3. Der Restklassenring $\mathbb{Z}/n$ und seine Einheitengruppe

3.0. Erinnerung: Teilen mit Rest, euklidscher Algorithmus, Bézoutsche Gleichung. Sei n eine feste natürliche Zahl. Sei $a \in Z$. Setze

$$\overline{a} = a + n\mathbb{Z},$$

man nennt dies die Restklasse von a modulo n (eigentlich müssten wir $\overline{a}^{(n)}$ schreiben, um zu betonen, dass $\overline{a}$ von n abhängt); die Menge $\overline{0} = n\mathbb{Z}$ ist ein "Ideal" im Ring $\mathbb{Z}$, das "von n erzeugte Hauptideal". Man schreibt für $a, b \in \mathbb{Z}$

$$a \equiv b \mod n$$

falls $a - b \in n\mathbb{Z}$ gilt (also $a - b$ durch n teilbar ist). Offensichtlich gilt: *Genau dann ist* $\overline{a} = \overline{b}$*, falls* $a \equiv b \mod n$ *gilt.*

Zu jedem $z \in \mathbb{Z}$ *gibt es genau eine Zahl* r *mit* $0 \leq r < n$*, so dass gilt* $\overline{z} = \overline{r}$*, so dass es also ein (ebenfalls eindeutig bestimmes)* $q \in \mathbb{Z}$ *gibt mit*

$$z = qn + r.$$

Man nennt dies *Teilen mit Rest,* insbesondere nennt man r den *Rest* von z modulo q.

Es gibt den euklidschen Algorithmus: Gegeben seien ganze Zahlen u, v mit $v \geq 1$. Man setzt $u = r_{-1}$ und $v = r_0$ und bildet als erstes

$$r_{-1} = q_1 r_0 + r_1$$

mit $0 \leq r_1 < r_0$. Induktiv findet man $r_0 > r_1 > \cdots > r_{i-1} > r_i \geq 0$.

$$\begin{aligned} r_0 &= q_2 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ &\vdots \\ r_{i-2} &= q_i r_{i-1} + r_i \end{aligned}$$

für $1 \leq i$. Das Verfahren bricht ab, sobald wir $r_i = 0$ erhalten (denn Teilen durch n mit Rest ist nur definiert, wenn man durch eine natürliche Zahl n teilt). Das Verfahren muss abbrechen (nach höchstens r_0 Schritten, denn wir erhalten ja die absteigende Folge $r_0 > r_1 > \cdots > r_{i-1} > r_i \geq 0$).

Das Verfahren breche ab für $t = i$, es ist dann also $r_t = 0$. Die t-te Gleichung ist also

$$r_{t-2} = q_t r_{t-1}.$$

Die Gleichung $r_{i-2} = q_i r_{i-1} + r_i$ zeigt:

$$(r_{i-1}, r_i) = (r_{i-1}, r_{i-2})$$

Demnach ist

$$r_{t-1} = (r_{t-1}, r_{t-2}) = \cdots = (r_0, r_{-1}) = (u, v).$$

Einsetzen zeigt: (u, v) ist eine ganzzahlige Linearkombination von u und v. Genauer: Die Ausgangszahlen $r_{-1} = u, r_0 = v$ sind natürlich ganzzahlige Linearkombinationen von u, v. Sei nun $i \geq 1$. Wir zeigen mit Induktion, dass auch r_i ganzzahlige Linearkombination von u, v ist. Wir nehmen an, dass wir schon wissen: $r_{i-1} = a_{i-1}u + b_{i-1}v$, und $r_{i-2} = a_{i-2}u + b_{i-2}v$. Die i-te Gleichung liefert:

$$\begin{aligned} r_i &= r_{i-2} - q_i r_{i-1} \\ &= a_{i-2}u + b_{i-2}v - q_i(a_{i-1}u + b_{i-1}v) \\ &= (a_{i-2} - q_i a_{i-1})\, u + (b_{i-2} - q_i b_{i-1})\,. \end{aligned}$$

Das heißt:

Bézout'sche Gleichung: *Zu jedem Paar natürlicher Zahlen u, v gibt es $a, b \in \mathbb{Z}$ mit*

$$(u, v) = au + bv.$$

Natürlich sind die Zahlen a, b nicht eindeutig, denn es ist

$$au + bv = au + zuv - zuv + bv = (a + zv) \cdot u + (b - zu) \cdot v$$

für alle $z \in \mathbb{Z}$. Insbesondere kann man immer erreichen, dass a (oder b, aber nicht beide) nicht-negativ ist.

Wichtig ist hier: Wir beginnen mit Zahlen $u, v \in \mathbb{N}$, müssen aber zu $\mathbb{Z}$ übergehen, um a, b zu finden! Üblicherweise ist eine der beiden Zahlen a, b negativ! Man verlässt hier also das Rechnen in $\mathbb{N}$. Wichtig ist nicht nur die Bézout'sche Gleichung selbst, sondern das Verfahren, wie man a und b findet!

Beispiel für das Rechnen per Hand: $a = 37, b = 26$.

$$\begin{array}{rl} 37 = 1 \cdot 26 + 11 & = 3 \cdot 26 - 7 \cdot (37 - 1 \cdot 26) = -7 \cdot 37 + 10 \cdot 26 \\ 26 = 2 \cdot 11 + \ 4 & = -11 + 3 \cdot (26 - 2 \cdot 11) = 3 \cdot 26 - 7 \cdot 11 \\ 11 = 2 \cdot 4 \ + \ 3 & = 4 - 1 \cdot (11 - 2 \cdot 4) = -11 + 3 \cdot 4 \\ 4 = 1 \cdot 3 \ + \ 1 & 1 = 4 - 1 \cdot 3 \\ 3 = 3 \cdot 1 \ + \ 0 & \end{array}$$

Erst wird links von oben nach unten gerechnet, dann rechts von unten nach oben. Wir erhalten demnach:

$$1 = (37, 26) = -7 \cdot 37 + 10 \cdot 26.$$

Der MAPLE-Befehl zur Bestimmung von (37,26) lautet `igcd(37,26);` - braucht man die Koeffizienten a, b, so gibt man `igcdex(37,26,'a','b');` ein, dann sind diese Koeffizienten unter den Variablennamen `a` und `b` gespeichert (`igcdex` steht für *greatest common divisor, extended Euclidean algorithm for integers.*

Wichtige Anwendungen. 1. Es ist die Bézout'sche Gleichung, die zeigt, dass die Primfaktorzerlegung in $\mathbb{Z}$ eindeutig ist: Der wesentliche Schritt ist folgender: Ist p eine Primzahl, die mn teilt, so teilt p eine der beiden Zahlen m, n. Sei etwa $mn = ps$. Wir nehmen an, dass p kein Teiler von m ist. Es ist also $(p, m) = 1$, also $1 = ap + bm$, für gewisse Zahlen a, b, also $n = apn + bmn = apn + bps = p(an + bs)$.

Die Eindeutigkeit der Primfaktorzerlegung beweist man nun wie folgt: Seien Primzahlen p_i, q_j gegeben mit $p_1 \cdots p_t = q_1 \cdots q_s$. Da p_1 die rechte Seite teilt und Primzahl ist, teilt p_1 mindestens einen der Faktoren der rechten Seite, etwa q_j. Da qJ Primzahl ist und p_1 ein von 1 verschiedener Teiler von q_j ist, gilt $p_1 = q_j$. Wir teilen links und rechts durch diese Zahl und erhalten $p_2 \cdots p_t = q_1 \cdots q_{j-1} q_{j+1} \cdots q_s$ (hier verwenden wir, dass $\mathbb{Z}$ nullteilerfrei ist). Induktion liefert die Behauptung.

Wichtige Anwendungen. 2. Ist p eine Primzahl, so ist $\mathbb{Z}/p$ ein Körper. Genauer: Ist $1 \leq u < p$, so ist $(u, p) = 1$. Also gibt es ganze Zahlen a, b mit $au + bp = 1$, also $\overline{a} \cdot \overline{u} = \overline{1}$. Demnach ist $\overline{u}$ in $\mathbb{Z}/n$ invertierbar und $(\overline{u})^{-1} = \overline{a}$.

Verallgemeinerung. *Ist $n \in \mathbb{N}$ beliebig und $u \in \mathbb{N}$, so gilt: Genau dann ist $\overline{u}$ in $\mathbb{Z}/n$ invertierbar, wenn $(u, n) = 1$ gilt.* Beweis: Ist $\overline{u}$ invertierbar, so gibt es $a \in \mathbb{Z}$ mit $\overline{au} = \overline{1}$ in $\mathbb{Z}/n$, also ist $1 - au$ durch n teilbar, etwa $1 - au = bn$, also $1 = au + bn$. Dann muss aber $(u, n) = 1$ gelten, denn jeder Teiler von u und n ist auch ein Teiler von $1 = au + bn$.. Umgekehrt: Sei $(u, n) = 1$. Bézout liefert $au + bn = 1$, also $\overline{a} \cdot \overline{u} = \overline{1}$. Demnach ist $\overline{a} = (\overline{u})^{-1}$.

Wir sehen also: Es ist $(\mathbb{Z}/n)^* = \{\overline{u} \mid 1 \leq u \leq n, (u, n) = 1\}$ und diese Menge entspricht bijektiv der Menge $\{u \mid 1 \leq u \leq n, (u, n) = 1\}$. Dies ist aber eine Menge der Kardinailtät $\phi(n)$. Insbesondere sehen wir

$$\boxed{|(\mathbb{Z}/n)^*| = \phi(n)}$$

Man kann das Ergebnis auf zweierlei Weisen interpretieren: Erstens, von links nach rechts: Wir wissen, wie wir die Kardinalität von $(\mathbb{Z}/n)^*$ berechnen. Zweitens (viel wichtiger), von rechts nach links gelesen: die Menge $\{u \mid 1 \leq u \leq n, (u, n) = 1\}$, die durch $\phi(n)$ abgezählt wird, ist keine gesichtslose Menge, sondern hat eine Struktur: die der Einheitengruppe $(\mathbb{Z}/n)^*$.

Bemerkungen. Sei $n \in \mathbb{N}$.

- $\mathbb{Z}/n$ ist nullteilerfrei genau dann, wenn n eine Primzahl ist.
- Genau dann besitzt $\mathbb{Z}/n$ von Null verschiedenen nilpotenten Elemente, wenn es eine Primzahl p gibt mit $p^2 | n$.

3.1. Produkte von Halbgruppen und Ringen.

Wir setzen voraus, dass bekannt ist, wie Halbgruppen, Gruppen, Ringe und Körper definiert sind. Ebenfalls wird vorausgesetzt, was man in der Algebra unter einem Homomorphismus versteht (z.B.: ein Ring-Homomorphismus $\eta\colon R \to R'$ ist eine Abbildung,

die verträglich mit Addition und Multiplikation ist und für die $\eta(1_R) = 1'_R$ gilt, dabei bedeutet die Verträglichkeit mit der Addition, dass $\eta(r_1 + r_2) = \eta(r_1) + \eta(r_2)$ gilt, usw.) Um zu zeigen, dass ein Ring-Homomorphismus $\eta\colon R \to R'$ injektiv ist, braucht man nur zu verifizieren, dass $\eta(r) = 0$ nur für $r = 0$ gilt. (Denn ist $\eta(r_1) = \eta(r_2)$, so ist $\eta(r_1 - r_2) = 0$. Gilt nun $\eta(r) = 0$ nur für $r = 0$, so sieht man, dass $r_1 - r_2 = 0$ gilt und daher $r_1 = r_2$.)

Sind H, H' zwei Halbgruppen, so wird die Produktmenge $H \times H'$ mit komponentenweiser Verknüpfung eine Halbgruppe, das *Produkt* von H und H' (nach Definition ist also

$$(h_1, h'_1)(h_2, h'_2) = (h_1h_2, h'_1h'_2)$$

für $h_1, h_2 \in H$ und $h'_1, h'_2 \in H'$; das Einselement von $H \times H'$ ist $(1_H, 1_{H'})$. (Hier und im Folgenden ist einiges zu verifizieren — dies sollte aber keine Schwierigkeiten bereiten.) Sind H, H' Gruppen, so ist auch $H \times H'$ eine Gruppe; es ist dann $(h, h')^{-1} = (h^{-1}, (h')^{-1})$. Sind H, H' kommutativ, so ist auch $H \times H'$ kommutativ.

Sind R, R' Ringe, so ist wird die Produktmenge $R \times R'$ durch komponentenweise Addition und komponentenweise Multiplikation ein Ring, das *Produkt* von R, R'. Das Element $(1, 1) = (1_R, 1_{R'})$ ist das Einselement $1 = 1_{R\times R'}$ von $R \times R'$. Sind R, R' kommutative Ringe, so ist auch $R \times R'$ kommutativ.

Beachte: die Elemente $e = (1, 0)$ und $e' = (0, 1)$ sind idempotent (das heißt $e^2 = e, (e')^2 = e'$) mit $1 = e + e'$. In jedem Ring gilt: Ist e ein Idempotent im Ring R, so ist auch $1 - e$ ein Idempotent. Auch gilt: Ist $e \in R$ ein Idempotent im Ring R, so ist eRe wieder ein Ring (mit Einselement e). Und es gilt: *Ist S ein kommutativer Ring, und ist $e \in R$ ein Idempotent, so ist R isomorph zu $eR \times (1 - e)R$ unter der Abbildung η mit $\eta(r) = (er, (1 - e)r)$ für $r \in R$.*

Beweis: Die Abbildung ist ein Ring-Homomorphismus: Verträglichkeit mit der Addition und Multiplikation: Sei $*$ Addition oder Multiplikation:

$$(e(x * y), (1 - e)(x * y)) = (ex * ey, (1 - e)x * (1 - e)y) = (ex, (1 - e)x) * (ey, (1 - e)y).$$

Es ist $\eta(1) = (e, (1-e)) = 1_{eR\times(1-e)R}$. Injektivität von η: Sei $(er, (1-e)r) = 0 = (0, 0)$. also $er = 0, (1 - e)r = 0$. Addition zeigt: $0 = er + (1 - e)r = r$. Surjektivität: Sei $x \in eR, y \in (1 - e)R$. Sei $r = x + y$. Da $x \in eR$, ist $ex = x$ (denn aus $x = er'$ mit $r' \in R$ folgt $ex = e \cdot er' = e^2r' = er' = x$, weil e Idempotent ist). Analog sieht man $(1 - e)y = y$, da $y \in (1 - e)R$ und auch $1 - e$ ein Idempotent ist.

Ist R ein Ring, so bezeichnen wir mit R^* die Menge der (bezüglichder Multiplikation) invertierbaren Elemente, dies ist eine Gruppe. Man nennt sie die *Einheitengruppe* des Rings R. Es gilt:

$$(R \times R')^* = (R^*, (R')^*)$$

(links und rechts stehen Teilmengen von $R \times R'$; behauptet wird also die Gleichheit dieser Teilmengen, zusätzlich aber auch, dass diese eine Gleichheit von Gruppen ist: dies gilt, weil sowohl im Produkt-Ring $R \times R'$ als auch in der Produkt-Gruppe $(R^*, (R')^*)$ die Multiplikation komponentenweise definiert ist.

3.2. Der Chinesische Restsatz.

3.2.1. Lemma. *Für beliebige natürliche Zahlen m, n gilt: Die kanonische Abbildung $\mathbb{Z}/(mn) \to \mathbb{Z}/m$ mit $\overline{u} \mapsto \overline{u}$ ist ein surjektiver Ring-Homomorphismus.* (Achtung: die Bezeichnung $\overline{u}$ steht hier für zwei ganz verschiedene Elemente, nämlich für Elemente, die man genauer mit $\overline{u}^{(nm)}, \overline{u}^{(n)}$ bezeichnen sollte...).

Beweis: Zu zeigen ist eigentlich gar nichts. Man muss sich nur überlegen, was zu zeigen ist, und dass all dies offensichtlich ist.

3.2.1. Satz. *Seien m, n natürliche Zahlen mit $(m, n) = 1$. Die kanonische Abbildung $\mathbb{Z}/(mn) \to (\mathbb{Z}/m) \times (\mathbb{Z}/n)$ mit $\overline{u} \mapsto (\overline{u}, \overline{u})$ ist ein Isomorphismus von Ringen.* (Achtung: die Bezeichnung $\overline{u}$ steht auch hier für drei verschiedene Elemente, nämlich für Elemente, die man genauer mit $\overline{u}^{(nm)}, \overline{u}^{(m)}, \overline{u}^{(n)}$ bezeichnen sollte...).

Beweis: Gar nicht offensichtlich ist, dass die Abbildung surjektiv ist. Sie ist aber offensichtlich injektiv: Denn sei $u \in \mathbb{Z}$ mit $(\overline{u}, \overline{u}) = 0 = (0, 0)$. Es gilt also $\overline{u} = 0$ in $\mathbb{Z}/m$ wie auch in $\mathbb{Z}/n$. Demnach ist u durch m teilbar und durch n teilbar. Da m, n teilerfremd sind, ist u auch durch mn teilbar, also gilt auch $\overline{u} = 0$ in $\mathbb{Z}/(mn)$. (Wir verwenden hier, dass man für die Injektivität eines Gruppen-Homomorphismus nur zeigen muss, dass der Kern einelementig ist; hier wird dies auf die additiven Gruppen angewandt.)

Nun ist aber $\mathbb{Z}/(mn)$ eine Menge der Kardinalität mn, und auch $(\mathbb{Z}/m) \times (\mathbb{Z}/n)$ hat die Kardinalität mn. Demnach ist eine injektive Abbildung $\mathbb{Z}/(mn) \to (\mathbb{Z}/m) \times (\mathbb{Z}/n)$ auch surjektiv.

Zweiter Beweis der Surjektivität (**konstruktiv**, deshalb auf jeden Fall von Interesse): Wir konstruieren explizit Urbilder. Wir beginnen folgendermaßen: Da m, n teilerfremd sind, gibt es nach Bézout Zahlen a, b mit

$$an + bm = 1.$$

Sei nun $(\overline{u}, \overline{v})$ in $(\mathbb{Z}/m) \times (\mathbb{Z}/n)$ gegeben. Setze

$$x = anu + bmv.$$

Es gilt

$$\begin{aligned} x = anu + bmv &\equiv anu + bmu = (an + bm)u = 1 \cdot u = u \mod m, \\ x = anu + bmv &\equiv anv + bmv = (an + bm)v = 1 \cdot v = v \mod n. \end{aligned}$$

also ist $(\overline{x}, \overline{x}) = (\overline{u}, \overline{v})$, die Zuordnung ist also surjektiv.

Zusatz: Die Linearkombination $an + bm = 1$ ist gerade so gewählt, dass die Restklasse von an modulo m das Einselement von $\mathbb{Z}/m$ liefert (und xn ein Vielfaches von n ist), während die Restklasse von bm modulo n das Einselement von $\mathbb{Z}/n$ liefert (und ym ein Vielfaches von y ist). Unter der kanonischen Abbildung $\mathbb{Z} \to (\mathbb{Z}/m) \times (\mathbb{Z}/n)$ wird also an auf das Idempotent $(1, 0)$, und bm auf das Idempotent $(0, 1)$ abgebildet.

Nachtrag: Sind m, n natürliche Zahlen mit $(m, n) = 1$ (also ohne einen echten gemeinsamen Teiler), so nennt man m, n *relativ prim.*

3.2.3. Allgemeiner Fall. *Seien $n_1, \ldots, n_t$ natürliche Zahlen, die paarweise relativ prim sind. Dann ist die kanonische Abbildung*

$$\mathbb{Z}/(n_1 \cdots n_t) \to (\mathbb{Z}/n_1) \times \cdots \times (\mathbb{Z}/n_t)$$

ein Ring-Isomorphismus (insbesondere also bijektiv).

3.2.4. Umformulierung der Bijektivität. *Seien $n_1, \ldots, n_t$ natürliche Zahlen, die paarweise relativ prim sind. Seien $u_1, \ldots, u_t \in \mathbb{Z}$. Dann gibt es eine Zahl $x \in \mathbb{Z}$ mit*

$$x \equiv u_i \mod n_i \qquad \textit{für} \qquad 1 \leq i \leq t,$$

und die Menge der Zahlen x mit dieser Eigenschaft bildet eine Restklasse modulo $n_1 \cdots n_t$.

Beweis mit Induktion. Oder auch explizit: Setze $m_i = n_1 \cdots n_{i-1} n_{i+1} \cdots n_t$. Dann gilt $(m_i, n_i) = 1$. Nach Bézout finden wir $a_i, b_i \in \mathbb{Z}$ mit

$$a_i m_i + b_i n_i = 1.$$

Unter der kanonischen Abbildung $\mathbb{Z} \to (\mathbb{Z}/n_1) \times \cdots \times (\mathbb{Z}/n_t)$ wird $a_i m_i$ auf das Element $(0, \ldots, 0, 1, 0, \ldots, 0)$ mit der Eins an der i-ten Stelle abgebildet (denn $a_i m_i$ ist ein Vielfaches von n_j für $j \neq i$, andererseits ist $a_i m_i = 1 - b_i n_i \equiv 1 \mod n_i$).

Eine gesuchte Lösung x ist also

$$\boxed{x = \sum\nolimits_i a_i m_i u_i}$$

Beispiel. Betrachte das Gleichungssystem

$$x \equiv 2 \mod 9, \quad x \equiv 1 \mod 5, \quad x \equiv 3 \mod 7.$$

Hier ist also

$$n_1 = 9 \qquad n_2 = 5 \qquad n_3 = 7$$

$$m_1 = 5 \cdot 7 = 35 \qquad m_2 = 9 \cdot 7 = 63 \qquad m_3 = 9 \cdot 5 = 45.$$

Als erstes suchen wir also Lösungen der drei Bézout'schen Gleichungen

$$35a_1 + 9b_1 = 1, \quad 63a_2 + 5b_2 = 1, \quad 45a_3 + 7b_3 = 1.$$

Zum Beispiel können wir nehmen:

$$\begin{aligned} a_1 &= -1 & b_1 &= \ \ 4 \\ a_2 &= \ \ 2 & b_2 &= -25 \\ a_3 &= -2 & b_3 &= \ 13 \end{aligned}$$

und demnach

$$a_1 m_1 = -1 \cdot 35 = -35, \quad a_2 m_2 = 2 \cdot 63 = 126, \quad a_3 m_3 = -2 \cdot 45 = -90.$$

Dies sind also die benötigten Zahlen, mit denen wir **jedes** Gleichungssystem der Form

$$x \equiv u_1 \mod 9, \quad x \equiv u_2 \mod 5, \quad x \equiv u_3 \mod 7.$$

lösen können.

In unserem Beispiel ist $u_1 = 2,\ u_2 = 1,\ u_3 = 3$. Also erhalten wir als Lösung

$$x = \sum\nolimits_i a_i m_i u_i = (-35) \cdot 2 + 126 \cdot 1 + (-90) \cdot 3 = -214.$$

Statt -214 nehmen wir lieber die positive Zahl $-214 + 315 = 101$. Offensichtlich ist $x = 101$ wirklich eine Lösung unseres Gleichungssystems.

(3.2.5.) *Ist p eine Primzahl und d eine natürliche Zahl, so besitzt $\mathbb{Z}/p^d$ genau zwei Idempotente, nämlich $\overline{0}$ und $\overline{1}$.* Demnach kann $\mathbb{Z}/p^d$ **nicht** als Produkt zweier von Null verschiedener Ringe geschrieben werden.

Beweis: Dies ist richtig für $d = 1$, denn $\mathbb{Z}/p$ ist ein Körper. Sei nun d beliebig. Wir betrachten die kanonische Abbildung $\mathbb{Z}/p^d \to \mathbb{Z}/p$. Sei $\overline{u}$ ein Idempotent in $\mathbb{Z}/p^d$. Dann ist $\overline{u} = \overline{u}^{(p)}$ ein Idempotent in $\mathbb{Z}/p$. Da $\mathbb{Z}/p$ ein Körper ist, sehen wir: entweder ist $\overline{u} = \overline{0}$ oder $\overline{u} = \overline{1}$. Im ersten Fall ist u durch p teilbar, also u^d durch p^d, also ist $u^d \equiv 0 \mod p$. Nun setzen wir aber voraus, dass $\overline{u}$ in $\mathbb{Z}/p^d$ idempotent ist, demnach ist $\overline{u} = (\overline{u})^d = \overline{u^d} = 0$.

Wir wenden uns nun dem zweiten Fall zu: $\overline{u} = \overline{1}$. Ist in einem Ring e idempotent, so ist auch $1 - e$ idempotent. Dies zeigt, das mit $\overline{u}$ auch $\overline{1 - u}$ in $\mathbb{Z}/p^d$ idempotent ist. Wie im ersten Fall folgt nun $\overline{u} = 1$. Damit ist die Behauptung bewiesen.

Zusatz, für Fortgeschrittene (wir verwendet den Begriff eines "Ideals"). Im Ring $\mathbb{Z}/p^d$ bilden die Restklassen der Elemente in $p\mathbb{Z}$ ein nilpotentes Ideal, und der Restklassenring nach diesem Ideal ist der Körper $\mathbb{Z}/p$. Es reicht, folgendes allgemeine Lemma zu beweisen:

Lemma. *Sei R Ring, sei I Ideal in R mit R/I Körper. Ist jedes Element in I nilpotent, so besitzt R nur zwei Idempotente, nämlich 0 und 1.* Beweis: Sei $e = e^2$ in R. Dann ist $\overline{e} \in R/I$ ebenfalls Idempotent, aber in einem Körper gibt es nur die Idempotente 0 und 1, also ist $e \in I$ oder $1 - e \in I$. Im ersten Fall ist $e^n = 0$ für ein n, aber $e^n = e$, weil e nilpotent ist. Im zweiten Fall ist entsprechend $(1 - e)^n = 0$. Aber mit e ist auch $1 - e$ ein Idempotent und demnach $1 - e = 0$, also $e = 1$.

3.3. Der Satz von Lagrange. Die Ordnung eines Gruppen-Elements.

3.3.1. (Satz von Lagrange). *Sei G eine endliche Gruppe, sei U eine Untergruppe. Dann ist $|U|$ ein Teiler von $|G|$.* Man nennt $|G|/|U|$ den *Index von U in G.*

Beweis: Ist $g \in G$, so nennt man $Ug = \{ug \mid u \in U\}$ die Rechtsnebenklasse von g in G. Da in einer Gruppe aus $u_1 g = u_2 g$ folgt, dass $u_1 = u_2$ gilt (= Kürzungsregel), haben alle Rechtsnebenklasse die gleiche Anzahl von Elementen. Wir zeigen, dass die Rechtsnebenklassen eine Partition von G bilden, dass also gilt: haben zwei Rechtsnebenklassen nicht-leeren Durchschnitt, so stimmen sie überein: Sei also $Ug_1 \cap Ug_2 \neq \emptyset$, also etwa $u_1 g_1 = u_2 g_2$ mit $u_1, u_2 \in U$, also $g_1 = u_1^{-1} u_2 g_2$. Sei $u \in U$. Es ist

$$ug_1 = uu_1^{-1} u_2 g_2 \in Ug_2,$$

also $Ug_1 \subseteq Ug_2$. Entsprechend sieht man $Ug_2 \subseteq Ug_1$. Ist demnach m die Anzahl der Rechtsnebenklassen von U in G, so gilt $m|U| = |G|$.

Eine Gruppe C heißt *zyklisch,* wenn es ein Element $g \in C$ gibt, sodass sich alle Elemente von C in der Form g^z mit $z \in \mathbb{Z}$ schreiben lassen; in diesem Fall nennt man g ein *erzeugendes Element* für C; man sagt auch: g erzeugt C und schreibt $G = \langle g \rangle$.

Sei nun $G = (G, \cdot)$ eine Gruppe. Genau dann ist G zyklisch und von g erzeugt, wenn es keine echte Untergruppe U von G gibt mit $g \in U$.

Ist $g \in G$. Wir bilden die Folge der Potenzen

$$1, g, g^2, g^3, \ldots$$

Fall 1: die Potenzen sind paarweise verschieden. Dann liefert die Zuordnung $(\mathbb{Z}, +) \to G$, die durch $z \mapsto g^z$ definiert ist, einen Gruppen-Isomorphismus $(\mathbb{Z}, +) \to \langle g \rangle$.

Fall 2: die Potenzen sind nicht paarweise verschieden (dies gilt insbesondere dann, wenn G eine endliche Gruppe ist). Sei n minimal mit $g^n \in \{1, g, \ldots, g^{n-1}\}$. Dann ist $g^n = 1$, und die Zuordnung $(\mathbb{Z}, +) \to G$, die durch $z \mapsto g^z$ definiert ist, liefert einen Gruppen-Isomorphismus $(\mathbb{Z}/n, +) \to \langle g \rangle$.

Beweis: Es ist $g^n = 1$ zu zeigen. Sei etwa $g^n = g^t$ für ein t mit $0 \leq t < n$. Wir können kürzen und erhalten $g^{n-t} = 1$. Die Minimalität von n besagt $n - t = n$, alsio $t = 1$.

Ist also n minimal mit $g^n = 1$, so ist $\langle g \rangle$ isomorph zur Gruppe $(\mathbb{Z}/n, +)$; insbesondere hat $\langle g \rangle$ genau n Elemente. Man nennt n die *Ordnung* von g, und $|G|/n$ den *Index* von g in G (nach dem Satz von Lagrange ist dies eine natürliche Zahl).

> Ist $(G, +)$ eine additiv geschrieben Gruppe, so ist die Definition der Ordnung eines Elements folgendermaßen umzuformulieren: Die Ordnung von $g \in (G, +)$ ist die kleinste natürliche Zahl n mit $ng = 0$.