

Primteiler-Normalform

Korollar Primteiler-Normalform

Jede endlich erzeugte abelsche Gruppe G ist isomorph zu

$$\mathbb{Z}^r \times \prod_{j=1}^s \prod_{i=1}^{s_j} \mathbb{Z}/p_j^{r_{ji}}\mathbb{Z}$$

für geeignete $p_j \in \mathbb{P}$, $r, s \in \mathbb{N}_0$ und $s_j, r_{ji} \in \mathbb{N}$.

Die Zahl r sowie die $\mathbb{Z}/p_j^{r_{ji}}\mathbb{Z}$ sind bis auf Reihenfolge eindeutig.

Beweis:

- Wir wissen bereits, dass $G \cong \mathbb{Z}^r \times \prod_{i=1}^{\ell} \mathbb{Z}/n_i\mathbb{Z}$.
- Für $n_i = \prod_{j=1}^{\ell_i} p_j^{r_{ji}}$ folgt mit CRT

$$\mathbb{Z}/n_i\mathbb{Z} \cong \prod_{j=1}^{\ell_i} \mathbb{Z}/p_j^{r_{ji}}\mathbb{Z}.$$

- Umsortieren der Faktoren liefert die obige Normalform.
- Für den Beweis der Eindeutigkeit verweisen wir auf [MS,P].

Anmerkung: r heißt der *Rang* der Gruppe G .

Bsp zuvor liefert $G \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Elementarteiler

Korollar Elementarteiler-Normalform

Jede endliche erzeugte abelsche Gruppe G ist isomorph zu

$$\mathbb{Z}^r \times \prod_{i=1}^{\ell} \mathbb{Z}/n_i\mathbb{Z},$$

für geeignete $r \in \mathbb{N}_0$, $n_i \in \mathbb{N}$ mit $n_i > 1$ und $n_{i+1} | n_i$ für $i = 1, \dots, \ell - 1$. Die Zahlen n_i heißen *Elementarteiler* und sind eindeutig bestimmt.

Beweis:

- Wir wissen bereits, dass $G \cong \mathbb{Z}^r \times \prod_{j=1}^s \prod_{i=1}^{s_j} \mathbb{Z}/p_j^{r_{ji}}\mathbb{Z}$.
- Durch Umsortieren erreichen wir $r_{j1} \geq r_{j2} \geq \dots$ für jedes j .
- Wir definieren $n_i := \prod_{j=1}^s p_j^{r_{ji}}$ mit $r_{ji} = 0$ für $i > s_j$.
- Aus dem CRT folgt die Form $G \cong \mathbb{Z}^r \times \prod_{i=1}^{\ell} \mathbb{Z}/n_i\mathbb{Z}$.
- Die Eigenschaft $n_{i+1} | n_i$ folgt aus der Sortierung der r_{ji} , da jede Primpotenz von n_i von den Primpotenzen von n_{i+1} geteilt wird.
- Für die Eindeutigkeit verweisen wir wieder auf [MS,P].

Bsp zuvor liefert $G \cong \mathbb{Z} \times \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Bsp. Struktur der Einheitengruppe

Bsp: Struktur der Einheitengruppe U_n für kleine n

- $U_2 = \{\bar{1}\} \cong \{0\}$, kongruent zur trivialen Gruppe.
- $U_3 = \{\bar{1}, \bar{2}\} \cong \mathbb{Z}/2\mathbb{Z}$, $\bar{2}$ generiert U_3 .
- $U_4 = \{\bar{1}, \bar{3}\} \cong \mathbb{Z}/3\mathbb{Z}$, $\bar{3}$ generiert U_4 .
- $U_5 = \{\bar{1}, \bar{2}, \bar{4} = \bar{2}^2, \bar{3} = \bar{2}^3\} \cong \mathbb{Z}/4\mathbb{Z}$, $\bar{2}$ generiert U_5 .
- $U_6 = \{\bar{1}, \bar{5}\} \cong \mathbb{Z}/2\mathbb{Z}$, $\bar{5}$ generiert U_6 .
- $U_7 = \{\bar{1}, \bar{3}, \bar{2} = \bar{3}^2, \bar{6} = \bar{3}^3, \bar{4} = \bar{3}^4, \bar{5} = \bar{3}^5\} \cong \mathbb{Z}/6\mathbb{Z}$, $\bar{3}$ generiert U_6 .
- $U_8 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. $(\bar{3}, \bar{5})$ generieren U_8 , denn
 $3 \cdot 5 \equiv 7 \pmod{8}$ und $3^2 \equiv 1 \pmod{8}$.

Anmerkung:

- Sei g ein Erzeuger der Gruppe U_n .
- Der Isomorphismus $(\mathbb{Z}/\varphi(n)\mathbb{Z}, +) \cong (U_n, \cdot)$ ist gegeben durch

$$\exp: \mathbb{Z}/\varphi(n)\mathbb{Z} \rightarrow U_n \text{ mit } i + \varphi(n)\mathbb{Z} \mapsto g^i + n\mathbb{Z}.$$

Untergruppen endlicher Körper

Satz Untergruppen zyklischer Gruppen

Sei \mathbb{F} ein Körper. Jede endliche Untergruppe (G, \cdot) , $G \subseteq \mathbb{F}$ ist zyklisch.

Beweis:

- Da G endlich ist, ist G auch endlich erzeugt und besitzt Rang 0.
- Nach Klassifikationssatz für endl. erzeugte abelsche Gruppen gilt

$$G \cong \prod_{j=1}^s \prod_{i=1}^{s_j} \mathbb{Z}/p_j^{r_{ji}}\mathbb{Z} \text{ für } s, s_j, r_{ji} \in \mathbb{N}, p_j \in \mathbb{P}.$$

- Falls $s_j = 1$ für alle j , dann gilt nach CRT

$$G \cong \prod_{j=1}^s \mathbb{Z}/p_j^{r_{ji}}\mathbb{Z} \cong \mathbb{Z}/(\prod_{j=1}^s p_j^{r_{ji}})\mathbb{Z}.$$

- Da die rechte Seite zyklisch ist, ist auch G zyklisch.
- Bleibt zu zeigen, dass $s_j = 1$ für $j = 1, \dots, s$.

Untergruppen endlicher Körper

- Annahme: $s_j > 1$ für ein j , oBdA $s_1 > 1$.
- Wir betrachten die Untergruppe $H := \prod_{i=1}^{s_1} \mathbb{Z}/p_1^{r_{1i}}\mathbb{Z} \times 0 \subseteq G$.
- Sei $r := \max_i \{r_{1i}\}$. Es gilt $|H| = \prod_{i=1}^{s_1} p_1^{r_{1i}} > p_1^r$.
- Für alle $h \in H$ gilt $\text{ord}(h) \mid p_1^r$. Es folgt
$$h^{p_1^r} = 1 \text{ für alle } h \in H \subseteq G \subseteq \mathbb{F}.$$
- Damit sind alle $h \in H \subseteq \mathbb{F}$ Nullstellen von $X^{p_1^r} - 1$.
- Dies sind $|H| > p_1^r$ Nullstellen für ein Polynom vom Grad p_1^r .
(Widerspruch: In \mathbb{F} kann $X^{p_1^r} - 1$ nur max. p_1^r Nst. besitzen.)

U_p ist zyklisch.

Satz U_p ist zyklisch

Sei p prim. Dann ist $U_p = \mathbb{F}_p^*$ zyklisch, d.h. $U_p \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Beweis:

- Da \mathbb{F}_p ein endlicher Körper ist, ist $U_p \subseteq \mathbb{F}_p^*$ zyklisch.
- Wegen $|U_p| = p - 1$ folgt aus dem Isomorphiesatz für zyklische Gruppen (Folie 84), dass $U_p \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Definition Primitivwurzel

Ein $g \in \mathbb{Z}$, das U_n erzeugt, heißt *Generator* oder *Primitivwurzel* mod n .

Übung: Zeigen Sie: Es gibt $\varphi(\varphi(n))$ viele Primitivwurzeln modulo n .

Test auf Primitivwurzel

Ziel: Entscheide effizient, ob g eine Primitivwurzel ist.

Satz Test auf Primitivwurzel

Sei $p \in \mathbb{P}$. Ein $g \in \mathbb{Z}$, $g \not\equiv 0 \pmod{p}$ ist Primitivwurzel modulo p gdw

$$g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p} \text{ f\"ur alle Primteiler } q \text{ von } p-1.$$

Beweis:

\Rightarrow Sei g eine Primitivwurzel, d.h. $\text{ord}(g) = p-1$.

- Damit gilt $p-1 = \min\{i \in \mathbb{N} \mid g^i \equiv 1 \pmod{p}\}$. Es folgt

$$g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}, \text{ wegen } \frac{p-1}{q} < p-1.$$

\Leftarrow Aus Satz von Lagrange folgt $\text{ord}(g) \mid p-1$, d.h. $\text{ord}(g) \cdot c = p-1$.

- Annahme: $c > 1$. Dann besitzt c einen Primteiler q und es gilt

$$g^{\frac{p-1}{q}} \equiv g^{\text{ord}(g) \cdot \frac{c}{q}} = (g^{\text{ord}(g)})^{\frac{c}{q}} \equiv 1 \pmod{p}. \quad (\text{Widerspruch})$$

- Aus $c = 1$ folgt $\text{ord}(g) = p-1$.
- Damit ist g eine Primitivwurzel modulo p .

Liften von Lösungen

Ziel: Wir zeigen, dass U_{p^r} mit $p \in \mathbb{P} \setminus \{2\}$, $r \geq 2$ zyklisch ist.

Lemma

Sei $x \in \mathbb{Z}$. Für $p \in \mathbb{P} \setminus \{2\}$ und $r \geq 2$ gilt

$$x \equiv 1 \pmod{p^{r-1}} \Leftrightarrow x^p \equiv 1 \pmod{p^r}$$

Beweis:

\Rightarrow Sei $x \equiv 1 \pmod{p^{r-1}}$, d.h. $x = 1 + cp^{r-1}$ für ein $c \in \mathbb{Z}$. Es folgt

$$x^p = (1 + cp^{r-1})^p = 1 + pcp^{r-1} + \sum_{i=2}^p \binom{p}{i} c^i p^{(r-1)i}.$$

- Für $i, r \geq 2$ gilt $(r-1)i \geq 2(r-i) = r + (r-2) \geq r$.
- Damit folgt $x^p \equiv 1 \pmod{p^r}$.

Liften von Lösungen

Beweis: (Fortsetzung)

⇐ Wir zeigen $x^p \equiv 1 \pmod{p^r} \Rightarrow x \equiv 1 \pmod{p^{r-1}}$ per Induktion über r .

- **IA** für $r = 2$. Nach Kleinem Satz von Fermat gilt $x^p \equiv x \pmod{p}$.
- Aus $x^p \equiv 1 \pmod{p^2}$ folgt $x^p \equiv 1 \pmod{p}$ und damit $x \equiv 1 \pmod{p}$.
- **IS** $r \rightarrow r + 1$: Sei $x^p \equiv 1 \pmod{p^{r+1}}$.
- Es folgt $x^p \equiv 1 \pmod{p^r}$. Nach IV folgt damit $x \equiv 1 \pmod{p^{r-1}}$ bzw.
$$x = 1 + cp^{r-1} \text{ für ein } c \in \mathbb{Z}.$$
- Falls $p \mid c$, dann folgt die Behauptung $x \equiv 1 \pmod{p^r}$. Es gilt
$$1 \equiv x^p = (1 + cp^{r-1})^p = 1 + cp^r + \sum_{i=2}^p \binom{p}{i} c^i p^{(r-1)i} \pmod{p^{r+1}}.$$
- Wir wissen bereits, dass $p \mid \binom{p}{i}$ für $2 \leq i < p$.
- Damit enthält die Summe einen Term $p^{(r-1)i+1}$ mit
$$(r-1)i + 1 \geq 2(r-1) + 1 = r + 1 + (r-2) \geq r + 1.$$
- Für $i = p$ ist
$$(r-1)i = (r-1)p \geq 3(r-1) = r + 1 + 2(r-2) \geq r + 1.$$
- Damit erhalten wir $1 \equiv 1 + cp^r \pmod{p^{r+1}}$ bzw. $cp^r \equiv 0 \pmod{p^{r+1}}$.
- Es folgt $p \mid c$ wie gewünscht.