Zerlegung in Torsionsanteil und freien Anteil

Satz (5.5)

Ist G eine endlich erzeugte abelsche Gruppe, dann gibt es ein $r \in \mathbb{N}_0$ mit $G \cong \mathbb{Z}^r \times \mathrm{Tor}(G)$. Darüber hinaus ist $\mathrm{Tor}(G)$ eine endliche abelsche Gruppe.

Die $\mathbb{F}_p$-Vektorraumstruktur auf p-Torsionsgruppen

Lemma (5.6)

(i) Sei G eine abelsche Gruppe, seien $s \in \mathbb{N}_0$, $m_1, ..., m_s \in \mathbb{N}$ und $g_1, ..., g_s \in G$ mit $\text{ord}(g_i) \mid m_i$ für $1 \leq i \leq s$. Sei $U = \langle g_1, ..., g_s \rangle$. Dann gibt es einen surjektiven Gruppenhomomorphismus $\phi : \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_s\mathbb{Z} \to U$ mit

$$\phi(\bar{a}_1, ..., \bar{a}_s) = a_1 g_1 + ... + a_s g_s \qquad \text{für alle } a_1, ..., a_s \in \mathbb{Z}.$$

(ii) Ist G eine abelsche Gruppe mit $G[p] = G$, dann gibt es eine Abbildung $\cdot : \mathbb{F}_p \times G \to G$ mit $\bar{a} \cdot g = ag$ für alle $a \in \mathbb{Z}$ und $g \in G$. Mit dieser Abbildung wird auf G die Struktur eines $\mathbb{F}_p$-Vektorraums definiert.

Zerlegung der Torsionsgruppen

Satz (5.7)

Sei G eine abelsche Gruppe.

(i) Sind $m, n \in \mathbb{N}$ teilerfremd, dann gilt $G[mn] \cong G[m] \times G[n]$.

(ii) Sei $n \in \mathbb{N}$ mit $G[n] = G$, und sei $n = \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung von n, mit $r \in \mathbb{N}_0$, Primzahlen $p_1, ..., p_r$ und Exponenten $e_1, ..., e_r \in \mathbb{N}$. Dann besteht ein Isomorphismus $G \cong G[p_1^{e_1}] \times ... \times G[p_r^{e_r}]$.

Als Chinesischer Restsatz bekannt ist die Aussage

Satz (5.8)

Sind $m, n \in \mathbb{N}$ teilerfremd, dann existiert ein Isomorphismus $\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ abelscher Gruppen.

Beweis von Satz 5.7, Teil (ii)

Beweis durch vollständige Induktion über die Anzahl $r \in \mathbb{N}_0$ der Faktoren in der Primfaktorzerlegung von n.

Ind.-Anf. $r = 0$ Dann ist $n = 1$ und G ist darstellbar durch ein Produkt von null Faktoren. Wenn wir ein solches Produkt als triviale Gruppe $\{e_G\}$ interpretieren, denn aus $G[1] = G$ folgt $G = \{e_G\}$.

ein solches Produkt als triviale Gruppe hat

Ind-schritt $r \longmapsto r+1$:

Ann.: n hat eine Primfaktorzerlegung der Form

$$n = \prod_{j=1}^{r+1} p_j^{e_j}$$ Nach Voraussetzung gilt

$G[n] = G$. Die Zahlen $m = \prod_{j=1}^{r} p_j^{e_j}$ und $p_{r+1}^{e_{r+1}}$ sind teilfremd, also gilt $G = G[n] \cong G[m] \times G[p_{r+1}^{e_{r+1}}]$ (*) nach Teil (i). Nach Induktionsvoraussetzung gilt außerdem $G[m] \cong G[p_1^{e_1}] \times \ldots \times G[p_r^{e_r}]$. Einsetzen in (*) liefert die gewünschte Aussage. □

Beweis von Satz 5.8:

Ansatz: Wende Satz 5.7 auf $G = (\mathbb{Z}/mn\mathbb{Z}, +)$ an.
Wegen $|G| = mn$ gilt $G[mn] = G$ (jede Elementordn. in G ist ein Teiler von mn.) Satz 5.7 $\Rightarrow G[mn] \cong G[m] \times G[n]$. Es genügt also z.zg: $G[m] \cong \mathbb{Z}/m\mathbb{Z}$ und $G[n] \cong \mathbb{Z}/n\mathbb{Z}$, gleichbedeutend: $G[m]$ ist zykl. von Ordnung m, $G[n]$ ist zykl. von Ordnung n. zeige dafür: $G[m] = \langle n + mn\mathbb{Z} \rangle$
(Der Beweis $G[n] = \langle m + mn\mathbb{Z} \rangle$ läuft analog)

(Der Beweis $G[n] = \langle m + mn\mathbb{Z} \rangle$ läuft analog.)

„$\supseteq$" genügt: $n + mn\mathbb{Z} \in G[m]$ Dies ist der Fall, denn $m \cdot (n + mn\mathbb{Z}) = mn + mn\mathbb{Z} = 0 + mn\mathbb{Z} = 0_G$.

„$\subseteq$" Sei $a + mn\mathbb{Z} \in G[m]$, mit $a \in \mathbb{Z}$. $\Rightarrow m(a + mn\mathbb{Z}) = 0_G = 0 + mn\mathbb{Z} \Rightarrow ma + mn\mathbb{Z} = mn\mathbb{Z} \Rightarrow ma \in mn\mathbb{Z}$
$\Rightarrow mn \mid ma \Rightarrow n \mid a \Rightarrow \exists k \in \mathbb{Z}$ mit $a = kn \Rightarrow$
$a + mn\mathbb{Z} = kn + mn\mathbb{Z} = k \cdot (n + mn\mathbb{Z}) \in \langle n + mn\mathbb{Z} \rangle$

Wegen $\operatorname{ord}(1 + mn\mathbb{Z}) = mn$ gilt $\operatorname{ord}(n + mn\mathbb{Z}) = \operatorname{ord}(n \cdot (1 + mn\mathbb{Z})) = \frac{mn}{n} = m$.

□

[additive Potenz: $m \cdot g = \underbrace{g + \cdots + g}_{m\text{-mal}}$]

Zerlegung einer abelschen p^e-Torsionsgruppe

Satz (5.9)

Sei $e \in \mathbb{N}_0$, p eine Primzahl und G eine endliche abelsche Gruppe mit $G[p^e] = G$. Dann gibt es ein $r \in \mathbb{N}_0$ und $n_1, ..., n_r \in \mathbb{N}$, so dass

$$G \quad \cong \quad \mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r}\mathbb{Z} \qquad \text{gilt.}$$

Beweis:

- Der Beweis erfolgt durch vollständige Induktion über e. Im Fall $e = 0$ ist $G = \{0_G\}$ und die Aussage offensichtlich.
- Im Induktionsschritt betrachten wir die Gruppe $H = pG$ mit $H[p^{e-1}] = H$. Nach Induktionsvoraussetzung existiert ein Isomorphismus

$$\phi : \mathbb{Z}/p^{n_1}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r}\mathbb{Z} \to H.$$

Beweis von Satz 5.9 (Forts.)

- Es seien $h_1, ..., h_r \in H$ die Bilder der „Einheitsvektoren“ $(\bar{1}, \bar{0}, ...)$, $(\bar{0}, \bar{1}, ...)$ usw. in H. Wegen $pG = H$ existiert jeweils ein $g_j \in G$ mit $pg_j = h_j$.
- Zeige mit Hilfe von Lemma 5.6 (i), dass $U = \langle g_1, ..., g_r \rangle$ isomorph zur Gruppe

$$\mathbb{Z}/p^{n_1+1}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r+1}\mathbb{Z} \quad \text{ist.}$$

- Nach Lemma 5.6 (ii) ist $G[p]$ ein $\mathbb{F}_p$-Vektorraum, und $G[p] \cap U$ ist ein Untervektorraum. Wähle eine Basis $\{v_1, ..., v_s\}$ von $G[p] \cap U$ und erweitere diese durch $v_{s+1}, ..., v_t$ zu einer Basis von $G[p]$.
- Setze $V = \langle v_{s+1}, ..., v_t \rangle$. Überprüfe nun, dass $G = U \oplus V$ gilt. Daraus folgt dann

$$G \cong U \times V \cong \mathbb{Z}/p^{n_1+1}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r+1}\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^{t-s}.$$

Beweis von Satz 5.9 (Forts.)

- Für den Nachweis von $U \cap V = \{0_G\}$ beachte zunächst, dass die Menge links wegen $V \subseteq G[p]$ mit $(U \cap G[p]) \cap V$ übereinstimmt. Die Aussage folgt nun aus der Tatsache, dass $G[p]$ als $\mathbb{F}_p$-Vektorraum gleich der direkten Summe $(U \cap G[p]) \oplus V$ ist, auf Grund der Definition von V durch Basisergänzung.

- Zum Nachweis von $U + V = G$ sei $g \in G$ vorgegeben. Stelle pg durch die Erzeuger h_j von pG dar. Definiere damit ein $g' \in U$ mit $pg' = pg$, und setze $g'' = g - g'$. Überprüfe, dass $g'' \in G[p]$ liegt. Daraus folgt $g'' \in U + V$, denn die Basis von $G[p]$ als $\mathbb{F}_p$-Vektorraum setzt sich aus Elementen von U und V zusammen.

Beweis von Satz 5.9 (Forts.)

- genauere Ausführung des letzten Punkts:

  Das Element pg hat die Form $\sum_{j=1}^{r} a_j h_j$ mit $a_1, ..., a_r \in \mathbb{Z}$. Setzen wir $g' = \sum_{j=1}^{r} a_j g_j$, dann folgt aus $pg_j = h_j$ für $1 \leq j \leq r$ die Gleichung $pg' = pg$. Für das Element g'' folgt damit

$$pg'' = pg - pg' = \left(\sum_{j=1}^{r} a_j h_j\right) - p\left(\sum_{j=1}^{r} a_j g_j\right) =$$

$$\left(\sum_{j=1}^{r} a_j h_j\right) - \left(\sum_{j=1}^{r} a_j pg_j\right) = \left(\sum_{j=1}^{r} a_j h_j\right) - \left(\sum_{j=1}^{r} a_j h_j\right) = 0_G.$$

  Also liegt g'' in $G[p]$.

Hauptsatz über endlich erzeugte abelsche Gruppe

Satz (5.10)

Sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es $r, s \in \mathbb{N}_0$ und $d_1, ..., d_s \in \mathbb{N}$ mit

$$G \quad \cong \quad \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_s\mathbb{Z}.$$

Dabei können die Zahlen d_i so gewählt werden, dass sie entweder

(i) alle Primzahlpotenzen sind oder

(ii) $d_i \mid d_{i+1}$ für $1 \leq i < s$ erfüllt ist.

Im Fall (ii) gezeichnet man die Zahlen d_i als Elementarteiler der abelschen Gruppe.

Beweis von Satz 5.10:

zu (i) geg.: endlich erzeugte abelsche Gruppe G

Satz 5.5 $\Rightarrow$ $G \cong \mathbb{Z}^r \times \mathrm{Tor}(G)$ für ein $r \in \mathbb{N}_0$,

und $\mathrm{Tor}(G)$ ist eine endliche Gruppe

Sei $m = |\mathrm{Tor}(G)|$ und $m = \prod_{j=1}^{r} p_j^{e_j}$ die Primfaktor-

zerlegung von m. Satz 5.7 (ii) $\Rightarrow$

$$\mathrm{Tor}(G) = \mathrm{Tor}(G)[m] = \prod_{j=1}^{r} \mathrm{Tor}(G)[p_j^{e_j}]$$

$\uparrow$ $m = |\mathrm{Tor}(G)|$

und $\mathrm{Tor}(G)$ ist eine endliche Gruppe

Sei $m = |\mathrm{Tor}(G)|$ und $m = \prod_{j=1}^{r} p_j^{c_j}$ die Primfaktor-

Satz 5.9 $\rightsquigarrow$ $\mathrm{Tor}(G)[p_j^{c_j}]$ ist isomorph zu einem Produkt zyklischer Gruppen von p_j-Potenzordnung, d.h. zu Produkt von Gruppen der Form $\mathbb{Z}/p_j^k\mathbb{Z}$ mit $k \in \mathbb{N}$ $(1 \le j \le r)$

Setzen wir dies ein, so erhalten wir eine Darstellung wie in Teil (i) von Satz 5.10 angegeben.

zu (ii) Nach Teil (i) gilt $G \cong \mathbb{Z}^r \times \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_s^{e_s}$ (*)

für geeignete $r \in \mathbb{N}_0$, Primzahlen $p_1, \dots, p_s$, $e_1, \dots, e_s \in \mathbb{N}$ (wobei $p_i = p_j$ für $i \neq j$ möglich). Folgendermaßen erhält man eine Darstellung von G wie in (ii) angegeben (genauer Beweis siehe Skript): Für jede Primzahl $p \in \{p_1, \dots, p_s\}$ wähle jeweils in

(*) den Faktor mit dem größten Exponenten $\mathbb{Z}/p^k\mathbb{Z}$. Fasse diese Faktoren zu einem neuen Produkt $H = \mathbb{Z}/q_1^{f_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/q_t^{f_t}$ (mit $t \leq s$) zusammen. (*) Auf die übrigen Faktoren wende dasselbe Verfahren wieder an, bis keine Faktoren mehr übrig sind. Dies liefert die Zerlegung wie in (ii) angegeben

(*) Da die Primzahlen $q_1, \ldots, q_t$ verschieden sind, sind die Faktoren $q_i^{f_i}$ paarweise teilerfremd. Der Chinesische Satz sagt somit, dass H zyklisch ist.

Beispiel: Aufzählung aller abelschen Gruppen der Ordnung 100 $(= 2^2 \cdot 5^2)$

- nach Teil (i) von Satz 5.10
  mögliche Darstellungen von 100 als Produkt von Primzahlpotenzen:

$$100 = 2^2 \cdot 5^2 = 2 \cdot 2 \cdot 5^2 = 2^2 \cdot 5 \cdot 5$$
$$= 2 \cdot 2 \cdot 5 \cdot 5$$

Satz 5.10 (i) $\Rightarrow$ Jede abelsche Gruppe der Ordnung 100 ist isomorph zu einer der Gruppen

$G_1 = \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z}$, $G_2 = (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/5^2\mathbb{Z}$

$G_3 = \mathbb{Z}/2^2\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^2$, $G_4 = (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/5\mathbb{Z})^2$

- nach Teil (ii) von Satz 5.10:
  Wende das im Beweis beschriebene Verfahren an, um die Gruppen $G_1, \ldots, G_4$ auf die Gestalt von 5.10 (ii) zu bringen.
  (1) für G_1: erhalte als ersten Faktor $H = \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z}$
  Chin. Restsatz $\Rightarrow H \cong \mathbb{Z}/100\mathbb{Z}$
  Also ist G_1 isomorph zu $H_1 = \mathbb{Z}/100\mathbb{Z}$.
  (2) für G_2: erhalte als ersten Faktor
  $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z} \cong \mathbb{Z}/50\mathbb{Z}$
  Der Faktor $\mathbb{Z}/2\mathbb{Z}$ bleibt übrig.
  Also ist G_2 isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$

(3) für G_3: erhalte als ersten Faktor

$$H = \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/20\mathbb{Z}$$

Übrig bleibt der Faktor $\mathbb{Z}/5\mathbb{Z}$.

$\Rightarrow$ G_3 ist isomorph zu $H_3 = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$

(4) für G_4: erhalte als ersten Faktor

$$H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/10\mathbb{Z}$$

Übrig bleiben die Faktoren $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/5\mathbb{Z}$.

Das Produkt der Faktoren ist wieder isom. zu $\mathbb{Z}/10\mathbb{Z}$.

$\Rightarrow$ G_4 ist isomorph zu $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.

Ergebnis hier: Jede abelsche Gruppe der Ordnung 100 ist isomorph zu eines der Gruppen $H_1 = \mathbb{Z}/100\mathbb{Z}$, $H_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$, $H_3 = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$, $H_4 = \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.

Proposition (6.1)

Sei G eine Gruppe, N ein Normalteiler und U eine Untergruppe von G. Dann ist jedem $u \in U$ durch $\tau_u(n) = unu^{-1}$ ein Automorphismus von N zugeordnet. Die Abbildung

$$\phi : U \to \mathrm{Aut}(N), \quad u \mapsto \tau_u$$

ist ein Homomorphismus von Gruppen.

Beweis von Proposition 6.1

Wegen $N \trianglelefteq G$ gilt $unu^{-1} \in N \quad \forall n \in N, u \in U$. Dies zeigt, dass jedes τ_u eine Abbildung $N \to N$ ist.

noch zu überprüfen:

(1) Jedes τ_u ist ein Automorphismus von N.

(2) $\phi: U \to \mathrm{Aut}(N), \; u \mapsto \tau_u$ ist ein Gruppenhom.

zu (1) Sei $u \in U$. Hom.-Eig. von τ_u: Seien $n, n' \in N$.

Dann gilt $\tau_u(nn') = u(nn')u^{-1} = unen'u^{-1} =$

$unu^{-1}un'u^{-1} = \tau_u(n)\tau_u(n')$.

Nachrechnen ergibt außerdem, dass $\tau_{u^{-1}}$ jeweils eine

zu (1) Sei $u \in U$. Hom.-Eig. von τ_u: Seien $n, n' \in N$.

Umkehrabb. von τ_u ist, d.h. $\tau_{u^{-1}} \circ \tau_u = \tau_u \circ \tau_{u^{-1}} = id_N$.

Daraus folgt, dass jedes τ_u bijektiv ist.

zu (2) Seien $u, u' \in U$. z.zg. $\phi(uu') = \phi(u) \circ \phi(u')$

gleichbedeutend: $\tau_{uu'} = \tau_u \circ \tau_{u'}$

Tatsächlich gilt für jedes $n \in N$ jeweils

$$\tau_{uu'}(n) = (uu')\, n\, (uu')^{-1} = uu' n (u')^{-1} u = u\, \tau_{u'}(n)\, u^{-1}$$

$$= \tau_u(\tau_{u'}(n)) = (\tau_u \circ \tau_{u'})(n)$$

□