Definition der p-Sylowgruppen

Definition (8.3)

Sei p eine Primzahl und G eine endliche Gruppe der Ordnung $n = p^r m$, wobei m und p teilerfremd sind.

- Eine p-Untergruppe von G ist eine Untergruppe der Ordnung p^s mit $0 \leq s \leq r$.
- Ist $r = s$, dann sprechen wir von einer p-Sylowgruppe.

Die Sylowsätze

Satz (8.6)

Sei G eine Gruppe der Ordnung n, p eine Primzahl und $n = mp^r$ mit $p \nmid m$.

(i) *Erster Sylowsatz:*
Jede p-Untergruppe von G ist in einer p-Sylowgruppe enthalten.

(ii) *Zweiter Sylowsatz:*
Je zwei p-Sylowgruppen sind zueinander konjugiert.

(iii) *Dritter Sylowsatz:*
Für die Anzahl ν_p der p-Sylowgruppen gilt
$\nu_p \equiv 1 \mod p$ und $\nu_p \mid m$.

Folgerung aus dem Zweiten Sylowsatz

Folgerung (8.7)

Sei G eine Gruppe und p eine Primzahl. Eine p-Sylowgruppe P ist genau dann ein Normalteiler von G, wenn die Anzahl ν_p der p-Sylowgruppen von G gleich 1 ist.

Beweis von Folgerung 8.7:

ggg endliche Gruppe G, Primzahl p

Sei P eine p-Sylowgruppe von G.

Beh.: $\nu_p = 1 \iff P \trianglelefteq G$

„$\Rightarrow$" Sei $g \in G$ zzg. $gPg^{-1} = P$ Mit P ist auch gPg^{-1} eine p-Sylowgruppe (weil die Konjugation mit g ein Automorphismus von G ist) Wegen $\nu_p = 1$ muss $P = gPg^{-1}$ gelten.

„$\Leftarrow$" Sei Q eine bel. p-Sylowgruppe. 2. Sylowsatz $\Rightarrow$ $\exists g \in G$ mit $Q = gPg^{-1}$ $\overset{P \trianglelefteq G}{\Rightarrow}$ $Q = P$ also: P ist die einzige p-Sylowgruppe. $\square$

Anwendung: Gruppen der Ordnung 15

Lemma (8.8)

Jede Gruppe der Ordnung 15 besitzt einen Normalteiler der Ordnung 3 und einen Normalteiler der Ordnung 5.

Folgerung (8.9)

Jede Gruppe der Ordnung 15 ist zyklisch.

Beweis von Lemma 8.8:

geg: Gruppe G. $|G| = 15 = 3 \cdot 5$ Für $p \in \{3, 5\}$ sei ν_p die Anzahl der p-Sylowgruppen von G.

3. Sylowsatz $\Rightarrow \nu_5 \mid 3 \Rightarrow \nu_5 \in \{1, 3\}$, außerdem $\nu_5 \equiv 1 \bmod 5$

$3 \not\equiv 1 \bmod 5 \Rightarrow \nu_5 = 1$ Sei P die einzige 5-Sylowgruppe von G $\overset{\text{Folgerung 8.7}}{\Rightarrow}$ $P \trianglelefteq G$, außerdem $|P| = 5$

ebenso: 3. Sylowsatz $\Rightarrow \nu_3 \mid 5 \Rightarrow \nu_3 \in \{1, 5\}$, außerdem

$\nu_3 \equiv 1 \bmod 3$, $5 \equiv 2 \not\equiv 1 \bmod 3 \Rightarrow \nu_3 = 1$ Sei Q die einzige 3-Sylowgruppe $\overset{\text{Folgerung 8.7}}{\Rightarrow}$ $Q \trianglelefteq G$, außerdem $|Q| = 3$ $\square$

Beweis von Satz 8.9:

geg.: Gruppe G mit $|G| = 15$

Bel.: $G \cong \mathbb{Z}/15\mathbb{Z}$ s.o. $\rightarrow$

G besitzt Normalteiler P, Q mit $|P| = 5$ und $|Q| = 3$

Beh.: G ist inneres direktes Produkt von P und Q

bereits bekannt: $P, Q \trianglelefteq G$, noch zu überprüfen (i) $P \cap Q = \{e\}$ (ii) $G = PQ$

zu ii) folgt aus der Teilerfremdheit von $|P| = 5$ und $|Q| = 3$

zu iii) Wegen $P \cdot Q \leq G$ ist PQ eine Untergruppe von G (sogar ein Normalteiler). Wegen $P \leq PQ$ ist $|P| = 5$ ein Teiler von $|PQ|$, und wegen $Q \leq PQ$ ist $|Q| = 3$ ein Teiler von $|PQ| \Rightarrow \text{kgV}(3,5) = 15$ ist Teiler von $|PQ| \Rightarrow |PQ| \geq 15 = |G| \overset{PQ \leq G}{\Rightarrow} PQ = G$

($\Rightarrow$ Beh.) Aus der Beh. folgt $G \cong P \times Q$

$|P| = 5$ Primzahl $\Rightarrow$ P zyklisch $\Rightarrow P \cong \mathbb{Z}/5\mathbb{Z}$

$|Q| = 3$ Primzahl $\Rightarrow$ Q zyklisch $\Rightarrow Q \cong \mathbb{Z}/3\mathbb{Z}$

$\Rightarrow G \cong P \times Q \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$

↳ Chin. Restsatz $\text{ggT}(5,3) = 1$ □

Bem: Nach dem gleichen Schema kann man zeigen, dass jede Gruppe der Ordnung $3p$ zyklisch ist, falls p Primzahl, $p > 3$ und $p \equiv 2 \bmod 3$.

Anwendung: Gruppen der Ordnung $2p$

Proposition (8.10)

Sei $n \in \mathbb{N}$ mit $n \geq 3$, G eine Gruppe und $\{g, h\}$ ein Erzeugendensystem von G, wobei $\mathrm{ord}(g) = n$, $\mathrm{ord}(h) = 2$ und $ghgh = e_G$ gilt. Dann ist G isomorph zur Diedergruppe D_n.

Satz (8.11)

Sei p eine ungerade Primzahl und G eine nicht-abelsche Gruppe der Ordnung $2p$. Dann ist G isomorph zur Diedergruppe D_p.

Beweis von Satz 8.11:

geg: Primzahl $p > 2$, Gruppe G, nicht abelsch von Ordnung $2p$ z.zg: $G \cong D_p$

Sei ν_p die Anzahl der p-Sylowgruppen von G.

3. Sylowsatz $\Rightarrow \nu_p \mid 2 \Rightarrow \nu_p \in \{1, 2\}$

außerdem: $\nu_p \equiv 1 \bmod p$ $p > 2 \Rightarrow 2 \equiv 1 \bmod p$

$\Rightarrow \nu_p = 1$ Sei N die einzige p-Sylowgruppe.

Folgerung 8.7 $\Rightarrow N \trianglelefteq G$

$|G| = 2p$, N p-Sylowgruppe $\Rightarrow |N| = p$

$\underline{p}$ Primzahl $\Rightarrow$ N ist zyklisch, d.h. $N = \langle g \rangle$ für ein $g \in N$

2 ist Primteiler von G $\overset{\text{Lemma von Cauchy}}{\Rightarrow}$

□

$\exists\, h \in G$ mit $\mathrm{ord}(h) = 2$. Außerdem gilt $G = \langle g, h \rangle$.

denn: $g \in \langle g, h \rangle \Rightarrow p = \mathrm{ord}(g)$ ist Teiler von $|\langle g, h \rangle|$

ebenso: $h \in \langle g, h \rangle \Rightarrow 2 = \mathrm{ord}(h)$ ist Teiler von $|\langle g, h \rangle|$

insgesamt: $\mathrm{kgV}(2, p) = 2p$ teilt $|\langle g, h \rangle| \Rightarrow$

$|\langle g, h \rangle| \geq 2p = |G| \overset{\langle g, h \rangle \leq G}{\Rightarrow} G = \langle g, h \rangle$

Wenn außerdem gilt: $ghgh = e$, dann folgt $G \cong D_p$

aus Proposition 8.10. $ghgh = e \Leftrightarrow hgh = g^{-1} \overset{h = h^{-1}}{\Leftrightarrow}$

$hgh^{-1} = g^{-1} \Leftrightarrow \tau_h(g) = g^{-1}$, wobei $\tau_h \in \mathrm{Aut}(G)$ gegeben durch Konjugation mit h. Wegen $\langle g \rangle \trianglelefteq G$ gilt $\tau_h(\langle g \rangle) = \langle g \rangle$, d.h. τ_h liefert einen Automorphismus von $\langle g \rangle$

$\Rightarrow \exists a \in \mathbb{Z}: \; hgh^{-1} = g^a$ Dabei muss (weil τ_a Aut.) g^a wiederum ein Erzeuger von $\langle g \rangle$ sein, d.h. $ggT(a,p) = 1$ oder (gleichbed.) $a \not\equiv 0 \bmod p$

$g^{a^2} = (g^a)^a = (\tau_a(g))^a = \tau_h(\tau_h(g)) = h \cdot (hgh^{-1}) h^{-1} =$

$h^2 g h^{-2} = g = g^1 \overset{p = ord(g)}{\Rightarrow} a^2 \equiv 1 \bmod p \Rightarrow p \mid (a^2 - 1)$

$\uparrow ord(h) = 2$

$\Rightarrow p \mid (a-1)(a+1) \Rightarrow a \equiv 1 \bmod p$ oder $a \equiv -1 \bmod p$

1. Fall: $a \equiv -1 \bmod p \Rightarrow hgh^{-1} = g^a \equiv g^{-1}$ (✓)

$\uparrow ord(g) = p$, $a \equiv -1 \bmod p$

2. Fall: $a \equiv 1 \bmod p \Rightarrow hgh^{-1} = g \Rightarrow hg = gh$

$(G : \langle g \rangle) = \frac{|G|}{|\langle g \rangle|} = \frac{2p}{p} = 2$, $h \notin \langle g \rangle \Rightarrow G = \langle g \rangle \cup \langle g \rangle h$

$= \{ g^c h^d \mid 0 \le c < p, d \in \{0,1\} \}$ Aus $hg = gh$ folgt sonst, dass G abelsch ist ↯ zur Voraussetzung. □

Definition (9.1)

Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$, genannt Addition und Multiplikation, so dass die folgenden Bedingungen erfüllt sind:

(i) Das Paar $(R, +)$ ist eine abelsche Gruppe.

(ii) Das Paar $(R, \cdot)$ ist ein kommutatives Monoid.

(iii) Es gilt das Distributivgesetz $a(b + c) = ab + ac$ für alle $a, b, c \in R$.

Notation: Sei $(R, +, \cdot)$ ein Ring

Dann ist $a - b$ die Kurzschreibweise für $a + (-b)$.

0_R = Nullelement von R = Neutralelement von $(R, +)$

1_R = Einselement von R = Neutralelement von $(R, \cdot)$

bereits bekannt: $0_R \cdot a = 0_R$, $a \cdot (-b) = (-a) \cdot b = -(ab)$

$(-a) \cdot (-b) = a \cdot b$

Beispiele für Ringe: (i) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, aber nicht $\mathbb{N}$ bzw. $\mathbb{N}_0$

(ii) $\mathbb{Z}/n\mathbb{Z}$ (Restklassenringe), für $n \in \mathbb{N}$

(iii) Für jeden Ring R existiert ein Polynomring $R[x]$.

(ii) $\mathbb{Z}/n\mathbb{Z}$ (Restklassenringe), für $n \in \mathbb{N}$

(iii) Für jeden Ring R existiert ein Polynomring $R[x]$.

Bem. Sind $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ Ringe, dann erhält man durch $(R \times S, \oplus, *)$ mit

$(a,b) \oplus (c,d) = (a +_R c, b +_S d)$, $(a,b) * (c,d) = (a \cdot_R c, b \cdot_S d)$

ein Ring, mit $0_{R\times S} = (0_R, 0_S)$, $1_{R\times S} = (1_R, 1_S)$.

Definition der Ringhomomorphismen

Definition (9.2)

Seien $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ Ringe. Eine Abbildung $\phi : R \to S$ heißt Ringhomomorphismus von $(R, +_R, \cdot_R)$ nach $(S, +_S, \cdot_S)$, wenn die Gleichung $\phi(1_R) = 1_S$ gilt und außerdem

$$\phi(a +_R b) = \phi(a) +_S \phi(b) \quad \text{und} \quad \phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$$

für alle $a, b \in R$ erfüllt ist.

Satz (9.3)

Für jeden Ring R existiert ein eindeutig bestimmter Ringhomomorphismus $\mathbb{Z} \to R$.

Anmerkung zur Def. des Ringhom.

Sind $(R, +_R, \cdot_R)$, $(S, +_S, \cdot_S)$ Ringe und $\phi : R \to S$ eine Abbildung, dann folgt aus $\phi(a +_R b) = \phi(a) +_S \phi(b)$ und $\phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$ im Allgemeinen nicht $\phi(1_R) = 1_S$.

Bsp.: $\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, $a \mapsto (a, 0)$

Es gilt $\phi(a+b) = \phi(a) + \phi(b)$ und $\phi(ab) = \phi(a)\phi(b)$ $\forall a, b \in \mathbb{Z}$ aber

$\phi(1_{\mathbb{Z}}) = \phi(1) = (1, 0) \neq (1, 1) = 1_{\mathbb{Z} \times \mathbb{Z}}$

Einheiten und Nullteiler

Definition (9.4)

Sei R ein Ring.

(i) Ein Element $a \in R$ heißt Einheit, wenn ein $b \in R$ mit $ab = 1_R$ existiert. Die Menge der Einheiten von R bezeichnen wir mit $R^\times$.

(ii) Man nennt es Nullteiler, wenn ein Element $b \in R$, $b \neq 0_R$ mit $ab = 0_R$ existiert.

Die Einheiten eines Rings R bilden eine Gruppe $R^\times$, die sogenannte Einheitengruppe.

Beispiele für Einheiten und Nullteiler:

(i) $R = \mathbb{Z}$ Einheiten $\mathbb{Z}^\times = \{\pm 1\}$ weg. $1 \cdot 1 = 1$,
$(-1)\cdot(-1) = 1$, $a \cdot b \neq 1 \; \forall b \in \mathbb{Z}$ falls $a \notin \{\pm 1\}$

Die 0 ist der einzige Nullteiler, denn:
$1 \neq 0$, $0 \cdot 1 = 0 \Rightarrow 0$ ist Nullteiler
Kein Element $a \neq 0$ ist Nullteiler, denn:
$b \neq 0 \Rightarrow a \cdot b \neq 0$

(ii) $R = \mathbb{Z}/4\mathbb{Z}$ Einheiten: $\bar{1}$, $\bar{3}$ (da $\bar{3}\cdot\bar{3} = \bar{1}$)
Nullteiler: $\bar{0}$, $\bar{2}$ (da $\bar{2} \neq \bar{0}$, $\bar{2}\cdot\bar{2} = \bar{0}$)

(iii) $R = \mathbb{Z} \times \mathbb{Z}$ Einheiten: $(1,1)$, $(-1,1)$, $(1,-1)$, $(-1,-1)$
Nullteiler: $(a,0)$, $(0,a)$ mit $a \in \mathbb{Z}$ beliebig

Integritätsbereiche und Körper

Definition (9.5)

Ein Ring R mit 0_R als einzigem Nullteiler heißt Integritätsbereich.
Gilt $R^\times = R \setminus \{0_R\}$, dann ist R ein Körper.

Eigenschaften von Nullteilern und Einheiten

Lemma (9.6)

(i) Ein Element a in einem Ring R kann nicht zugleich Nullteiler und Einheit sein.

(ii) Jeder Körper ist ein Integritätsbereich.

(iii) In jedem Integritätsbereich R gilt die Kürzungsregel: Sind $a, b, c \in R$ mit $c \neq 0_R$, dann folgt aus $ac = bc$ die Gleichung $a = b$.

Beweis von Lemma 9.6.

zu (i) Sei R ein Ring. Ang. $a \in R$ ist Nullteiler und Einheit.

a ist Nullteiler $\Rightarrow \exists\, b \in R \setminus \{0_R\}$ mit $b \cdot a = 0_R$

a ist Einheit $\Rightarrow \exists\, c \in R$ mit $a \cdot c = 1_R$

$\Rightarrow b = b \cdot 1_R = b \cdot (a \cdot c) = (b \cdot a) \cdot c = 0_R \cdot c = 0_R$

$\lightning$ zu Vor. $b \neq 0_R$

zu (ii) Vor: R ist Körper, d.h. $R^\times = R \setminus \{0_R\}$

z.zg.: R ist Integritätsbereich, dafür zu überprüfen (1) 0_R ist Nullteiler

(2) Es gibt keine weiteren Nullteiler

zu (1) Es gilt $1_R \neq 0_R$, da $1_R \in R^\times$ und sonst $1_R \in R \setminus \{0_R\}$

(Bem.: Gilt in einem Ring $1_R = 0_R$, dann folgt $R = \{0_R\}$, denn: $a \in R \Rightarrow a = a \cdot 1_R = a \cdot 0_R = 0_R$)

Die Gleichung $0_R \cdot 1_R = 0_R$ zeigt also, dass 0_R ein Nullteiler in R ist.

zu (2) Ang. $a \in R \setminus \{0_R\}$ ist Nullteiler.

Vor. $\Rightarrow a \in R^\times \Rightarrow$ a ist Einheit und Nullteiler $\lightning$ zu (i)

zu (iii) Vor.: R ist Integritätsbereich. Seien a, b, c mit $ac = bc$ und $c \neq 0_R$. z.zg.: $a = b$

5

$ac = bc \Rightarrow ac - bc = 0_R \Rightarrow (a-b)c = 0_R$ $\xrightarrow{c \neq 0_R}$ R ist Nullteilerbereich

0_R ist einziger Nullteiler, $a - b = 0_R \Rightarrow a = b$ □