Algebra und Zahlentheorie
Zusammenfassung

Michael Jaeger

22. Januar 2001

1 Teilbarkeit

1.1 $\mathbb{N}$ und $\mathbb{Z}$

- **Peanoaxiome:** „Natürliche Zahlen" sind eine Menge $\mathbb{N}$ mit

  1. $\mathbb{N} \ni$ Zahl namens 1 ($\Rightarrow \mathbb{N} \neq \emptyset$)
  2. Jede Zahl in $\mathbb{N}$ hat einen „Nachfolger" $N(n)$ (später „$n+1$")
  3. Es gibt kein $n \in \mathbb{N}$ mit $1 = N(n)$
  4. N ist injektiv, d.h. $N(n) = N(m) \Rightarrow n = m$
  5. Prinzip der „vollständigen Induktion": Jede Menge von natürlichen Zahlen, welche 1 enthält und mit n auch $N(n)$ enthält, enthält bereits alle nat. Zahlen. (Dieses Axiom lässt sich für „induktive" oder „rekursive" Definitionen verwenden.)

  Beispiel: Fibonacci-Folge: $a_1 = a_2 = 1 \qquad a_{n+1} = a_n + a_{n-1} \quad \forall n > 1$

- **Addition, Multiplikation, Ordnung:** $n + 1 := N(n)$. Angenommen, $n + n$ sei bereits definiert, dann sei $n + N(n) = N(n + m)$.

- **Teiler:** $n \in \mathbb{Z}$ „teilt" $m \in \mathbb{Z}$ („Teiler von"), geschrieben $n|m :\Leftrightarrow \exists x \in \mathbb{Z}$ mit $m = n \cdot x$.
  Für alle $a, b, c, d, x, y \in \mathbb{Z}$ gilt:

  1. $d|a \Rightarrow d|ab$
  2. $d|c$ und $c|a \Rightarrow d|a$ ($c = kd, a = mc = (mk)d$)
  3. $d|a$ und $d|b \Rightarrow d|(xa + yb)$ (bleibt auch richtig für Lin.komb. von mehr als zwei Zahlen)
  4. $d|c \Rightarrow c = 0$ oder $|d| \leq |c|$
  5. $d|c$ und $c|d \Leftrightarrow c = \pm d$

- **Division mit Rest:** Sei $a, b \in \mathbb{Z}, b \neq 0$. Dann $\exists q \in \mathbb{Z}$ und ein Rest $r \in \{0, 1, \ldots, |b|\}$ mit $a = bq + r$.

1.2 ggT und euklidischer Algorithmus

- **ggt und kgV:** $\forall a, b \in \mathbb{Z}$, nicht beide $= 0$, sei $d =: (a, b)$ der „größte gemeinsame Teiler" (≥ 0) (existiert immer!). Konvention: $(0, 0) := 0$ und $(0, b) := |b|$
  Je zwei $a, b \in \mathbb{Z}$ besitzen ein „kleinstes gemeinsames Vielfaches" $\in \mathbb{N} \cup \{0\}$ (weil $|a| \cdot |b|$ gem. Vielfaches ist).

- **Teilerfremd:** Seien $a, b \in \mathbb{Z}$, nicht beide $= 0$, mit $d := (a, b)$. Dann ist $\{xa + yb | x, y \in \mathbb{Z}\} = d\mathbb{Z} = \{m \cdot d | m \in \mathbb{Z}\}$ und d ist die kleinste nat. Zahl, die sich als ganzzahlige Linearkomb. von a und b schreiben lässt.
  a und b heissen „teilerfremd" $:\Leftrightarrow d = (a, b) = 1$. In diesem Fall (und nur dann!) ist die „**lineare diophantische Gleichung**" $xa + yb = 1$ durch $a, y \in \mathbb{Z}$ lösbar. (Wenn $a = b = 0$, dann $L = \{x0 + y0 | x, y \in \mathbb{Z}\} = \{0\} = 0 \cdot \mathbb{Z}$.)
  Die Teilbarkeit liefert eine „**Teilordnung**" auf $\mathbb{N}$ bzw. $\mathbb{Z}$. Auch bezüglich dieser Teilordnung haben ggT und kgV Optimalitäts- bzw. Minimalitätseigenschaft.

- **Eigenschaften von ggT und kgV:** Seien $a, b \in \mathbb{Z}$, nicht beide $= 0$, ferner $c, t \in \mathbb{N}$, t gemeinsamer Teiler von a, b. Dann gilt:

  - $(ca, cb) = c \cdot (a, b)$
  - $(\frac{a}{t}, \frac{b}{t}) = \frac{(a,b)}{t}$
  - Für kgV $(a, b) := [a, b]$
    Für $a|v, b|v$ ist $[a, b]|v$, und $[a, b] \cdot (a, b) = |a \cdot b|$ und es gilt:

$$\mathbb{Z}[a, b] = \mathbb{Z}a \cdot \mathbb{Z}b = \mathbb{Z}a \cap \mathbb{Z}b \qquad \mathbb{Z}(a, b) = \mathbb{Z}a + \mathbb{Z}b$$

- **Euklidischer Algorithmus:** Seien $a, b \in \mathbb{Z}$, beide $\neq 0$. $b|a \Rightarrow d = (a, b) = |b|$. Andernfalls ergibt sich $d = (a, b)$ als letzter nicht-verschwindender Rest von r_n des folgenden Schemas von Div. mit Rest:

  - $a = q_1 b + r_1 \qquad (r_1 \neq 0 \Rightarrow r_1 \in \mathbb{N})$
  - $b = q_2 r_1 + r_2$
  - $r_1 = q_3 r_2 + r_3$
  - $\vdots$
  - $r_{n-2} = q_n r_{n-1} + r_n$
  - $r_{n-1} = q_{n+} r_n$

  Die r_k bilden eine absteigende Folge $\in \mathbb{N} \Rightarrow$ brechen ab. Letzte Zeile: $r_n | r_{n-1}$, n-te Zeile: $r_n | r_{n-2} \ \ldots \Rightarrow^{vollst.Ind.} r_n | a, b \Rightarrow r_n | d = (a, b)$. Ausserdem: r_n ist (ganzzahlige Linearkombination) von der Form $xa + yb \Rightarrow d | r_n \Rightarrow d = r_n$ und damit

$$\begin{aligned} r_n &= r_{n-2} - q_n r_{n-1} \\ &= r_{n-2} - q_n (r_{n-3} - q_{n-1} r_{n-2}) \\ &= (1 + q_n q_{n-1}) r_{n-2} - q_n r_{n-3} \\ &\vdots \\ &= xa + yb \end{aligned}$$

  Die Reste bilden eine umgekehrt durchlaufene Fibonacci-Folge ($a_1 = a_2 = 1, \quad a_{n+1} := a_n + a_{n-1}$). Damit ergibt sich für die **Laufzeit**, dass wenn $a, b \in \mathbb{Z} \setminus \{0\}$, der euklidische Algorithmus für die Berechnung des ggT von a und b weniger Schritte benötigt als

$$\frac{\log\left(\frac{1}{\sqrt{5}} + \min\{|a|, |b|\}\right) + \log\sqrt{5}}{\log\left(\frac{\sqrt{5}+1}{2}\right)}$$

1.3 Primfaktorzerlegung

- **Primzahl:** $p \in \mathbb{N}$ heißt „Primzahl", wenn $p > 1$ und p nur die trivialen Teiler $\pm 1, \pm p$ besitzt. Jedes $n \in \mathbb{N}$ ist ein Produkt von Primzahlen.

- **Irreduzible Elemente:** Elemente, die sich höchstens trivial in Produkte zerlegen lassen, die Primfaktorzerlegung aber nicht eindeutig ist. Z.B. $\underbrace{n + m\sqrt{-26}}_{d}$, die nur ± 1 und $\pm d$ als Teiler haben (z.B. 3).

- **Hilfssätze:** Seien $a, b, c \in \mathbb{Z}$ und $(a, b) = 1$ (teilerfremd), dann gilt: $a|bc \Rightarrow a|c$.
  Seien $b, c \in \mathbb{Z}$, p Primzahl mit $p|b \cdot c \Rightarrow p|b$ oder c

- **Satz der eindeutigen Primzahlzerlegung:** Jede nat. Zahl n$\in \mathbb{N}$ lässt sich als Produkt von Primzahlen schreiben. Diese Faktoren („Primfaktoren") sind bis auf Reihenfolge eindeutig.

- **p_j-Ordnung:** Jedes $a \in \mathbb{Z} \setminus \{0\}$ besitzt eine Darstellung als

$$a = \pm \Pi_{j=1}^{m} p_j^{\nu_{p_j}(a)}$$

  Dabei ist $\nu_{p_j}(a)$ die „p_j-Ordnung" von a und $\nu_{p_j}(a) = 0$, wenn $p_j \nmid a \Rightarrow a = \pm \Pi_{\text{alle Primzahlen}} p^{\nu_p(a)}$.
  Es gilt weiterhin:

  - $\nu_p(0) := \infty$
  - $a, b \in \mathbb{Z}, p \in \mathbb{P} \Rightarrow (a, b) = \Pi_{\mathbb{P}} p^{\min\{\nu_p(a), \nu_p(b)\}}$
  - $[a, b] = \Pi_{\mathbb{P}} p^{\max\{\nu_p(a), \nu_p(b)\}}$
  - $\mathbb{Q} := \{\frac{m}{n} | m \in \mathbb{Z}, n \in \mathbb{Z} \setminus \{0\}\}$ und $\nu_p\left(\frac{m}{n}\right) := \nu_p(m) - \nu_p(n)$ ($= \infty$ für $m = 0$ und $= \nu_p(m)$, wenn $n = 1$). $m = p^{\nu_p(m)} m'$ und $n = p^{\nu_p(n)} n'$ sind wohldefiniert und ändern sich nicht beim Erweitern oder Kürzen.
    $\alpha \in \mathbb{Q} \Rightarrow \nu_p(\alpha)$ definiert durch $\alpha = p^{\nu_p(\alpha)} \cdot \frac{m'}{n'}, \quad p \nmid m', n'$.

- **Satz:** $a, b \in \mathbb{Q}$, p Primzahl $\Rightarrow \nu_p(a + b) = \nu_p(a) + \nu_p(b)$ und $\nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b)$.
  $b \neq 0$: $\nu_p(a + b) \geq \min\{\nu_p(a), \nu_p(b)\}$.
  $\nu_p(r^2) = 2\nu_p(r) \Rightarrow \sqrt{2} \notin \mathbb{Q}$, andernfalls wäre $1 = \nu_2(2) = \nu_2(\sqrt{2}^2) = 2\nu_2(\sqrt{2})$ ↯
  $\forall d \in \mathbb{N}$, die nicht bereits in $\mathbb{N}$ Quadratwurzel sind gilt $\sqrt{d} \notin \mathbb{Q}$

1.4 Primzahlen

- **Existenz unendlich vieler Primzahlen:** Die Menge der Primzahlen $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ ist unendlich.

- **Primzahlsatz von Hadamar und Vallee-Poussin:**

$$\Pi(x) \backsim \frac{x}{\log x}, \text{ d.h. } \lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$

  Es gilt $\frac{x}{\log x} \backsim li(x)$, genauer: $li(x) = \frac{x}{\log x} + O(\frac{x}{\log^2 x})$ heißt $f(x) = g(x) + O(h(x))$ heißt: $|f(x) - g(x)| \leq ch(x)$ mit einem $c \in \mathbb{R}$ unabh. von x.
  $\pi(x) \backsim li(x) = \int_2^x \frac{dt}{\log t}$ hat folgende Interpretation: $\frac{1}{\log n}$ gibt die Wahrscheinlichkeit, dass eine zufällig gewählte grosse Zahl $n \in \mathbb{N}$ prim ist! Also $\pi(x) = li(x) + O(\sqrt{x} \log c)$ würde aus der **Riemannschen Vermutung** folgen: $\zeta(s) := \Sigma_{\mathbb{N}} \frac{1}{n^s}$ konvergiert für $s > 1$, $s \in \mathbb{R}$ und $\Pi_{\mathbb{P}} \frac{1}{1 - p^{-s}}$ konv. in Re$s > 1$ lässt sich eindeutig fortsetzenn nach $\mathbb{C} \setminus \{1\}$.
  Die Riemannsche Vermutung ist nun: ζ hat in $0 <$ Re$s < 1$ Nullstellen nur auf der Geraden Re$s = \frac{1}{2}$.

- **Primzahlsatz (Vinogradov, Korobar):** $\exists$Konstante $c > 0$ mit

$$\pi(x) = \mathrm{li}x + O\left(x \exp\left(-c \log^{\frac{3}{5}} x/(\log\log x)^{\frac{1}{5}}\right)\right)$$

- **Goldbach-Vermutung:** Jede gerade Zahl < 2 ist die Summe zweier Primzahlen. Jedes $n \in 2\mathbb{N}+1$ ist die Summe von drei Primzahlen.

- **Vermutung über Primzahlzwillinge:** Es gibt unendlich viele $p, p+2 \in \mathbb{P}$; genauer: #Primzahlzwillinge $\leq x$ sollte $\pi_2(x) \backsim \frac{x}{\log^2 x} \cdot 2 \cdot \Pi_{p\in\mathbb{P}, p>2}\left(1 - \frac{1}{(p-2)^2}\right)$. π konv. $\Leftrightarrow \Sigma_{p>2, p \text{ prim}} \log\left(1 - \frac{1}{(p-1)^2}\right)$ konv.

- **Satz von Tschebyscheff:** $\forall x$ gilt: $\frac{1}{4} \cdot \frac{x}{\log x} < \pi(x) \leq 6\frac{x}{\log x}$

1.5 Kongruenzen und Reste

- **Kongruent:** Seien $a, b \in \mathbb{Z}$. a heißt „kongruent" zu b „modulo n" kurz $a \equiv b \mod m$ oder $a \equiv b(m)$ oder $a \equiv^m b$, wenn gilt: $m|a-b$ oder auch $\exists k \in \mathbb{Z}$ mit $a = b + km$ oder „bei Division mit Rest durch m haben a und b den gleichen Rest" (wenn $m \neq 0$).
„$\equiv^m$" ist eine Äquivalenzrelation auf m. $m = 0 \Rightarrow$ „$\equiv^m$" bedeutet „$=$".

- **Eine Klasseneinteilung:**

$$[a]_m := \{b = a + km \mid k \in \mathbb{Z}\}$$

Z.B.: $[0]_2$ =gerade Zahlen, $[1]_2$ =ungerade Zahlen.
$\mathbb{Z}/m\mathbb{Z} := \{$alle Äquivalenzklassen $\mod m\}$.
Z.B. $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ und $m \neq 0 \Rightarrow \mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$

- **Multiplikation und Addition auf $\mathbb{Z}/m\mathbb{Z}$:** Sei $m \in \mathbb{Z}$. Addition und Multiplikation werden auf $\mathbb{Z}/m\mathbb{Z}$ definiert durch $[a]_m + [b]_m := [a+b]_m$, $[a]_m \cdot [b]_m := [a \cdot b]_m$ (kurz: $[a]+[b] = [a+b]$, wenn m fest gewählt; nicht verwechseln mit der Gaussklammer!).
Diese Operationen sind „**wohldefiniert**", d.h. unabh. von der Wahl der Repräsentanten.
$0, 1, \ldots, m-1$ heißen „kleinste nicht-negative Reste $\mod m$" und bilden ein Repräsentantensystem.

- **Satz:** In $\mathbb{Z}/m\mathbb{Z}$ gelten für alle $[a], [b], [c] \in \mathbb{Z}/m\mathbb{Z}$:

  - $([a] + [b]) + [c] = [a] + ([b] + [c])$
  - $[a] + [0] = [a]$
  - $\forall [a]\ \exists [x] \in \mathbb{Z}/m\mathbb{Z}$ mit $[a] + [x] = [0]$ nämlich $[x] = [-a]$
  - $[a] + [b] = [b] + [a]$
  - $([a] \cdot [b]) \cdot [c]) = [a] \cdot ([b] \cdot [c])$
  - $([a] + [b]) \cdot [c] = [a] \cdot [c] + [b] \cdot [c]$

- **Prime Restklasse:** Seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$. Aus $a \equiv b \mod m$ und $(a, m) = 1$ folgt $(b, m) = 1$. $[a]_m$ heißt darum „prime Restklasse $\mod m$" (repräsentantenunabhängig).
Sei $m \in \mathbb{N}, (\mathbb{Z}/m\mathbb{Z})^*$ die Menge der primen Restklassen $\mod m_i$, $[a], [b] \in (\mathbb{Z}/m\mathbb{Z})^*$. Dann gilt:

  1. auch $[a][b] \in (\mathbb{Z}/m\mathbb{Z})^*$
  2. die Gleichung $[a][x] = [1]$ ist in $(\mathbb{Z}/m\mathbb{Z})^*$ lösbar, d.h. $\exists x \in \mathbb{Z}: \quad ax \equiv 1 \mod m$. Dabei ist $x \mod m$ eindeutig bestimmt.

$[a]^{-1}$ bestimmt sich durch den euklidischen Algorithmus.
Für $m \in \mathbb{Z},\ a, c \in \mathbb{Z},\ (a, m) = 1,\ a_1, \ldots, a_m \in \mathbb{Z}$ sei irgendein vollst. Restsystem $\mod m$. Dann gilt:

1. Die Kongruenz $ax \equiv c \mod m$ hat eine $\mod m$ eindeutige Lösung $x \in \mathbb{Z}$
2. Auch $aa_1, aa_2, \ldots, aa_m$ ist ein vollst. Restsystem

Für $m \in \mathbb{N},\ a, c \in \mathbb{Z}$ ist also die Kongruenz $ax \equiv c(m)$ lösbar $\Leftrightarrow d := (a, m) \mid c$. Die Lösung ist dann $\mod \frac{m}{d}$ eindeutig bestimmt, d.h. mit $[x]_m$ ist auch $[x]_m, [x + \frac{m}{d}]_m, [x + 2\frac{m}{d}]_m, \ldots, [x + (d-1)\frac{m}{d}]_m$ Lösung.

- **Haskos Siebenerregel:**

$$\forall b_j \in \{0, 1, \ldots, 99\} : 7 \mid m = b_0 + b_1 100 + \ldots + b_n 100^n \Leftrightarrow 7 \mid b_0 + 2b_1 + \ldots + 2^n b_n$$

- **Chinesischer Restsatz:** Seien $m_1, \ldots, m_n$ paarweise teilerfremd $\in \mathbb{N}$ und $a_1, \ldots, a_n \in \mathbb{Z}$ $\Rightarrow \exists x \in \mathbb{Z}$ mit $x \equiv a_1(m_1), x \equiv a_2(m_2), \ldots, x \equiv a_n(m_n)$ und x ist eindeutig bestimmt $\mod m_1 \cdot m_2 \cdot \ldots \cdot m_n$.
Die Abbildung $[x]_{m_1 \cdot \ldots \cdot m_n} \mapsto ([x]_{m_1}, \ldots, [x]_{m_n})$ ist eine bijektive Abb.:

$$\mathbb{Z}/(m_1 \cdot \ldots \cdot m_n)\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_n\mathbb{Z}$$
$$(\mathbb{Z}/(m_1 \cdot \ldots \cdot m_n)\mathbb{Z})^* \to (\mathbb{Z}/m_1\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/m_n\mathbb{Z})^*$$

wenn $m_1, \ldots, m_n$ paarweise teilerfremd.

- **Eulersche Phi-Funktion:** $\varphi(1) := 1$. Für $m \in \mathbb{N},\ m > 1$ sei $\varphi(m) := \#\mathbb{Z}/m\mathbb{Z}^* = \#\{0 < a < m \mid a \in \mathbb{N}, (a.m) = 1\}$
Die Eulersche φ-Funktion ist „multiplikativ", d.h. $\varphi : \mathbb{N} \to \mathbb{R}$ mit $\varphi(1) = 1$ und $\varphi(mn) = \varphi(m)\varphi(n)$ für $(m, n) = 1 \Rightarrow \varphi(n) = n \cdot \Pi_{p \in \mathbb{P},\, p \mid n}(1 - \frac{1}{p})$, weil $n = \Pi_{\mathbb{P}} p^{\nu_p(n)}$
Also ist $\mathbb{P}$ unendlich!
$\varphi(n)$ ist die Anzahl der natürlichen Zahlen $a \leq n$, welche zu n teilerfremd sind.

2 Gruppen

2.1 Kongruenzen und Reste

- **Multiplikative Gruppe:** G heißt multiplikative Gruppe, wenn gilt:

1. In G existiert eine „**innere Verknüpfung**", d.h. Abb. $G \times G \to G : (a, b) \mapsto a \cdot b \in G\ \forall a, b \in G$
2. $(ab)c = a(bc) \quad \forall a, b, c \in G$
3. $\exists$„**Einselement**" oder „**neutrales Element**" $e \in G$ und $ae = a \quad \forall a \in G$
4. $\forall a \in G\ \exists$„**inverses Element**" $a^{-1} \in G$ mit $aa^{-1} = e$. G heißt „**kommutativ**" oder **abelsche Gruppe**, wenn zusätzlich gilt:
5. $ab = ba \quad \forall a, b \in G$. In diesem Fall häufig „ +" anstelle von „$\cdot$", dabei „0" anstelle „e"; bei multipl. Gruppen häufig „1" statt „e". Zur Präzisierung wird häufig die Verknüpfung mitgenannt, z.B. in der Form $(G, \cdot)$ oder $(G, +)$, z.B. $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$. Bei additiv geschriebenen Gruppen schreibt man „$-a$" anstelle von „a^{-1}".

Aus der Induktion über die Anzahl der Faktoren folgt, dass sich das Assioziativgestz (und gegebenenfalls auch das Kommutativgesetz) auf n Faktoren überträgt, d.h. in $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ sind beliebige Klammersetzungen erlaubt (bzw. Umordnungen).
Sei G eine (multiplikative) Gruppe. Dann gilt:

1. $ea = ae = a \quad \forall a \in G$
2. e ist eindeutig bestimmt.
3. $a^{-1}a = aa^{-1} = e \quad \forall a \in G$
4. $\forall a \in G$ ist a^{-1} eind. bestimmt durch a
5. $(ab)^{-1} = b^{-1}a^{-1} \quad \forall a, b \in G$
6. $(a^{-1})^{-1} = a$
7. $ax = b$ und $ya = b$ sind eindeutig lösbar für $a, b \in G$, nämlich $x = a^{-1}b,\ y = ba^{-1}$
8. Kürzungsregel: $ab = ac \Rightarrow b = c, \quad ba = ca \Rightarrow b = c$

- **Permutationen:** Permutationen können geschrieben werden als $2 \times n$-Matrix:

$$\begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{\pi(1)} & x_{\pi(2)} & \dots & x_{\pi(n)} \end{pmatrix}$$

oder in **Zykelschreibweise**

$$x_1 \to x_{\pi(1)} \to x_{\pi(\pi(1))} \to \dots \to x_{\pi^n(1)}$$

- **Symmetrische Gruppen:** Die Symmetrische Gruppe S_n mit $n \in \mathbb{N}$ ist die Gruppe der Bijektionen oder Permutationen S_s einer n-elementigen Menge auf sich selbst. Es gilt:

1. ord$S_n = n!$
2. S_n ist nicht kommutativ für $n > 2$
3. S_n wird von Transpositionen erzeugt
4. Für jeden Zykel gilt $(a_1 a_2 \dots a_k)^{-1} = (a_k a_{k-1} \dots a_1) = (a_1 a_k a_{k-1} \dots a_2)$ zyklische Vertauschung in der Schreibweise erlaubt.
5. Zwei disjunkte Zykeln $(a_1 \dots a_k), (b_1 \dots b_m)$ (d.h. $\underbrace{\{a_1, \dots, a_k\}}_{\sigma} \cap \underbrace{\{b_1 \dots b_m\}}_{\tau} = \emptyset$) kommutieren miteinander, d.h. für σ und τ gilt: $\sigma\tau = \tau\sigma$
6. Bei „Konjugation" durch $\sigma \in S_n$, d.h. bei Abbildungen $S_n \to S_n : \tau \mapsto \sigma\tau\sigma^{-1}$ werden Zykeln nach folgenden Vorschriften transformiert: $\sigma(\underbrace{a_1 \dots a_k}_{\tau})\sigma^{-1} = (\sigma(a_1)\sigma(a_2) \dots \sigma(a_k))$

2.2 Untergruppen und Homomorphismen

- **Untergruppe:** Sei $(G, \cdot)$ Gruppe. Eine Untermenge $U \subseteq G$ heißt „Untergruppe" von G, wenn sie bzgl. der in G definierten Verknüpfung die Gruppenaxiome erfüllt, d.h. wenn

1. $\forall a, b \in U$ auch $ab \in U$
2. Das neutrale Element $e \in U$
3. $\forall a \in U$ liegt auch $a^{-1} \in U$

Oder einfacher:

1. $U \neq \emptyset$
2. $\forall a, b \in U$ ist $ab^{-1} \in U$

- **Homomorphismus:** $f : G \to H$ sei Abbildung für die (mult.) Gruppen G, H. f heißt (Gruppen-)Homomorphismus , wenn gilt:

$$\forall a, b \in G : \quad f(ab) = f(a)f(b)$$

$f(e) = e$, wenn e für das Einsel. in G und in H steht. $f(a) = f(ae) = f(a)f(e) \Rightarrow f(e)$ auch neutrales Element in H. Genauso $e = f(e) = f(aa^{-1}) = f(a)f(a^{-1}) \Rightarrow_{\text{Eindeutigkeit des Inversen}} f(a)^{-1} = f(a^{-1})$

- **Gruppenhomomorphismus:** Sei $h : G \to H$ Gruppenhomomorphismus (beide multiplikativ geschrieben, mit e und Inversen $(\,)^{-1}$). Dann gilt:
  - $h(e) = e$
  - $h(a^{-1}) = h(a)^{-1}$
  - $\forall$Untergruppen $U \subseteq G$ ist $h(U)$ Untergruppe von H (inbes. $H(G)$)
  - $\forall$Untergruppeen $V \subseteq H$ ist $h^{-1}V := \{x \in G \mid h(x) \in V\}$ Untergruppe von G
  - $h^{-1}(\{e\}) = h^{-1}(e) =: \text{Kern}h$ Untergruppe von G
  - h injektiv $\Leftrightarrow \text{Kern}h = \{e\}$

- **Isomorphismus:** $f : G \to H$ bijektiver Gruppenhom. (injektiv+surjektiv!). Dann heißt f „Isomorphismus". Wenn für zwei Gruppen G, H so ein Isomorphismus existiert, heissen G und H isomorph, $G \cong H$.
  Für Isomorphismen $f : G \to H$ ist auch $f^{-1} : H \to G$ Isomorphismus und jede endliche Gruppe der Ordnung n ist isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.

- **Zyklische Gruppe:** Eine (mult.) Gruppe heißt „zyklisch", wenn $\exists x \in G$ mit: G besteht nur aus x-Potenzen, d.h. $G\{\ldots, x^{-2}, x^{-1}, x^0 = e, x^1, x^2, \ldots\}$. Schreibweise dann: $G = \langle x \rangle$, bei additiven Gruppen $G = \langle x \rangle = \{\ldots, -2x, -x, 0, x, 2x, \ldots\}$.
  Eine zyklische Gruppe ist immer isomorph zu entweder $(\mathbb{Z}, +)$ oder einer additiven G $(\mathbb{Z}/m\mathbb{Z}, +)$ $(m \in \mathbb{N})$. Wenn in dieser Gruppe $x^r = e$, so gilt $m|r$.
  Das erzeugende El. von $\langle x \rangle$ ist nicht eindeutig. Für zylische Gruppen $G = \langle x \rangle$ ist jeder Gruppenhom. $h : G \Rightarrow H$ eindeutig best. durch $h(x)$, denn $h(x^n) = (h(x))^n$. Wenn $\text{ord}x = m \in \mathbb{N}$ ($x^m = e$, m minimal), dann muß auch $(h(x))^m = e \in H \Rightarrow \text{ord}h(x) \mid m = \text{ord}x$.

2.3 Index und Ordnung

- **Äquivalenzklassen:** $\forall a, b \in G$ sei $a \backsim b :\Leftrightarrow ab^{-1} \in H \Leftrightarrow a \in Hb := \{hb \mid h \in H\}$ (ist Äquivalenzrelation).
  Die Äquivalenzklassen heissen „**Rechtsnebenklassen**" von H. Genauso: **Linksnebenklassen** bH zur Äquivalenzrelation $a \backsim b \Leftrightarrow b^{-1}a \in H$ (gleicher Begriff, wenn G kommutativ ist).
  Menge der Rechtsnebenklassen: $H\backslash G$, Menge der Linksnebenklassen: G/H.
  Äquivalenzklassen bilden eine Partition von G in disjunkte Teilmengen ab, hier der Form Hb, dabei durchläuft b ein Repräsentantensystem von $H\backslash G$. Für H endlich sind alle Hb gleich mächtig, nämlich wie $\#H$ $(h_1 b = h_2 b \Rightarrow h_1 = h_2)$.
  Außerdem gilt: $\text{ord}G = (\#H\backslash G) \cdot (\text{ord}H)$

- **Index von H in G:** $\#H\backslash G =: (G : H)$ und $|G| = (G : H) \cdot |H|$
  $\#H\backslash G = \#G/H$, denn $\exists$Bijektion zwischen Rechts- und Linksrestklassen vermöge $Hb \mapsto (Hb)^{-1} = \{b^{-1}h^{-1} \mid h \in H\} = b^{-1}H$
  Sei G endliche Gruppe, $x \in G \Rightarrow \text{ord}x \mid \text{ord}G$, denn $\text{ord}x = \text{ord}\underbrace{\langle x \rangle}_{H} = \frac{\text{ord}G}{G:H} \mid \text{ord}G$
  So ist $\text{ord}\mathbb{Z}/m\mathbb{Z} = m$ und für $t \mid m$ ist $\text{ord}[\frac{m}{t}]_m = t$

- **Satz von Euler:** Sei G eine endliche Gruppe und $x \in G$. Dann ist $x^{\text{ord}G} = e$.
  $\text{ord}x \mid \text{ord}G = k \cdot \text{ord}x \Rightarrow x^{\text{ord}G} = (x^{\text{ord}x})^k = e$
  Folgerung von **Fermat**: Für $G = (\mathbb{Z}/m\mathbb{Z})^*$ $(m > 1)$ gilt: $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \mod m$, insbesondere $m = p$ prim $a^{p-1} \equiv 1 \mod p \Rightarrow a^p \equiv a \mod p$ sogar für alle $a \in \mathbb{Z}$. Problem: Klassifikation aller (endlichen) Gruppen bis auf Isomorphie.
  Jede endliche Gruppe von Primzahlordnung p ist isomorph zu $(\mathbb{Z}/p\mathbb{Z}, +)$

2.4 Normalteiler und Faktorgruppen

- **Konjugierte Untergruppe von H:** Sei G eine mult. Gruppe, H Untergruppe. $\forall g \in G$ sei $H^g := gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ die (durch g) „konjugierte Untergruppe von H".
Für nicht-kommutative Gruppen G kann ebenfalls $H = H^g$ sein.

- **Normalteiler / Invariante Untergruppe:** Eine Untergruppe H von G heißt „Normalteiler" oder „invariante Untergruppe", wenn $\forall g \in G : H^g = H$, geschrieben $H \lhd G$. Äquivalent sind dazu die Bedingungen $Hg = gH$ oder $\forall g \in G \forall h \in H \exists k \in H : ghg^{-1} = k$ (Rechtsnebenklassen=Linksnebenklassen).
Es genügt zu verlangen, dass die konjugierte Gruppe in H liegt: $H^g \subseteq H \forall g \in G$, weil dann auch $g^{-1}Hg = H^{g^{-1}} \subseteq H \Rightarrow H \subseteq gHg^{-1} = H^g$.

Seien G', G Gruppen, $f : G' \to G$ Homomorphismus $N \lhd G \Rightarrow f^{-1}(N) \lhd G'$.

- **Faktorgruppe:** Sei N Normalteiler der (multiplikativen) Gruppe G. Dann ist die Menge der Restklassen $G/N = N/G$ wieder Gruppe bzgl. repräsentantenweiser Multiplikation (mit $\mathrm{ord} G/N = (G : N)$) $(Ng) \cdot (Nh) := Ngh$ (mit neutralem Element $Ne = N$ und inversem Element $(Na)^{-1} = Na^{-1}$).

2.5 Isomorphiesätze

- **Kanonische Projektion:** Sei $N \lhd$ Gruppe G mit Restklassengruppe G/N. Die „kanonische Projektion"

$$\pi : G \to : g \mapsto Ng$$

ist ein surjektiver Gruppenhomomorphismus mit Kern$= N$.

- **Homomorphiesatz:** Seien G und B Gruppen, $f : G \to B$ surjektiver Gruppenhomomorphismus. Dann ist $B \cong G/\mathrm{Kern} f$ und zwar wird die Isomorphie durch die Abbildung i gegeben durch $i\,(\mathrm{Kern} g) = f(g)$.

- **Hilfssatz:** Sei G Gruppe mit Untergruppen H_1, H_2 und Normalteiler N. Dann ist:
  1. auch $H_1 \cap H_2$ Untergruppe von G
  2. $N \cap H_1$ Untergruppe von G
  3. aus $H_2 \subseteq H_1 \subseteq G$ folgt $(G : H_2) = (G : H_1) \cdot (H_1 : H_2)$
  4. auch $H_1 N := \{hg \mid h \in H, g \in N\}$ Untergruppe von G und besitzt H_1 als Untergruppe und N als Normalteiler

- **1. Isomorphiesatz:** Sei G Gruppe mit Untergruppe U und Normalteiler N

$$\Rightarrow U/(U \cap N) \cong UN/N$$

- **2. Isomorphiesatz:** Sei $f : G \to G' = f(G)$ ein surjektiver Gruppenhomomorphismus mit Kern$K$. Dann gibt es zwischen der Menge der Untergruppen $H \supseteq K$ von G und der Menge aller Untergruppen $H' \subseteq G'$ eine Bijektion $H \to H' = f(h)$, gegeben durch $H' = f(H)$, $H = f^{-1}(H')$. Diese Bijektion ist inklusionserhaltend und bildet Normalteiler auf NT ab, und für $NT\ K \lhd N \lhd G$ gilt

$$G/N \cong G'/N' \cong (G/K)/(N/K)$$

2.6 Operation von Gruppen auf Mengen

G (Gruppe, multipl.) „**operiert**" auf der Menge $M :\Leftrightarrow \exists$Abbildung $G \times M \to M : (x,s) \mapsto xs \in M$ mit den folgenden Eigenschaften:

1. $(xy)s = x(ys)$ (keine Mult. in G!) $\forall x, y \in G \forall s \in M$
2. $es = s \quad \forall s \in M$

M wird auch G-Menge genannt. $s \mapsto xs : M \to M$ ist eine Bijektion, denn die Abb. läßt sich durch x^{-1} umkehren und gehört somi zur Gruppe S_M der Bijektionen auf sich.
Jedes $x \in G$ definiert eine „**Translation**" $T_x : M \to M : s \mapsto xs$, $T_x \in S_M$, $T_e = id_M$, $T_{xy} = T_x T_y$ $\Rightarrow x \mapsto T_x : G \to S_M$ ist Homomorphismus.
$\forall s \in M$ heißt $Gs := \{xs \in M \mid x \in G\}$ die „**Bahn**" oder der „**Orbit**" von s unter der Operation von G auf M und

$$G_s := \{x \in G \mid xs = s\} \quad \text{(Untergruppe von } G\text{)}$$

die „**Isotropiegruppe**", „**Fixgruppe**" oder „**Stabilisator**" von $s \in M$.
G operiert „**transitiv**" auf M, wenn $\exists s \in M$ mit $Gs = M$. (Wenn transitiv $\Rightarrow \forall t \in M : Gt = M, \exists x \in G : t = xs, \forall t' \in M \exists x' \in G$ mit $t' = x's = x' \underbrace{(x^{-1}t)}_{=s}$)

Der **Zentralisator** von s ist

$$C_a(s) := \{x \in Gmid\sigma_x(s) = s, \text{ also } xs = sx\}$$

mit der Operation $G \times G \to G : (x,y) \to xyx^{-1}$. Das **Zentrum** ist $C_G = \{x \in G \mid xs = sx \forall s \in G\}$.

- **Bahnenlängen und Indizes:** Die Gruppe G operiere auf der Menge M.
  1. Die Einteilung der Menge M in Bahnen ist eine Einteilung in Äquivalenzklassen bzgl. der Relation $s \backsim t :\Leftrightarrow \exists x \in G : xs = t$.
  2. Innerhalb einer Bahn gilt: $t(\in M) = x \cdot s \Leftrightarrow y^{-1} \cdot x \cdot s = s \Leftrightarrow y^{-1}x \in G_s \Leftrightarrow x$ und y liegen in der gleichen Linksnebenklasse von G.
  3. $\exists$Bijektion zwischen Linksrestklassen $\mod G_s$ und den Elementen der Bahn Gs von s.
  4. Die **Länge dieser Bahn** $|G \cdot s|$=Anzahl der Elemente der Menge $G \cdot s = (G : G_s)$
  5. $\forall t = x \cdot s$ aus der Bahn von s gilt: Die Isotropiegruppe $G_t = \{y \in G \mid yt = t \Leftrightarrow y \underbrace{xs}_{t} = xs \Leftrightarrow x^{-1}yxs = s\} = x \cdot G_s x^{-1}$, d.h. die Isotropiegruppen einer Bahn sind alle zueinander konjugiert.
  6. Isotropiegruppe G_s eines Elements ist Normalteiler in G ($G_s \lhd G$) $\Leftrightarrow G_s$ stabilisiert alle Elemente aus der Bahn von s.

- **Klassenformel:** Sei R ein Repräsentantensystem der Bahnen für die Operation der Gruppe G auf der Menge M. Dann ist M also die disjunkte Vereinigung aller $G \cdot r$ mit $r \in \mathbb{R}$: $M = \bigcup_{r \in \mathbb{R}} Gr \Rightarrow |M| = \Sigma_{r \in \mathbb{R}}(G : G_r)$.

- **RSA-Schema:** Ein public-key Kryptosystem. Seien p, q zwei sehr grosse Primzahlen (geheim). Sie bilden das Produkt $p \cdot q = n$ (öffentlich) mit $\varphi(n) = (p-1) \cdot (q-1)$ (geheim). Wenn $\varphi(n)$ nicht geheim bleibt, kann man p und q aus $n = p \cdot q$ und $n - \varphi(n) + 1 = p + q$ errechnen. Nun wähle man eine Zahl s mit $(s, \varphi(n)) = 1$ (öffentlich) und verschlüssele $a \mapsto a^s \mod n$. Das Entschlüsseln geht dann mittels $(s, \varphi(n)) = 1 \quad \exists t : s \cdot t \equiv 1 \mod \varphi(n)$
  $\big(s \in (\mathbb{Z}/\varphi(n)\varphi(n)\mathbb{Z})^* \Rightarrow \exists t = s^{-1}$ (Inverses in $(\mathbb{Z}/\varphi(n)\mathbb{Z} =^*))\big)$
  t kann mit dem euklidischen Algorithmus konstruiert werden. Andere Schreibweise: $s \cdot t = 1 + k \cdot \varphi(n) \quad k \in \mathbb{N}$ und
  $(a^s)^t \equiv a^{s \cdot t} \equiv a^{1+k \cdot \varphi(n)} \equiv a \cdot a^{k \cdot \varphi(n)} \equiv a \mod n$ (klar für $(a,n) = 1$ wg. kleinem Satz von Fermat)

- **Kleiner Satz von Fermat:** $a^{\varphi(n)} \equiv 1 \mod n \Rightarrow a^{k\varphi(n)} \equiv 1 \mod n \Rightarrow a \cdot a^{k\varphi(n)} \equiv a \mod n$

2.7 Sylowuntergruppen

- **p-Gruppe:** G heißt p-Gruppe (p Primzahl), wenn $\text{ord}(G) = p^n$ ($n \in \mathbb{N}$). Für G endliche Gruppe, H Untergruppe $\subseteq G$, H „**p-Untergruppe**", wenn H ist p-Gruppe. H heißt „**p-Sylowuntergruppe**" von G, wenn $\text{ord}H = p^n$ mit $p^n \mid \text{ord}G$ und $p \nmid \frac{\text{ord}G}{p^n}$ (also ist p^n die höchste p-Potenz, die $\text{ord}G$ teilt).
Sei G endliche abelsche Gruppe und $n \in \mathbb{N}$ mit $x^n = e \forall x \in G$. Dann gibt es ein $m \in \mathbb{N}$ mit $\text{ord}G \mid n^m \Rightarrow$ so ein n kann nicht teilerfremd zur Gruppenordnung sein!
Sei G eine endliche abelsche Gruppe, p prim mit $p \mid \text{ord}G \Rightarrow G$ hat eine Untergruppe der Ordnung p.
Sei G endliche Gruppe, p Primteiler von $\text{ord}G$, dann gilt:

  1. Es existiert eine p-Sylowuntergruppe von G.
  2. Jede p-Untergruppe H von G ist in einer p-Sylowuntergruppe enthalten.
  3. Alle p-Sylowuntergruppen sind zueinander konjugiert
  4. Die Anzahl der p-Sylowuntergruppen von p ist $\equiv 1 \mod p$.

  Daraus folgt:

  1. Sei G endliche p Gruppe $\neq \{e\}$. Dann hat G ein Zentrum $Z \neq \{e\}$.
  2. Sei p prim. Gruppen G der Ordnung p^2 sind kommutativ.
  3. Sei $p > 2$ prim, G Gruppe mit $\text{ord}G = 2p$. Dann ist G entweder zyklisch, d.h. $\cong \mathbb{Z}/2p\mathbb{Z}$ oder „**Didiererweiterung**" einer zyklischen Untergruppe $\langle x \rangle$ der Ordnung p, d.h. alle $y \in G \setminus \langle x \rangle$ haben Ordnung 2 und erfüllen $y \times y^{-1} = x^{-1}$ (Symmetriegruppe des regelmässigen p-Ecks).

- **Klassenformel:** Sei γ_0 die G-Bahn von S und $H \neq \{e\}$ p-Untergruppe von G. Auch H operiert per Konjugation auf γ und auf γ_0, γ_0 zerfällt dabei in H-Bahnen $\gamma_1, \ldots, \gamma_k$:

$$p \nmid |\gamma_0| = \Sigma_{i=1}^{k} |\gamma_i| = \Sigma_{s \in \gamma_i} (\underbrace{H : H_{s_i}}_{p\text{-Untergruppe}}) \quad \text{(Indizes sind } p\text{-Potenzen)}$$

  $\Rightarrow \exists i$ oBdA $s_i = s'$, mit $(H : H_{s_i}) = 1 \Rightarrow H_{s'} = H$

  $\Rightarrow S \in \gamma_i$ ist invariant unter Konjunktion mit allen $x \in H$

  $\Rightarrow xS'x^{-1} = S' \Rightarrow$ alle $x \in H$ erfüllen $x \in N_G(S') \Rightarrow \subseteq N_G(S')$

  $\Rightarrow HS'$ ist Untergruppe von G und enthält S' als Normalteiler.

  Wähle H wie oben als p-Sylowuntergruppe, d.h. $H \in \gamma$. Nun folgt zusätzlich $H = S'$:

  $\Rightarrow \delta'$ liegt in der G-Bahn von S

  $\Rightarrow$ alle Sylowuntergruppen liegen in der gleichen Bahn! (D.h. alle sind zueinander konjugiert)

  Sei noch spezieller $H = S$ gewählt, dann gilt $|\gamma| = |\gamma_0| = \Sigma_{i=1}^{K} (H : H_{s_i})$.
  Seien rechts nur p-Potenzen, dabei einmal die 1, wenn $S = S_1 = H$ (oBdA), die anderen S_i sind echt konjugiert zu S_1, erfüllen daher $H_{s_i} \subsetneq H$, also $(H : H_{s_i}) = 0 \mod p \Rightarrow \Sigma_{i=1}^{k} \equiv 1 \mod p$.
  Außerdem ist jede (endliche) p-Gruppe G „**auflösbar**", d.h. $\exists$Kette von Untergruppen $\{e\} = G_0 \lhd G_1 \lhd \ldots \lhd G_{n-1} \lhd G_n = G$, jedes $G_i \lhd G_{i+1}$ mit zyklischer Faktorgruppe G_{i+1}/G_i.

2.8 Produkte

- **Direktes Produkt:** Seien U und V (multiplikative) Gruppen. Das mengentheoretische Produkt $U \times V = \{(u,v) \mid u \in U, v \in V\}$ läßt sich mit Gruppenstrukturen versehen vermöge $(u_1v_1)(u_2v_2) = (u_1u_2, v_1v_2)$. Einselement: (e_U, e_V), Inverses $(u,v)^{-1} = (u^{-1}, v^{-1})$. $U \times V$ heißt dann „direktes Produkt" von U und V. Für $V = U$ einfach U^2 geschrieben. Ebenso für mehr als zwei Faktoren, ebenso additiv.
  Beispiel: $\mathbb{R}^n = n$-faches direktes Prdoukt von $(\mathbb{R}, +)$ mit sich.
  Sei $G = U \times V$ direktes Produkt der Gruppen U, V, dann gilt:

  1. $\mathrm{ord}(U \times V) = (\mathrm{ord}U) \cdot (\mathrm{ord}V)$
  2. G enthält Normalteiler $U' := \{(u,e) \mid u \in U\}$ und $V' := \{(e,v) \mid v \in V\}$, isomorph zu U bzw. V. Diese erfüllen $U' \cap V' = \{(e,e)\}$
  3. U' und V' kommutieren elementweise miteinander, d.h. $u'v' = v'u' \; \forall u' \in U', v' \in V'$
  4. G wird erzeugt von U', V', d.h. sogar genauer $U'V' = G$. (Gilt nicht für Produkte aus unendlich vielen Faktoren!)
  5. Die natürlichen Projektionen p_u, p_v auf die Komponenten, also $(u,v) \mapsto u$ bzw. v sind Gruppenhomomorphismen. $\mathrm{Kern}p_u = V', \mathrm{Kern}p_v = U'$.

- **Satz:** Die Gruppe G enthalte zwei Normalteiler U, V mit folgenden Eigenschaften:

  1. $U \cap V = \{e\}$
  2. $G = UV$
  3. U und V kommutieren elementweise miteinander (d.h. $uv = vu \; \forall u \in U, v \in V$) $\Rightarrow G \cong U \times V$

- **Chinesischer Restsatz (verfeinert):** Seien $m, n \in \mathbb{N}$ teilerfremd. Dann gilt:

  1. $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (als Isomorphie additiver Gruppen)
  2. $\mathbb{Z}/mn\mathbb{Z})^* \cong /\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ (als Isomorphie multiplikativer Gruppen)

  Damals galt $\forall a \mod m, b \mod n \exists! x \mod mn$ mit $x \equiv a(m), x \equiv b(n)$, außerdem: wenn $[a]_m \in (\mathbb{Z}/m\mathbb{Z})^*, b \in (\mathbb{Z}/n\mathbb{Z})^*$, dann $x \in (\mathbb{Z}/mn\mathbb{Z})^*$. Jetzt gilt zusätzlich: $[x]_{mn} \mapsto ([a]_m, [b]_n)$ ist Gruppenhomomorphismus. Genauso gilt dies für die Multiplikation.

2.9 Klassifikation endlicher abelscher Gruppen

Direkte Produkte zyklischer Gruppen $\Pi_{i=1}^n \langle a_i \rangle$ sind abelsch.

- **Hilfssätze:** Sei $\langle b \rangle$ endliche und zyklisch (multipl. geschrieben), dann gilt:

$$\mathrm{ord}b = \mathrm{ord}\langle b \rangle = m \quad \text{und} \quad t \mid m \Rightarrow \mathrm{ord}b^t = \frac{m}{t}$$

  Sei $\langle a \rangle$ endl. zykl., $\mathrm{ord}a = \mathrm{ord}\langle a \rangle = n \Rightarrow \mathrm{ord}a^v = \frac{n}{(n,r)}$
  Sei A endliche abelsche Gruppe, $Z = \langle a \rangle$ eine zyklische Untergruppe maximaler Ordnung. $\mathrm{ord}z = \mathrm{ord}a =: n$. Die Faktorgruppe A/Z (wieder abelsch) hat zyklische Untergruppen U/Z (vgl. 2. Isomorphiesatz) mit erzeugendem Element $b \mod Z = bZ = Zb$ mit einem Repräsentanten $b \in A$. Dieses b kann so gewählt werden, dass $\mathrm{ord}(b \mod Z) = \mathrm{ord}b$ (d.h. die kleinste Potenz b^t mit $b^t \in Z$ erfüllt bereits $b^t = e$).
  Jede endliche abelsche Gruppe A ist isomorph zu einem direkten Produkt zyklischer Untergruppen.
  Sei U abelsche Gruppe, erzeugt von $b_1, \ldots, b_r$, d.h. $U = \langle b_1 \rangle \langle b_2 \rangle \ldots \langle b_r \rangle$, dann gilt $U \cong \langle b_1 \rangle \times \ldots \times \langle b_r \rangle$ genau dann, wenn aus $b_1^{m_1} b_2^{m_2} \ldots b_r^{m_r} = e$ folgt: $t_1 \mid m_1, t_2 \mid m_2, \ldots, t_r \mid m_r$.
  Außerdem gilt für jede endliche abelsche Gruppe A, dass diese isomorph ist zu

1. einem direkten Produkt $\Pi(\mathbb{Z}/q\mathbb{Z})$ mit Primpotenzen q
2. einem direkten Produkt $\Pi(\mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z})$ mit $d_\nu \in \mathbb{N}$ (> 1) mit $d_1 \mid d_2 \mid \ldots \mid d_{r-1} \mid d_r$ (d_ν heissen „**Elementarteiler**" für A).
   Sowohl die Menge und Multiplizität der Primpotenzen q und der Elementarteiler d_ν sind durch A eindeutig bestimmt und bestimmen A eindeutig bis auf Isomorphie.

Nun gilt: U_r =maximale Elementordnung in $\mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}$

$\Rightarrow$ eindeutig bestimmt durch A

$\Rightarrow$ $A/(\mathbb{Z}/d_r\mathbb{Z})$ hat nur noch maximale Element-Ordnung $d_r = 1$, ebenso eindeutig bestimmt

$\Rightarrow$ $d_1 \mid d_2 \mid \ldots \mid d_r$ eindeutig bestimmt

Die Elementarteiler sind eindeutig bestimmt, nicht aber die Untergruppen selbst.

3 Ringe

- **Ring:** R heißt „Ring", wenn gilt:

1. Es existieren zwei innere Verknüpfungen (Addition und Multiplikation)
$$R \times R \to R : (a, b) \mapsto a + b$$
$$R \times R \to R : (a, b) \mapsto a \cdot b$$
2. $(R, +)$ ist abelsche Gruppe (mit neutralem Element 0 und Inversem $-a$)
3. Die Multiplikation ist assoziativ, d.h.
$$(ab)c = a(bc) \quad \forall a, b, c, \in R$$
4. Das Distributivgesetz gilt, d.h.
$$a(b + c) = ab + ac \quad (b + c)a = ba + ca \quad \forall a, b, c \in R$$

Für kommutative Ringe mit Eins gilt ferner:

- $ab = ba \quad \forall a, b \in R$
- $\exists 1 \in R$ mit: $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$

- **Nullteiler:** In einem Ring kann es vorkommen, dass $0 = a$ gilt. Außerdem kann es passieren, dass $a, b \in \mathbb{R}$ existieren mit $a \neq 0 \neq b$, aber $ab = 0$ (sog. „Nullteiler").

- **Integritätsbereich:** Ringe ohne Nullteiler heißen „Integritätsbereiche", wenn $R \neq \{0\}$ kommutativ mit 1 ist.
  In Integritätsbereichen gilt die „**Kürzungsregel**":
$$ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b - c) = 0 \Rightarrow a = 0 \ \vee \ b = c$$

- **Körper:** R heißt „Körper", wenn $R = \{0\}$ abelsche Gruppe bzgl. der Multiplikation ist ($\Rightarrow$ automatisch Integritätsbereich, weil $a, b \in R \setminus \{0\} \Rightarrow$ ebenso ab).

- **Einheit:** $a \in R$ heißt „Einheit", wenn $a \mid 1$ gilt. Geschrieben $a \in R^*$. $(1 = ac \Rightarrow$ jedes $b = 1 \cdot b = a(c \cdot b) \Rightarrow a \mid$jedes andere El. $b)$

R^* ist die Menge der Einheiten in R.
In den Restklassenringen ist $(\mathbb{Z}/n\mathbb{Z})^*$ gerade die Menge der primen Restklassen.
Sei $R \neq \{0\}$ kommutativer Ring mit 1. Dann gilt

1. $1 \neq 0$
2. R^* enthält keine Nullteiler
3. R^* ist multiplikative abelsche Gruppe
4. Seien $a, b \in R$ nicht Nullteiler:

$$a \mid b \text{ und } b \mid a \quad \Leftrightarrow \quad a \in bR^* \quad \Leftrightarrow \quad \exists c \in R^* \text{ mit } a = bc,\ b = c^{-1}a$$

- **Primkörper/Charakteristik:** Endliche Integritätsbereiche sind Körper. Insbesondere ist $\mathbb{Z}/m\mathbb{Z}$ Körper $\Leftrightarrow$ $m = p$ prim, dann $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ („Primkörper" der „Charakteristik p" genannt).

- **Ringhomomorphismus:** $f : R \to S$ heißt Ringhomomorphismus, wenn R, S Ringe:

$$f(a+b) = f(a) + f(b) \quad f(a \cdot b) = f(a) \cdot f(b) \quad \forall a, b \in R$$

$\Rightarrow$ f ist Homomorphismus für $(R, +)$, d.h. z.B. $f(0) = 0$. $f \equiv 0$ zugelassen! D.h. nicht notwendig $f(1) = 1$.
f „**Körperhomomorphismus**" $\Leftrightarrow$ $f(1) = 1$ und Ringhom. für R, S Körper.
Für bijektive Ring- und Körperhomomorphismen ist f^{-1} ebenfalls Homomorphismus.
R, S heissen „**isomorph**", wenn ein „Isomorphismus" $f : R \to S$ exisitert, d.h. umkehrbarer Homomorphismus.
Sei f Körperhomomorphismus, $f : R \to S$, $c \in R, c \neq 0$ $f(c) = f(c^{-1}) = f(cc^{-1}) = f(1) = 1$

$\Rightarrow$ $f(R^*) \subseteq S^* = S \setminus \{0\}$

$\Rightarrow$ f induziert auch Homomorphismus $R^* \to S^*$
f sogar injektiv: $f^{-1}\{0\} = \{0\}$ (als Homomorphismus der additiven Gruppe)

Körperhomomorphismen sind injektiv.

- **Einsetzungshomomorphismus:** $\mathbb{Q}[0] \to \mathbb{Q} : p(x) \mapsto p(a) \in \mathbb{Q}$ ($a \in \mathbb{R}$ fest)

3.1 Einfache Gruppen

Eine endliche Gruppe G heißt „einfach", wenn sie außer $\{1\}$ und G keinen Normalteiler besitzt.
Wenn es nur abelsche einfache Gruppen gibt, ist jede endliche Gruppe auflösbar! (G auflösbar $\Leftrightarrow$ $\exists$Kette $\{1\} \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_n = G$ $\forall G_i$ Normalteiler in G_{i+1})
Bezüglich der Konjugationsoperation von A_5 auf sich zerfällt A_5 in

1 Bahn der Länge 1 ((1))

1 Bahn der Länge 15 (alle $(ij)(kl)$)

1 Bahn der Länge 20 (alle (ijk))

2 Bahnen der Länge 12 jeweils aus Fünferzyklen

- **Klassenformel:** ΣBahnenlängen $= 60 = \#A_5$

- **Polynomringe:** „**Einsetzungshomomorphismen**" $\mathbb{Q}[x] \to \mathbb{C} : p(x) \mapsto p(\alpha)$

- **Quadratischer Zahlkörper:** Sei $d \in \mathbb{Z}$, $d \neq 0, 1$ und „**quadratfrei**", d.h. $v(d) = 0$ oder 1 für alle $p \in \mathbb{P}$ und sei

$$\alpha := \begin{cases} \sqrt{d} & \text{für } d \equiv 2, 4 \mod 4 \\ \frac{1+\sqrt{d}}{2} & \text{für } d \equiv 1 \mod 4 \end{cases}$$

Dann gilt

$$\mathbb{Q}[\alpha] = \{r + s\alpha \mid r, s \in \mathbb{Q}\} \quad \text{ist Körper („quadratischer Zahlkörper"}$$
$$\mathbb{Z}[\alpha] = \{m + n\alpha \mid m, n \in \mathbb{Z}\} \quad \text{ist Ring (Ring } O_d \text{ der ganzen Zahlen in } \mathbb{Q}[\alpha])$$

Invertierbarkeit von $r + s\alpha$ für r, s nicht beide $= 0$. $r + s\alpha = u + v\sqrt{d}$ mit $u, v \in \mathbb{Q}$, beide $= 0$.
wenn $n, m \in \mathbb{Z}$, $(n, m) = 1$, so ist

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \quad \textbf{Produkt von Ringen}$$

Für $N = \Pi_{\mathbb{P}} p^{v_p(N)}$ ist damit $\mathbb{Z}/N\mathbb{Z} \cong \Pi_{\mathbb{P}} \mathbb{Z}/p^{v_p(N)}\mathbb{Z}$.

- **Quotientenkörper:** Zu jedem Integritätsbereich R gibt es einen „Quotientenkörper" K mit einem (injektiven) Einbettungshomomorphismus $i : R \to K$, so daß K der kleinste Körper ist, der $i(R)$ enthält. K besitzt die folgende Eigenschaft („**universelle Eigenschaft**"):
$\forall$injektive Ringhomomorphismen $j : R \to L$ in einem Körper L gibt es genau einen Körperhomomorphismus $k : K \to L$ mit $j = k \circ i$ (K ist durch diese universelle Eigenschaft sogar bis auf Isomorphie eindeutig bestimmt).

3.2 Ideale und Restklassenringe

- **Ideal:** Sei R kommutativer Ring mit 1. $I \subseteq R$ heißt „Ideal", wenn

  1. I bzgl. „+" eine Untergruppe von R,
  2. $xI \subseteq I \quad \forall x \in R$

  Für alle Ringhomomorphismen $f : R \to S$ ist Kern$f := \{x \in R \mid f(x) = 0\}$ ein Ideal von R.
  $x, y \in$ Kern $\Rightarrow f(x) = f(y) = 0$. $f(x - y) = 0 \Rightarrow x - y \in$ Kern.
  Sei $x \in$ Kern, $r \in R \Rightarrow f(rx) = f(r)f(x) = f(r) \cdot 0 = 0 \Rightarrow rx \in$ Kern.

- **Kongruent modulo I:** Sei I Ideal eines kommutativen Rings R und

$$x \equiv y \mod I :\Leftrightarrow x - y \in I \Leftrightarrow x \in y + I$$

  Dies ist eine Äquivalenzrelation: Die Menge der Äquivalenzklassen $[x]_I$ wird mit R/I bezeichnet. R/I ist der „**Restklassenring**" von R mod I vermöge

$$[x]_I + [y]_I := [x + y]_I$$
$$[x]_I \cdot [Y]_I := [xy]_I$$

  Wohldefniniertheit wie in $\mathbb{Z}/m\mathbb{Z}$: 0 in $\mathbb{R}/I$ ist $[0]_I = I$ und 1 in $\mathbb{R}/I$ ist $[1]_I = 1 + I$. „**Kanonische Projektion**" $R \to R/I : x \mapsto [x]_I$ ist Ringhomomorphismus mit Kern$= I$.

- **Homomorphiesatz für Ringe:** Sei $f : R \to S$ surjektiver Ringhomomorphismus mit Kern$f = I$. Dann gilt $R/I \cong S$ vermöge $i : R/I \to S : [x]_I \mapsto f(x) \quad$ mit $i \circ k = f$.

- **Noether'scher Ring:** R heißt „Noether'scher Ring", wenn jedes Ideal in R endl. erzeugt ist.

- **Primideal:** Sei R kommutativer Ring mit 1, P heißt „Primideal" in R, wenn $\forall a, b \in R$ mit $ab \in P$ gilt: a oder $b \in P$.
  $M \subsetneq R$ heißt „**maximales Ideal**" wenn gilt: M ist Ideal in R und wenn aus $I \supsetneq M$, $I \neq M$, I Ideal, folgt $I = R$.
  R sei kommutativer Ring mit 1:

  1. $p \subsetneq R$ Primideal $\Rightarrow R/P$ Integritätsbereich
  2. $M \subsetneq R$ maximales Ideal $\Rightarrow R/M$ Körper
  3. $M \subsetneq R$ maximales Ideal $\Rightarrow M$ Primideal
  4. Jedes Ideal $I \subsetneq R$ ist in einem maximalen Ideal enthalten.

- **Zorn'sches Lemma:** Solche vollst. geordneten Ketten besitzen maximale Elemente. ??

3.3 Polynome

- **Polynomfuntion:** Sei R kommutativer Ring mit 1 und $f : R \to R : x \mapsto f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, alle $a_j \in R$.

- **Polynome:** Polynome sind Funktionen $\mathbb{N} \cup \{0\} \to R : j \mapsto a_j$, die für alle bis auf endlich viele j erfüllen $a_j = 0$. Jede solche Abbildung $\mathbb{N}_0 \to \mathbb{R}$ wird durch $a_n x^n + \ldots + a_0$ gekennzeichnet. (x „Variable" oder „Unbestimmte")
  Bezüglich der Addition bilden die Polynome eine abelsche Gruppe mit dem Nullpolynom als Null ($j \mapsto 0 \, \forall j$).
  Das Produkt sei gegeben durch die „**Faltung**" von $f : j \mapsto a_j$ und $g :\mapsto b_j$:

$$(f * g)(k) := \Sigma_{j=0}^{k} f(j)g(k-j)$$

- **Grad eines Polynoms:** $n = \max\{j \in \mathbb{N}_0 \mid f(j) = a_j \neq 0\}$ für $f \not\equiv 0$.
  grad0:=$-\infty$ $\Rightarrow$ $G_n = f(n)$ „**führender Koeffizient**" von f.
  Sei R Integritätsbereich, $f, g \in R[x]$. Dann gilt:

$$\text{grad}(f \cdot g) = \text{grad}f + \text{grad}g$$

  also ist $R[x]$ selbst Integritätsbereich. Dieser Satz gilt nicht für Polynomfunktionen der Art „Bilde in $\mathbb{F}_2[x]$ $x \cdot (x+1)$".

- **Symmetrie, Elementarsymmetrische Polynome:** R komm. Ring mit 1, $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ heißt „symmetrisch", wenn $f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \quad \forall \sigma \in S_n$. Polynome der Form $s_1(x_1, \ldots, x_n) := x_1 + x_2 \ldots + x_n$ heissen „Elementarsymmetrische Polynome"
  Sei $f \in R[x_1, \ldots, x_n]$ symmetrisches Polynom. Dann existiert ein eindeutig bestimmtes $q(t_1, \ldots, t_n) \in R[t_1, \ldots, t_n]$ mit

$$f(x_1, \ldots, x_n) = q(s_1(x_1, \ldots, x_n), s_2(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n))$$

- **Diskriminante:** Diskriminante von

  $f(x) = (x-x_1)\cdot(x-x_2)\cdot\ldots\cdot(x-x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} \mp \ldots + (-1)^n s_n$ ist $D(f) := \Pi_{i \leq k j \leq n}(x_j - x_i)^n$

  ein symmetrisches Polynom in $x_1, \ldots, x_n$.
  Die elementarsymmetrischen Funktionen $s_1, \ldots, s_n$ sind „**algebraisch unabhängig**", d.h. für $h(t_1, \ldots, t_n) \in R[t_1, \ldots, t_n]$ ist $h(s_1(x_1, \ldots, x_n), s_n(x_1, \ldots, x_n)) = 0 \Leftrightarrow h \equiv 0$.

3.4 Euklidische und faktorielle Ringe

Sei K Körper, $a = a(x)$ und $b = b(x) \neq 0$ Polynome in $K[x]$. Dann gibt es Polynome $q = q(x)$ und $r = r(x) \in K[x]$ mit $a = qb + r$ und grad$r <$ grad$b$.
Sei R Integritätsbereich $\Rightarrow$ die Einheitengruppe von $(R[x])^* = R^*$, also $(K[x])^* = K^*$.

- **Normiert:** $f(x) \in K[x]$ heißt „normiert" $\Leftrightarrow f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$

- **Primpolynom:** $f(x)$ heißt „Primpolynom" $\Leftrightarrow$ f ist normiert und besitzt keine Teiler q außer $q \in K^*$ oder $K^* f$.
  Z.B. sind in jedem Körper lineare normierte Polynome $x - a$ Primpolynome. Abhängig von K kann es viele weiter Polynome geben, z.B. $x^2 + 1 \in \mathbb{R}[x]$, weil $x^2 + 1 = (x+a)(x+b)$ $a, b \notin \mathbb{R}$.
  Sei K Körper. Im Polynomring $K[x]$

  1. ist jedes Ideal ist Hauptideal.
  2. gibt es für $a, b \in K[x]$ einen (normierten) ggT.

3. der sich durch höchstens $n = \min\{\text{grad}a, \text{grad}b\}$ Divisionen mit Rest bestimmen läßt.
4. $\forall a, b \in K[x]$ $\forall$Primpolynome $p \in K[x]$ gilt: $p \mid ab \Rightarrow p \mid a$ oder $p \mid b$.
5. jedes Polynom ($\neq 0$) lässt sich in ein Produkt von Einheiten und Primpolynomen zerlegen, und zwar eindeutig bis auf die Reihenfolge.

Sei R Integritätsbereich, $a(x) \in R[x], \text{grad}a = n$, dann hat a höchstens n Nullstellen in R (d.h. $x_j \in R$ mit $a(x_j) = 0$, hier a aufgefaßt als Polynomfunktion $R \to R$). Wenn $R = K$ Körper, $\exists$Bijektion $x_j \mapsto (x - x_j)$ zwischen Nullstellen von a und linearen Primpolynomen-Teilern $(x - x_j) \mid a(x)$. Für beliebige Integritätsbereiche via $R[x] \subseteq K[x]$.

! Der Satz ist falsch für R mit Nullteilern: $a(x) = x^2 - 1$ in $R = \mathbb{Z}/8\mathbb{Z}$, hat Nullstellen $x = [1]_8, [3]_8, [5]_8, [7]_8$. $\text{grad}fg = \text{grad}f\,\text{grad}g$ falsch, wenn R Nullteiler besitzt.

! $a(x) \in K[x]$ verschwindet in $y \in K$ „von der Ordnung n" $\Leftrightarrow (x-y)^n \mid a(x)$ und $(x-y)^{n+1} \nmid a(x)$, geschrieben $\nu_y(a(x)) = n$.

Involution für zyklische Gruppen $(\mathbb{Z}/p\mathbb{Z}, +)$ p prim $\sigma : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ Automorphismus mit $\sigma \neq id, \sigma^2 = id$ ($\Rightarrow$ Klassifikation der Gruppen der Ordnung $2p$).
σ kann nur von der Form sein $[n]_p \mapsto [-n]_p$.

- **Satz von Wilson:** In $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ist $(p-1)! \equiv -1 \mod p$.

- **Euklidischer Ring, Gradfunktion:** Ein Integritätsbereich heißt „euklidischer Ring", wenn eine „Gradfunktion" g auf R existiert mit $g : R \setminus \{0\} \to \mathbb{N}_0$ mit der Eigenschaft: $\forall a, b \in R \setminus \{0\}$ $\exists q, r \in R$ mit $a = bq + r$ und dabei $r = 0$ oder $\text{grad}r < \text{grad}b$ erfüllt.
Solche euklidischen Ringe sind Hauptidealringe und besitzen eine eindeutige Primfaktorzerlegung (R euklidisch $\Rightarrow$ R Hauptidealring $\Rightarrow$ eind. Primfaktorzerlegung). (Es genügt sogar, daß die Grade eine diskrete, nach unten beschränkte Wertemenge durchlaufen.)

- **Irreduzibel:** $p \in R, p \neq 0, p \notin R^*$ heißt „irreduzibel" $\Leftrightarrow$ alle Teiler $t \mid p$ sind $\in R^*$ oder $\in R^*p$.
In R existiert eine Zerlegung in irr. Elemente $\langle a\rangle c\langle t_1\rangle c\langle t_2\rangle c \ldots$ ($t_2 \mid t_1 \mid a$ oBdA echte Teiler, d.h. echte Inklusionen echt aufsteigende Kette von Hauptidealen).
In R gibt es eine Eindeutigkeit der Primfaktorzerlegung genau dann, wenn

1. Jede aufsteigende Kette von Hauptidealen besitzt ein maximales Element.
2. Jedes irreduzible Element ist prim (Bsp.: $R = \mathbb{Z}[x]$).

In Hauptidealringen ist jedes irreduzible Element prim.

4 Arithmetik modulo n

Ziel ist die Lösbarkeit von $x^m \equiv c(n)$ insbesondere von $x^2 \equiv c(n)$. Da $\mathbb{Z}/n\mathbb{Z} = \pi\mathbb{Z}/p^{\nu_r(n)}\mathbb{Z}$ bekannt ist, muß nun die Lösbarkeit von $\mod p^\nu$ betrachtet werden. Ermittle dafür die gruppentheoretische Struktur von $(\mathbb{Z}/p\mathbb{Z})^*$ bzw. $(\mathbb{Z}/p^\nu\mathbb{Z})^*$.

4.1 Multiplikative zahlentheoretische Funktionen

- **Multiplikative zahlentheoretische Funktion:** $f : \mathbb{N} \to \mathbb{C}$ heißt multiplikative zahlentheoretische Funktion $\Leftrightarrow f(1) = 1$ und $f(n \cdot m) = f(n) \cdot f(m)$ $\forall (n, m) = 1$.
f ist eindeutig bestimmt durch die Werte $f(p^s)$.
Bsp: Identität, Einsfunktion, **Teilerfunktion** ($\sigma_0(n) := \#\{d \mid n \mid d \in \mathbb{N}\}$), **Teilersummenfunktion** ($\sigma_1(n) := \Sigma_{d|n, d\in\mathbb{N}} d \mid \sigma_1(p^\nu) = \Sigma_{\mu=0}^{\nu} p^\mu = \frac{p^{\nu+1}-1}{p-1}$, also $\sigma_1(nm) = \sigma_1(n) \cdot \sigma_1(m)$ und $\sigma_k(n) := \Sigma_{d|n} d^k$).

- **Multplikativität:** Seien f, g mult. zth. Funktionen und

$$(f * g)(n) := \Sigma_{d|n} f(d) g\left(\frac{n}{d}\right)$$

$f * g$ ist multiplikativ! und $(f * g)(1) = f(1)g(1) = 1$. (z.B. $g = 1$ und $g = \varepsilon$)

4.2 Die Struktur der primen Restklassengruppe

Sei $n = p_1^{\nu_1} \cdot \ldots \cdot p_s^{\nu_s} \Rightarrow (\mathbb{Z}/n\mathbb{Z})^* = \Pi(\mathbb{Z}/p_i^{\nu_i}\mathbb{Z})^*$. Wie sieht also $(\mathbb{Z}/p^n\mathbb{Z})^*$ aus? Ordnung $\varphi(p^n) = p^n - p^{n-1}$

- **Primitivwurzel:** Die multiplikative Gruppe $\mathbb{F}^*$ eines endlichen Körpers ist zyklisch. Insbesondere gilt das für $f = \mathbb{Z}/p\mathbb{Z}$, $p \in d\mathbb{P}$. Ein erzeugendes Element $[k]_p$ heißt dann „Primitivwurzel" ($\mod p$).
  p sei Primzahl, $s \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Dann gilt

  1. $a \equiv b \mod p^s \Rightarrow a^p \equiv b^p \mod p^{s+1}$
  2. $s \geq 2$, $p \neq 2 \Rightarrow (1 + ap)^{p^{s-2}} \equiv 1 + ap^{s-1} \mod p^s$

  $(\mathbb{Z}/p\mathbb{Z})^*$ ist zyklisch $= \langle [a]_p \rangle$ mit a „Primitivwurzel $\mod p$"

$$\begin{cases} \Sigma_{d|n}\varphi(d) = n \\ \text{In Körpern } \mathbb{F} \text{ hat } x^a - 1 = 0 \text{ genau } d \text{ Nullstellen, wenn } d \mid \mathbb{F}^* \end{cases}$$

  In jedem Körper ist eine endliche mult. Untergruppe von $\mathbb{F}^*$ zyklisch!

  1. $a \equiv b(p^s) \Rightarrow a^p \equiv b^p \mod p^{s+1}$
  2. $s \geq 2, p \not\equiv 2 \Rightarrow (1 + ap)^{p^{s-2}} \equiv 1 + ap^{s-1}(p^s)$
  3. $p \nmid a,\ b \neq 2,\ s \geq 2 \Rightarrow$ In $(\mathbb{Z}/p^s\mathbb{Z})^*$ ist $\operatorname{ord}[1 + ap]_{p^s} = p^{s-1}$

  Sei $p > 2$ prim, $s \in \mathbb{N}$. Dann ist $(\mathbb{Z}/p^s\mathbb{Z})^*$ zyklisch.
  $(\mathbb{Z}/2^s\mathbb{Z})^*$ ist zyklisch für $s = 1$ und 2 ($[1]_2$ bzw. $\{[1]_4, [-1]_4\}$). Für $s > 2$ ist $(\mathbb{Z}/2^s\mathbb{Z})^* = \{[(-1)^b s^e]_{s^s} \mid b = 0, 1, c = 0, 1, \ldots, 2^{s-1} - 1\} \cong \langle [-1]_{2^s} \rangle \times \langle [5]_{2^s} \rangle$
  $(\mathbb{Z}/m\mathbb{Z})^*$ zyklisch $\Leftrightarrow m = 2, 4, p^s$ oder $2p^s$ (p ungerade prim).

  Für $b \not\equiv 0(p)$ ist $x^n \equiv b \mod p^s$ genau dann lösbar, wenn $b^{z \cdot \frac{(p-1)p^{s-1}}{(n,(p-1)p^{s-1})}} \equiv 1 \mod p^s$. $x^n \equiv b(n)$ („b ist n-ter Potenzrest $\mod p$") $\Leftrightarrow b^{\frac{p-1}{(n,p-1)}} \equiv 1(p)$. Dazu:

  1. $n = 2, p > 2$ prim: $x^2 \equiv b$ lösbar („b quadratischer Rest $\mod p$") $\Leftrightarrow b^{\frac{p-1}{2}} \equiv 1 \mod p$
  2. $n = 2, p > 2$. b ist quad. Rest $\mod p \Leftrightarrow b$ quad. Rest $\mod p^s$, jeweils mit 2 Lösungen.
  3. Sei $p \nmid b, p \nmid n \Rightarrow (n, p-1) = (n, (p-1)p^{s-1}) \Rightarrow x^n \equiv b \mod p^s$ lösbar $\Leftrightarrow x^n \equiv b \mod p$ lösbar, mit gleicher Lösungsanzahl.

$$(\mathbb{Z}/2^s\mathbb{Z})^* = \begin{cases} \{[1]\} & \text{für } s = 1 \\ \{\pm[1]\} & \text{für } s = 2 \\ \langle [-1]_{2^s} \rangle \times \langle [5]_{2^s} \rangle & \text{sonst} \end{cases}$$

  4. Sei $2 \nmid b, s > 2, \in \mathbb{N}$. Dann gilt: wenn $2 \nmid n \Rightarrow x^n \equiv b \mod 2^s$ eindeutig in $(\mathbb{Z}/2^s\mathbb{Z})^*$ lösbar.
     Wenn $n = 2 \Rightarrow x^n \equiv b \mod 2^s$ genau dann lösbar, wenn $b \equiv 5^{2c}(2^s) \Leftrightarrow b \equiv 1 \mod 8$.

$\frac{a}{b}$ besitzt eine abbrechende Dezimalbruchentwicklung $\Leftrightarrow b$ besitzt nur Primfaktoren 2 und 5. Wenn nicht, schreibe $b = b' \cdot c$ mit $b' \mid 10^v, (c, 10) = 1 \rightarrow \exists$Darstellung $\frac{a}{b} = \frac{s}{10^v} + \frac{d}{c}$. (Funktioniert für jedes andere Ziffernsystem anstelle des Dezimalsystems ebenso!)

4.3 Quadratische Reste

- **Quadratischer Rest:** Sei $(b, N) = 1$. b „quadratischer Rest" $\mod N \Leftrightarrow x^2 \equiv b(N)$ lösbar $\Leftrightarrow$ b quad. Rest $\mod$ allen p^s (Primpotenzteiler von N). Andernfalls heißt $b \in (\mathbb{Z}/N\mathbb{Z})^*$ „ **quadratischer Nichtrest**" $\mod N$.
  Es gilt.

  1. b quadratischer Rest $\mod 2 \Leftrightarrow b \equiv 1(2)$
     b quad. Rest $\mod 4 \Leftrightarrow b \equiv 1(4)$
  2. b quadratischer Rest $\mod 2, s \geq 3 \Leftrightarrow b \equiv 1(8)$
  3. Sei $s \in \mathbb{N}, p > 2$ prim, $p \nmid b$, b quad. Rest $\mod p^s \Leftrightarrow b$ quadr. Rest $\mod p$
  4. Die quad. Reste $b \mod p, p > 2$ prim, bilden eine Untergruppe vom Index 2 in $(\mathbb{Z}/p\mathbb{Z})^*$, charakterisiert durch $b^{\frac{p-1}{2}} \equiv 1(p)$
  5. Für $p > 2$ prim sei das „**Legendresymbol**" definiert durch

$$\left(\frac{b}{p}\right) := \begin{cases} 1, & \text{wenn } b \text{ quad. Rest} \\ -1, & \text{wenn } b \text{ quad. Nichtrest} \\ 0, & \text{wenn } b \equiv 0 \mod p \end{cases}$$

     $\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \mod p$ ist das „**Eulersche Kriterium**".
  6. Das Legendresymbol ist multiplikativ zahlentheoretische Funktion $\mathbb{Z} \to \{0, 1, -1\} : b \mapsto (\frac{b}{p})$. Der Wert hängt nur von $b \mod p$ ab, definiert Gruppenhomomorphismus $(\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$. Kern ist der quadr. Rest $\mod p$.

- **Erstes Ergänzungsgesetz zum quadratischen Reziprozitätsgestz:** Für $p > 2$ prim ist

$$\left(\frac{-1}{p} = (-1)^{\frac{p-1}{2}}\right) = \begin{cases} +1, & p \equiv 1(4) \\ -1, & p \equiv -1(4) \end{cases}$$

  In jeder primen Restklasse $\mod 4$ liegen unendlich viele Primzahlen.

- **Satz von Gauß:** Sei p prim $< 2, p \nmid a \in \mathbb{Z}$ und $s := \{1, 2, \ldots, \frac{p-1}{2}\}$, $-s := \{-1, -2, \ldots, -\frac{p-1}{2}\}$. $s \cup -s$ bilden das „**absolut kleinste Restsystem**" von $(\mathbb{Z}/p\mathbb{Z})^*$. μ sei die Anzahl der Repräsentanten aus $-s$, welche $\equiv \mod p$ zu einer Restklasse $a, 2a, 3a, \ldots, \frac{p-1}{2}a$. Dann ist $\left(\frac{a}{p}\right) = (-1)^{\mu}$.

- **Zweites Ergänzungsgesetz:** Sei $p > 2$ prim $\Rightarrow \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \Leftrightarrow p \equiv \pm 1(8) \\ -1 & \Leftrightarrow p \equiv \pm 3(8) \end{cases}$

- **Quadratisches Reziprozitätsgesetz:** Seien $p \neq q$ Primzahlen $\neq 2$, dann ist $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right)$ außer wenn $p \equiv q \equiv 3(4)$.

- **Jacobisymbol:** $b \in \mathbb{N}, 2 \nmid b$ und $b = p_1 \cdot p_2 \cdot \ldots \cdot p_m$ Primfaktorzerlegung $(\frac{a}{b}) = (\frac{a}{p_1}) \cdot (\frac{a}{p_2}) \cdot \ldots \cdot (\frac{a}{p_m})$. Im Fall $b \in \mathbb{P}, b = p$, simmt es mit dem Legendresymbol überein. $(a, b) > 1 \Rightarrow (\frac{a}{b}) = 0$.
  Seien $a, b \in \mathbb{N}$ und ungerade und teilerfremd. dann gilt

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}} \quad \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}} \quad \left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$$

  Die Rechenschritte im Algorithmus zur Berechnung von $(\frac{a}{p})$ können durchgeführt werden unabh. davon, ob Zähler bzw. Nenner prim sind!

4.4 Verzweigung von Primzahlen

Was hat die Zahlentheorie in O_d zu tun mit der Zahlentheorie in $\mathbb{Z}$?

- **algebraisch konjugierte Element zu β:** Für $\beta = r + s\sqrt{d} \quad (r, s \in \mathbb{Q})$ ist dies $\beta' := r - s\sqrt{d}$. Die Abbildung $\beta \mapsto \beta'$ ist

  1. ein Körper-Automorphismus von $\mathbb{Q}(\sqrt{d})$, der genau die Elemente von $\mathbb{Q}$ fest läßt.
  2. Ein Automorphismus von O_d, der genau die Elemente von $\mathbb{Z}$ invariant läßt.
  3. erhält Teilbarkeit, Einheiten, irreduzible Elemente.

  Die „Norm" von β ist

  $$N(\beta) := \beta\beta' = (r + s\sqrt{d})(r - s\sqrt{d}) = r^2 - s^2 d \in \mathbb{Q}$$

  bildet $\mathbb{Q}(\sqrt{s})$ in $\mathbb{Q}$ ab und O_d in $\mathbb{Z}$, und N verhält sich multiplikativ, d.h.

  $$N(\gamma\beta) = \gamma\beta(\gamma\beta)' = \gamma\beta\gamma'\beta' = N(\gamma)N(\beta)$$

  Ferner gilt $r \in \mathbb{Q} \Rightarrow N(r) = r^2$, insbes. $N(1) = 1 \Rightarrow$ die Norm bildet Einheiten auf ± 1 ab, denn $\beta \mid 1$ heißt: $\exists \gamma : \beta\gamma = 1 \Rightarrow \underbrace{N(\beta)}_{\in\mathbb{Z}}\underbrace{N(\gamma)}_{\in\mathbb{Z}} = N(1) = 1.$ und für $\beta, \gamma \in O_d$ ist $N(\beta), N(\gamma) = \pm 1$
  Allgemeiner: $\beta \mid \alpha,\ \beta, \alpha \in O_d \Rightarrow N(\beta) \mid N(\alpha)$ in $\mathbb{Z}$.
  Sei O_d Ring der ganzen Zahlen in $\mathbb{Q}(\sqrt{d})$, in O_d gelte die eindeutige Primfaktorzerlegung. Sei p Primzahl in $\mathbb{Z} \subsetneq O_d$. p besitzt in O_d die folgenden möglichen Primfaktorzerlegungen:

  1. p ist auch prim in O_d („p ist träge")
  2. $p = \pm\pi \cdot \pi = \pm N(\pi)$ für zwei Primzahlen, die algebraisch konjugiert sind, π, π', die nicht zueinander assoziiert sind, d.h. sich nicht nur durch eine Einheit unterscheiden
  3. $p \backsim \pi^2$ für ein Primelement $\pi \in O_d$, d.h. $p \in \varepsilon\pi^2$ mit $\varepsilon \in O_d^* \Leftrightarrow \varepsilon \mid 1$.

  Jedes Primelement $\pi \in O_d$ ist Teiler einer eindeutig best. rationalen Primzahl $p \in \mathbb{Z}$.