Definition innerer direkter Produkte

Definition (8.1)

Sei G eine Gruppe, und seien U, N Untergruppen von G.

- Wir bezeichnen G als inneres direktes Produkt von U und N, wenn U und N beides Normalteiler von G sind und $G = UN$ sowie $U \cap N = \{e\}$ gilt.
- Ist lediglich N eine Normalteiler von G, aber nicht notwendigerweise die Untergruppe U, dann spricht man von einem inneren semidirekten Produkt.

Innere und äußere direkte Produkte

Proposition (8.2)

Sei G eine Gruppe und inneres direktes Produkt ihrer Untergruppen U und N. Dann gilt

$$G \cong U \times N.$$

Man nennt $U \times N$ auch das äußere direkte Produkt von U und N.

Definition der Torsionsuntergruppen

Definition (8.4)

Sei G eine abelsche Gruppe und $m \in \mathbb{N}$.

(i) Man nennt $G[m] = \{g \in G \mid mg = 0_G\}$ die *m-Torsionsuntergruppe* von G.

(ii) Die Teilmenge $\mathrm{Tor}(G) = \bigcup_{n \in \mathbb{N}} G[n]$ wird die *Torsionsuntergruppe* von G genannt.

Zerlegung in Torsionsanteil und freien Anteil

Satz (8.7)

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 (8.8)

(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 $\mathrm{ord}(g_i) \mid m_i$ für $1 \le i \le s$. 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

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

(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.

$\ldots_{(a_1,\dots,a_s)}$ $\quad \varphi_{(a_1,\dots,a_s)}(a_{s+1})$

Beweis von Lemma 8.8. G abelsche Gruppe

zu (i) geg.: $s \in \mathbb{N}$, $m_1, \dots, m_s \in \mathbb{N}$, $g_1, \dots, g_s \in G$
mit $\mathrm{ord}(g_i) \mid m_i$ für $1 \leq i \leq s$, $U = \langle g_1, \dots, g_s \rangle$

Beh.: Es gibt eine Abb. $\phi : \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_s\mathbb{Z} \to U$ mit $\phi(\bar{a}_1, \dots, \bar{a}_s) = a_1 g_1 + \dots + a_s g_s$

Bew. durch vollständige Ind. über s

$s = 0$ nichts z.zg., beide Gruppen sind trivial
definiere $\phi : \{\bar{0}\} \to \{e_G\}$ durch $\phi(\bar{0}) = e_G$

Ind-schritt $s \mapsto s+1$: geg. $g_1, \dots, g_{s+1}$, $m_1, \dots, m_{s+1} \in \mathbb{N}$

$\operatorname{ord}(g_i) \mid m_i$ für $1 \leq i \leq s+1$ $\quad U = \langle g_1, \ldots, g_{s+1} \rangle$

Ind.-V. $\Rightarrow \exists$ Abb. $\psi : \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_s\mathbb{Z} \to U$ mit

$\psi(\bar{a}_1, \ldots, \bar{a}_s) = a_1 g_1 + \cdots + a_s g_s$

Sei $(a_1, \ldots, a_s) \in \mathbb{Z}^s$ vorgeg., betrachte die Abb. $\psi : \mathbb{Z} \to U$

$\hat{\phi}_{(\bar{a}_1, \ldots, \bar{a}_s)}(a_{s+1}) = \psi(\bar{a}_1, \ldots, \bar{a}_s) + a_{s+1} g_{s+1}$

Sind $a_{s+1}, a_{s+1}' \in \mathbb{Z}$ mit $a_{s+1} \equiv a_{s+1}' \bmod m_{s+1}$.

$\Rightarrow \exists k \in \mathbb{Z} : a_{s+1}' = a_{s+1} + k m_{s+1} \Rightarrow$

$a_{s+1}' g_{s+1} = (a_{s+1} + k m_{s+1}) g_{s+1} = a_{s+1} g_{s+1} + k(m_{s+1} g_{s+1})$

$= a_{s+1} g_{s+1} + k \cdot 0_G = a_{s+1} g_{s+1} \Rightarrow \hat{\phi}_{(a_1, \ldots, a_s)}(a_{s+1}) = \hat{\phi}_{(a_1, \ldots, a_s)}(a_{s+1}')$

$\operatorname{ord}(g_{s+1}) \mid m_{s+1}$

Satz 3.10 von der induzierten Abb.

$$\Rightarrow \exists\, \phi_{(\bar{a}_1,\dots,\bar{a}_s)} : \mathbb{Z}/m_{s+1}\mathbb{Z} \to U,$$

mit $\phi_{(\bar{a}_1,\dots,\bar{a}_s)}(\bar{a}_{s+1}) = \hat{\phi}_{(\bar{a}_1,\dots,\bar{a}_s)}(a_{s+1})$

$$= \psi(\bar{a}_1,\dots,\bar{a}_s) + a_{s+1} g_{s+1}$$

$$= a_1 g_1 + \dots + a_s g_s + a_{s+1} g_{s+1} \quad (*)$$

Definiere nun $\phi : \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_{s+1}\mathbb{Z} \to U$ durch $\phi(\bar{a}_1,\dots,\bar{a}_s,\bar{a}_{s+1}) =$

$$\phi_{(\bar{a}_1,\dots,\bar{a}_s)}(\bar{a}_{s+1}) = (*) \quad (\Rightarrow \text{Beh.})$$

Zeige noch, dass ϕ ein surjektiver Gruppen-homomorphismus ist. Seien $a_1, \ldots, a_s$, $b_1, \ldots, b_s \in \mathbb{Z}$. Dann gilt

$$\phi((\bar{a}_1, \ldots, \bar{a}_s) + (\bar{b}_1, \ldots, \bar{b}_s)) =$$

$$\phi(\bar{a}_1 + \bar{b}_1, \ldots, \bar{a}_s + \bar{b}_s) =$$

$$\phi(\overline{a_1 + b_1}, \ldots, \overline{a_s + b_s}) =$$

$$(a_1 + b_1) g_1 + \cdots + (a_s + b_s) g_s \overset{\text{Potenzgesetze in abelschen Gruppen}}{=}$$

$$a_1 g_1 + \ldots + a_s g_s + b_1 g_1 + \ldots + b_s g_s =$$

$$\phi(\bar{a}_1, \ldots, \bar{a}_s) + \phi(\bar{b}_1, \ldots, \bar{b}_s)$$

)

(*)

$/m_{s+1}\mathbb{Z}$

=

Beh.)

Surjektivität: Nach § 2 ist $U = \langle g_1, \dots, g_s \rangle$
$= \{ a_1 g_1 + \dots + a_s g_s \mid a_1, \dots, a_s \in \mathbb{Z} \}$ also:
$g_1^{a_1} \circ \dots \circ g_s^{a_s}$

Ist $u \in U$, dann gibt es $a_1, \dots, a_s \in \mathbb{Z}$ mit
$u = a_1 g_1 + \dots + a_s g_s = \phi(\bar{a}_1, \dots, \bar{a}_s)$

<u>zu (ii)</u> Vor: p Primzahl mit $G[p] = G$, d.h.
$pg = 0_G \ \forall g \in G$, d.h. $\mathrm{ord}(g) \mid p \ \forall g \in G$.

Wiederum zeigt man mit Satz 3.10, dass eine
Abb. $\cdot : \mathbb{F}_p \times G \to G$ mit $\bar{a} \cdot g = ag \ \forall a \in \mathbb{Z}, g \in G$
existiert. Überprüfe für $(G, +, \cdot)$ die Vektorraum-Axiome. $(G, +)$ abelsche Gruppe: erfüllt n. V.

gen-

esetze
belschen
ppen

außerdem noch zu überprüfen $\forall \bar{a}, \bar{b} \in \mathbb{F}_p,\ g, h \in G$

(i) $(\bar{a}+\bar{b})\cdot g = \bar{a}\cdot g + \bar{b}\cdot g$

(ii) $\bar{a}\cdot(g+h) = \bar{a}\cdot g + \bar{a}\cdot h$

(iii) $\bar{a}\cdot(\bar{b}\cdot g) = (\bar{a}\bar{b})\cdot g$

(iv) $\bar{1}\cdot g = g$

Seien $\bar{a} = a + p\mathbb{Z},\ \bar{b} = b + p\mathbb{Z} \in \mathbb{F}_p$ (mit $a, b \in \mathbb{Z}$) und $g, h \in G$

zu (i) $(\bar{a}+\bar{b})\cdot g = \overline{a+b}\cdot g = (a+b)g \overset{\text{Potenzg. in } (G,+)}{=} ag + bg = \bar{a}\cdot g + \bar{b}\cdot g$

zu (ii) $\bar{a}\cdot(g+h) = a(g+h) = \underset{\uparrow \text{ multiplikativ: } (gh)^a = g^a h^a}{ag + ah} = \bar{a}\cdot g + \bar{a}\cdot h$

zu (ii) „$\supseteq$" klar „$\subseteq$" Sei $g \in G[m] \cap G[n] \Rightarrow mg = ng = 0_G$

zu (iii) $\bar{a} \cdot (\bar{b} \cdot g) = \bar{a} \cdot (bg) = a(b g) = (ab) g$
↑ Potenzgesetze
$= \overline{ab}\, g = (\bar{a} \cdot \bar{b}) \cdot g$

zu (iv) $\bar{1} \cdot g = 1 \cdot g = g$ $\square$

Zerlegung der Torsionsgruppen

Satz (8.9)

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 ist $G \cong G[p_1^{e_1}] \times ... \times G[p_r^{e_r}]$.

Beweis von Lemma 8.9, nur (i)

geg.: abelsche Gruppe G, $m, n \in \mathbb{N}$ teilerfremd

__Beh__: $G[mn] \cong G[m] \times G[n]$

genügt z.zg.: $G[mn]$ ist inneres direktes Produkt von $G[m]$ und $G[n]$ überprüfe: (i) $G[m], G[n] \trianglelefteq G[mn]$

(ii) $G[m] \cap G[n] = \{0_G\}$ (iii) $G[mn] = G[m] + G[n]$

__zu (i)__ $G[m] \leq G[mn]$, denn: $g \in G[m] \Rightarrow mg = 0_G \Rightarrow mng = nmg = n \cdot 0_G = 0_G \Rightarrow g \in G[mn]$ ebenso: $G[n] \leq G[mn]$

Da $G[m], G[n]$ Untergr. von G sind, sind sie auch Untergr. von $G[mn]$, sogar Normalteiler, da G abelsch.

__zu (ii)__ „$\supseteq$" klar „$\subseteq$" Sei $g \in G[m] \cap G[n] \Rightarrow mg = ng = 0_G$

„$\supseteq$" klar „$\subseteq$" Sei $g \in G[m] \cap G[n] \Rightarrow mg = ng = 0_G$

Lemma von Bézout $\Rightarrow \exists\, k, l \in \mathbb{Z}$ mit $km + ln = \mathrm{ggT}(m,n) = 1$

$\Rightarrow g = 1 \cdot g = (km + ln) \cdot g = k \cdot mg + l \cdot ng = k\, 0_G + l\, 0_G = 0_G$

zu (iii) „$\supseteq$" klar, da $G[m], G[n] \subseteq G[mn]$, $G[mn] \leq G$

„$\subseteq$" Sei $g \in G[mn] \Rightarrow mng = 0_G$. s.o. $\Rightarrow g = \underbrace{kmg}_{g'} + \underbrace{lng}_{g''}$

falls $km + ln = 1$. Dann gilt $mg'' = m \cdot lng = l \cdot (mng) \underset{[g \in G[mn]]}{=} l \cdot 0_G = 0 \Rightarrow g'' \in G[m]$, ebenso $g' \in G[n]$

insgesamt: $g = g'' + g' \in G[m] + G[n]$. $\square$

Der Chinesische Restsatz

Satz (8.10)

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.

Zerlegung einer endlichen abelschen Gruppe in zyklische Grupen

Satz (8.11)

Sei $e \in \mathbb{N}_0$, p eine Primzahl und G eine endliche abelsche Gruppe mit $G[p^e] = G$. Dann gibt es ein $r \in N_0$ 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 von Satz 8.11: (Skizze)

geg: endliche abelsche Gruppe G, $e \in \mathbb{N}$, p Primzahl

mit $G = G[p^e]$

z.zg: $\exists\, r \in \mathbb{N}_0$ und $n_1, \dots, n_r \in \mathbb{N}$ mit

$$G \cong \mathbb{Z}/p^{n_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{n_r}\mathbb{Z}$$

Beweis durch vollständige Induktion über $e \in \mathbb{N}_0$

$\underline{n=0}$ $G = G[p^0] = G[1] \Rightarrow G = \{0_G\}$

nichts zu zeigen (setze $r=0$)

Ind.-Schritt: $e \mapsto e+1$ Vor: $G[p^{e+1}] = G$

Betrachte $H = pG = \{pg \mid g \in G\}$

Dann gilt $H[p^e] = H$ Ind-V. angewendet auf H

$\Rightarrow \exists\, r \in \mathbb{N}_0,\ n_1, \dots, n_r \in \mathbb{N}$ mit $H \cong \mathbb{Z}/p_1^{n_1} + \dots + \mathbb{Z}/p_r^{n_r}$

Seien $h_1, \dots, h_r \in H$ die Urbilder der „Einheitsvektoren“ in $\mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{n_r}\mathbb{Z}$, also von $(\bar{1}, \bar{0}, \dots, \bar{0}), \dots$

Dann gilt $H = \langle h_1, \dots, h_r \rangle$ (weil die „Einheitsvektoren“ die Gruppe rechts erzeugen). $h_j \in H,\ H = pG \Rightarrow \exists\, g_j \in G$ mit $p g_j = h_j$ für $1 \leq j \leq r$

Setze $V = \langle g_1, \dots, g_r \rangle$, überprüfe:

$$V \cong \mathbb{Z}/p_1^{n_1+1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{n_r+1}\mathbb{Z}$$

siehe Satz 8.9 (ii)

Betrachte nun den $\mathbb{F}_p$-Vektorraum $G[p]$. Ergänze eine

Basis des Untervektorraums $G[p] \cap V$ zu einer Basis von $G[p]$, durch gewisse Elemente $g_{r+1}, \ldots, g_s \in G[p]$.

Setze $U = \langle g_{r+1}, \ldots, g_s \rangle$. Auf Grund der $\mathbb{F}_p$-Vektorraum-Struktur gilt

$$U \cong \mathbb{F}_p^{s-r} = (\mathbb{Z}/p\mathbb{Z})^{s-r}$$

Überprüfe nun, dass G inneres direktes Produkt von U und V ist $\longrightarrow$

$$G \cong V \times U \cong \mathbb{Z}/p^{n_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{n_r}\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^{s-r}$$

$\square$

Hauptsatz über endlich erzeugte abelsche Gruppe

Satz (8.12)

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

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

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.

__Beispiel__: Klassifikation der abelschen Gruppen der Ordnung 100 bis auf Isomorphie, mit Satz 8.12

$100 = 2^2 \cdot 5^2 \Rightarrow$ Möglichkeiten, 100 als Produkt von Primzahlpotenzen >1 zu schreiben: $4 \cdot 25$, $2 \cdot 2 \cdot 25$, $4 \cdot 5 \cdot 5$, $2 \cdot 2 \cdot 5 \cdot 5$. Satz 8.12 (i) $\Rightarrow$ Jede abelsche Gruppe der Ordnung 100 ist isomorph zu einer der Gruppen

$$G_1 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}, \quad G_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$$

$$G_3 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, \quad G_4 = (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/5\mathbb{Z})^2$$

Satz 8.12 (ii) $\Rightarrow$ Jede abelsche Gruppe der Ordnung 100 ist isomorph zu einer der Gruppen

$H_1 = \mathbb{Z}/100\mathbb{Z}$, $H_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$,

$H_3 = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$, $H_4 = \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$

(Nach dem Chin. Restsatz gilt $G_1 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$

$\cong \mathbb{Z}/100\mathbb{Z} = H_1$ wg $\mathrm{ggT}(4,25) = 1$. genauso:

$G_2 \cong H_2$, $G_3 \cong H_3$, $G_4 \cong H_4$.)

Anhand der Elementordnungen kann man erkennen, dass H_1, H_2, H_3, H_4 paarweise <u>nicht-isomorph</u> sind. Deshalb muss dasselbe für G_1, G_2, G_3, G_4 gelten.