Gruppentheorie II

von Nicole Drüke

Abelsche Gruppen

DEFINITION „Multiplikative und Additive Gruppe“

Sei A eine abelsche Gruppe mit $x \in A$, dieses wird erzeugt durch $a_1, ..., a_n \in A$

$$x = a_1^{\alpha_1} * ... * a_n^{\alpha_n} \qquad \text{für} \quad \alpha_1, .., \alpha_n \in \mathbb{Z}$$

dann nennt man A in diesem Fall multiplikative Gruppe.

$$x = \alpha_1 a_1 + ... + \alpha_n a_n \qquad \text{für} \quad \alpha_1, ..., \alpha_n \in \mathbb{Z}$$

dann nennt man A in diesem Fall additive Gruppe.

DEFINITION „Zyklische Gruppen“

Eine Gruppe G heißt zyklisch, falls ein $b \in G$ existiert mit

$$G = \{ b^n | n \in \mathbb{Z} \}$$

b heißt Erzeuger oder erzeugendes Element von G.

Bemerkung

Jede zyklische Gruppe ist abelsch aber nicht jede abelsche Gruppe ist zyklisch.

Beispiele

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(0,0);(0,1);(1,0);(1,1)\}$ ist eine abelsche Gruppe aber keine zyklische Gruppe. Man findet kein Element welches die Menge $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ erzeugt.

$\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0,0);(0,1);(0,2);(1,0);(1,1);(1,2)\}$ ist eine zyklische Gruppe die erzeugt wird durch das Element $(1,1)$ d.h.

$(1,1)+(1,1)=(0,2)$;
$(1,1)+(1,1)+(1,1)=(1,0)$;
$(1,1)+(1,1)+(1,1)+(1,1)=(0,1)$;
$(1,1)+(1,1)+(1,1)+(1,1)+(1,1)=(1,2)$;
$(1,1)+(1,1)+(1,1)+(1,1)+(1,1)+(1,1)=(0,0)$,
$(1,1)+(1,1)+(1,1)+(1,1)+(1,1)+(1,1)+(1,1)=(1,1)$

DEFINITION „tA Untergruppe“

Sei A eine Gruppe. Wir bezeichnen mit tA die Untermenge von A, die aus endlichen Elementen besteht.

Präposition 1

Es sei A eine abelsche Gruppe, dann ist die Teilmenge tA eine Untergruppe mit Elementen die endliche Ordnung haben.

Die Untergruppe tA wird als Torsionsuntergruppe von A genannt.

DEFINITION „freie abelsche Gruppe“

Eine abelsche Gruppe A heißt freie abelsche Gruppe, wenn ein $a_1,\dots,a_n\in A$ existiert, so dass

1. $\forall a \;\; \exists\, \alpha_1,\dots,\alpha_n\in\mathbb{Z},\;\; a=\alpha_1 a_1+\dots+\alpha_n a_n$
2. *Diese Darstellung ist eindeutig.*

Dann heißt $\{a_1,\dots,a_n\}$ Basis.

BEMERKUNG

Zwei verschiedene Basen von einer freien abelschen Gruppe A haben die gleiche Anzahl von Elementen.

Beweis

Wir betrachten die Anzahl der Nebenklassen (Index) von

$$2\mathrm{A}=\{2\mathrm{a}|a\in A\}\subseteq A$$

Satz

Wenn A eine freie abelsche Gruppe mit der Basis $a_1,\dots,a_n$ *ist, dann gilt*

$$|A:2\mathrm{A}|=2^n$$

Es sei

$$M=\{0+2\mathrm{A}, a_1+2\mathrm{A}, \ldots . a_n+2\mathrm{A}; (a_i+a_j)+2\mathrm{A}; \ldots .(a_1+a_2+\ldots a_n)+2\mathrm{A}\}$$
$$\text{für alle } i\neq j$$

Dann ist M die Menge aller Nebenklassen von 2A in A und alle Elemente von M sind verschieden.

$$\begin{gathered}(a_1+a_2)+2\mathrm{A}=(a_2+a_3+a_6)+2\mathrm{A}\\ \Rightarrow\ (a_2+a_3+a_6)-(a_1+a_2)\ \in 2\mathrm{A}\\ \Leftrightarrow\qquad (a_3+a_6-a_1)\ \in 2\mathrm{A}\\ \text{Somit gilt } a_3+a_6-a_1=2\mathrm{a}=2(\alpha_1*a_1+\ldots\alpha_n*a_n)\\ \Leftrightarrow 0=(2\alpha_1+1)a_1+2\alpha_2*a_2+(2\alpha_3-1)a_3+2\alpha_5*a_5+(2\alpha_6-1)a_6\end{gathered}$$

Da A eine freie abelsche Gruppe ist mit der Basis $a_1,\ldots,a_n$ *ist* $2\alpha_1+1=0$ *ein Widerspruch.*

q.e.d

<u>Präposition 2</u>

Eine endlich erzeugte abelsche Gruppe ist genau dann frei, wenn sie torsionsfrei ist.

<u>Korollar</u>

Jede endlich erzeugte abelsche Gruppe ist die direkte Summe von einer endlichen Gruppe und einer freien abelschen Gruppe.

Beweis

Zeige A= tA + (eine freie abelsche Gruppe)

Wir wissen dass jede Untergruppe in einer abelschen Gruppe normal ist, (Definition von normal folgt im Anschluss) d.h.

$$\begin{gathered}\text{Es gilt } tA\lhd A\\ \text{Bilde einen Homomorphismus } A\to A/tA\\ A/tA \text{ ist frei und es sei } b_1+tA,\ldots b_n+tA \text{ eine Basis dieser freien Gruppe.}\\ \text{Definieren wir } B=\langle b_1,\ldots,b_n\rangle\subseteq A.\end{gathered}$$

Behauptungen

1. *B ist frei mit der Basis* $b_{1,..}b_n$
2. $A=tA\oplus B$

Zu 1. Annahme es sei

$$\beta_1 \cdot b_1 + \ldots + \beta_n \cdot b_n = 0$$
$$\Rightarrow \quad \beta_1 (b_1 + tA) + \ldots + \beta_n (b_n + tA) = 0 + tA = 0$$
$$\Rightarrow \quad \beta_1, \ldots, \beta_n = 0$$

Zu 2.

Zeige $A = tA \oplus B$
da es sich hier um eine Gleichheit handelt muss man zwei Mengeninklusionen zeigen

$$A \supseteq tA \oplus B$$

diese Inklusion ist trivila , betrachte hier für den Schnitt der beiden Mengen tA *und* B

$$tA \cap B = 0$$

Betrache nun die andere Inklusion

$$A \subseteq tA \oplus B$$

Es sei $a \in A$ *beliebig , betrachte die Nebenklassen*

$$a + tA = \beta_1 (b_1 + tA) + \ldots + \beta_n (b_n + tA)$$
$$\Rightarrow \quad a - (\beta_1 b_1 + \ldots + \beta_n b_n) \quad \in tA$$
$$\Rightarrow \quad a - (\beta_1 \cdot b_1 + \ldots + \beta_n \cdot b_n) = c \quad \in tA$$
$$\Rightarrow \quad a = c + (\beta_1 \cdot b_1 + \ldots + \beta_n \cdot b_n)$$

q.e.d

DEFINITION „Normalteiler und normal „

Sei G eine Gruppe und $N \subseteq G$ ein Untergruppe von G. Dann sind folgende Aussagen äquivalent:

1. Für alle $g \in G$ gilt $gN = Ng$
2. Es gilt $G/N = N \backslash G$
3. Für alle $g \in G$ und alle $n \in N$ gilt $gng^{-1} \in N$

Eine Untergruppe die diese Bedingungen erfüllt heißt Normalteiler von G oder normale Untergruppe. Bez.: $G \rhd N$

Sei p eine Primzahl

DEFINITION „ p-Gruppe“

Eine endliche Gruppe nennt man p-Gruppe, wenn ihre Ordnung eine Potenz von p ist.

Es sei p eine Primzahl und A eine abelsche Gruppe. Dann bezeichnen wir mit

$$A_p = \{x \in A \mid p^r x = 0 \quad \forall r \geq 0\} \quad .$$

Offensichtlich ist A_p eine Untergruppe.

Präposition 3

Jede endliche abelsche Gruppe kann als direkte Summe von p-Gruppen geschrieben werden. (für verschiedene Primzahlen p)
Genauer
A ist endlich und es existieren die Primzahlen $p_i \; für \; i = 1,.., n$ diese sind ein Teiler der Ordnung von A

$$A = A_{p_1} \oplus ... \oplus A_{p_n}$$

Beweis

Die Ordnung von A lässt sich als ein Produkt von Primzahlen schreiben.

$$|A| = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \; p_k^{\alpha_k}$$

Sei $a \in A$

Dann gilt nach Lagrange das die Ordnun von a die Ordung von A teilt d.h.

$$ord(a) \mid |A| = p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k}$$

$$\Rightarrow \quad ord(a) = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_k^{\beta_k} \qquad mit \; 0 \leq \beta_i \leq \alpha_i$$

Es sei

$$p_2^{\beta_2} \cdot p_3^{\beta_3} \cdot ... \cdot p_k^{\beta_k} \cdot a = b_1$$
$$p_1^{\beta_1} \cdot p_3^{\beta_3} \cdot ... \cdot p_k^{\beta_k} \cdot a = b_2$$
$$\vdots$$
$$p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_{k-1}^{\beta_{k-1}} \cdot a = b_{k-1}$$

Dann ist die Ordung von den b_i *für* $i = 1,\dots, k$ *wie folgt*

$$\begin{aligned} ord(b_1) &= p_1^{\beta_1} \\ ord(b_2) &= p_2^{\beta_2} \\ ord(b_3) &= p_2^{\beta_3} \\ &\vdots \\ ord(b_k) &= P_k^{\beta_k} \end{aligned}$$

Die $p_i^{\beta_i}$ *sind alle Teilerfremd* $\Rightarrow$ $(p_2^{\beta_2} \dots p_k^{\beta_k}); (p_1^{\beta_1} p_3^{\beta_3} \dots p_k^{\beta_k}); \dots; (p_1^{\beta_1} \dots p_{k-1}^{\beta_{k-1}})$ *sind teilerfremd.*

Daraus folgt , dass der ggT dieser Zahlen gleich 1 *ist.*

Dann existiert ein q_i *für* $i = 1,.., k$

$$\begin{aligned} & q_1 \cdot (p_2^{\beta_2} \cdot \dots \cdot p_k^{\beta_k}) + \dots + q_k \cdot (p_1^{\beta_1} \cdot \dots \cdot p_{k-1}^{\beta_{k-1}}) = 1 \\ \Rightarrow \quad & q_1 \cdot (p_2^{\beta_2} \cdot \dots \cdot p_k^{\beta_k}) \cdot a + \dots + q_k \cdot (p_1^{\beta_1} \cdot \dots \cdot p_{k-1}^{\beta_{k-1}}) \cdot a = 1 \cdot a = a \\ \Leftrightarrow \quad & q_1 \cdot b_1 + \dots\dots\dots\dots\dots + q_k \cdot b_k = a \end{aligned}$$

Somit konnte das a als eine Summe aus Elementen von A_{p_i} *dargestellt werden*

q.e.d.

Sylow Gruppe

Sätze von Sylow

Es sei G eine endliche Gruppe und p eine Primzahl, dann gilt

1. G enthält p-Sylow-Untergruppen
2. Jede p-Untergruppe von G ist in einer p-Sylow-Untergruppe enthalten
3. Je zwei p-Sylow-Gruppen von G sind Konjugiert
4. Die Anzahl der p-Sylow-Gruppen von G ist kongurent zu 1 modulo p
5. Schreibe $|G| = p^l m$,mit $p \nmid m$.
   Dann ist die Anzahl der p-Sylow-Untergruppen in G ein Teiler von m

Beispiel 1

$$|G| = 15, \quad 15 = 3 \cdot 5$$

somit ergibt sich für die Sylow − Gruppen folgendes

verwende schritt 4

$$S(3) \equiv_3 1 \quad \textit{diesen entspricht} \quad 1 + 3\mathbb{Z} := \{1,4,7,..\} \quad \textit{und} \quad S(3) | 5 \Rightarrow S(3) = 1$$

Das gleich Verfahren wenden wir jetzt auf die 5 *an*

$$S(5) \equiv_5 1 \quad \textit{dieses entspricht} \quad 1 + 5\mathbb{Z} := \{1,6,11..\} \quad \textit{und} \quad S(5) | 3 \Rightarrow S(5) = 1$$

Bilde den Schnitt der Mengen von $S(3) | 5$ *und* $S(5) | 3$

Somit sind die $3 - Sylow - Untergruppe$ $S(3)$ *und die* $5 - Sylow - Untergruppe$ $S(5)$ *normal.*

Beispiel 2

$$|G| = 21 = 7 \cdot 3$$

Somit ergibt sich für die Sylow − Gruppen folgendes

$S(3) \equiv_3 1$ *dieses entspricht der Menge* $1 + 3\mathbb{Z} := \{1,4,7,...\}$ *und*

$$S(3) | 7 \Rightarrow S(3) = \{1,7\}.$$

Daraus folgt das $S(3)$ *nicht umbedingt normal ist. Untersuche* $S(3) = 1$ *oder* $S(3) = 7$

Es sei $S(3) = 7$

Es exsitieren 7 *zyklische Untergruppen der Ordung* 3 *mit*

$2 \cdot 7 = 14$ *Elemente der Ordung* 3

Diese sind im Schnitt bis aus das neutrale Element disjunkt

Es sei $S(3) = 1$

Es exsitiert 1 *zyklische Untergruppe der Ordnung* 3 *mit*

$1 \cdot 2 = 2$ *Elemente der Ordung* 3

Betrachte nun weiterhin die Sylow − Gruppe $S(7)$

$$S(7) \equiv_7 1 \quad \textit{diese entspricht der Menge} \quad 1+7\mathbb{Z} := \{1,8,..\} \quad \textit{und}$$

$$S(7) | 3 \;\Rightarrow\; S(7) = \{1\}.$$

Daraus folgt das es nur eine zyklische Untergruppe der Ordung 7 *gibt mit*

$$1 \cdot 6 = 6 \quad \textit{Elemente der Ordnung } 7$$

1. *Fall*

Es sei $S(3) = 7$ *und* $S(7) = 1$

Dann folgt für die Element folgendes

$$2 \cdot 7 + 1 \cdot 6 + 1 = 21$$

die letzte 1 *ist das neutrale Element , und es existiert kein Element mit der Ordnung* 21 .

Deshalb muss man sich eine neue Gruppe konstuieren und dies würde wie folgt seien

$$G = \langle (a^i, b^j) | 0 \leqslant i \leqslant 2 \,;\, 0 \leqslant j \leqslant 6 \rangle$$

Definiere eine Verknüpfung auf dieser Menge G

$$(a^{i_1}, b^{j_1}) \cdot (a^{i_2}, b^{j_2}) = (a^{i_1+i_2}, b^{j_1 \cdot 2^{i_2} + j_2})$$

Mit diese Wahl erfasst man alle 21 *Element* .

2. *Fall*

Es sei $S(3) = 1$ *und* $S(7) = 1$

Dann folgt für die Element folgendes

$$1 \cdot 2 + 1 \cdot 6 + 1 = 9$$

Die fehlenden Elemente haben die Ordnung 21.

Daraus folgt

$$G = \mathbb{Z}_3 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_{21}$$