6. Anhang: Mathematische Grundlagen

Um den Haupttext besser zugänglich zu machen, wollen wir in diesem Anhang einige grundlegende mathematische Tatsachen zusammenstellen. Wir verzichten dabei weitgehend auf Beweise und auf Literaturhinweise. Die Aussagen in 6.1 bis 6.8 sollten sich in den gängigen Lehrbüchern zur Algebra bzw. elementaren Zahlentheorie finden lassen. Eine ausführliche Quelle zu endlichen Körpern ist [Li-Nie]. Informationen über p-adische Zahlen findet man in [Am].

6.1 Ganze Zahlen

Wir schreiben wie üblich

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$$

für die Menge der natürlichen Zahlen und

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

für die Menge der ganzen Zahlen.

Mit $\mathbb{Q}, \mathbb{R}$ bzw. $\mathbb{C}$ bezeichnen wir die rationalen, reellen bzw. komplexen Zahlen. Für eine reelle Zahl x schreiben wir $[x]$ für die größte Zahl, die kleiner oder gleich x ist, und $\lceil x \rceil$ für die kleinste ganze Zahl, die größer oder gleich x ist.

Eine natürliche Zahl $p \geq 2$ heißt **Primzahl**, falls sie als Teiler nur 1 und p besitzt.

Jede ganze Zahl $n \geq 2$ hat eine Zerlegung in Primfaktoren, d.h. wir können n schreiben als Produkt

$$n = p_1^{\lambda_1} \cdot \ldots \cdot p_t^{\lambda_t}$$

A. Werner, *Elliptische Kurven in der Kryptographie*

mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_t$ und natürlichen Exponenten λ_i. Abgesehen von der Reihenfolge der Faktoren ist diese Darstellung eindeutig.

Eine weitere wichtige Eigenschaft ganzer Zahlen ist die sogenannte **g-adische Entwicklung**. Dazu sei $g \geq 2$ eine beliebige natürliche Zahl. Dann können wir jede natürliche Zahl n schreiben als Linearkombination von Potenzen von g:

$$n = a_r g^r + a_{r-1} g^{r-1} + \ldots + a_1 g + a_0$$

mit Koeffizienten $a_0, \ldots, a_r$ aus $\{0, \ldots, g-1\}$, wobei $a_r \neq 0$ ist. Die Folge $(a_r \ldots a_0)$ ist sogar eindeutig bestimmt. Außerdem ist $r = [\log_g n]$, wobei $\log_g$ den Logarithmus zur Basis g bezeichnet, die Folge $(a_r \ldots a_0)$ besteht also aus $([\log_g n] + 1)$-vielen Elementen.

Für $g = 10$ ist $(a_r \ldots a_0)$ gerade die Folge der Ziffern in unserer Dezimalschreibweise, so ist z.B.

$$1234 = 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 4 \, .$$

Für $g = 2$ nennen wir die Folge $(a_r \ldots a_0)$ von Nullen und Einsen die **Binärentwicklung** der Zahl n. Sie hat die Länge $[\log_2 n] + 1$. So ist z.B.

$$16 = 1 \cdot 16 + 0 \cdot 8 + 0 \cdot 4 + 0 \cdot 2 + 0 \cdot 1 \, , \text{ das entspricht } 10000, \text{ und}$$
$$43 = 1 \cdot 32 + 0 \cdot 16 + 1 \cdot 8 + 0 \cdot 4 + 1 \cdot 2 + 1 \, , \text{ das entspricht } 101011 \, .$$

Eine weitere wichtige Eigenschaft ganzer Zahlen ist die **Division mit Rest**: Für eine ganze Zahl a und eine natürliche Zahl b gibt es eindeutig bestimmte ganze Zahlen q und r, so daß $0 \leq r < b$ ist, und sich a schreiben läßt als

$$a = qb + r \, .$$

Die Zahl r heißt auch Rest der Division von a durch b.

Für zwei ganze Zahlen a und b nennen wir die größte natürliche Zahl d, die sowohl a als auch b teilt, den **größten gemeinsamen Teiler** von a und b. Wir bezeichnen sie mit

$$d = \mathrm{ggT}\,(a, b) \, .$$

Falls $\mathrm{ggT}\,(a, b) = 1$ ist, so nennen wir a und b teilerfremd.

Lemma 6.1.1 *Der größte gemeinsame Teiler von a und b läßt sich linear aus a und b kombinieren, d.h. es gibt ganze Zahlen x und y mit*

$$xa + yb = \mathrm{ggT}\,(a, b)\ .$$

Der größte gemeinsame Teiler d von a und b läßt sich mit Hilfe des **Euklidischen Algorithmus** berechnen, den wir nun vorstellen wollen. Da offenbar $\mathrm{ggT}\,(0, b) = |b|$ ist, können wir annehmen, daß a und b von Null verschieden sind. Nun bestimmen wir induktiv eine Folge nicht-negativer ganzer Zahlen r_k wie folgt: Zunächst sei

$$r_0 = |a| \quad \text{und} \quad r_1 = |b|.$$

Sind $r_0, r_1, \ldots, r_k$ konstruiert und $r_k \neq 0$, so sei

$$r_{k+1} \text{ der Rest bei der Division von } r_{k-1} \text{ durch } r_k,$$

d.h. es ist

$$0 \leq r_{k+1} < r_k \quad \text{und} \quad r_{k-1} = q_k r_k + r_{k+1}$$

für eine ganze Zahl q_k. Dies wird so lange durchgeführt, bis wir ein n erreichen mit $r_n = 0$. In diesem Fall ist r_{n-1} der gesuchte größte gemeinsame Teiler von a und b. Wieso funktioniert dieses Verfahren? Nun, aus der Konstruktion von r_{k+1} folgt, daß ein gemeinsamer Teiler von r_{k-1} und r_k auch ein gemeinsamer Teiler von r_k und r_{k+1} ist und umgekehrt. Daher gilt

$$\mathrm{ggT}\,(r_{k-1}, r_k) = \mathrm{ggT}\,(r_k, r_{k+1}).$$

Außerdem ist die Folge der nicht-negativen ganzen Zahlen r_k streng monoton fallend, so daß es in der Tat ein n mit $r_n = 0$ geben muß. Insgesamt gilt also

$$\mathrm{ggT}\,(a, b) = \mathrm{ggT}\,(r_0, r_1) = \mathrm{ggT}\,(r_1, r_2) = \ldots = \mathrm{ggT}\,(r_{n-1}, 0) = r_{n-1}.$$

Der Euklidische Algorithmus läßt sich außerdem noch erweitern, um auch Zahlen x und y mit

$$xa + yb = \mathrm{ggT}\,(a, b)$$

zu bestimmen. Dazu nehmen wir ohne Einschränkung an, daß a und b positiv sind und setzen außer $r_0 = a$ und $r_1 = b$ noch

$$x_0 = 1, x_1 = 0, y_0 = 0 \text{ und } y_1 = 1.$$

Solange $r_k \neq 0$ ist, bestimmen wir nun wie oben r_{k+1} und q_k und setzen

$$x_{k+1} = x_{k-1} - q_k x_k \quad \text{und} \quad y_{k+1} = y_{k-1} - q_k y_k.$$

Eine leichte Induktion zeigt nun

$$r_k = x_k a + y_k b$$

für alle $k = 0, 1, \ldots, n-1$. Für $x = x_{n-1}$ und $y = y_{n-1}$ gilt also

$$\text{ggT}\,(a, b) = r_{n-1} = xa + yb.$$

Für eine Abschätzung des Zeit- und Platzbedarfs dieses Algorithmus sei auf [Bu], 1.10 verwiesen.

6.2 Kongruenzen

Es seien a und b zwei ganze Zahlen und n eine natürliche Zahl. Dann nennen wir a kongruent zu b modulo n und notieren dies als

$$a \equiv b \bmod n\,,$$

falls n ein Teiler der Differenz $(a - b)$ ist.

Für jede ganze Zahl a nennen wir die Menge aller ganzen Zahlen b mit

$$a \equiv b \bmod n$$

die Restklasse von a modulo n.

Wenn wir mit $n\mathbb{Z}$ alle Vielfachen von n bezeichnen, also

$$n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}\,,$$

so ist die Restklasse von a modulo n gerade

$$a + n\mathbb{Z}\,.$$

Wir bezeichnen sie oft auch mit $a \bmod n$.

Zwei solche Restklassen $a + n\mathbb{Z}$ und $a' + n\mathbb{Z}$ sind entweder gleich (nämlich dann, wenn $a \equiv a' \bmod n$ ist), oder aber sie haben kein Element gemeinsam.

Die Menge aller Restklassen modulo n bezeichnen wir mit

$$\mathbb{Z}/n\mathbb{Z}\,.$$

Wir haben dann eine natürliche Abbildung

$$\begin{aligned}\rho : \mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ a &\longmapsto a + n\mathbb{Z} \quad (\text{ oder auch } a \longmapsto a \bmod n)\,,\end{aligned}$$

die jeder ganzen Zahl ihre Restklasse zuordnet. Wir nennen a auch einen Vertreter der Restklasse $a + n\mathbb{Z}$.

Oft fassen wir einfach ganze Zahlen als Elemente in $\mathbb{Z}/n\mathbb{Z}$ auf, dann geschieht dies immer durch Anwenden der Abbildung ρ.

Wieviele Restklassen gibt es, d.h. wieviele Elemente hat $\mathbb{Z}/n\mathbb{Z}$? Betrachten wir für $a \in \mathbb{Z}$ die Division mit Rest von a durch n, so ist

$$a = qn + r$$

mit einem Rest $r \in \{0, \ldots, n-1\}$. Also ist $a \equiv r \bmod n$. Außerdem sieht man leicht, daß r die einzige Zahl in $\{0, \ldots, n-1\}$ ist, die kongruent zu a modulo n ist.

Daher gibt es für jede ganze Zahl a genau ein $r \in \{0, \ldots, n-1\}$, so daß die Restklasse von a mit der Restklasse von r übereinstimmt, d.h. so daß $a + n\mathbb{Z} = r + n\mathbb{Z}$ gilt.

Also besteht $\mathbb{Z}/n\mathbb{Z}$ aus den n Restklassen

$$n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\,.$$

Daher ist $\rho : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$ eine Bijektion. Mit dieser Abbildung identifiziert man manchmal stillschweigend $\mathbb{Z}/n\mathbb{Z}$ mit $\{0, 1, \ldots, n-1\}$.

Eine sehr nützliche Tatsache über Kongruenzen ist der sogenannte Chinesische Restsatz:

Satz 6.2.1 (Chinesischer Restsatz) *Es seien $n_1, \ldots, n_t$ paarweise teilerfremde natürliche Zahlen und $b_1, \ldots, b_t$ beliebige ganze Zahlen. Dann gibt es eine ganze Zahl a mit*

$$\begin{aligned} a &\equiv b_1 \bmod n_1\,, \\ a &\equiv b_2 \bmod n_2\,, \\ &\ldots \\ a &\equiv b_t \bmod n_t\,. \end{aligned}$$

Außerdem ist a modulo $n = n_1 n_2 \dots n_t$ eindeutig bestimmt, d.h. wenn sowohl a und a' die obigen Kongruenzen erfüllen, so gilt

$$a \equiv a' \bmod n .$$

Man kann den Chinesischen Restsatz auch so ausdrücken: Die Abbildung

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_t\mathbb{Z} \\ a \bmod n &\longmapsto (a \bmod n_1, \dots, a \bmod n_t) \end{aligned}$$

ist eine Bijektion.

In der Situation von 6.2.1 läßt sich eine Zahl a, die simultan die Kongruenzen

$$a \equiv b_1 \bmod n_1, \dots, a \equiv b_t \bmod n_t$$

erfüllt, folgendermaßen berechnen: Wir setzen für $i = 1, \dots, t$

$$m_i = \frac{n}{n_i} = \prod_{j \neq i} n_j .$$

Dann gilt $\mathrm{ggT}(n_i, m_i) = 1$, da $n_1, \dots, n_t$ paarweise teilerfremd sind. Also kann man mit Hilfe des erweiterten euklidischen Algorithmus (siehe 6.1) ganze Zahlen x_i und y_i berechnen mit $x_i n_i + y_i m_i = 1$. Für dieses y_i gilt also

$$y_i m_i \equiv 1 \bmod n_i .$$

Nun setzen wir

$$a = \sum_{i=1}^{t} b_i y_i m_i .$$

Da n_i für alle $j \neq i$ ein Teiler von m_j ist, folgt offenbar

$$a \equiv b_i y_i m_i \equiv b_i \bmod n_i .$$

Daher löst diese Zahl a die gegebenen Kongruenzen. Für eine Abschätzung des Zeit- und Platzbedarfs dieses Verfahrens siehe [Bu], 2.15.

6.3 Gruppen

Definiton 6.3.1 *Eine Gruppe ist eine Menge G zusammen mit einer Verknüpfung*

$$\begin{aligned} G \times G &\longrightarrow G \\ (a,b) &\longmapsto a \circ b\,, \end{aligned}$$

die folgende Axiome erfüllt:

i) (Assoziativität) Es ist $a \circ (b \circ c) = (a \circ b) \circ c$ für alle $a, b, c \in G$.

ii) (neutrales Element) Es gibt ein Element $e \in G$ mit $a \circ e = e \circ a = a$ für alle $a \in G$.

iii) (Inverses) Für jedes $a \in G$ existiert ein $b \in G$ mit $a \circ b = b \circ a = e$.

Falls G zusätzlich die Bedingung

iv) (Kommutativität) Es ist $a \circ b = b \circ a$ für alle $a, b \in G$

erfüllt, so heißt G abelsche Gruppe.

Ein einfaches Beispiel für eine Gruppe ist die Menge $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ zusammen mit der Multiplikation. Hier ist 1 das neutrale Element und $\frac{1}{a}$ das Inverse zu a.

Ein weiteres Beispiel ist die Menge $\mathbb{Z}/n\mathbb{Z}$ der Restklassen modulo einer natürlichen Zahl n zusammen mit der Operation

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}\,,$$

die wie folgt definiert ist:

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}\,.$$

Man kann leicht nachrechnen, daß dies wohldefiniert ist (d.h. nicht von der Wahl der Vertreter a und b der Restklassen abhängt) und $\mathbb{Z}/n\mathbb{Z}$ zu einer abelschen Gruppe macht. Das neutrale Element ist $0 = 0 + n\mathbb{Z}$ und das Inverse zu a mod n ist $(-a)$ mod n.

Wir werden es immer mit Gruppen zu tun haben, deren Verknüpfung wie in den Beispielen durch Multiplikation oder Addition

gegeben ist, daher schreiben wir einfach $a + b$ oder $ab = a \cdot b$ für die Verknüpfung $\circ$.

Es sei nun G eine Gruppe, deren Verknüpfung wir additiv schreiben.

Falls die Menge G aus endlich vielen Elementen besteht, so nennt man die Anzahl der Elemente in G auch die **Ordnung von** G und bezeichnet sie mit $\operatorname{ord}(G)$. So ist z.B.

$$\operatorname{ord}(\mathbb{Z}/n\mathbb{Z}) = n \, .$$

Eine Teilmenge H von G heißt Untergruppe von G, falls H eine Gruppe bezüglich der auf H eingeschränkten Gruppenoperation von G ist.

Ist G endlich, so ist die Ordnung jeder Untergruppe ein Teiler der Ordnung von G. Diese Aussage heißt auch **Satz von Lagrange**.

Für jedes Element a von G definieren wir

$$ka = \begin{cases} \underbrace{a + \ldots + a}_{k} & , \text{falls } k > 0 \\ 0 & , \text{falls } k = 0 \\ -(\underbrace{a + \ldots + a}_{-k}) & , \text{falls } k < 0 \, . \end{cases}$$

Dann ist die Teilmenge aller Vielfachen von a

$$\langle a \rangle = \{ka : k \in \mathbb{Z}\}$$

eine Untergruppe von G.

Eine Gruppe H, für die es ein $a \in H$ mit $H = \langle a \rangle$ gibt, nennt man zyklisch. Das Element a heißt dann auch Erzeuger von H. Jede Untergruppe einer zyklischen Gruppe ist selbst wieder zyklisch. Ein Beispiel für eine zyklische Gruppe ist die Gruppe $\mathbb{Z}/n\mathbb{Z}$, die etwa von dem Element $1+n\mathbb{Z}$ erzeugt wird. In einer beliebigen Gruppe G erzeugt jedes $a \in G$ die zyklische Untergruppe $\langle a \rangle$. Falls diese endlich ist, so nennt man ihre Ordnung auch die **Ordnung von** a und bezeichnet sie mit $\operatorname{ord}(a)$.

Nach dem Satz von Lagrange ist $\operatorname{ord}(a)$ ein Teiler der Ordnung von G, falls G endlich ist. Außerdem gilt folgende einfache, aber wichtige Aussage über die Ordnung von $a \in G$:

Lemma 6.3.2 *$m = \mathrm{ord}\,(a)$ ist die kleinste natürliche Zahl mit $ma = 0$. Außerdem gilt $ka = 0$ genau dann, wenn $\mathrm{ord}\,(a)$ ein Teiler von k ist.*

Beweis: Da wir annehmen, daß $\langle a \rangle$ endlich ist, können nicht alle ka verschieden sein. Falls $k_1 a = k_2 a$ gilt, so folgt $(k_1 - k_2)a = 0$. Es gibt also natürliche Zahlen, die a annulieren. Es sei m die kleinste solche Zahl.

Angenommen, ka sei gleich 0. Nach Division mit Rest durch m gilt

$$k = qm + r$$

für ein $r \in \{0, \ldots, m-1\}$. Dann ist auch $ra = 0$. Wegen der Minimalität von m kann r keine natürliche Zahl sein, so daß $r = 0$ und m ein Teiler von k ist. Umgekehrt gilt für jedes Vielfache $k = qm$ von m:

$$ka = q(ma) = 0\,.$$

Nun bleibt nur noch zu beweisen, daß $m = \mathrm{ord}(a)$ ist. Dafür genügt es zu zeigen, daß

$$\langle a \rangle = \{0, a, 2a, \ldots, (m-1)a\}$$

gilt. In der Tat sind alle ra für $r \in \{0, \ldots, m-1\}$ paarweise verschieden, denn aus $r_1 a = r_2 a$ folgt $(r_1 - r_2)a = 0$, so daß $r_1 - r_2$ ein Vielfaches von m und damit gleich 0 ist. Außerdem ist jedes $ka = ra$ für den Rest r der Division von k durch m, wie wir oben gesehen haben, so daß wir die zyklische Untergruppe $\langle a \rangle$ tatsächlich so beschreiben können. □

Aus dem Lemma folgt sofort, daß in einer endlichen Gruppe G jedes Element a von der Gruppenordnung annuliert wird:

$$\mathrm{ord}\,(G)a = 0\,.$$

Eine Abbildung $f : G \to H$ zwischen zwei Gruppen heißt (Gruppen-) Homomorphismus, falls f mit der Gruppenoperation vertauscht, d.h. falls $f(a+b) = f(a) + f(b)$ für alle $a, b \in G$ gilt. Ein bijektiver Homomorphismus heißt Isomorphismus.

Ist G endlich und $f : G \to H$ ein Gruppenhomomorphismus, so gilt der sogenannte Homomorphiesatz:

$$\mathrm{ord}\,(G) = \#\mathrm{Kern}\,(f)\ \#\mathrm{Bild}\,(f)\ ,$$

wobei $\text{Kern}(f) = \{a \in G : f(a) = 0\} \subseteq G$ und $\text{Bild}(f) = \{f(a) : a \in G\} \subseteq H$ ist.

Wir wollen nun noch ein weiteres Beispiel für eine endliche abelsche Gruppe studieren.

Für jede natürliche Zahl n können wir auf der Menge der Restklassen $\mathbb{Z}/n\mathbb{Z}$ eine Multiplikation durch

$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = (ab) + n\mathbb{Z}$$

definieren. Allerdings ist $\mathbb{Z}/n\mathbb{Z}$ zusammen mit dieser Multiplikation im allgemeinen keine Gruppe. Zwar erfüllt $1+n\mathbb{Z}$ das Axiom des neutralen Elements, doch müssen nicht immer Inverse existieren. Gilt nämlich $n = kl$ mit natürlichen Zahlen $k > 1$ und $l > 1$, so ist

$$(k + n\mathbb{Z})(l + n\mathbb{Z}) = kl + n\mathbb{Z} = 0 + n\mathbb{Z} = 0 .$$

Wäre $\mathbb{Z}/n\mathbb{Z}$ bezüglich der Multiplikation eine Gruppe, so hätte $k+n\mathbb{Z}$ ein multiplikatives Inverses, d.h. es gäbe ein $k' + n\mathbb{Z}$ mit $(k' + n\mathbb{Z})(k + n\mathbb{Z}) = 1 + n\mathbb{Z}$, so daß aus obiger Gleichung nach Multiplikation mit $k' + n\mathbb{Z}$

$$l + n\mathbb{Z} = 0$$

folgte. Da aber $1 < l < n$ ist, kann dies nicht sein.

Wir erhalten allerdings eine Gruppe, wenn wir einfach nur diejenigen Elemente in $\mathbb{Z}/n\mathbb{Z}$ betrachten, die ein multiplikatives Inverses haben. Es sei also

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} : \text{ es gibt ein } b \in \mathbb{Z}/n\mathbb{Z} \text{ mit } ab = 1\} ,$$

wobei wir auch 1 für $1+n\mathbb{Z}$ schreiben. $(\mathbb{Z}/n\mathbb{Z})^\times$ bildet dann zusammen mit der Multiplikation eine abelsche Gruppe. Sie heißt Einheitengruppe in $\mathbb{Z}/n\mathbb{Z}$ oder auch **prime Restklassengruppe** modulo n.

Lemma 6.3.3 *Es ist* $(\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} : a \text{ ist teilerfremd zu } n\}$.

Beweis: Falls $(a + n\mathbb{Z})(b + n\mathbb{Z}) = 1 + n\mathbb{Z}$ ist, so ist n ein Teiler von $ab - 1$. Jeder gemeinsame Teiler von n und a teilt dann $ab - 1$ und ab, also auch 1. Falls umgekehrt a teilerfremd zu n ist, so folgt aus 6.1.1 die Gleichung

$$1 = xa + yn$$

für gewisse ganze Zahlen x und y.

Gehen wir hier zu Restklassen über, so ist

$$1 + n\mathbb{Z} = xa + n\mathbb{Z} = (x + n\mathbb{Z})(a + n\mathbb{Z}) .$$

Daher ist $a + n\mathbb{Z}$ invertierbar. □

Wir haben in 6.2 schon gesehen, daß wir $\mathbb{Z}/n\mathbb{Z}$ mit der Menge $\{0, 1, \ldots, n-1\}$ identifizieren können. Unter dieser Identifikation entspricht $(\mathbb{Z}/n\mathbb{Z})^\times$ also der Menge aller $a \in \{0, 1, \ldots, n-1\}$, die teilerfremd zu n sind. Die Anzahl dieser Elemente bezeichnet man auch mit $\varphi(n)$, d.h. es ist

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times .$$

Die Funktion φ heißt **Eulersche φ-Funktion**. Sie hat folgende Eigenschaften:

$$\varphi(p) = p - 1 \quad \text{für eine Primzahl } p \text{ und}$$
$$\varphi(mn) = \varphi(m)\varphi(n) \text{ , falls ggT } (m, n) = 1 .$$

Wenn wir den Satz, daß die Gruppenordnung jedes Element annulliert, auf die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ anwenden, so ergibt sich $(a + n\mathbb{Z})^{\varphi(n)} = 1 + n\mathbb{Z}$ für alle $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Mit anderen Worten, für alle zu n teilerfremden Zahlen a ist

$$a^{\varphi(n)} \equiv 1 \bmod n .$$

Diese Aussage wird manchmal auch "**Kleiner Satz von Fermat**" genannt. Zum Abschluß dieses Abschnittes wollen wir noch kurz das quadratische Reziprozitätsgesetz formulieren.

Definiton 6.3.4 *Eine zu n teilerfremde ganze Zahl a heißt quadratischer Rest modulo n, falls es eine ganze Zahl b gibt mit*

$$a \equiv b^2 \ mod \ n .$$

Die Zahl a ist also genau dann quadratischer Rest modulo n, falls ihre Restklasse $a + n\mathbb{Z}$ ein Quadrat in $\mathbb{Z}/n\mathbb{Z}$ ist, d.h. falls es eine Restklasse $b + n\mathbb{Z}$ gibt mit

$$a + n\mathbb{Z} = (b + n\mathbb{Z})^2 \quad in \ \mathbb{Z}/n\mathbb{Z} .$$

Ab sofort nehmen wir an, daß $n = p$ eine Primzahl ist. Ob a ein quadratischer Rest modulo p ist, drückt man durch das Legendresymbol $\left(\frac{a}{p}\right)$ aus, das folgendermaßen definiert ist: Für jedes zu p teilerfremde a sei

$$\left(\frac{a}{p}\right) = \begin{cases} 1\,, & \text{falls } a \text{ quadratischer Rest modulo } p \text{ ist} \\ -1\,, & \text{sonst}\,. \end{cases}$$

Das Legendresymbol ist multiplikativ, d.h. es gilt

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\,,$$

und es genügt dem folgenden wichtigen Satz:

Satz 6.3.5 (Quadratisches Reziprozitätsgesetz)
i) Für jede Primzahl $p \neq 2$ ist $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ *und* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
ii) Für zwei verschiedene ungerade Primzahlen p und q gilt

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right)\,.$$

Das quadratische Reziprozitätsgesetz erlaubt es, die Rollen von p und q zu vertauschen. Mit Hilfe der offensichtlichen Rechenregel $\left(\frac{q+mp}{p}\right) = \left(\frac{q}{p}\right)$ kann man es daher benutzen, um auszurechnen, ob eine Zahl quadratischer Rest modulo p ist oder nicht. So gilt etwa $\left(\frac{67}{257}\right) = \left(\frac{257}{67}\right) = \left(\frac{56}{67}\right) = \left(\frac{7}{67}\right)\left(\frac{2}{67}\right)^3 = -\left(\frac{7}{67}\right) = \left(\frac{67}{7}\right) = \left(\frac{4}{7}\right) = 1$, d.h. 67 ist ein Quadrat modulo 257.

6.4 Ringe und Körper

Definiton 6.4.1 *Ein Ring ist eine Menge R zusammen mit zwei Verknüpfungen*

$$(a,b) \longmapsto a+b \quad \textit{und} \quad (a,b) \longmapsto ab\,,$$

so daß folgende Axiome erfüllt sind:

i) $(R,+)$ ist eine abelsche Gruppe, deren neutrales Element wir mit 0 bezeichnen.

ii) Die Multiplikation ist assoziativ, d.h. für $a, b, c \in R$ *gilt* $a(bc) = (ab)c$.

iii) Es existiert ein neutrales Element 1 *bezüglich der Multiplikation, d.h. für alle* $a \in R$ *ist*

$$1a = a1 = a \, .$$

iv) Es gelten die Distributivgesetze

$$a(b+c) = ab + ac \quad \textit{und} \quad (b+c)a = ba + ca$$

für alle $a, b, c \in R$.

Falls zusätzlich für alle $a, b \in R$

$$ab = ba$$

gilt, so heißt R *kommutativer Ring.*

Aus den Axiomen folgt sofort, daß $0a = 0$ für alle $a \in R$ gilt, denn es ist

$$0a + a = 0a + 1a = (0+1)a = 1a = a \, .$$

Ein Beispiel ist der kommutative Ring $\mathbb{Z}$ der ganzen Zahlen mit der gewöhnlichen Addition und Multiplikation.

Ein weiteres Beispiel für einen kommutativen Ring ist die Menge der Restklassen $\mathbb{Z}/n\mathbb{Z}$ zusammen mit der Addition und der Multiplikation, die wir oben definiert haben.

Falls R und R' kommutative Ringe sind, so heißt eine Abbildung

$$f : R \longrightarrow R'$$

Ringhomomorphismus, falls f mit der Addition und der Multiplikation verträglich ist, d.h., falls für alle $a, b \in R$

$$f(a+b) = f(a) + f(b) \quad \text{und} \quad f(ab) = f(a)f(b) \quad \text{sowie} \quad f(1) = 1$$

gilt. Falls f zusätzlich bijektiv ist, so heißt f Isomorphismus. In diesem Fall schreiben wir $R \simeq R'$.

Der Kern eines Ringhomomorphismus f ist die Menge

$$\text{Kern}\,(f) = \{a \in R : f(a) = 0\} \subseteq R \, ,$$

das Bild von f ist definiert als

$$\text{Bild}\,(f) = \{f(a) : a \in R\} \subseteq R' \,.$$

Man kann nun – ähnlich wie bei der Definition von $\mathbb{Z}/n\mathbb{Z}$ – einen Quotientenring $R/\text{Kern}\,(f)$ als Menge aller Restklassen modulo $\text{Kern}\,(f)$ definieren. Dann gilt der sogenannte **Homomorphiesatz**:

$$R/\text{Kern}\,(f) \simeq \text{Bild}\,(f) \,.$$

Definiton 6.4.2 *i) Ein kommutativer Ring mit* $1 \neq 0$, *in dem jedes von Null verschiedene Element ein Inverses bezüglich der Multiplikation hat, heißt Körper.*
ii) Ein Körper F *hat die Charakteristik* 0, *falls für alle natürlichen Zahlen* m *das Element*

$$m1 = \underbrace{1 + \ldots + 1}_{m-\text{mal}}$$

von Null verschieden ist.
Falls es hingegen eine natürliche Zahl m *gibt, so daß* $m1 = 0$ *ist, so heißt die kleinste natürliche Zahl mit dieser Eigenschaft Charakteristik von* F.

Man kann leicht zeigen, daß die Charakteristik eines Körper F entweder 0 oder eine Primzahl ist. Wir bezeichnen Sie mit $\text{char}\,(F)$. Falls $\text{char}\,(F) = p \neq 0$ ist, so gilt für alle $a \in F$

$$pa = \underbrace{a + \ldots + a}_{p-\text{mal}} = 0 \,,$$

denn es ist $pa = (p1)a$.

Bekannte Beispiele für Körper sind die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$ und die komplexen Zahlen $\mathbb{C}$. Alle drei haben Charakteristik 0.

Der Ring $\mathbb{Z}$ der ganzen Zahlen ist offenbar kein Körper, da nur die Elemente 1 und -1 ein Inverses bezüglich der Multiplikation besitzen.

Weitere Beispiele für Körper werden durch bestimmte Restklassenringe gegeben, es gilt nämlich

Lemma 6.4.3 *Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

Beweis: Definitionsgemäß ist $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper, wenn $n \geq 2$ und

$$(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$$

gilt. Nach 6.3.3 bedeutet dies, daß jede Zahl aus $\{1, 2, \ldots, n-1\}$ teilerfremd zu n ist, mit anderen Worten, daß n Primzahl ist. □

Für jede Primzahl p ist $\mathbb{Z}/p\mathbb{Z}$ also ein Körper, den wir auch mit $\mathbb{F}_p$ bezeichnen. $\mathbb{F}_p$ hat p Elemente, nämlich die Restklassen vertreten durch $0, 1, \ldots, p-1$. Definitionsgemäß gilt für alle $y \in \mathbb{Z}$

$$py \equiv 0 \bmod p\,,$$

so daß für jedes $x \in \mathbb{F}_p$ die Gleichung $px = 0$ folgt. Eine solche Gleichung kann für keine kleinere Zahl $m > 0$ erfüllt sein, denn aus $m1 = 0$ in $\mathbb{F}_p$ folgte $m \equiv 0 \bmod p$, was für $0 < m < p$ unmöglich ist. Daher hat $\mathbb{F}_p$ die Charakteristik p.

Für alle $a \in \mathbb{F}_p$ gilt die Gleichung

$$a^p = a\,.$$

Die ist klar für $a = 0$ und folgt für $a \neq 0$ aus dem kleinen Satz von Fermat (siehe 6.3), der besagt, daß in $\mathbb{F}_p^\times$

$$a^{p-1} = a^{\varphi(p)} = 1$$

gilt.

Wir haben nun für jede Primzahl p einen endlichen Körper mit p Elementen der Charakteristik p kennengelernt. Es gibt allerdings noch mehr endliche Körper. Um diese zu definieren, benötigen wir zuvor einige Tatsachen über Polynome.

6.5 Polynome

Es sei F ein Körper. Ein Polynom über F in den n Variablen $x_1, \ldots, x_n$ ist ein Ausdruck der Form

$$f(x_1,\ldots,x_n) = \sum_{\nu_1,\ldots,\nu_n \geq 0} \gamma_{\nu_1,\ldots,\nu_n} x_1^{\nu_1} \ldots x_n^{\nu_n}$$

mit Koeffizienten $\gamma_{\nu_1,\ldots,\nu_n} \in F$, von denen nur endlich viele ungleich Null sind. Die Menge aller Polynome über F in $x_1,\ldots,x_n$ bezeichnen wir mit

$$F[x_1,\ldots,x_n]\,.$$

Man kann zwei Polynome auf natürliche Weise addieren und multiplizieren, so daß $F[x_1,\ldots,x_n]$ zu einem kommutativen Ring wird.

Für ein Polynom $f(x_1,\ldots,x_n) = \sum_{\nu_1,\ldots,\nu_n \geq 0} \gamma_{\nu_1,\ldots,\nu_n} x_1^{\nu_1} \ldots x_n^{\nu_n} \in F[x_1,\ldots,x_n]$ ist für alle $j = 1,\ldots,n$ die Ableitung $\frac{\partial f}{\partial x_j}$ folgendermaßen definiert:

$$\frac{\partial f}{\partial x_j}(x_1,\ldots,x_n) = \sum_{\nu_1,\ldots,\nu_n \geq 0, \nu_j > 0} \gamma_{\nu_1,\ldots,\nu_n}\, \nu_j\, x_1^{\nu_1} \ldots x_j^{\nu_j - 1} \ldots x_n^{\nu_n}\,.$$

$\frac{\partial f}{\partial x_j}$ ist also wieder ein Polynom in $F[x_1,\ldots,x_n]$.

Auf diese Weise können wir Polynome über beliebigen Körpern ableiten. Falls $F = \mathbb{R}$ ist, so stimmt unsere Definition natürlich mit der üblichen Definition über Grenzwerte überein.

Man kann leicht nachrechnen, daß für alle $a \in F$ und alle Polynome $f, g \in F[x_1,\ldots,x_n]$ die Regeln

$$\frac{\partial(af)}{\partial x_j} = a\frac{\partial f}{\partial x_j} \quad \text{und} \quad \frac{\partial(f+g)}{\partial x_j} = \frac{\partial f}{\partial x_j} + \frac{\partial g}{\partial x_j}$$

gelten. Außerdem gilt die **Produktregel**

$$\frac{\partial(f \cdot g)}{\partial x_j} = f\frac{\partial g}{\partial x_j} + g\frac{\partial f}{\partial x_j}$$

und die **Kettenregel**, die besagt, daß für $g_1,\ldots,g_m \in F[x_1,\ldots,x_n]$ und $f \in F[x_1,\ldots,x_m]$

$$\frac{\partial(f(g_1,\ldots,g_m))}{\partial x_j}(x_1,\ldots,x_n) = \frac{\partial f}{\partial x_1}(g_1,\ldots,g_m)\frac{\partial g_1}{\partial x_j}(x_1,\ldots,x_n) + \ldots + \frac{\partial f}{\partial x_m}(g_1,\ldots,g_m)\frac{\partial g_m}{\partial x_j}(x_1,\ldots,x_n)$$

ist. Hier ist $f(g_1,\ldots,g_m)$ das Polynom, das entsteht, wenn man anstelle der Variablen $x_1,\ldots,x_m$ die Polynome $g_1,\ldots,g_m$ in f einsetzt.

Ein Polynom in einer Variablen $f(x) \in F[x]$ sieht einfach so aus:

$$f(x) = \gamma_k x^k + \ldots + \gamma_1 x + \gamma_0$$

für gewisse $\gamma_i \in F$. Falls $f \neq 0$ ist, so heißt das kleinste m mit $\gamma_m \neq 0$ der Grad von f. Wir bezeichnen diesen auch mit $\deg(f)$.

Man kann in $f(x)$ Elemente aus F einsetzen und erhält so eine Abbildung

$$\begin{aligned} f : F &\longrightarrow F \\ b &\longmapsto f(b). \end{aligned}$$

Ein Element $b \in F$ heißt Nullstelle von $f(x)$, falls $f(b) = 0$ ist. Dies ist genau dann der Fall, wenn $(x - b)$ ein Teiler von $f(x)$ im Polynomring $F[x]$ ist.

Falls b eine Nullstelle von $f \neq 0$ ist, so gibt es ein $k \geq 1$, so daß $f(x)$ im Polynomring $F[x]$ durch $(x-b)^k$, aber nicht mehr durch $(x-b)^{k+1}$ teilbar ist. Diese Zahl k heißt **Ordnung der Nullstelle** b. Ist $f(b) \neq 0$, so definiert man die Nullstellenordnung von f in b als 0.

Für ein Polynom $f(x) \in F[x]$ können wir den Restklassenring

$$F[x]/(f)$$

betrachten. Die Konstruktion von $F[x]/(f)$ ist ganz ähnlich wie die von $\mathbb{Z}/n\mathbb{Z}$: Seine Elemente sind gerade die Restklassen

$$g + fF[x]$$

für $g \in F[x]$, wobei $fF[x]$ die Menge $\{fh : h \in F[x]\}$ aller Vielfachen von f ist. Zwei Polynome g_1 und g_2 definieren also genau dann dieselbe Restklasse, wenn f ein Teiler von $g_1 - g_2$ im Polynomring ist. Wir nennen g einen Vertreter der Restklasse $g + fF[x]$ und definieren die Addition bzw. Multiplikation von Restklassen über die Addition bzw. Multiplikation ihrer Vertreter, also etwa

$$(g_1 + fF[x]) + (g_2 + fF[x]) = (g_1 + g_2) + fF[x]\,.$$

Auf diese Weise wird $F[x]/(f)$ zu einem kommutativen Ring. Ähnlich wie in $\mathbb{Z}$ gibt es im Polynomring $F[x]$ eine Division mit Rest: Für $g(x), h(x) \in F[x]$ mit $h \neq 0$ gibt es Polynome $q(x), r(x) \in F[x]$ mit $r = 0$ oder $\deg r < \deg h$, so daß

$$g(x) = q(x)h(x) + r(x)$$

ist. Die Polynome q und r mit diesen Eigenschaften sind eindeutig bestimmt. Daher gibt es für jede Restklasse in $F[x]/(f)$ genau einen Vertreter g, für den entweder $g = 0$ oder $\deg g < \deg f$ gilt.

Definiton 6.5.1 *Ein Polynom $f(x) \in F[x]$ vom Grad ≥ 1 heißt irreduzibel, wenn es nicht als Produkt zweier Polynome in $F[x]$, die beide vom Grad ≥ 1 sind, geschrieben werden kann.*

Damit können wir folgende wichtige Tatsache formulieren: Ist $f(x)$ ein irreduzibles Polynom, so ist der Restklassenring $F[x]/(f)$ ein Körper.

Der Körper F ist in $F[x]/(f)$ enthalten, wenn wir $a \in F$ mit der Restklasse des konstanten Polynoms a identifizieren.

6.6 Endliche Körper

Es sei p eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der endliche Körper mit p Elementen.

Für jede natürliche Zahl r gibt es dann ein irreduzibles Polynom $f(x) \in \mathbb{F}_p[x]$ vom Grad r. Somit ist

$$\mathbb{F}_p[x]/(f)$$

ein Körper, der $\mathbb{F}_p$ enthält.

Da $\mathbb{F}_p[x]/(f)$ gerade aus den Restklassen aller Polynome in $\mathbb{F}_p[x]$ besteht, die Null oder von kleinerem Grad als f sind, hat $\mathbb{F}_p[x]/(f)$ genau p^r Elemente. Der Körper $\mathbb{F}_p[x]/(f)$ ist im wesentlichen (d.h. genauer gesagt bis auf Isomorphie) der einzige Körper mit p^r Elementen, wir bezeichnen ihn daher auch mit $\mathbb{F}_{p^r}$.

Es gilt sogar: Jeder Körper F mit endlich vielen Elementen ist einer dieser Körper $\mathbb{F}_{p^r}$.

Da $\mathbb{F}_{p^r}$ den Körper $\mathbb{F}_p$ enthält, gilt $p \cdot 1 = 0$ im $\mathbb{F}_{p^r}$, so daß $\mathrm{char}\,(\mathbb{F}_{p^r}) = p$ folgt. Wir schreiben oft $q = p^r$ und $\mathbb{F}_q = \mathbb{F}_{p^r}$. Um eine konkrete Beschreibung der Elemente von $\mathbb{F}_q$ zu erhalten, kann

man $\mathbb{F}_q = \mathbb{F}_p[X]/(f)$ mit der Menge der Polynome in $\mathbb{F}_p[x]$ vom Grad kleiner r (inklusive 0) identifizieren:

$$\mathbb{F}_q = \{a_{r-1}x^{r-1} + \ldots + a_1 x + a_0 : a_i \in \mathbb{F}_p\} .$$

Diese wiederum kann man durch die Vektoren $(a_{r-1} \ldots a_0) \in \mathbb{F}_p^r$ darstellen. Will man mit solchen Vektoren rechnen, so rechnet man mit den zugehörigen Polynomen und reduziert das Ergebnis modulo f. Das wollen wir an einem Beispiel verdeutlichen:

Es sei $q = 8 = 2^3$. Das Polynom

$$f(x) = x^3 + x + 1$$

ist irreduzibel über $\mathbb{F}_2$, also ist

$$\mathbb{F}_8 = \mathbb{F}_2[x]/(f) .$$

Die Elemente von $\mathbb{F}_8$ kann man identifizieren mit der Menge

$$\{(000), (001), (010), (011), (100), (101), (110), (111)\} ,$$

und man rechnet zum Beispiel:

$$(010) \cdot (111) = (101) ,$$

denn (010) bzw. (111) entsprechen den Polynomen x bzw. $x^2 + x + 1$, und es gilt

$$x(x^2 + x + 1) = x^3 + x^2 + x = (x^3 + x + 1) + (x^2 + 1) \quad \text{in } \mathbb{F}_2[x] ,$$

so daß die Restklasse von $x(x^2 + x + 1)$ durch $(x^2 + 1)$ gegeben wird.

(Statt $f(x)$ hätte man auch das irreduzible Polynom $x^3 + x^2 + 1$ zur Konstruktion von F_8 nehmen können, dann würden sich entsprechend andere Rechenregeln für die Vektoren ergeben.)

In dem folgenden Satz stellen wir noch zwei wichtige Eigenschaften endlicher Körper zusammen:

Satz 6.6.1 *Es sei $q = p^r$. Dann gilt für den endlichen Körper $\mathbb{F}_q$:*

i) Für alle $a \in \mathbb{F}_q$ ist $a^q = a$. Es gilt sogar die Polynomgleichung

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a) \quad \text{in } \mathbb{F}_q[x] .$$

ii) Die multiplikative Gruppe $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ *ist zyklisch.*

Eine weitere wichtige Rechenregel in endlichen Körpern wollen wir zum Abschluß ebenfalls noch festhalten. Sie gilt allgemeiner in jedem Körper der Charakteristik p:

Lemma 6.6.2 *Sei F ein beliebiger Körper der Charakteristik $p > 0$. Dann gilt für $a, b \in F$ und alle natürlichen Zahlen t:*

$$(a+b)^{p^t} = a^{p^t} + b^{p^t}.$$

6.7 Algebraisch abgeschlossene Körper

Definiton 6.7.1 *Ein Körper F heißt algebraisch abgeschlossen, wenn sich jedes Polynom $f(x) \in F[x]$ von positivem Grad als Produkt von Polynomen vom Grad 1 schreiben läßt, d.h. wenn*

$$f(x) = d(x - c_1) \dots (x - c_m)$$

für Elemente c_i, d aus F gilt. In diesem Fall ist $m = \deg(f)$ und d der Koeffizient vor x^m.

Insbesondere hat also jedes Polynom von positivem Grad eine Nullstelle in F, falls F algebraisch abgeschlossen ist.

Ein Beispiel für einen algebraisch abgeschlossenen Körper ist der Körper $\mathbb{C}$ der komplexen Zahlen.

Man kann jeden Körper F in einen algebraisch abgeschlossenen Körper einbetten. Es gibt einen kleinsten algebraisch abgeschlossenen Erweiterungskörper von F. Dieser heißt algebraischer Abschluß von F. Wir bezeichnen ihn mit $\overline{F}$.

So ist z.B. der Körper $\mathbb{C}$ der komplexen Zahlen der algebraische Abschluß des Körpers $\mathbb{R}$ der reellen Zahlen. Das Polynom $f(x) = x^2+1$ etwa läßt sich in $\mathbb{R}[x]$ nicht als Produkt von Polynomen vom Grad 1 schreiben, wohl aber in $\mathbb{C}[x]$, wo $f(x) = (x-i)(x+i)$ gilt.

Der algebraische Abschluß $\overline{\mathbb{F}_p}$ des endlichen Körpers $\mathbb{F}_p$ enthält für alle $r \geq 1$ einen endlichen Körper $\mathbb{F}_{p^r}$ mit p^r Elementen. Umgekehrt ist jedes Element von $\overline{\mathbb{F}_p}$ schon in einem dieser $\mathbb{F}_{p^r}$ enthalten.

6.8 Einheitswurzeln

Es sei F ein Körper. Ein Element $a \in F$ mit $a^m = 1$ heißt m-te Einheitswurzel in F. Wir bezeichnen die Menge der m-ten Einheitswurzeln in F mit

$$\mu_m(F) = \{a \in F : a^m = 1\} .$$

$\mu_m(F)$ besteht also aus allen Nullstellen des Polynoms $x^m - 1$ in F. Bezüglich der Körpermultiplikation ist $\mu_m(F)$ eine Untergruppe von $F^\times$.

Falls m teilerfremd zu p und F der algebraische Abschluß $F = \overline{\mathbb{F}}_q$ für ein $q = p^r$ ist, so besteht $\mu_m(F)$ aus m Elementen. Daher muß es ein s geben, so daß $\mathbb{F}_{p^s}$ alle diese Elemente enthält. Dann ist $\mu_m(\overline{\mathbb{F}}_q)$ also eine Untergruppe der zyklischen Gruppe $\mathbb{F}_{p^s}^\times$ und somit selbst eine zyklische Gruppe.

Jeder Erzeuger der zyklischen Gruppe $\mu_m(\overline{\mathbb{F}}_q)$ heißt primitive m-te Einheitswurzel. Es gibt genau $\varphi(m)$ primitive m-te Einheitswurzeln, wobei φ die Eulersche φ-Funktion ist. Falls nämlich ζ ein beliebiger Erzeuger von $\mu_m(\overline{\mathbb{F}}_q)$ ist, so ist ein anderes Element ζ^k genau dann ein Erzeuger, wenn es ein l gibt mit $\zeta^{kl} = \zeta$, d.h. mit $kl \equiv 1 \bmod m$. Also ist ζ^k genau dann ein Erzeuger von $\mu_m(\overline{\mathbb{F}}_q)$, wenn k in $(\mathbb{Z}/m\mathbb{Z})^\times$ liegt.

6.9 p-adische Zahlen

Es sei p eine Primzahl. Für jede natürliche Zahl $n \geq 1$ betrachten wir den Restklassenring $\mathbb{Z}/p^n\mathbb{Z}$. Die Restklassenabbildung $\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, die x auf $(x \bmod p^n)$ abbildet, verschwindet auf $p^m\mathbb{Z}$ für alle $m \geq n$, d.h. wir haben Restklassenabbildungen $\mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$. Insbesondere erhalten wir Abbildungen $\rho_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$. Wir definieren nun einen neuen Ring $\mathbb{Z}_p$ als Menge aller Folgen $(x_n)_{n\geq 1}$ für $x_n \in \mathbb{Z}/p^n\mathbb{Z}$, die unter diesen Restklassenabbildungen zusammenpassen:

$$\mathbb{Z}_p = \{(x_n)_{n\geq 1} : x_n \in \mathbb{Z}/p^n\mathbb{Z} \text{ mit } \rho_n(x_{n+1}) = x_n \text{ für alle } n \geq 1\} .$$

(Man sagt auch, $\mathbb{Z}_p$ ist der inverse Limes der $\mathbb{Z}/p^n\mathbb{Z}$.)

Man kann die Elemente in $\mathbb{Z}_p$ komponentenweise addieren und multiplizieren und so eine Ringstruktur auf $\mathbb{Z}_p$ definieren. Der Ring $\mathbb{Z}$ der ganzen Zahlen läßt sich über die Abbildung

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z}_p \\ x &\longmapsto (x \bmod p^n)_{n\geq 1} \end{aligned}$$

als Unterring von $\mathbb{Z}_p$ auffassen.

Da $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ der endliche Körper mit p Elementen ist, so ist die Projektion auf die erste Komponente einer Folge in $\mathbb{Z}_p$ ein Ringhomomorphismus

$$\begin{aligned} \pi : \mathbb{Z}_p &\longrightarrow \mathbb{F}_p \\ (x_n)_{n\geq 1} &\longmapsto x_1 \, . \end{aligned}$$

Dieser ist offensichtlich surjektiv, und sein Kern besteht aus allen Folgen $(x_n)_{n\geq 1}$ in $\mathbb{Z}_p$ mit $x_1 = 0$. Offenbar ist die Menge $p\mathbb{Z}_p$ aller Vielfachen von p im Kern enthalten, da $\pi(p(x_n)_{n\geq 1}) = px_1 = 0$ ist. Falls umgekehrt für eine Folge $(x_n)_{n\geq 1}$ in $\mathbb{Z}_p$ die erste Komponente $x_1 = 0$ ist, so bildet für alle $n \geq 1$ die Restklassenabbildung $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ das Element x_{n+1} auf 0 ab. Für jedes $a_{n+1} \in \mathbb{Z}$ mit $a_{n+1} \equiv x_{n+1} \bmod p^{n+1}$ ist also $a_{n+1} \equiv 0 \bmod p$, d.h. es ist $a_{n+1} = pb_n$ für ein $b_n \in \mathbb{Z}$. Es sei nun y_n die Restklasse von b_n in $\mathbb{Z}/p^n\mathbb{Z}$. Dann ist $(y_n)_{n\geq 1}$ ein Element von $\mathbb{Z}_p$: Da $(x_n)_{n\geq 1}$ in $\mathbb{Z}_p$ liegt, gilt nämlich $a_{n+2} \equiv a_{n+1} \bmod p^{n+1}$, woraus $pb_{n+1} \equiv pb_n \bmod p^{n+1}$, also $b_{n+1} \equiv b_n \bmod p^n$ folgt.

Offenbar ist $p(y_n)_{n\geq 1} = (x_n)_{n\geq 1}$, da $pb_n = a_{n+1} \equiv a_n \equiv x_n \bmod p^n$ ist. Daher ist $(x_n)_{n\geq 1}$ in $p\mathbb{Z}_p$ enthalten. Insgesamt erhalten wir

$$\operatorname{Ker} \pi = p\mathbb{Z}_p \, ,$$

so daß nach dem Homomorphiesatz $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$ ist.

Auf ganz analoge Weise zeigt man für alle $n \geq 1$

$$p^n\mathbb{Z}_p = \{(\underbrace{0, \ldots, 0}_{n}, x_{n+1}, x_{n+2} \ldots) \in \mathbb{Z}_p\} \, .$$

Also hat insbesondere der surjektive Homomorphismus abelscher Gruppen

$$\begin{aligned} p\mathbb{Z}_p &\longrightarrow \mathbb{F}_p \text{ , gegeben durch} \\ p \cdot (x_1, x_2, \ldots) &\longmapsto x_1 \end{aligned}$$

den Kern $p^2\mathbb{Z}_p$, so daß

$$p\mathbb{Z}_p/p^2\mathbb{Z}_p \simeq \mathbb{F}_p$$

als abelsche Gruppe gilt. Wir können nun die Einheitengruppe $\mathbb{Z}_p^\times$ von $\mathbb{Z}_p$ bestimmen. (Definitionsgemäß ist $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p : \text{ es gibt ein } y \in \mathbb{Z}_p \text{ mit } xy = 1\}$.)

Lemma 6.9.1 *Es ist $\mathbb{Z}_p^\times = \mathbb{Z}_p \backslash p\mathbb{Z}_p$. Ein Element in $\mathbb{Z}_p$ ist also genau dann invertierbar, wenn es nicht ein Vielfaches von p ist.*

Beweis: Für $x \in p\mathbb{Z}_p$ gilt $\pi(x) = 0$. Ein solches Element kann also nicht invertierbar sein. Falls $x = (x_n)_{n\geq 1}$ hingegen nicht in $p\mathbb{Z}_p$ liegt, so ist $x_1 = \pi(x) \in \mathbb{F}_p$ invertierbar. Für alle $n \geq 1$ sei $a_n \in \mathbb{Z}$ ein Element mit $a_n \equiv x_n \bmod p^n$. Dann ist insbesondere $a_n \equiv x_1 \bmod p$. Für $b \in \mathbb{Z}$ mit $b \equiv x_1^{-1} \bmod p$ gilt also $a_n b \equiv 1 \bmod p$, d.h. $a_n b = 1 - pc_n$ für ein $c_n \in \mathbb{Z}$. Also folgt mit der geometrischen Summenformel

$$\begin{aligned} &a_n b(1 + pc_n + p^2 c_n^2 + \ldots + p^{n-1} c_n^{n-1}) \\ &= a_n b \frac{1 - p^n c_n^n}{1 - pc_n} = 1 - p^n c_n^n \equiv 1 \bmod p^n \,. \end{aligned}$$

Definieren wir also $y_n \in \mathbb{Z}/p^n\mathbb{Z}$ als Restklasse von $b(1+pc_n+p^2c_n^2+\ldots+p^{n-1}c_n^{n-1})$, so ist $(y_n)_{n\geq 1}$ ein Element von $\mathbb{Z}_p$ und invers zu $(x_n)_{n\geq 1}$. □

Aus diesem Lemma folgt sofort, daß sich jedes von Null verschiedene Element $x = (x_n)_{n\geq 1}$ aus $\mathbb{Z}_p$ schreiben läßt als $p^m u$ für ein $m \geq 0$ und eine Einheit $u \in \mathbb{Z}_p^\times$. Es sei nämlich m der größte Index, so daß $x_1 = x_2 = \ldots = x_m = 0$ ist. Dann ist x in $p^m\mathbb{Z}_p$, aber nicht in $p^{m+1}\mathbb{Z}_p$. Wir können x also darstellen als $x = p^m u$ mit einem $u \in \mathbb{Z}_p \backslash p\mathbb{Z}_p = \mathbb{Z}_p^\times$.

Die Menge

$$\mathbb{Q}_p = \left\{ \frac{a}{b} : a \in \mathbb{Z}_p, b \in \mathbb{Z}_p \setminus \{0\} \right\}$$

aller Brüche mit nicht-verschwindendem Nenner, versehen mit den üblichen Rechenregeln, ist ein Körper. Diesen bezeichnet man mit $\mathbb{Q}_p$ und nennt ihn auch "Körper der p-adischen Zahlen". Er enthält den Ring $\mathbb{Z}_p$, den wir über $x \mapsto \frac{x}{1}$ in $\mathbb{Q}_p$ einbetten können, und den Körper $\mathbb{Q}$ der rationalen Zahlen. Da wir $a, b \neq 0$ in $\mathbb{Z}_p$ schreiben können als $a = p^{m_a} u_a$ und $b = p^{m_b} u_b$ mit $u_a, u_b \in \mathbb{Z}_p^\times$, gilt $\frac{a}{b} = p^{m_a - m_b} \frac{u_a}{u_b}$. Jedes Element x in $\mathbb{Q}_p^\times$ läßt sich also schreiben als $x = p^m u$ für ein $m \in \mathbb{Z}$ und ein $u \in \mathbb{Z}_p^\times$. Falls $m \geq 0$ ist, so liegt x in $\mathbb{Z}_p$. Daher gilt für jedes $x \in \mathbb{Q}_p^\times$, daß x oder x^{-1} in $\mathbb{Z}_p$ liegen.

Der Ring $\mathbb{Z}_p$ und der Körper $\mathbb{Q}_p$ haben einige nützliche Eigenschaften, die die viel kleineren Mengen $\mathbb{Z}$ und $\mathbb{Q}$ nicht haben. So kann man

zum Beispiel Nullstellen von Polynomen über $\mathbb{F}_p$ mit Hilfe des Henselschen Lemmas nach $\mathbb{Z}_p$ liften:

Henselsches Lemma: *Es sei*

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}_p[x]$$

ein Polynom mit Koeffizienten in $\mathbb{Z}_p$. *Mit* $\pi(f)$ *bezeichnen wir das Polynom* $\pi(f)(x) = \pi(a_n)x^n + \ldots + \pi(a_1)x + \pi(a_0)$ *in* $\mathbb{F}_p[x]$. *Falls* $\pi(f)$ *eine Nullstelle* $\alpha \in \mathbb{F}_p$ *hat, für die die Ableitung* $\frac{\partial \pi(f)}{\partial x}(\alpha) \neq 0$ *ist, so besitzt* f *eine Nullstelle* $\beta \in \mathbb{Z}_p$ *mit* $\pi(\beta) = \alpha$.

6.10 Komplexität

Um die Größenordnung abzuschätzen, mit der eine Funktion wächst, bedient man sich oft folgender nützlicher Schreibweise:

Definiton 6.10.1 *Es seien* $f : \mathbb{N} \to \mathbb{R}$ *und* $g : \mathbb{N} \to \mathbb{R}$ *zwei reellwertige Funktionen auf den natürlichen Zahlen. Dann schreiben wir*

$$f = O(g) \ ,$$

falls es eine Konstante $c > 0$ *und eine natürliche Zahl* n_0 *gibt, so daß*

$$0 < f(n) \leq cg(n)$$

für alle $n \geq n_0$ *gilt.*

Als Beispiel betrachten wir die Funktion f, die jeder natürlichen Zahl die Länge ihrer Binärentwicklung, d.h. die Länge des Bitstrings, mit dem man n darstellen kann, zuordnet. Wir haben in 6.1 gesehen, daß

$$f(n) = [\log_2 n] + 1$$

gilt. Daher ist für $n \geq 2$

$$0 < f(n) \leq \log_2 n + 1 = \frac{\log n}{\log 2} + 1 = \log n \left(\frac{1}{\log 2} + \frac{1}{\log n} \right),$$

wobei log den natürlichen Logarithmus bezeichnet.

Da sich $\frac{1}{\log n}$ für $n \geq 2$ durch eine positive Konstante nach oben abschätzen läßt, folgt

$$f(n) = O(\log n) .$$

Um die Effektivität verschiedener Algorithmen miteinander zu vergleichen, ist es nützlich, die Größenordnung ihrer Laufzeiten zu bestimmen. Hier ist die Laufzeit eines Algorithmus mit einem bestimmten Input die Anzahl der ausgeführten Schritte in einem bestimmten Sinn. Solche Schritte können z.B. Bitoperationen oder bestimmte Rechenoperationen, etwa Gruppenoperationen, sein. Die Anzahl der Bits, die notwendig sind, um den Input eines Algorithmus darzustellen, nennt man auch Inputgröße.

Definiton 6.10.2 *i) Ein Algorithmus hat polynomiale Laufzeit, falls es eine natürliche Zahl k und eine obere Schranke für seine Laufzeit bei Inputs der Größe n von der Form $O(n^k)$ gibt.*
ii) Ein Algorithmus hat exponentielle Laufzeit, falls es eine positive Konstante c und eine obere Schranke für seine Laufzeit bei Inputs der Größe n von der Form $O(\exp(cn))$ gibt.

Im Zusammenhang mit dem DL-Problem in einer endlichen abelschen Gruppe stellt sich oft die Frage, ob es einen Algorithmus subexponentieller Laufzeit gibt.

Definiton 6.10.3 *Ein Algorithmus, der als Input entweder die Zahl q oder Elemente des endlichen Körpers $\mathbb{F}_q$ erhält, hat subexponentielle Laufzeit, falls diese von der Form*

$$L_q[\alpha, c] = O(\exp(c(\log q)^{\alpha}(\log\log q)^{1-\alpha}))$$

ist. Hier sind c und α Konstanten mit

$$c > 0 \quad \textit{und} \quad 0 < \alpha < 1 .$$

Viele interessante Algorithmen sind probabilistisch, d.h. sie treffen in ihrem Verlauf zufällige Wahlen. Ihr Ergebnis ist also nicht vollständig durch den Input determiniert. In diesem Fall sind Laufzeiten immer als erwartete Laufzeiten zu verstehen, siehe [Hb], Abschnitt 2.3.4.