei Möglichkeiten: a und b sind beide selbstinvers, oder a und b sind zueinander invers. Mit der ersten Möglichkeit wäre die Diagonale der Tabelle festgelegt:

$*$	e	a	b
e	e	a	b
a	a	e	?
b	b	?	e

Man sieht, dass diese Belegung nicht korrekt ist, denn jede Belegung der Fragezeichen mit a oder b führt zu Widersprüchen (siehe Übung 2.10 b). Es gibt also nur die folgende Verknüpfungstafel:

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Abgesehen von der Benennung der Elemente gibt es also nur eine Gruppe mit drei Elementen.

Aufgabe 2.27

(1) (i) Die Abbildung $\varphi : \mathbb{K}_4 \to F$ definiert durch $\varphi(0) = id$, $\varphi(1) = nid$, $\varphi(2) = rez$ und $\varphi(3) = nrez$ ist ein Isomorphismus, was man durch Vergleich der Verknüpfungstafeln leicht nachvollziehen kann.

(ii) Die Abbildung $\varphi : \mathbb{K}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ definiert durch $\varphi(0) = (0,0)$, $\varphi(1) = (0,1)$, $\varphi(2) = (1,0)$ und $\varphi(3) = (1,1)$ ist ein Isomorphismus.

(iii) Die Abbildung $\varphi : \mathbb{K}_4 \to \mathbb{Z}_8^*$ definiert durch $\varphi(0) = 1$, $\varphi(1) = 3$, $\varphi(2) = 5$ und $\varphi(3) = 7$ ist ein Isomorphismus.

(2) Wir definieren $z : \mathbb{R} \to \mathbb{R}_+ - \{0\}$ durch: $z(x) = 2^x$. Die Exponentialfunktion z ist bijektiv und es gilt:

$$z(x+y) = 2^{x+y} = 2^x \cdot 2^y = z(x) \cdot z(y)$$

Dieser Isomorphismus ist die Grundlage für den dualen Logarithmus $\log$: Es gilt $y = z^x$ genau dann, wenn $x = \log y$ ist. $\log$ ist die Umkehrfunktion von z und damit auch ein Isomorphismus (siehe Korollar 2.11 b). Es gilt also $\log(a \cdot b) = \log a + \log b$. Man kann also eine Multiplikation von zwei Zahlen a und b mithilfe der Addition ihrer Logarithmen berechnen. Einfaches Beispiel:

$$16 \cdot 64 = z(\log(16 \cdot 64)) = z(\log 16 + \log 64) = z(4+6) = z(10) = 2^{10} = 1024$$

(3) Wir definieren $\varphi : \mathbb{Z} \to m \cdot \mathbb{Z}$ durch $\varphi(x) = mx$. Es gilt: φ ist bijektiv sowie

$$\varphi(x+y) = m(x+y) = mx + my = \varphi(x) + \varphi(y)$$

Aufgabe 2.28

Wir zeigen: Ist $y, z \in \mathit{Bild}(\varphi))$, dann ist auch $y^{-1} *_2 z \in \mathit{Bild}(\varphi)$. Sei also $y, z \in \mathit{Bild}(\varphi)$. Dann gibt es $a, b \in \mathcal{G}_1$ mit $\varphi(a) = y$, d.h. mit $(\varphi(a))^{-1} = y^{-1}$, bzw. mit $\varphi(b) = z$. Damit gilt

$$y^{-1} *_2 z = (\varphi(a))^{-1} *_2 \varphi(b) = \varphi(a^{-1}) *_2 \varphi(b) = \varphi(a^{-1} *_1 b) \in \mathit{Bild}(\varphi)$$

Zu $y, z \in \mathit{Bild}(\varphi)$ gilt also $y^{-1} *_2 z \in \mathit{Bild}(\varphi)$, woraus mit Satz 2.5 a) die Behauptung folgt.

Aufgabe 2.29

a) φ ist offensichtlich eine *totale* Abbildung.

φ ist *injektiv*, denn aus $\varphi(x) = \varphi(y)$ folgt $x^{-1} = y^{-1}$ und daraus unmittelbar $x = y$.

φ ist *surjektiv*: Sei $y \in \mathcal{G}$, setze $x = y^{-1}$, dann gilt $\varphi(x) = x^{-1} = (y^{-1})^{-1} = y$. Es gibt also zu jedem $x \in \mathcal{G}$ ein $y \in \mathcal{G}$ mit $\varphi(x) = y$.

Damit φ ein Homomorphismus ist, muss $\mathcal{G}$ abelsch sein, sonst gilt die Strukturgleichung nicht:

$$\varphi(x * y) = (x * y)^{-1} = y^{-1} * x^{-1} = x^{-1} * y^{-1} = \varphi(x) * \varphi(y)$$

b) (1) Da $t * x * t^{-1} \neq t * y * t^{-1}$ ist für $x \neq y$, ist φ_t rechtseindeutig, also eine Funktion, und φ_t ist offensichtlich für alle t total definiert.

Aus $\varphi_t(x) = \varphi_t(y)$ folgt $t * x * t^{-1} = t * y * t^{-1}$ und daraus $x = y$. φ_t ist also injektiv für alle t.

Es sei $y \in \mathcal{G}$. Wir setzen $x = t^{-1} * y * t$. Dann gilt

$$\varphi_t(x) = \varphi_t(t^{-1} * y * t) = t * (t^{-1} * y * t) * t^{-1} = y$$

Zu jedem y gibt es also ein x mit $\varphi_t(x) = y$. φ_t ist also surjektiv.

Des Weiteren erfüllt φ_t die Strukturgleichung:

$$\begin{aligned}\varphi_t(x * y) &= t * (x * y) * t^{-1} \\ &= t * x * e * y * t^{-1} \\ &= (t * x * t^{-1}) * (t * y * t^{-1}) \\ &= \varphi_t(x) * \varphi_t(y)\end{aligned}$$

(3) $\mathcal{AUT}$ ist offensichtlich abgeschlossen und $\circ$, die Komposition von Funktionen, ist bekanntermaßen assoziativ. φ_e ist das Einselement von $\mathcal{AUT}$, denn es gilt

$$\varphi_e(x) = e * x * e^{-1} = x = \mathit{id}_{\mathcal{G}}(x)$$

Das Inverse von φ_t ist $\varphi_{t^{-1}}$, denn es gilt

$$\varphi_t \circ \varphi_{t^{-1}}(x) = \varphi_t(t^{-1} * x * t) = t * (t^{-1} * x * t) * t^{-1} = x = \mathit{id}_{\mathcal{G}}(x) = \varphi_e(x)$$

Aufgabe 2.30

a) Es muss gezeigt werden, dass f_a total, surjektiv und injektiv ist.

f_a ist für jedes $x \in \mathcal{G}$ definiert, da wegen der Abgeschlossenheit von $\mathcal{G}$ für jedes $x \in \mathcal{G}$ das Produkt $a * x$ definiert ist. f_a ist also *total*.

Sei $y \in \mathcal{G}$. Wir setzen $x = a^{-1} * y$. Dann gilt

$$f_a(x) = a * x = a * (a^{-1} * y) = (a * a^{-1}) * y = e * y = y$$

Zu jedem $y \in \mathcal{G}$ gibt es also ein $x \in \mathcal{G}$ (nämlich $x = a^{-1} * y$) mit $f_a(x) = y$, d.h. f_a ist *surjektiv*.

Es sei $f_a(x_1) = f_a(x_2)$. Dann ist gemäß Definition von f_a: $a * x_1 = a * x_2$, woraus mit der Kürzungsregel $x_1 = x_2$ folgt. Aus $f_a(x_1) = f_a(x_2)$ folgt also $x_1 = x_2$, womit die *Injektivität* von f_a gezeigt ist.

b) Multiplikationstafel von $(\mathbb{Z}_5^*, \cdot)$:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Für die Abbildungen f_1, f_2, f_3, f_4 ergibt sich:

x	$f_1(x) = 1 \cdot x$	$f_2(x) = 2 \cdot x$	$f_3(x) = 3 \cdot x$	$f_4(x) = 4 \cdot x$
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

c) *Abgeschlossenheit:* Es seien $f_a, f_b \in \mathcal{F}(\mathcal{G})$. Dann gilt:

$$(f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(b * x) = a * (b * x) = (a * b) * x = f_{a*b}(x)$$

Es folgt, dass

$$f_a \circ f_b = f_{a*b} \tag{E.23}$$

ist. Da $a * b \in \mathcal{G}$ ist, ist auch $f_{a*b} \in \mathcal{F}(\mathcal{G})$ und damit $f_a \circ f_b \in \mathcal{F}(\mathcal{G})$, womit die Abgeschlossenheit von $\mathcal{F}(\mathcal{G})$ gezeigt ist.

Assoziativität: Die Komposition von Funktionen ist generell assoziativ. In diesem Beispiel lässt sich die Assoziativität von $\circ$ auch durch die Assoziativität von $*$ begründen (dabei verwenden wir die Gleichung (E.23)):

$$f_a \circ (f_b \circ f_c) = f_a \circ f_{b*c} = f_{a*(b*c)} = f_{(a*b)*c} = f_{a*b} \circ f_c = (f_a \circ f_b) \circ f_c$$

Das *Einselement* von $\mathcal{F}(\mathcal{G})$ ist f_e, denn es gilt mit (E.23):

$$f_e \circ f_a = f_{e*a} = f_a = f_{a*e} = f_a \circ f_e$$

Inverse: Zu f_a ist $f_{a^{-1}}$ invers, denn es gilt mit (E.23):

$$f_a \circ f_{a^{-1}} = f_{a*a^{-1}} = f_e$$

d) Eine Multiplikationstafel für $\mathcal{F}(\mathbb{Z}_5^*)$ ist:

$\cdot$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_4	f_1	f_3
f_3	f_3	f_1	f_4	f_2
f_4	f_4	f_3	f_2	f_1

e) Wir definieren $\phi : \mathcal{G} \to \mathcal{F}(\mathcal{G})$ durch $\phi(a) = f_a$. Wir zeigen, dass ϕ ein Isomorphismus zwischen $\mathcal{G}$ und $\mathcal{F}(\mathcal{G})$ ist:

(i) ϕ ist bijektiv: ϕ ist offensichtlich total und surjektiv. Es bleibt noch zu zeigen, dass ϕ auch injektiv ist. Sei $\phi(a) = \phi(b)$. Dann ist $f_a(x) = f_b(x)$, d.h. $a*x = b*x$

für alle $x \in \mathcal{G}$, woraus mit der Kürzungsregel $a = b$ folgt. Aus $\phi(a) = \phi(b)$ folgt also $a = b$, d.h. ϕ ist injektiv.

(ii) Wir müssen nun noch zeigen, dass ϕ die Homomorphieeigenschaft besitzt, d.h. dass

$$\phi(a * b) = \phi(a) \circ \phi(b)$$

gilt. Dies folgt unmittelbar aus (E.23):

$$\phi(a * b) = f_{a*b} = f_a \circ f_b = \phi(a) \circ \phi(b)$$

Aus (i) und (ii) folgt, dass ϕ ein Isomorphismus zwischen $\mathcal{G}$ und $\mathcal{F}(\mathcal{G})$ ist.

f) Wenn man sich die beiden Multiplikationstafeln aus b) und d) ansieht, sieht man sofort, dass die beiden Gruppen $\mathbb{Z}_5^*$ und $\mathcal{F}(\mathbb{Z}_5^*)$ isomorph sind. Den Isomorphismus erkennt man unmittelbar aus den Tafeln: Er entspricht der allgemeinen Abbildung $\phi(x) = f_x$ aus e).

Aufgabe 2.31

a) Es gilt, dass φ offensichtlich total definiert ist, sowie

$$\begin{aligned}\varphi((a,b)+(c,d)) &= \varphi(a+c, b+d)\\ &= b+d-(a+c)\\ &= (b-a)+(d-c)\\ &= \varphi(a,b)+\varphi(c,d)\end{aligned}$$

und damit ist φ ein Homomorphismus von $(\mathbb{Z}^2, +)$ nach $(\mathbb{Z}, +)$.

b) Es ist

$$\begin{aligned}Kern(\varphi)) &= \Big\{(a,b) \in \mathbb{Z}^2 \mid \varphi(a,b) = 0\Big\}\\ &= \Big\{(a,b) \in \mathbb{Z}^2 \mid b-a = 0\Big\}\\ &= \{(a,a) \mid a \in \mathbb{Z}\}\end{aligned}$$

c) Da $Kern(\varphi) \neq \{(0,0)\}$ ist, folgt sofort, dass φ nicht injektiv und damit kein Isomorphismus ist.

d) Die Nebenklasse mit dem Repräsentanten $(3,7)$ ist gegeben durch:

$$\begin{aligned}(3,7) + Kern(\varphi) &= (3,7) + \{(a,a) \mid a \in \mathbb{Z}\}\\ &= \{(3,7) + (a,a) \mid a \in \mathbb{Z}\}\\ &= \{(x,y) \mid y - x = 7 - 3\}\\ &= \{(x,y) \mid y - x = 4\}\end{aligned}$$

Die Nebenklasse mit dem Repräsentanten (a, b) ist gegeben durch:

$$\begin{aligned}(a,b) + Kern(\varphi) &= (a,b) + \{(\alpha,\alpha) \mid \alpha \in \mathbb{Z}\} \\ &= \{(a,b) + (\alpha,\alpha) \mid \alpha \in \mathbb{Z}\} \\ &= \{(x,y) \mid y - x = b - a\} \\ &= \{(x,y) \mid y - x = \varphi(a,b)\} \end{aligned} \tag{E.24}$$

Aufgabe 2.32

a) φ_b ist offensichtlich total definiert. Es gilt

$$\varphi_b(k+l) = b^{k+l} = b^k * b^l = \varphi_b(k) + \varphi_b(l)$$

und damit ist φ_b ein Homomorphismus von $\mathbb{Z}$ nach $\mathcal{G}$.

b) Es ist $Kern(\varphi_b) = \{\, k \in \mathbb{Z} \mid \varphi_b(k) = e \,\}$. Hieraus folgt mit Satz 2.2 b):

$$\begin{aligned} Kern(\varphi_b) &= \{\, k \in \mathbb{Z} \mid b^k = e \,\} \\ &= \{\, k \in \mathbb{Z} \mid \mathit{ord}_{\mathcal{G}}(b) | k \,\} \\ &= \{k \in \mathbb{Z} \mid k = \mathit{ord}_{\mathcal{G}}(b) \cdot l,\ l \in \mathbb{Z}\} \\ &= \mathit{ord}_{\mathcal{G}}(b) \cdot \mathbb{Z} \end{aligned}$$

c) $\mathit{ord}_{\mathcal{G}}(b) \cdot \mathbb{Z}$ besitzt die $\mathit{ord}_{\mathcal{G}}(b)$ vielen Nebenklassen $r + \mathit{ord}_{\mathcal{G}}(b) \cdot \mathbb{Z}$, $0 \leq r \leq \mathit{ord}_{\mathcal{G}}(b) - 1$. $\mathbb{Z}/Kern(\varphi_b)$ hat also $\mathit{ord}_{\mathcal{G}}(b)$ viele Elemente; diese sind:

$$\begin{gathered} 0 + Kern(\varphi_b) \\ 1 + Kern(\varphi_b) \\ \vdots \\ (\mathit{ord}_{\mathcal{G}}(b) - 1) + Kern(\varphi_b) \end{gathered}$$

Aufgabe 3.1

Die *Abgeschlossenheit* sowie die *Kommutativität* von $\oplus$ und $\otimes$ sind offensichtlich.

Assoziativität von $\oplus$:

$$\begin{aligned} a \oplus (b \oplus c) &= a \oplus (b + c + 1) \\ &= a + (b + c + 1) + 1 \\ &= (a + b + 1) + c + 1 \\ &= (a \oplus b) + c + 1 \\ &= (a \oplus b) \oplus c \end{aligned}$$

Assoziativität von $\otimes$: Es gilt einerseits

$$\begin{aligned} a \otimes (b \otimes c) &= a \otimes (b + c + bc) \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc \end{aligned}$$

und andererseits

$$\begin{aligned} (a \otimes b) \otimes c &= (a + b + ab) \otimes c \\ &= a + b + ab + c + (a + b + ab)c \\ &= a + b + ab + c + ac + bc + abc \end{aligned}$$

woraus unmittelbar folgt: $a \otimes (b \otimes c) = (a \otimes b) \otimes c$.

Additives Einselement: $e_{\oplus}$: Für $a \in \mathbb{Z}$ muss $a \oplus e_{\oplus} = a$ sein, d.h. es muss $a + e_{\oplus} + 1 = a$ sein, also ist $e_{\oplus} = -1$.

Additives Inverses: $\overline{a}$ zu a: Für $a \in \mathbb{Z}$ muss $a \oplus \overline{a} = -1$ sein, d.h. es muss $a + \overline{a} + 1 = -1$ sein, also ist $\overline{a} = -a + (-2) = -(a + 2)$.

Multiplikatives Einselement: $e_{\otimes}$: Für $a \in \mathbb{Z} - \{-1\}$ muss $a \otimes e_{\otimes} = a$ sein, d.h. es muss $a + e_{\otimes} + a \cdot e_{\otimes} = a$, also $(1 + a)e_{\otimes} = 0$ sein. Da $a \neq -1$ und damit $(1 + a) \neq 0$ ist, muss $e_{\otimes} = 0$ sein.

Distributivität: Wegen der Kommutativität der Multiplikation braucht nur die Linksdistributivität gezeigt zu werden: Einerseits gilt

$$\begin{aligned} a \otimes (b \oplus c) &= a \otimes (b + c + 1) \\ &= a + (b + c + 1) + a(b + c + 1) \\ &= 2a + ab + ac + b + c + 1 \end{aligned}$$

und andererseits

$$\begin{aligned} (a \otimes b) \oplus (a \otimes c) &= (a + b + ab) \oplus (a + c + ac) \\ &= (a + b + ab) + (a + c + ac) + 1 \\ &= 2a + ab + ac + b + c + 1 \end{aligned}$$

woraus insgesamt folgt: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$.

Aufgabe 3.2

(1) Es gilt:

$$\begin{aligned} \mathbb{Z}_2^* &= \{1\} \\ \mathbb{Z}_3^* &= \{1, 2\} \\ \mathbb{Z}_4^* &= \{1, 3\} \\ \mathbb{Z}_5^* &= \{1, 2, 3, 4\} \\ \mathbb{Z}_6^* &= \{1, 5\} \\ \mathbb{Z}_7^* &= \{1, 2, 3, 4, 5, 6\} \\ \mathbb{Z}_8^* &= \{1, 3, 5, 7\} \end{aligned}$$

(2) Das multiplikative Einselement 1_m ist zu sich selbst invers: $1_m \cdot 1_m = 1_m$. Ebenso ist das additive Inverse $(-1)_m = (m-1)_m$ des multiplikativen Einselementes selbstinvers:

$$\begin{aligned}(-1)_m \cdot_m (-1)_m &= (m-1)_m \cdot_m (m-1)_m \\ &= m_m \cdot_m m_m +_m 2_m \cdot_m m_m +_m 1_m \\ &= 1_m\end{aligned}$$

(3)

$\cdot_2$	1
1	1

$\cdot_3$	1	2
1	1	2
2	2	1

$\cdot_4$	1	3
1	1	3
3	3	1

$\cdot_6$	1	5
1	1	5
5	5	1

$\cdot_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\cdot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\cdot_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Bei allen Strukturen handelt es sich um Gruppen. $\mathbb{Z}_3^*$, $\mathbb{Z}_4^*$ und $\mathbb{Z}_6^*$ sind als zweielementige Gruppen isomorph zueinander. $\mathbb{Z}_5^*$ ist isomorph zu $\mathbb{Z}_4$, und $\mathbb{Z}_8^*$ ist isomorph zu $\mathbb{K}_4$ (siehe Beispiel 2.7 und Bemerkung 2.3).

Aufgabe 3.4

(1) Nullteiler: $3, 6$, da $3 \cdot 6 = 0$ (auch $3 \cdot 3 = 0$ sowie $6 \cdot 6 = 0$).

(2) $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$

(3)

$\cdot$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

(d) $2 : 1 = 2 \cdot 1 = 2$, $2 : 2 = 2 \cdot 5 = 1$, $2 : 4 = 2 \cdot 7 = 5$, $2 : 5 = 2 \cdot 2 = 4$, $2 : 7 = 2 \cdot 4 = 8$, $2 : 8 = 2 \cdot 8 = 7$.

Aufgabe 3.5

(1) Es ist $999 = -1\,(1000)$, daraus folgt $999 \in \mathbb{Z}_{10^3}^*$.

(2) -1 ist selbstinvers, also gilt $999^{-1} = 999\,(1000)$.

(3) Wir testen mit dem Euklidischen Algorithmus, ob $(1000, 101) = 1$ ist:

$$\begin{aligned} 1000 &= 101 \cdot \ \ 9 + 91 \\ 101 &= \ \ 91 \cdot \ \ 1 + 10 \\ 91 &= \ \ 10 \cdot \ \ 9 + \ \ 1 \\ 10 &= \ \ \ \ 1 \cdot 10 + \ \ 0 \end{aligned}$$

Es gilt also $(1000, 101) = 1$, also ist 101 invertierbar.

(4) Mit der Erweiterung des Euklidischen Algorithmus berechnen wir 101^{-1}:

$$\begin{aligned} 91 &= 1000 \cdot 1 + 101 \cdot (-9) && \text{(E.25)} \\ 10 &= 101 \cdot 1 + 91 \cdot (-1) \\ &= 101 \cdot 1 + (\,1000 \cdot 1 + 101 \cdot (-9)\,) \cdot (-1) && \text{mit (E.25)} \\ &= 1000 \cdot (-1) + 101 \cdot 10 && \text{(E.26)} \\ 1 &= 91 \cdot 1 + 10 \cdot (-9) \\ &= (\,1000 \cdot 1 + 101 \cdot (-9)\,) \cdot 1 + (\,1000 \cdot (-1) + 101 \cdot 10\,) \cdot (-9) && \text{mit (E.26)} \\ &= 1000 \cdot 10 + 101 \cdot (-99) \end{aligned}$$

Es gilt also

$$\begin{aligned} 1 &= 1000 \cdot 10 + 101 \cdot (-99) = 101 \cdot (-99)\,(1000) \\ &= 101 \cdot 901\,(1000) \end{aligned}$$

womit folgt: $101^{-1} = 901\,(1000)$.

Aufgabe 3.6

Die Faktorisierung von 1331 ist: $1331 = 11^3$. Mit Korollar 3.8 folgt

$$\varphi(1331) = \varphi(11^3) = 11^2 \cdot 10 = 1210$$

Aufgabe 3.7

Für alle durch 5 teibaren Zahlen $n \in \mathbb{N}_0$ ist die Aussage offensichtlich wahr, denn für diese Zahlen gilt $5 | n^5 - n$. Also betrachten wir die nicht durch 5 teilbaren Zahlen $n \in \mathbb{N}_0 - \{5k \mid k \in \mathbb{N}_0\}$. Für diese gilt $(n, 5) = 1$. Da $5 \in \mathbb{P}$ ist, können wir den Kleinen Satz von Fermat anwenden:

$$n^4 = 1\,(5)$$

Durch Multiplikation dieser Gleichung mit n erhalten wir auch für diesen Fall die Behauptung.

Aufgabe 3.8

Für $a = b$ ist die Aussage trivial; es sei also $a \neq b$. Des Weiteren gilt: Ist $(a, p) > 1$, dann muss auch $(b, p) > 1$ sein, oder ist $(b, p) > 1$, dann muss auch $(a, p) > 1$ sein, und die Aussage gilt in beiden Fällen wiederum offensichtlich. Sei also $(a, p) = 1$ und $(b, p) = 1$. Dann gilt mit dem Kleinen Satz von Fermat $a^p = a\,(p)$ und $b^p = b\,(p)$, woraus $a = b\,(p)$ und damit $p|a - b$ folgt. Aus der Lösung von Aufgabe 1.2 (4) wissen wir, dass

$$a^n - b^n = (a - b) \cdot \sum_{i=1}^{n} a^{n-i} b^{i-1}$$

ist; diese Gleichung gilt natürlich auch für $n = p \in \mathbb{P}$. Da wir schon wissen, dass $p|a - b$ gilt, müssen wir noch zeigen, dass auch $p| \sum_{i=1}^{p} a^{p-i} b^{i-1}$ gilt, dann ist $p^2|a^p - b^p$ und damit die Behauptung $a^p = b^p\,(p^2)$ gezeigt.

Aus $a = b\,(p)$ folgt $a^i = b^i\,(p)$ für alle $i \in \mathbb{N}_0$. Damit und mit dem Kleinen Satz von Fermat folgt

$$a^{p-i} \cdot b^{i-1} = a^{p-i} \cdot a^{i-1} = a^{p-1} = 1\,(p)$$

für alle i mit $1 \leq i \leq p$. Daraus folgt

$$\sum_{i=1}^{p} a^{p-i} b^{i-1} = \sum_{i=1}^{p} 1 = p \cdot 1 = 0\,(p)$$

und daraus $p| \sum_{i=1}^{p} a^{p-i} b^{i-1}$, was noch zu zeigen war.

Aufgabe 3.11

Durch Probieren findet man heraus, dass $P = 3(x + 1)(x + 4)(x^2 + x + 1)$ die gesuchte Zerlegung ist.

Aufgabe 3.12

Die Anzahl der Restklassen ist gleich der Anzahl der Restpolynome, die bei Division der Polynome $A \in \mathbb{F}_p[x]$ durch P bleiben. Die möglichen Restpolynome sind alle Polynome $R \in \mathbb{F}_p[x]$ mit $grad(R) < grad(P)$. Sei $n = grad(P)$, dann ist

$$\left\{ a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \mid a_i \in \mathbb{F}_p,\ 0 \leq i \leq n - 1 \right\}$$

die Menge dieser Restpolynome. Jeder Koeffizient a_i kann die p Werte $0, 1, \ldots, p - 1$ annehmen. Es folgt $\left|\mathbb{F}_p[x]/P\right| = p^{grad(P)}$.

Aufgabe 3.13

(1) Zunächst klammern wir 2 aus und erhalten $P(x) = 2(x^5 + 7x^4 + 2x^3 + 2x^2 + 3x + 6)$. 5 ist eine Nullstelle des eingeklammerten Polynoms; dieses dividieren wir durch $(x - 5) = (x + 6)$ und erhalten $x^5 + 7x^4 + 2x^3 + 2x^2 + 3x + 6 =$

$(x+6)(x^4+x^3+7x^2+4x+1)$. 5 ist auch Nullstelle des eingeklammerten Polynoms; dieses dividieren wir durch $(x-5)=(x+6)$ und erhalten $x^4+x^3+7x^2+4x+1=(x+6)(x^3+6x^2+4x+2)$. 5 ist ebenfalls eine Nullstelle des Quotientenpolynoms. Dessen Division durch $(x-5)=(x+6)$ ergibt $x^3+6x^2+4x+2=(x+6)(x^2+4)$. Das Quotientenpolynom x^2+4 ist irreduzibel über $\mathbb{F}_{11}$. Somit erhalten wir insgesamt die irreduziuble Zerlegung von P über $\mathbb{F}_{11}$:

$$P(x)=2(x+6)^3(x^2+4)$$

(2) Da für $b=-1$ für ungerade n eine Nullstelle des Polynoms x^n+1 ist, folgt die Behauptung unmittelbar aus Satz 3.19.

Aufgabe 4.1

Sei α Nullstelle von P. Dann gilt $\alpha^3=\alpha+2$. Damit ergibt sich die in Abbildung 17 dargestellte Multiplikations- und Logarithmentafel für $\mathbb{F}_3[x]/(x^3+2x+1)$.

Mithilfe der Tafel lässt sich leicht berechnen:

$$7\cdot 21=\alpha^{16}\cdot\alpha^{17}=\alpha^{33\,(26)}=\alpha^7=17$$

Aufgabe 6.3

Die Faktorisierung ergibt $2821=7\cdot 13\cdot 31$, sie ist offensichtlich quadratfrei. Des Weiteren ist $6|2820$, $12|2820$ und $30|2820$. Für alle Primteiler $p\in\{7,13,31\}$ von $m=2821$ gilt also: $p-1|m-1$. Daraus folgt mit dem Satz 6.7 die Behauptung.

Weiterer Beweis durch Nachrechnen mithilfe des Kleinen Satzes von Fermat:

Für alle a mit $(a,2821)=1$ gilt $(a,7)=1$, $(a,13)=1$ und $(a,31)=1$ und damit (Satz von Fermat) $a^6=1\,(7)$, $a^{12}=1\,(13)$ bzw. $a^{30}=1\,(31)$. Damit gilt

$$\begin{aligned}a^{2821}&=a(a^6)^{470}=a\,(7)\\ a^{2821}&=a(a^{12})^{235}=a\,(13)\\ a^{2821}&=a(a^{30})^{94}=a\,(31)\end{aligned}$$

und damit mit Satz 5.3

$$a^{2821}=a\,(2821)$$

Aufgabe 6.4

(1) Es ist $p-1=12=2^2\cdot 3$ und damit $s=2$ und $d=3$. Zu berechnen ist

$$\left\langle b^3,b^6,b^{12}\right\rangle$$

für die gewählten Basen.

Es ergibt sich für

$b = 2 : \langle 8, -1, 1 \rangle$ $Ausgabe : m$ ist prim?

$b = 3 : \langle 1, 1, 1 \rangle$ $Ausgabe : m$ ist prim?

$b = 4 : \langle -1, 1, 1 \rangle$ $Ausgabe : m$ ist prim?

$b = 5 : \langle 8, -1, 1 \rangle$ $Ausgabe : m$ ist prim?

$b = 6 : \langle 8, -1, 1 \rangle$ $Ausgabe : m$ ist prim?

$b = 7 : \langle 5, -1, 1 \rangle$ $Ausgabe : m$ ist prim?

$b = 8 : \langle 5, -1, 1 \rangle$ $Ausgabe : m$ ist prim?

$b = 9 : \langle 1, 1, 1 \rangle$ $Ausgabe : m$ ist prim?

$b = 10 : \langle -1, 1, 1 \rangle$ $Ausgabe : m$ ist prim?

$b = 11 : \langle 5, -1, 1 \rangle$ $Ausgabe : m$ ist prim?

Es kommen alle drei Arten von b-Sequenzen für Primzahlen vor, wie wir es in der Vorlesung überlegt haben. Die Ausgabe des Algorithmus ist in jedem Fall korrekt.

(2) Es ist $m - 1 = 64 = 2^6 \cdot 1$ und damit $s = 6$ und $d = 1$. Zu berechnen ist

$$\left\langle b^1, b^2, b^4, b^8, b^{16}, b^{32}, b^{64} \right\rangle$$

für die gewählten Basen. Es ergibt sich für

$b = 2 : \langle 2, 4, 16, 61, 16, 61, 16 \rangle$ $Ausgabe : m$ ist nicht prim

$b = 8 : \langle 8, -1, 1, 1, 1, 1, 1 \rangle$ $Ausgabe : m$ ist prim?

$b = 12 : \langle 12, 14, 1, 1, 1, 1, 1 \rangle$ $Ausgabe : m$ ist nicht prim

$b = 18 : \langle 18, -1, 1, 1, 1, 1, 1 \rangle$ $Ausgabe : m$ ist prim?

65 ist also bezüglich der Basen 8 und 18 stark pseudoprim.

$\mathbb{F}_3(\alpha)$	$\mathbb{F}_3^3$	$\mathbb{GF}(3^3)$	$\mathbb{F}_3[x]/(x^3+2x+1)$
0	000	0	0
$\alpha^0 = 1$	001	1	1
$\alpha^1 = \alpha$	010	3	x
α^2	100	9	x^2
$\alpha^3 = \alpha + 2$	012	5	$x + 2^3$
$\alpha^4 = \alpha^2 + 2\alpha$	120	15	$x^2 + 2x$
$\alpha^5 = 2\alpha^2 + \alpha + 2$	212	23	$2x^2 + x + 2$
$\alpha^6 = \alpha^2 + \alpha + 1$	111	13	$x^2 + x + 1$
$\alpha^7 = \alpha^2 + 2\alpha + 2$	122	17	$x^2 + 2x + 2$
$\alpha^8 = 2\alpha^2 + 2$	202	20	$2x^2 + 2$
$\alpha^9 = \alpha + 1$	011	4	$x + 1$
$\alpha^{10} = \alpha^2 + \alpha$	110	12	$x^2 + x$
$\alpha^{11} = \alpha^2 + \alpha + 2$	112	14	$x^2 + x + 2$
$\alpha^{12} = \alpha^2 + 2$	102	11	$x^2 + 2$
$\alpha^{13} = 2$	002	2	2
$\alpha^{14} = 2\alpha$	020	6	$2x$
$\alpha^{15} = 2\alpha^2$	200	18	$2x^2$
$\alpha^{16} = 2\alpha + 1$	021	7	$2x + 1$
$\alpha^{17} = 2\alpha^2 + \alpha$	210	21	$2x^2 + x$
$\alpha^{18} = \alpha^2 + 2\alpha + 1$	121	16	$x^2 + 2x + 1$
$\alpha^{19} = 2\alpha^2 + 2\alpha + 2$	222	26	$2x^2 + 2x + 2$
$\alpha^{20} = 2\alpha^2 + \alpha + 1$	211	22	$2x^2 + x + 1$
$\alpha^{21} = \alpha^2 + 1$	101	10	$x^2 + 1$
$\alpha^{22} = 2\alpha + 2$	022	8	$2x + 2$
$\alpha^{23} = 2\alpha^2 + 2\alpha$	220	24	$2x^2 + 2x$
$\alpha^{24} = 2\alpha^2 + 2\alpha + 1$	221	25	$2x^2 + 2x + 1$
$\alpha^{25} = 2\alpha^2 + 1$	201	19	$2x^2 + 1$
$\alpha^{26} = 1$	001	1	1

Abb. 17: Multiplikations- und Logarithmentafel für $\mathbb{F}_3[x]/(x^3+2x+1)$

Literatur

Artin, M.: *Algebra;* Birkhäuser, Basel, 1998

Bartholome, A., Jung, J., Kern, H.: *Zahlentheorie für Einsteiger, 7. Auflage;* Vieweg+Teubner, Wiesbaden 2010

Bundschuh, P.: *Einführung in die Zahlentheorie, 6. Auflage,* Springer, Berlin/Heidelberg, 2008

Crandall, R., Pomerance, C.: *Prime Numbers – A Computational Perspective, 2nd Edition;* Springer, New-York, 2005

Diekert, V., Kufleitner, M., Rosenberger, G.: *Diskrete algebraische Methoden;* De Gruyter, Berlin, 2013

Dietzfelbinger, M.: *Primality Testing in Polynomial Time;* Springer, Berlin, 2004

Karpfinger, C., Meyberg, K.: *Algebra, 3. Auflage;* Springer Spektrum, Heidelberg, 2013

Lüneburg, H.: *Gruppen, Ringe, Körper;* Oldenbourg, München, 1999

Matthes, R.: *Algebra, Kryptologie und Kodierungstheorie;* Fachbuchverlag, Leipzig, 2003

Müller-Stach, S., Piontkowski, J.: *Elementare und algebraische Zahlentheorie, 2. Auflage;* Vieweg+Teubner, Wiesbaden, 2011

Rempe, L., Waldecker, R.: *Primzahltests für Einsteiger;* Vieweg+Teubner, Wiesbaden, 2009

Schwarz, F.: *Einführung in die Elementare Zahlentheorie;* Teubner, Stuttgart/Leipzig, 1998

Wolfart, J.: *Einführung in die Zahlentheorie und Algebra, 2. Auflage;* Vieweg+Teubner, Wiesbaden, 2011

Yan, S.Y.: *Number Theory for Computing;* Springer, Berlin, 2002

Stichwortverzeichnis