3.3.2. Satz (Charakterisierung zyklischer Gruppen). *Sei G eine Gruppe der Ordnung n. Die folgenden Aussagen sind äquivalent:*
(1) *G ist zyklisch.*
(2) *Die Anzahl der Elemente der Ordnung d ist $\phi(d)$, für jeden Teiler d von n.*
(3) *Die Anzahl der Elemente der Ordnung d ist kleiner oder gleich $\phi(d)$, für jeden Teiler d von n.*

Beweis: Sei $M(d)$ die Menge der Element von G mit Ordnung d.

(3) impliziert (1): Nach Voraussetzung gilt: $|M(d)| \leq \phi(d)$. Nach dem Satz von Lagrange gilt: $G = \bigcup_{d|n} M(d)$ (und die Teilmengen $M(d)$ sind paarweise disjunkt). Es ist also $n = |G| = \sum_{d|n} |M(d)| \leq \sum_{d|n} \phi(n) = n$. Wäre $|M(d)| < \phi(d)$ für ein d, so würde auch $\sum_{d|n} |M(d)| < \sum_{d|n} \phi(n)$ gelten. Damit haben wir (2) gezeigt, wir wollen aber eigentlich (1) zeigen: dies ist der Spezialfall $|M(n)| = \phi(n) \geq 1$, der ja besagt: es gibt ein Element der Ordnung n.

(1) impliziert (2): Wir brauchen folgende Vorbermerkung:

Lemma. *Die kleinste natürliche Zahl t mit $n|ta$ ist $t = \frac{n}{(a,n)}$, also ist $\frac{n}{(a,n)}$ die Ordnung von $\overline{a}$ in $(\mathbb{Z}/n, +)$.*

Beweis: Setze $n = d(a,n)$, und $a = d'(a,n)$, mit $(d,d') = 1$. Es ist $n = d(a,n)|da$, also gilt $n|da$ (da $d = n/(a,n)$). Sei nun t gegeben mit $n|ta$. Also

$$d(a,n) = n|ta = td'(a,n),$$

kürzen liefert $d|td'$. Wegen $(d,d') = 1$ folgt $d|t$.

Sei d ein Teiler von n. Sei a eine natürliche Zahl mit $1 \leq a \leq n$ und $(a,n) = \frac{n}{d}$. Dann hat $\overline{a}$ in $(\mathbb{Z}/n, +)$ die Ordnung d. Sei $d' = \frac{n}{d}$ (also $n = dd'$). Jede natürliche Zahl a mit $1 \leq a \leq n$ und $(a,n) = \frac{n}{d} = d'$ ist durch d' teilbar, und das Teilen durch d' liefert eine Bijektion

$$\{a \mid 1 \leq a \leq n \text{ und } (a,n) = \tfrac{n}{d}\} \longrightarrow \{b \mid 1 \leq b \leq d \text{ und } (b,d) = 1\}$$

(beachte: $n/(d') = d$). Die Menge rechts hat nach Definition gerade die Kardinalität $\phi(d)$. Dies zeigt: *Es gibt genau $\phi(d)$ Elemente in $(\mathbb{Z}/n, +)$ der Ordnung d.*

3.3.3. Folgerung. *Ist G eine zyklische Gruppe der Ordnung n und ist d ein Teiler von n, so besitzt G genau eine Untergruppe der Ordnung d und die ist zyklisch.*

Beweis: Wegen (2) besitzt G mindestens ein Element der Ordnung d (denn $\varphi(d) \geq 1$); die von g erzeugte Untergruppe U ist natürlich zyklisch und hat die Ordnung d. In U gibt es $\phi(d)$ Elemente der Ordnung d, also sehen wir: alle Elemente von G der Ordnung d liegen in U.

Ist U' eine beliebige Untergruppe von G der Ordnung d, so muss diese wegen der Implikation (3) $\implies$ (*i*) zyklisch sein: denn ist e ein Teiler von d, so ist e ein Teiler von $|G|$, also gibt es nach (2) in G genau $\phi(e)$ Elemente der Ordnung e, daher kann es in U' höchstens $\phi(e)$ Elemente der Ordnung d' geben. Die Untergruppe U' werde also

von g' erzeugt. Nun ist g' ein Element der Ordnung d, liegt also in U. Damit sehen wir $U' \subseteq U$, also $U' = U$ (denn beide Gruppen haben die Ordnung d).

3.3.4. Folgerung. *Eine zyklische Gruppe G besitzt höchstens ein Element der Ordnung* 2 (und zwar existiert ein derartiges Element genau dann, wenn G endliche Gruppe mit gerader Ordnung ist).

Beweis: Ist G eine unendliche zyklische Gruppe, so hat nur das neutrale Element endliche Ordnung, nämlich Ordnung 1. Sei also G eine endliche zyklische Gruppe, mit Ordnung $|G| = n$. Ist n ungerade, so gibt es kein Element der Ordnung 2, denn die Ordnung eines jeden Elements ist ein Teiler der Gruppen-Ordnung. Ist n gerade, so besitzt G genau eine Untergruppe U der Ordnung 2, siehe 3.3.3. In U gibt es genau ein Element der Ordnung 2. Ist umgekehrt g ein Element der Ordnung 2, so ist $U' = \{1, g\}$ eine Untergruppe der Ordnung 2, also $U' = U$.

3.3.5. Folgerung. *Eine endliche Gruppe G ist genau dann zyklisch, wenn es zu jedem Teiler d von $|G|$ höchstens eine Untergruppe der Ordnung d gibt.*

Beweis: Eine der beiden Implikationen steht in 3.3.3. Umgekehrt setzen wir nun voraus, dass G eine Gruppe ist, die zu jedem Teiler d von $|G|$ höchstens eine Untergruppe der Ordnung d besitzt. Sei d ein Teiler von $|G|$. Ist g ein Element der Ordnung d, so erzeugt g eine Untergruppe U der Ordnung g. Da U die einzige Untergruppe der Ordnung d ist, müssen in U alle Elemente der Ordnung d enthalten sein. Da U zyklisch ist, gibt es in U genau $\phi(d)$ Elemente der Ordnung d. Wir sehen also: entweder gibt es gar kein Element der Ordnung d, oder aber es gibt $\phi(d)$ Elemente der Ordnung d. Es gilt demnach (3) in 3.3.2, also ist G zyklisch.

Wir notieren hier einige ganz elementare Eigenschaften der Ordnung eines Gruppen-Elements (mit direkten Beweisen).

3.3.6. Lemma. (a) *Sei G eine Gruppe. Ist $g^d = 1$, mit $d \geq 1$, so ist die Ordnung von g ein Teiler von d.*

(b) *Das Element $g \in G$ habe die Ordnung n. Ist d ein Teiler von n, so hat g^d die Ordnung $\frac{n}{d}$. Sind die Zahlen t, n teilerfremd, so hat g^t die Ordnung n.*

(c) *Ist $\eta\colon G \to H$ ein Gruppen-Homomorphismus und hat $g \in G$ die Ordnung m, so ist die Ordnung von $\eta(g)$ ein Teiler von m.*

(d) *Sei G eine Gruppe, sei g ein Element von G der Ordnung d und h ein Element von G der Ordnung e. Sind die Zahlen d, e teilerfremd und gilt $gh = hg$, so ist gh ein Element der Ordnung de.*

Beweis: (a) Sei e die Ordnung von g. Sei d' der größte gemeinsame Teiler von d und e. Seien a, b ganze Zahlen mit $d' = ad + be$. Dann ist $g^{d'} = g^{ad+be} = (g^d)^a \cdot (g^e)^b = 1$. Wegen der Minimalität von e ist $e \leq d'$, also $e = d'$. Aber d' ist ein Teiler von d.

(b) Das Element $g \in G$ habe die Ordnung n. Sei d ein Teiler von n. Dann ist $(g^d)^{n/d} = g^n = 1$, also ist die Ordnung von g^d ein Teiler von $\frac{n}{d}$. Sei e die Ordnung von g^d. Dann ist $g^{de} = (g^d)^e = 1$, also ist $n \leq de$. Wegen $e|\frac{n}{d}$ ist aber auch $de \leq n$. Also $n = de$.

Für beliebiges $t \in \mathbb{Z}$ gilt $(g^t)^n = g^{tn} = (g^n)^t = 1$, Also ist die Ordnung e von g^t ein Teiler von n. Seien nun die Zahlen n, t teilerfremd. Wähle eine Bézout'sche Gleichung $1 = an + bt$ mit ganzen Zahlen a, b. Es ist $g^e = (g^{an+bt})^e = g^{ane} \cdot g^{bte} = 1$, also ist $n \leq e$ und demnach $n = e$.

(c) Aus $g^d = 1$ folgt $\eta(g)^d = 1$. Verwende nun (a).

(d) Aus $gh = hg$ folgt $(gh)^n = g^n h^n$ für jedes n. Insbesondere gilt $(gh)^{de} = g^{de}h^{de} = (g^d)^e \cdot (h^e)^d = 1$. Die Ordnung von gh ist also ein Teiler von de. Sei t die Ordnung von gh. Dann ist

$$1 = (gh)^t = (gh)^{te} = g^{te}h^{te} = g^{te}$$

(denn $h^{te} = 1$). Daraus folgt $d|te$, also $d|t$ (weil $(d, e) = 1$). Entsprechend sieht man: $e|t$, und demnach $de|t$, also $t = de$..

3.3.7. Sei $C_n = (\mathbb{Z}/n, +)$, dies ist unser Standard-Modell einer zyklischen Gruppe der Ordnung n (additiv geschrieben!). Beachte: Ist $(n, m) = 1$, so ist die kanonische Abbildung

$$C_{nm} = (\mathbb{Z}/nm, +) \longrightarrow (\mathbb{Z}/n, +) \times (\mathbb{Z}/m, +) = C_n \times C_m$$

ein Gruppen-Isomorphismus (siehe 3.2.1 = Chinesischer Restsatz). Das heißt: *Ist* $(n, m) = 1$*, so ist* $C_n \times C_m$ *wieder eine zyklische Gruppe.*

3.4. Endliche Untergruppen der multiplikativen Gruppe eines Körpers.

3.4.1. Satz. *Sei K ein Körper. Ist G eine endliche Untergruppe der multiplikativen Gruppe $K^* = (K \setminus \{0\}, \cdot)$ von K, so ist G zyklisch.*

Beweis: Sei $|G| = n$, sei d ein Teiler von n. Wir zeigen: Es gibt in G höchstens eine Untergruppe der Ordnung d. Die Behauptung folgt dann nach 3.3.5.

Sei Z_d die Menge der Elemente $x \in K$ mit $x^d = 1$, dies ist die Menge der Nullstellen des Polynoms $X^d - 1 \in K[X]$. Ein Polynom vom Grad d (mit Koeffizienten in einem Körper K) hat höchstens d Nullstellen, also ist $|Z_d| \leq d$.

Sei nun H eine Untergruppe von G der Ordnung d. Ist $h \in H$, so gilt $h^d = 1$ (nach dem Satz von Lagrange: die Ordnung eines Elements einer endlichen Gruppe ist ein Teiler der Gruppen-Ordnung). Wir sehen also: $H \subseteq Z_d$. Nun ist $|H| = d$ und $|Z_d| \leq d$, also folgt $H = Z_d$. Dies zeigt: H ist eindeutig bestimmt. Es gibt also höchstens eine Unterguppe der Ordnung d.

3.4.2. Folgerung. *Für jede Primzahl p gilt: Die Gruppe $(\mathbb{Z}/p)^*$ ist zyklisch.*

Beweis: $\mathbb{Z}/p$ ist ein Körper.

Ist a eine ganze Zahl, sodass $\overline{a} \in (\mathbb{Z}/p)^*$ ein erzeugendes Element ist, so nennt man a eine *Primitivwurzel modulo p*. Es ist nicht ganz einfach, zu einer Primzahl p

eine Primitivwurzel modulo p zu finden — dafür gibt es Listen, ansonsten hilft nur Probieren.

3.5. Die Gruppe $(\mathbb{Z}/2^d)^*$.

Ist $d = 1$, so ist $|(\mathbb{Z}/2^d)^*| = \phi(2) = 1$, ist $d = 2$, so ist $|(\mathbb{Z}/2^d)^*| = \phi(4) = 2$. Jede Gruppe der Ordnung 2 ist offensichtlich zyklisch. Die Gruppe $(\mathbb{Z}/2^d)^*$ besteht aus den Restklassen $\overline{1}$ und $g = \overline{3} = \overline{-1}$, sie wird von g erzeugt.

Wir können nun annehmen, dass $d \geq 3$ gilt.

3.5.1. Satz. *Sei $d \geq 2$. Die Gruppe $(\mathbb{Z}/2^d)^*$ wird von den Elementen $\overline{5}$ und $\overline{-1}$ erzeugt, die Ordnung von $\overline{5}$ ist 2^{d-2}, die von $\overline{-1}$ ist 2.*

Beweis: Dass $\overline{-1}$ die Ordnung 2 hat, ist offensichtlich. Wir zeigen nun, dass $\overline{5}$ die Ordnung 2^{d-2} hat. Für $d = 2$ ist dies klar, wir können also $d \geq 3$ annehmen.

3.5.2. Lemma. *Ist $a \in \mathbb{Z}$ ungerade, und $d \geq 3$, so gilt $a^{2^{d-2}} \equiv 1 \mod 2^d$.*

Beweis mit Induktion. Für $d = 3$ ist zu zeigen: $a^2 \equiv 1 \mod 8$. Ist $a = 1, 3, 5, 7$, so ist $a^2 = 1, 9, 25, 49$, in allen Fällen gilt $8|(a^2 - 1)$. Sei nun $d > 3$. Wir setzen voraus, dass gilt

$$a^{2^{d-3}} \equiv 1 \mod 2^{d-1},$$

also gibt es $n \in \mathbb{Z}$ mit $a^{2^{d-3}} = 1 + 2^{d-1}n$. Demnach ist

$$a^{2^{d-2}} = (1 + 2^{d-1}n)^2 = 1 + 2^d n + 2^{2d-2}n^2 \equiv 1 \mod 2^d,$$

denn $2d - 2 \geq d$.

3.5.3. Folgerung. *Für $d \geq 3$ ist die Gruppe $(\mathbb{Z}/2^d)^*$ nicht zyklisch.*

Beweis: Die Gruppe $G = (\mathbb{Z}/2^d)^*$ hat die Ordnung $\phi(2^d) = 2^{d-1}$. Die Elemente von G sind die Restklassen $\overline{a}$ mit $a \in \mathbb{Z}$ ungerade — alle diese Elemente haben als Ordnung einen Teiler von 2^{d-2}.

3.5.4. Behauptung: $5^{2^{d-3}} \equiv 1 + 2^{d-1} \mod 2^d$.

Beweis, mit Induktion. Die Behauptung ist richtig für $d = 3$. Sei nun $d \geq 4$. Wir setzen voraus: $5^{2^{d-4}} \equiv 1 + 2^{d-2} \mod 2^{d-1}$, also $5^{2^{d-4}} = 1 + 2^{d-2} + n2^{d-1}$ für ein $n \in \mathbb{Z}$. Also

$$\begin{aligned} 5^{2^{d-3}} &= (1 + 2^{d-2} + n2^{d-1})^2 \\ &= (1 + 2^{d-2}(1 + 2n))^2 \\ &= 1 + 2^{d-1}(1 + 2n) + 2^{2d-4}(1 + 2n)^2 \\ &\equiv 1 + 2^{d-1} \mod 2^d, \end{aligned}$$

dabei verwenden wir $d \geq 4$.

Wegen 3.5.4 sehen wir, dass gilt: $5^{2^{d-3}} \not\equiv 1 \mod 2^d$. Dies zeigt zusammen mit 3.5.2, dass $\overline{5}$ die Ordnung 2^{d-2} hat.

3.5.5. Es bliebt zu zeigen, dass $\overline{-1}$ nicht in der von $\overline{5}$ erzeugten Untergruppe liegt. Angenommen, $5^n \equiv -1 \mod 2^d$, für ein $n \in \mathbb{N}$, also $5^n = -1 + m2^d$ mit $m \in \mathbb{Z}$. Modulo 4 erhalten wir

$$1 = 1^n \equiv 5^n \equiv -1 \mod 4,$$

dies ist unsinnig.

3.5.6. *Für $d \geq 2$ gilt*

$$\boxed{(\mathbb{Z}/2^d)^* \simeq C_{2^{d-2}} \times C_2}$$

Man erhält einen Isomorphismus $\eta\colon C_{2^{d-2}} \times C_2 \longrightarrow (\mathbb{Z}/2^d)^*$ folgendermaßen:

$$\eta(n,m) = 5^n(-1)^m.$$

Dies ist natürlich ein Gruppen-Homomorphismus. Zu zeigen ist, dass η injektiv ist. Ist $\eta(n,m) = \overline{1}$, so ist $5^n(-1)^m \equiv 1 \mod 2^d$, also $5^n \equiv (-1)^{-m} \mod 2^d$. Mit Hilfe von 3.5.5 sieht man, dass dies nur für $n \equiv 0 \mod 2^{d-2}$ und $m \equiv 0 \mod 2$ möglich ist. Da also η injektiv ist, ist η sogar bijektiv (denn beide Gruppen $C_{2^{d-2}} \times C_2$ und $(\mathbb{Z}/2^d)^*$ haben die Ordnung 2^{d-1}).

3.6. Die Gruppe $(\mathbb{Z}/p^d)^*$ mit p ungerade.

3.6.1. Satz. *Sei $p > 2$ und $d \geq 1$. Dann hat $1 + 2p$ die Ordnung p^{d-1} in $(\mathbb{Z}/p^d)^*$.* (Ganz allgemein gilt: Jedes Element $1 + ap$ mit $(a,p) = 1$ hat die Ordnung p^{d-1} in $(\mathbb{Z}/p^d)^*$).

Beweis: Wir beginnen mit folgendem Lemma:

Lemma. *Gilt $a \equiv b \mod p^e$ für ein $e \geq 1$, so gilt $a^p \equiv b^p \mod p^{e+1}$.*

Beweis: Sei $a = b + cp^e$. Also ist

$$a^p = (b + cp^e)^p = b^p + \tbinom{p}{1} b^{p-1} cp^e + x,$$

dabei ist x eine Summe von Zahlen mit Faktoren $(cp^e)^i = c^i p^{ie}$ mit $i \geq 2$, diese Zahlen sind also alle durch p^{ie} teilbar und damit durch p^{e+1} (denn $i \geq 2, e \geq 1$). Wegen $\binom{p}{1} = p$ ist aber auch der mittlere Summand $\binom{p}{1} b^{p-1} cp^e$ durch p^{e+1} teilbar. Damit ist die Behauptung gezeigt.

Wir zeigen als erstes mit Induktion:

$$(1 + ap)^{p^e} \equiv 1 \mod p^{e+1} \qquad \text{für alle} \qquad e \geq 0.$$

Für $e = 0$ ist die Behauptung offensichtlich. Sei die Behauptung richtig für e, also $(1+ap)^{p^e} \equiv 1 \mod p^{e+1}$. Das Lemma liefert nun $(1+ap)^{p^{e+1}} \equiv 1 \mod p^{e+2}$.

Demnach sehen wir: Die Ordnung von $1+ap$ in $(\mathbb{Z}/p^{e+1})^*$ ist ein Teiler von p^e, für jedes a. Es reicht zu zeigen, dass die Ordnung von $(1+2p)$ in $(\mathbb{Z}/p^{e+1})^*$ kein Teiler von p^{e-1} ist.

Wieder mit Induktion zeigen wir:

$$(1+ap)^{p^{e-1}} \equiv 1 + ap^e \mod p^{e+1}.$$

Die Behauptung ist richtig für $e = 1$. Setzen wir voraus, dass sie für ein e richtig ist, und wenden wir das Lemma an, so erhalten wir

$$(1+ap)^{p^e} \equiv (1+ap^e)^p \mod p^{e+2}.$$

Wieder schreiben wir

$$(1+ap^e)^p = 1 + \tbinom{p}{1} ap^e + y$$

dabei ist y eine Summe von Zahlen, die jeweils einen Faktor $\binom{p}{i}(ap)^{ei}$ mit $i \geq 2$ haben. Ist $2 \leq i < p$, so ist p ein Teiler des Binomialkoeffizienten, und zusätzlich hat man einen Faktor p^{2e}. Wegen $e \geq 1$ ist $2e \geq e+1$, insgesamt hat man also mindestens einen Faktor p^{e+2}. Für $i = p$ lautet der letzte Summand $(ap^e)^p = a^p p^{ep}$ und wegen $p \geq 3$ ist $ep \geq e+2$. Damit ist der Induktionsschritt abgeschlossen.

Für $a = 2$ ist $1 + ap^e$ modulo p^{e+1} nicht zu 1 äquivalent. Daher sehen wir, dass die Ordnung von $1 + 2p$ modulo p^{e-1} kein Teiler von p^{e-1} sein kann.

3.6.2. Satz. *Ist p eine ungerade Primzahl und $e \in \mathbb{N}$, so ist $(\mathbb{Z}/p^e)^*$ zyklisch.*

Beweis: Wir kennen ein Element h der Ordnung p^{e-1}. Es gibt auch ein Element der Ordnung $p-1$: Denn ist g eine Primitivwurzel modulo p, ist also die Ordnung von g modulo p gleich $p-1$, so ist die Ordnung von g modulo p^e ein Vielfaches von $p-1$, etwa $a(p-1)$. Dann ist die Ordnung von g^a modulo p^e gerade $p-1$. Das Produkt von g^a und h hat die gesuchte Ordnung $(p-1)p^{e-1}$.

3.7. Die Gruppe $(\mathbb{Z}/n)^*$.

3.7.1. Satz (Gauß). *Die Gruppe $(\mathbb{Z}/n)^*$ ist genau dann zyklisch, wenn einer der folgenden Fälle vorliegt:*

- $n = 1, 2, 4$
- $n = p^e$ *für eine ungerade Primzahl p und $e \geq 1$.*
- $n = 2p^e$ *für eine ungerade Primzahl p und $e \geq 1$.*

Beweis: Sei $n = p_1^{e_1} \cdots p_t^{e_t}$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_t$. Der chinesische Restsatz besagt:

$$(\mathbb{Z}/n)^* \qquad \text{ist isomorph zu} \qquad (\mathbb{Z}/p_1^{e_1})^* \times \cdots \times (\mathbb{Z}/p_1^{e_1})^*.$$

Ist $n = 1, 2, 4$ so ist $\phi(n) = 1, 1, 2$ und jede Gruppe der Ordnung höchstens 2 ist zyklisch. In 3.6.2 haben wir gesehen, dass $(\mathbb{Z}/p^e)^*$ für jede ungerade Primzahl p zyklisch ist. Ist $n = 2p^e$, so ist $\mathbb{Z}/n$ zu $(\mathbb{Z}/2)^* \times (\mathbb{Z}/p^e)^*$ isomorph, also zu $(\mathbb{Z}/p^e)^*$, denn $(\mathbb{Z}/2)^* = \{1\}$.

Wir zeigen nun, dass nur in den genannten Fällen $(\mathbb{Z}/n)^*$ zyklisch sein kann. Dabei verwenden wir: *Ist $(\mathbb{Z}/n)^*$ zyklisch, so ist auch $(\mathbb{Z}/n')^*$ zyklisch für jeden Teiler n' von n.* Es ist also zu zeigen, dass die folgenden Gruppen nicht zyklisch sind:

$$(\mathbb{Z}/8)^*, \quad (\mathbb{Z}/4p)^*, \quad (\mathbb{Z}/pq)^*$$

dabei sind p, q verschiedene ungerade Primzahlen. Wir zeigen, dass es jeweils mindestens zwei Elemente der Ordnung 2 gibt (wir wissen: eine zyklische Gruppe enthält höchstens ein Element der Ordnung 2, siehe 3.3.4).

Für $n = 8$ liefern die Restklassen von 3 und 5 Elemente in $(\mathbb{Z}/8)^*$ der Ordnung 2 (denn $3^2 = 9 \equiv 1 \mod 8$, und $5^2 = 25 \equiv 1 \mod 8$, und natürlich sind die Elemente $\overline{1}$, $\overline{3}$, $\overline{5}$ in $(\mathbb{Z}/8)^*$ paarweise verschieden.

In den beiden anderen Fällen $n = 4p$ und $n = pq$ verwenden wir den chinesischen Restsatz und die Tatsache, dass ein Produkt $G \times H$ zweier Gruppen, die jeweils ein Element der Ordnung 2 besitzen, nicht zyklisch sein kann (da das Produkt mindestens zwei Elemente der Ordnung besitzt: haben $g \in G$ und $h \in H$ die Ordnung 2, so haben die Elemente $(g, 1), (1, h)$ (und auch (g, h)) in $G \times H$ die Ordnung 2).

Sei nun $n = 4p$ mit p eine ungerade Primzahl. Der chinesische Restsatz besagt: $(\mathbb{Z}/4p)^* \simeq (\mathbb{Z}/4)^* \times (\mathbb{Z}/p)^*$. Entsprechend liefert der chinesische Restsatz für verschiedene Primzahlen p, q, dass gilt: $(\mathbb{Z}/pq)^* \simeq (\mathbb{Z}/p)^* \times (\mathbb{Z}/q)^*$. Es bleibt also zu zeigen: Die Gruppen $(\mathbb{Z}/4)^*$ und $(\mathbb{Z}/p)^*$ (wobei p eine ungerade Primzahl ist) besitzen ein Element g der Ordnung 2: Nimm $g = \overline{-1}$. Hier verwenden wir die offensichtliche Aussage: *Die Restklasse von -1 gehört immer zu $(\mathbb{Z}/n)^*$, sie hat für $n \geq 3$ die Ordnung 2.*

3.8. Zusammenfassung.

Der Chinesische Restsatz besagt, dass für jede natürliche Zahl n mit Primfaktorzerlegung $n = p_1^{e_1} \cdots p_t^{e_t}$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_t$ die kanonische Abbildung $\eta(\overline{a}) = (\overline{a}, \ldots, \overline{a})$ ein Ring-Isomorphismus ist:

$$\eta\colon \mathbb{Z}/n \longrightarrow (\mathbb{Z}/p_1^{e_1}) \times \cdots \times (\mathbb{Z}/p_t^{e_t}).$$

Dies besagt, dass man sich beim Rechnen mit Kongruenzen modulo n immer auf den Fall zurückziehen kann, wo n eine Primzahlpotenz ist.

Insbesondere liefert η einen Isomorphismus der Einheitengruppen:

$$(\mathbb{Z}/n)^* \longrightarrow (\mathbb{Z}/p_1^{e_1})^* \times \cdots \times (\mathbb{Z}/p_t^{e_t})^*.$$

Der Satz von Gauß beschreibt alle natürlichen Zahlen n, für die die multiplikative Gruppe $(\mathbb{Z}/n)^*$ zyklisch ist, es also eine Primitivwurzel g modulo n gibt. In diesem Fall ist die Abbildung

$$\psi\colon C_{\phi(n)} = (\mathbb{Z}/\phi(n), +) \longrightarrow (\mathbb{Z}/n)^* \qquad \text{mit} \qquad \psi(x) = g^x$$

ein Isomorphismus. Dies bedeutet, dass man die Elemente von $(\mathbb{Z}/n)^*$ als Potenzen *eines* Elements g schreibt. Die Umkehrabbildung zu ψ wird mit ind_g bezeichnet, man nennt $\mathrm{ind}_g(y)$ den *Index* von y zur Basis g. Es gelten die folgenden Rechenregeln:

$$\begin{aligned}\mathrm{ind}_g(y_1y_2) &= \mathrm{ind}_g(y_1) + \mathrm{ind}_g(y_2)\\ \mathrm{ind}_g(y^{-1}) &= -\mathrm{ind}_g(y)\\ \mathrm{ind}_g(y^e) &= e\cdot \mathrm{ind}_g(y).\end{aligned}$$

Ist g' ebenfalls eine Primitivwurzel modulo n, so sind die beiden Funktionen ind_g und $\mathrm{ind}_{g'}$ zueinander proportial, es gilt:

$$\mathrm{ind}_g(y) = \mathrm{ind}_g(g')\cdot \mathrm{ind}_{g'}(y).$$

Bemerkung. Diese Regeln entsprechen den Regeln für das Rechnen mit Logarithmen - wir sind hier in einer ganz ähnlichen Situation. Sei $a \in \mathbb{R}_{>0} = \{r \in \mathbb{R} \mid r > 0\}$ Die Exponentialabbildungen

$$\exp_a : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_{>0}, \cdot)$$

ist ein Gruppen-Isomorphismus, die Umkehrabbildung wird mit $\log_a$ bezeichnet (also $\log_a(y)$ ist der Logarithmus von y zur Basis a, dies ist definiert für $y \in \mathbb{R}_{>0}$, es ist $\log_a(y)$ die eindeutig bestimmte reelle Zahl mit $a^{\log_a(y)} = y$.)

$$\begin{aligned}\log_a(y_1y_2) &= \log_a(y_1) + \log_a(y_2)\\ \log_a(y^{-1}) &= -\log_a(y)\\ \log_a(y^e) &= e\cdot \log_a(y).\\ \log_a(y) &= \log_a(a')\cdot \log_{a'}(y).\end{aligned}$$

3.9. Ganz wichtige (teilweise aber ganz elementare) Aussagen.

Sie gehören eigentlich ganz an den Anfang von Kapitel 3, wurden aber zurückgehalten, um sie hier gebündelt zu präsentieren.

3.9.1. Satz von Euler. *Sei* $(a, n) = 1$. *Es ist* $a^{\phi(n)} \equiv 1 \mod n$.

Dies ist eine direkte Folge des Satzes von Lagrange: $\overline{a}$ ist ein Element der Gruppe $(\mathbb{Z}/n)^*$. Natürlich ist $|(\mathbb{Z}/n)^*| = \phi(n)$. Die Ordnung eines Elements ist **immer** ein Teiler der Gruppenordnung. Das wars.

3.9.2. Spezialfall: der kleine Fermat. *Sei* p *eine Primzahl. Für* $1 \le a \le p-1$ *gilt* $a^{p-1} \equiv 1 \mod p$.

Natürlich: $\phi(p) = p - 1$.

3.9.3. Folgerung. *Sei p eine Primzahl. Für alle a gilt $a^p \equiv a \mod p$.*

Beweis: Ist a nicht durch p teilbar, so ist dies der "kleine Fermat". Ist a durch p teilbar, so ist auch a^p durch p teilbar, also $a^p \equiv 0 \equiv p \mod p$.

3.9.4. Satz von Wilson. *Ist p eine Primzahl, so ist $(p-1)! \equiv -1 \mod p$.*

Übungsaufgabe 8.1.

3.8.5. Quadrate in $(\mathbb{Z}/p)^*$. *Sei p ungerade Primzahl und $1 \leq a < p$. Genau dann ist a ein Quadrat in $(\mathbb{Z}/p)^*$, wenn $a^{(p-1)/2} \equiv 1 \mod p$ gilt.*

Beweis: Ist $a \equiv b^2 \mod p$, so ist $a^{(p-1)/2} \equiv (b^2)^{(p-1)/2} = b^{p-1} \equiv 1 \mod p$ (kleiner Fermat).

Umgekehrt setzen wir nun voraus: $a^{(p-1)/2} \equiv 1 \mod p$. Wir brauchen die Existenz einer Primitivwurzel g modulo p. Da g Primitivwurzel modulo p ist und p kein Teiler von a ist, gibt es ein $j \in \mathbb{N}$ mit $g^j \equiv a \mod p$. Es ist $(g^j)^{(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \mod p$, also ist $p-1$ ein Teiler von $j \cdot \frac{p-1}{2}$. Dies besagt aber, dass $\frac{j}{2}$ ganzzahlig ist. Setzen wir $b = g^{j/2}$, so sehen wir: $b^2 = (g^{j/2})^2 = g^j \equiv a \mod p$, also ist a ein Quadrat modulo p.

3.9.6. Primzahl-Tests. Wir haben gesehen: Ist p eine Primzahl, so gilt

- $(p-1)! \equiv -1 \mod p$. (Satz von Wilson)
- $a^p \equiv a \mod p$ für jedes a. (Kleiner Fermat)
- $2^p \equiv 2 \mod p$ (Spezialfall des kleinen Fermat)
- $a^p \equiv a \mod p$ für jedes a mit $(a, n) = 1$. (Euler)

Es gilt die Umkehrung für den Satz von Wilson: *Ist $n > 1$ und $(n-1)! \equiv -1 \mod n$, so ist n eine Primzahl.*

Beweis: Sei also $n > 1$ und $(n-1)! \equiv -1 \mod n$, also n ein Teiler von $(n-1)!+1$. Ist $1 \leq d < n$, so ist d Teiler von $(n-1)!$. Ist d auch ein Teiler von n, so auch von $(n-1)!+1$, also von 1, und demnach $d = 1$.

Man nennt eine Zahl n eine *Pseudo-Primzahl* zur Basis a, falls die folgenden Bedingungen erfüllt sind: Es ist $n > 1$, zweitens $(a, n) = 1$, und drittens $a^n \equiv a \mod n$, aber n ist keine Primzahl.

Beispiel: $n = 341 = 11 \cdot 31$ ist eine Pseudo-Primzahl zur Basis 2 (und zwar die kleinste). Beweis: Es ist

$$2^{10} = 1024 = 3 \cdot 11 \cdot 31 + 1, \qquad \text{also} \qquad 2^{10} \equiv 1 \mod 11, \quad 2^{10} \equiv 1 \mod 31,$$

und daher

$$2^{341} = 2 \cdot 2^{340} \equiv 2 \mod 11, \qquad \text{und} \qquad 2^{341} = 2 \cdot 2^{340} \equiv 2 \mod 31.$$

Lemma. *Ist n eine Pseudo-Prinzahl zur Basis 2, so ist auch $2^n - 1$ eine Pseudo-Primzahl zu dieser Basis.*

(Da wir mindestens eine Pseudo-Primzahl zur Basis 2 kennen, nämlich 341, gibt es also unendlich viele Pseudo-Primzahlen.)

Beweis. Sei n Pseudo-Primzahl zur Basis 2, also ist $2^n \equiv 2 \mod n$. Demnach gibt es t mit $tn = 2^n - 2$. Also $2^{tn} = 2^{2^n-2}$, und daher

$$(2^n)^t - 1 = 2^{tn} - 1 = 2^{2^n-2} - 1$$

Die linke Seite wird von $2^n - 1$ geteilt (im Polynomring $\mathbb{Z}[X]$ gilt: $X - 1$ teilt $X^t - 1$, hier setzen wir 2^n für X ein), also ist

$$(2^n - 1) \mid (2^{2^n-2} - 1) \mid 2^{2^n-1} - 2.$$

Natürlich ist $(2, 2^n - 1) = 1$. Es bleibt noch zu zeigen, dass $2^n - 1$ keine Primzahl ist: Ist $d|n$ mit $1 < d < n$, so ist $2^d - 1$ ein Teiler von $2^n - 1$ (wieder verwenden wir, dass $X - 1$ ein Teiler von $X^m - 1$ ist, für jedes $m \in \mathbb{N}$).

Ist n eine Pseudo-Primzahl für alle Basen a mit $(a, n) = 1$, so nennt man n eine *Carmichael-Zahl*. Die kleinste Carmichael-Zahl ist $561 = 3 \cdot 11 \cdot 17$. Es gilt (ohne Beweis): Eine Carmichael-Zahl n ist ungerade, quadratfrei und hat mindestens drei Primfaktoren. Es gibt unendlich viele Carmichael-Zahlen.

Bemerkung. Wenn man wissen möchte, ob eine Zahl eine Primzahl ist, verwendet man einen Primzahltest. Das bekannteste und älteste Verfahren ist das Sieb des Eratosthenes. In der Praxis wird am häufigsten der **Miller-Rabin-Test** verwendet, der eine extrem schnelle Laufzeit hat, allerdings mit kleiner Wahrscheinlichkeit daneben liegen kann. Für Aufsehen hat in den letzten Jahren der **AKS-Primzahltest** (Agrawal-Kayal-Saxena, 2002) gesorgt: er erlaubt es, Zahlen in polynomialer Laufzeit zu testen *(Primes is in P)*, allerdings ist dieses Verfahren in der Praxis deutlich langsamer als der Miller-Rabin-Test ("polynomiale Laufzeit" bedeutet, dass es ein Polynom gibt $f(n)$ gibt, sodass die Anzahl der Rechenoperationen, die zum Test einer n-stelligen Zahl durchzuführen sind, durch $f(n)$ nach oben beschränkt ist).

3.9.7. Mersenne'sche und Fermat'sche Primzahlen.

Lemma. *Ist $2^t - 1$ eine Primzahl, so ist t eine Primzahl. Ist $2^t + 1$ eine Primzahl, so ist t eine Zweierpotenz.*

Beweis: Ist $1 < d < t$ ein Teiler von t, so ist $2^d - 1$ ein Teiler von $2^t - 1$ (wieder verwendet man, dass $X - 1$ ein Teiler von $X^m - 1$ ist). Ist $1 < d < t$ ein ungerader Teiler von t, etwa $de = t$, so ist $2^e + 1$ ein Teiler von $2^t + 1$ (denn $X + 1$ ist ein Teiler von $X^d + 1$, wegen $(X + 1)(X^{d-1} - X^{d-2} + - \cdots - X + 1) = X^d + 1$; setze hier für X die Zahl 2^e ein).

Primzahlen der Form $2^t - 1$ heißen *Mersenne'sche Primzahlen*; solche der Form $2^t + 1$ heißen *Fermat'sche Primzahlen.* Es wird vermutet, dass es unendlich viele Mersenne'sche Primzahlen gibt, und man kennt sehr viele (aber nicht für jede Primzahl p ist $2^p - 1$ wieder eine Primzahl — Beispiel: $2^{11} - 1 = 2047 = 23 \cdot 89$.) Man kennt nur 5 Fermat'sche Primzahlen, nämlich $F_n = 2^{2^n} + 1$ mit $n = 0, 1, 2, 3, 4$, also

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65\,537,$$

und man vermutet, dass dies die einzigen sind.

3.10. RSA

Hier ist nun auf eine Anwendung hinzuweisen, die im täglichen Leben heute eine wichtige Rolle spielt: Das RSA-Verfahren zur Verschlüsselung von Nachrichten. Dabei sei an den Zahlentheoretiker Hardy erinnert, der noch 1941 formulierte, dass die Ergebnisse der Zahlentheorie zwar ihren ästhetischen Reiz haben, aber kein derartiges Ergebnis *has made, or is likely to make, for good or ill, the least difference to the amenity of the world* (amenity = Annehmlichkeit).

Es handelt sich dabei darum, eine Nachricht von A (Alice) nach B (Bob) zu schicken, sie wird von A verschlüsselt, von B entschlüsselt, die verschlüsselte Nachricht kann von allen eingesehen werden, nur Bob ist allerdings in der Lage, die Nachricht zu entschlüsseln. Auch der Schlüssel zum Verschlüsseln ist öffentlich zugänglich (*public key*), der Schlüssel zum Entschlüsseln (*private key*) natürlich nicht - ihn kennt nur Bob. Das RSA-Verfahren wurde von Rivest, Shamir und Adleman 1978 vorgestellt und wird gegenwärtig in vielen Situationen eingesetzt. Der mathematische Kern ist folgende Variante des Satzes von Euler-Fermat:

Satz. *Sei m eine quadratfreie natürliche Zahl. Sei f eine natürliche Zahl mit $f \equiv 1 \mod \phi(m)$. Dann ist $a^f \equiv a \mod m$ für alle ganzen Zahlen a.*

Beweis: Sei also $f = 1 + t\phi(m)$. Wir behaupten, dass gilt: $a^f \equiv a \mod p$ für jeden Primteiler p von m. Da m das Produkt seiner Primteiler ist, folgt dann die Behauptung aus dem chinesischen Restsatz (oder einfacher: Ist $m = p_1 \cdots p_t$ mit paarweise verschiedenen Primzahlen p_i, und ist jedes p_i ein Teiler von $a^f - a$, so ist m ein Teiler von $a^f - a$.)

Sei also p ein Primteiler von m. Wenn p ein Teiler von a ist, so ist p auch ein Teiler von a^f, also $a^f \equiv 0 \equiv a \mod p$. Ist p kein Teiler von f, so ist $p - 1$ ein Teiler von $\phi(m)$, also auch von $t\phi(m)$, etwa $t\phi(m) = (p-1)x$, also $a^{t\phi(m)} = a^{(p-1)x} \equiv 1^x = 1 \mod p$, nach dem kleinen Fermat. Daher gilt $a^f = a^{1+t\phi(m)} = a \cdot a^{t\phi(m)} \equiv a \cdot 1 = a \mod m$.

Folgerung. *Sei m eine quadratfreie natürliche Zahl. Seien e, d natürliche Zahlen mit $de \equiv 1 \mod \phi(m)$, so liefert die Zuordnung $a \mapsto a^e$ eine bijektive Abbildung $\mathbb{Z}/m \longrightarrow \mathbb{Z}/m$, mit inverser Zuordnung $a \mapsto a^d$.*

Beweis: Wegen $(\overline{a}^e)^d = \overline{a}$ sehen wir, dass die Zuordnung $a \mapsto a^e$ injektiv ist. Als injektive Abbildung einer m-elementigen Menge in sich ist diese Zuordnung bijektiv. Und natürlich folgt aus $(\overline{a}^e)^d = \overline{a}$, dass $a \mapsto a^d$ die inverse Zuordnung ist.

Beachte: Der Satz ist im Fall dass $m = p$ eine Primzahl ist, gerade die übliche zweite Formulierung des kleinen Fermat: $a^p \equiv a \mod p$ für alle ganzen Zahlen a, denn $phi(p) = p - 1$, also ist $p = 1 + (p-1) \equiv 1 \mod \phi(p)$.

Hier die Beschreibung des RSA-Verfahrens. Bob wählt paarweise verschiedene Primzahlen $p_1, \ldots, p_t$ (üblicherweise große Primzahlen, und $t = 2$) und setzt $m = p_1 \cdots p_t$. Dann ist $\phi(m) = (p_1 - 1) \cdots (p_t - 1)$. Weiter wählt er eine zu $\phi(m)$ teilerfremde Zahl e (meist eine Zahl der Form $2^r + 1$, damit das e-fache Potenzieren so einfach wie möglich ist) und berechnet eine Bézout-Gleichung $de + t\phi(m) = 1$ mit $d \in \mathbb{N}$. Der öffentliche Schlüssel ist das Zahlenpaar $[m, e]$, sei privater Schlüssel ist das Zahlenpaar $[m, d]$. Verschlüsselt wird so: man ersetzt $0 \leq a < m$ durch $0 \leq b < m$ mit $b \equiv a^e \mod m$, entschlußselt wird entsprechend durch d-faches Potenzieren.

Beispiel (wegen der kleinen Zahlen natürlich unrealististisch): Wir nehmen die Primzahlen $p = 11, q = 13$, also $m = 143$ und $\phi(m) = (p-1)(q-1) = 120$. Sei $e = 2^4 + 1 = 17$. Eine Bézout'sche Gleichung lautet $1 = 1 \cdot 120 - 7 \cdot 17$, wir wollen aber $d > 0$, also

$$1 = (1 - 17) \cdot 120 + (-7 + 120) \cdot 17 = -16 \cdot 120 + 113 \cdot 17 (= -1920 + 1921).$$

der öffentliche Schlüssel ist also das Paar $[143, 17]$, Bob's privater Schlüssel ist $[143, 113]$. Will Alice die Nachricht $a = 7$ übermitteln, so verschlüsselt sie sie: sie bildet $a^{17} \equiv 50 \mod 143$, also sendet sie $b = 50$. Bob entschlüsselt die Nachricht: $b^{113} \equiv 7 \mod 143$.

Statt $e = 17$ hätte man bei Vorgabe von $m = 143$ jede Zahl $1 \leq e \leq 120$ nehmen können, die nicht durch 2, 3 oder 5 teilbar ist, also $e = 7, 11, 13, 17, 19, \ldots$. Es ist also $[143, 11]$ ein möglicher öffentlicher Schlüssel; wegen $11 \cdot 11 = 121 = 1 + 120$ ist der zugehörige private Schlüssel ebenfalls $[143, 11]$.

Anhang: Der Struktursatz für endlich erzeugte abelsche Gruppen.

Eine abelsche Gruppe, die isomorph zur Gruppe $\mathbb{Z}^n = \mathbb{Z} \times \cdots \times \mathbb{Z}$ mit n Faktoren $\mathbb{Z} = (\mathbb{Z}, +)$ ist, heißt *freie abelsche Gruppe vom Rang n.*

Das Arbeiten mit Produkten zyklischer Gruppen braucht etwas Übung, ist aber dann ganz einfach. Arbeitet man mit additiv geschriebenen Gruppen so spricht man von *direkten Summen* (statt von Produkten), und verwendte statt der Symbole $\times$ und $\prod$ die Symbole $\oplus$ und $\bigoplus$. Statt $\mathbb{Z} \times \mathbb{Z}$ schreibt man also auch $\mathbb{Z} \oplus \mathbb{Z}$, statt $\prod_{i=1}^t \mathbb{Z}$ schreibt man entspechend $\bigoplus_{i=1}^t \mathbb{Z}$.

Die hier im Anhang betrachteten abelschen Gruppen G seien alle additiv geschrieben. Sei also G eine abelsche Gruppe. Sind $g_1, \ldots, g_t$ Elemente in G, so erhält man durch

$$(*) \qquad \eta \colon \mathbb{Z}^t \longrightarrow G, \qquad \text{mit} \qquad \eta(z_1, \ldots, z_t) = \sum_i z_i g_i$$

einen Gruppen-Homomorphismus (es ist zu verifizieren, dass dies wirklich ein Gruppen-Homomorphismus ist, dies ist aber einfach!).

Man nennt $g_1, \ldots, g_t$ ein *Erzeugenden-System* von G, falls sich jedes Element $g \in G$ in der Form $g = \sum_i z_i g_i$ mit $z_i \in \mathbb{Z}$ schreiben lässt, falls also der Gruppen-Homomorphismus η in $(*)$ surjektiv ist. Besitzt die Gruppe G ein Erzeugendensystem $g_1, \ldots, g_t$, so sagt man, die Gruppe sei *endlich erzeugt.* Jede endliche Gruppe ist trivialerweise endlich erzeugt. Die Gruppe $(\mathbb{Q}, +)$ dagegen ist **nicht** endlich-erzeugt.

Lemma 1. *Jede Untergruppe einer freien abelschen Gruppe vom Rang n ist eine freie abelsche Gruppe vom Rang m mit $m \leq n$.*

Beweis mit Induktion nach n. Für $n = 0$ ist nichts zu zeigen (und auch für $n = 1$ ist die Aussage wohlbekannt). Sei also $n \geq 1$. Sei also U eine Untergruppe von $\mathbb{Z}^n$. Haben alle Elemente von U die Form $(x_1, x_2, \ldots, x_{n-1}, 0)$ mit $x_i \in \mathbb{Z}$ für $2 \leq i \leq n$, so ist U offensichtliche eine Untergruppe von $\mathbb{Z}^{n-1}$ und nach Induktion gilt die Behauptung. Wir können also annehmen, dass es ein Element der Form $x = (x_1, \ldots, x_n)$ in U gibt mit $x_n \neq 0$. Mit x ist auch $-x$ in U, also gibt es ein derartiges Element mit $x_n > 0$. Wir wählen ein derartiges Element mit x_n minimal. Sei $U' = U \cap \mathbb{Z}^{n-1} \times \{0\}$. Dies ist eine Untergruppe von $\mathbb{Z}^{n-1} \times \{0\} = \mathbb{Z}^{n-1}$, und offensichtlich ist $U' \cap \mathbb{Z}x = \{0\}$. Wir zeigen nun

$$U' + \mathbb{Z}x = U.$$

Sei $u = (u_1, \ldots, u_n) \in U$. Wir behaupten, dass u_n ein Vielfaches von x_n ist. Um dies zu zeigen, bilden wir den größten gemeinsamen Teiler d von u_n und x_n und wählen eine Bézout-Gleichung $d = au_n + bx_n$. Das Element $au + bx$ gehört zu U, seine n-Komponente ist $d \geq 1$. Wegen der Minimalität von x_n gilt $x_n \leq d$. Da d Teiler von x_n ist, folgt $d = x_n$. Dies zeigt, dass u_n ein Vielfaches von x_n ist, etwa $u_n = cx_n$. Sei $u' = u - cx$. Dies ist ein Element von U, dessen n-te Komponente gleich 0 ist, also gehört u' zu $U \cap \mathbb{Z}^{n-1} \times \{0\} = U'$. Wegen $u = u' + cx$ liegt u in $U' + \mathbb{Z}$.

Wegen $U' \cap \mathbb{Z}x = \{0\}$ und $U' + \mathbb{Z}x = U$ Da U' eine Untergruppe von $\mathbb{Z}^{n-1} \times \{0\} = \mathbb{Z}^{n-1}$ ist, ist U' nach Induktion eine freie abelsche Gruppe vom Rang m' mit $m' \leq n-1$, also isomorph zu $\mathbb{Z}^{m'}$. Sei etwa $\eta' \colon \mathbb{Z}^{m'} \to U$ ein Isomorphismus. Dann können wir durch

$$\eta \colon \mathbb{Z}^{m'+1} \longrightarrow U \qquad \text{mit} \qquad \eta(z_1, \ldots, z_{m'+1}) = \eta(z_1, \ldots, z_{m'}) + z_{m'+1}x$$

einen Isomorphismus definieren. Damit ist die Behauptung bewiesen.

Nun betrachten wir Matrizen mit Koeffizienten in $\mathbb{Z}$. Die Menge aller $(m \times n)$-Matrizen mit Koeffizienten in $\mathbb{Z}$ werde mit $M(m \times n, \mathbb{Z})$ bezeichnet. Beachte: eine $(n \times n)$-Matrix P mit Koeffizienten in $\mathbb{Z}$ ist genau dann *über $\mathbb{Z}$ invertierbar* (das heißt: es gibt eine $(n \times n)$-Matrix P' mit Koeffizienten in $\mathbb{Z}$, sodass $PP' = I$ gilt, I die Einheitsmatrix), wenn für die Determinante $\det P$ gilt: $\det P \in \{1, -1\}$. Wir bezeichnen mit $\mathrm{GL}(n, \mathbb{Z})$ die Menge der Matrizen $P \in M(m \times m, \mathbb{Z})$, die über $\mathbb{Z}$ invertierbar sind.

Lemma 2. *Zu jede Matrix $A \in M(m \times n, \mathbb{Z}$ gibt es Matrizen $P \in \mathrm{GL}(m, \mathbb{Z})$ und $Q \in \mathrm{GL}(n, \mathbb{Z})$, sodass PAQ die folgende Form hat:*

$$\left[\begin{array}{ccc:c} d_1 & & 0 & \\ & d_2 & & 0 \\ & & \ddots & \\ 0 & & & d_r \\ \hdashline & 0 & & 0 \end{array}\right]$$

mit natürlichen Zahlen $d_1, \ldots, d_r$ (und $r \geq 0$).