

Thema: Gruppen - Ordnung - Index

Übung 6

Ist $\#G = p$ eine Primzahl, so ist $G = \langle g \rangle$ für ein $g \in G$.

Lösung:

Da $p \geq 2$ ist, existiert ein vom neutralen Element verschiedenes Element $g \in G$.

$\Rightarrow \langle g \rangle \leq G$

Nach dem Satz von Lagrange gilt $\text{ord}(g) \mid \#G = p$. Da g nicht das neutrale Element der Gruppe G ist, muss $\text{ord}(g) = \#\langle g \rangle \geq 2$ und damit $\text{ord}(g) = \#\langle g \rangle = p$. Folglich ist also $G = \langle g \rangle$.

Übung 7

Sei $f : G \rightarrow H$ ein Epimorphismus endlicher Gruppen. Zeigen Sie, dass $|f^{-1}(h)| = |\text{Ker}(f)|$ für jedes $h \in H$. Schließen Sie, dass $\#G = \#H \cdot \#\text{Ker}(f)$.

Lösung:

Es sei $h \in H$.

f surjektiv $\Rightarrow \exists g_0 \in G : f(g_0) = h$

Für $g \in \text{Ker}(f)$ gilt

$$f(g \cdot g_0) = f(g) \cdot f(g_0) = 1 \cdot h = h$$

d.h. die Abbildung $\varphi : \text{Ker}(f) \rightarrow f^{-1}(h), g \mapsto \varphi(g) := g \cdot g_0$ ist wohldefiniert.

▷ φ ist surjektiv: Sei $g \in f^{-1}(h)$. Dann haben wir

$$f(g \cdot g_0^{-1}) = f(g) \cdot f(g_0)^{-1} = h \cdot h^{-1} = 1,$$

d.h. $g \cdot g_0^{-1} \in \text{Ker}(f)$ und $\varphi(g \cdot g_0^{-1}) = g \cdot g_0^{-1} \cdot g_0 = g$.

▷ φ ist injektiv: Es seien $g_1, g_2 \in \text{Ker}(f)$ mit $\varphi(g_1) = \varphi(g_2)$, d.h. $g_1 \cdot g_0 = g_2 \cdot g_0$
 $\Rightarrow g_1 = g_2$.

▷ Dann ist φ bijektiv, d.h. $|f^{-1}(h)| = |\text{Ker}(f)|$.

Die Urbilder von h sind disjunkt, denn: Für $h \neq h' \in H$ haben wir

$$f^{-1}(h) = \{g \in G : f(g) = h\}$$

$$f^{-1}(h') = \{g \in G : f(g) = h'\}$$

Ist $g \in f^{-1}(h) \cap f^{-1}(h')$, so ist $h = f(g) = h'$ im Widerspruch zur Annahme $h \neq h'$.

Aus $G = \bigsqcup_{h \in H} f^{-1}(h)$ folgt

$$\begin{aligned} |G| &= \left| \bigsqcup_{h \in H} f^{-1}(h) \right| = \sum_{h \in H} |f^{-1}(h)| \\ &= \sum_{h \in H} |\text{Ker}(f)| \\ &= |\text{Ker}(f)| \cdot |H| \end{aligned}$$

Übung 8

Zeigen Sie: Für $k, n \in \mathbb{N}$ ist $\text{ord}(k + n\mathbb{Z}) = \frac{\text{kgV}(k, n)}{k} = \frac{n}{\text{ggT}(k, n)}$.

Lösung:

Es seien $k \in \mathbb{N}$ und $n \in \mathbb{N} \setminus \{0\}$. Außerdem sei $d = \text{ggT}(k, n)$. Dann existieren $k_1, n_1 \in \mathbb{N}$ mit

$$\begin{aligned} k &= d \cdot k_1 \\ n &= d \cdot n_1 \\ \text{ggT}(k_1, n_1) &= 1 \end{aligned}$$

Für $m \in \mathbb{N} \setminus \{0\}$ gilt

$$\begin{aligned} m \cdot (k + n\mathbb{Z}) = n\mathbb{Z} &\Leftrightarrow n \mid m \cdot k \\ &\Leftrightarrow d \cdot n_1 \mid m \cdot d \cdot k_1 \\ &\Leftrightarrow n_1 \mid m \cdot k_1 \\ &\Leftrightarrow n_1 \mid m \end{aligned}$$

Dann ist $\text{ord}(k + n\mathbb{Z}) = n_1 = \frac{n}{\text{ggT}(k, n)}$.

Übung 17 (Präsenz)

Zeigen oder widerlegen Sie:

Genau dann kommutieren Zykel $\tau_1, \tau_2 \in S_n$, wenn sie disjunkt sind.

Lösung:

Die Rückrichtung ist richtig laut Vorlesung (vgl. 1.13). Für die Hinrichtung verwenden wir folgendes Gegenbeispiel: Sei $\tau_1 = (1\ 2) = \tau_2$. Dann ist $\tau_1 \circ \tau_2 = \tau_2 \circ \tau_1$ aber offensichtlich ist $\tau_1 \cap \tau_2 = \tau_1 = \tau_2 \neq \emptyset$.

Übung 18 (Präsenz)

Zeigen oder widerlegen Sie:

- a) Sind $K, N \leq G$, so ist $K \cup N \leq G$.
- b) Sind $K, N \leq G$, so ist $K \cdot N \leq G$.

Lösung:

- a) Die Aussage ist falsch. Sei dazu $K := (2\mathbb{Z}, +)$ und $N := (3\mathbb{Z}, +)$. Dann ist $2 \in 2\mathbb{Z}$ und $3 \in 3\mathbb{Z}$, aber $2 + 3 = 5 \notin K \cup N$ und $K \cup N$ ist somit nicht abgeschlossen bezüglich der Addition.
- b) Auch diese Aussage ist falsch. Betrachte dazu $K := \{\text{id}, (1\ 2)\} \leq S_3$ und $N := \{\text{id}, (1\ 3)\} \leq S_3$. Dann ist $K \cdot N = \{\text{id}, (1\ 2), (1\ 2)(1\ 3) = (1\ 3\ 2)\} \not\leq S_3$ nach dem Satz von Lagrange, da $|KN| = 4 \nmid 6 = \#S_3$.

Thema: Normalteiler, abelsche Gruppen, Produkte

Übung 24

Es seien G eine Gruppe und H eine Untergruppe von G . Wenn G/H mit dem Komplexprodukt eine Gruppe bildet, so ist $H \trianglelefteq G$.

Lösung:

Angenommen, G/H mit dem Komplexprodukt wäre eine Gruppe.

Zunächst zeigen wir, dass H das neutrale Element von G/H ist. Es sei g_0H das neutrale Element von G/H . Für jedes $g \in G$ gilt $gH \cdot g_0H = g_0H \cdot gH = gH$. Insbesondere gilt $g \cdot g_0 = g \cdot 1 \cdot g_0 \cdot 1 \in gH \cdot g_0H = gH$, das heißt es existiert $h \in H$ mit $gg_0 = g \cdot h$. Deswegen gilt $g_0 = h$, somit $g_0H = H$.

Jetzt zeigen wir, dass H Normalteiler von G ist. Sei $g \in G$. Aus $H \cdot gH = gH$ folgt $gH \subseteq H \cdot gH = gH$, das heißt $H \subseteq gHg^{-1}$. Analog bekommen wir $H \subseteq g^{-1}Hg$, das heißt $gHg^{-1} \subseteq H$. Deswegen gilt $gHg^{-1} = H$, also $gH = Hg$. Mit 3.3 schließen wir, dass $H \trianglelefteq G$.

Übung 25

Für jedes $n \in \mathbb{N}$ mit $n \geq 2$ ist $S_n = \langle (12) \rangle \rtimes A_n$.

Lösung:

Es sei $n \in \mathbb{N}$ mit $n \geq 2$. Nach 5.6 ist zu zeigen, dass $A_n \trianglelefteq S_n$, $A_n \cap \langle (12) \rangle = \{\text{id}\}$ und $\langle (12) \rangle \cdot A_n = S_n$ gelten. Da A_n der Kern des Homomorphismus $\text{sgn} : S_n \rightarrow \mu_2$ ist, gilt $A_n \trianglelefteq S_n$ (vgl. 3.5). Aus $(12) \notin A_n$ folgt $A_n \cap \langle (12) \rangle = \{\text{id}\}$. Dann zeigen wir, dass $H = \langle (12) \rangle \cdot A_n = S_n$ gilt. Es sei $\sigma \in S_n$. Ist $\sigma \in A_n$, so gilt $\sigma = \text{id} \cdot \sigma \in H$. Ist $\sigma \notin A_n$, so gelten $(12) \cdot \sigma \in A_n$ und $\sigma = (12) \cdot ((12) \cdot \sigma) \in H$.

Alternativer Beweis für die dritte Eigenschaft: Wir wissen, dass $A_n \subsetneq H \leq S_n$, und da $(S_n : A_n) = 2$ prim ist, folgt aufgrund der Multiplikativität des Index schon, dass $H = S_n$.

Übung 27

Zeigen Sie: Es gibt bis auf Isomorphie genau zwei Gruppen der Ordnung 6, nämlich C_6 und S_3 .

Lösung:

Sei G eine endliche Gruppe der Ordnung 6. Aus dem Satz von LAGRANGE gilt $\text{ord}(g) \in \{1, 2, 3, 6\}$ für jedes $g \in G$.

- ▷ Ist $\text{ord}(g) \in \{1, 2\}$ für jedes $g \in G$, so ist G abelsch (vgl. W2). Aus 4.8 und $\#G = 6$ folgt $G \cong C_6$, was unmöglich ist, da C_6 ein Element der Ordnung 6 hat.
- ▷ Somit gibt es ein $g \in G$ mit $\text{ord}(g) \in \{3, 6\}$. In beiden Fällen, gibt es ein $g_1 \in G$ mit $\text{ord}(g_1) = 3$ (ist $\text{ord}(g) = 6$, so ist $\text{ord}(g^2) = 3$). Außerdem gibt es $g_2 \in G$ mit $\text{ord}(g_2) = 2$ (vgl. H10). Dann bekommen wir: $\langle g_1 \rangle \trianglelefteq G$ (vgl. P41), $\langle g_1 \rangle \cap \langle g_2 \rangle = \{1\}$ (da $\text{ggT}(2, 3) = 1$) und $\langle g_1 \rangle \cdot \langle g_2 \rangle = G$ mit dem selben Argument wie in Ü25. Somit ist $G = \langle g_2 \rangle \rtimes \langle g_1 \rangle$ (vgl. 5.6). Aus 5.12 folgt dann $G \cong C_6$ oder $G \cong S_3$.

Übung 28

Zu welcher Ihnen bekannten Gruppe ist $\text{Aut}(V_4)$ isomorph?

Lösung:

Aus W4 ergibt sich $\text{Aut}(V_4) \cong \text{Aut}((\mathbb{Z}/2\mathbb{Z})^2) = \text{Aut}(\mathbb{F}_2^2)$ (siehe auch V44). Aber \mathbb{F}_2^2 ist ein \mathbb{F}_2 -Vektorraum und die Automorphismen der Gruppe \mathbb{F}_2^2 sind genau die \mathbb{F}_2 -Automorphismen des \mathbb{F}_2 -Vektorraums \mathbb{F}_2^2 . Somit ist $\text{Aut}(V_4) \cong \text{GL}_2(\mathbb{F}_2)$, die eine nicht abelsche Gruppe der Ordnung 6 ist (zählen Sie einfach die Elemente der $\text{GL}(\mathbb{F}_2)$ auf). Mit Ü27 schließen wir, dass $\text{Aut}(V_4) \cong S_3$.

Direkt sieht man dies so: Die V_4 hat neben dem neutralen Element e der Ordnung 1 noch drei Elemente der Ordnung 2, und jede Permutation σ dieser 3 Elemente der Ordnung 2 setzt sich durch $\sigma(e) = e$ zu einer Permutation der Menge V_4 fort. Nun muss man allerdings nachprüfen, dass $\sigma : V_4 \rightarrow V_4$ auch tatsächlich ein Gruppenhomomorphismus ist.

Übung 41 (Präsens)

Sei $H \leq G$. Zeige oder widerlege:

a) $(G : H) = 2 \Rightarrow H \trianglelefteq G$

b) $(G : H) = 3 \Rightarrow H \trianglelefteq G$

Lösung:

- a) richtig. Angenommen $H \not\trianglelefteq G$. Sei $h \in H$ mit $hH = H = Hh$ und $g \in G \setminus H$ mit $gH \neq Hg$. Wegen $(G : H) = 2$ gilt $gH = H$, das heißt $\exists h \in H$ mit $gh \in H$. Dann folgt

$$\underbrace{gh}_{\in H} \cdot \underbrace{h^{-1}}_{\in H} = g \in H$$

was im Widerspruch zu $g \in G \setminus H$ steht. Also ist $H \trianglelefteq G$.

- b) falsch, zum Beispiel $(S_3 : \langle (1\ 2) \rangle) = 3$, aber

$$\begin{aligned} (1\ 3)\langle (1\ 2) \rangle &= \{(1\ 3), (1\ 3\ 2)\} \\ \langle (1\ 2) \rangle(1\ 3) &= \{(1\ 3), (1\ 2\ 3)\} \end{aligned}$$

Thema: Gruppenwirkungen, Sylowgruppen

Übung 47

Für $n \geq 2$ ist $S_n = \langle (12), (12 \dots n) \rangle$.

Lösung:

Sei $G = \langle (12), (12 \dots n) \rangle$ und $c = (12 \dots n)$. Nach Ü26 gilt für alle $i \in \{0, \dots, n-2\}$:

$$c \circ (12) \circ c^{-1} = (c^i(1) \ c^i(2)) = (i+1 \ i+2)$$

Dann gilt $\{(12), (23), (34), \dots, (n-1 \ n)\} \subseteq G$. Aus V44 folgt dann $G = S_n$.

Übung 48

Sei $S \in \text{Syl}_p(G)$. Zeigen Sie: Ist $(G : S) < p$, so ist $S \trianglelefteq G$.

Lösung:

Schreibe $\#G = p^n \cdot m$ mit $n \geq 0$ und $p \nmid m$. Es sei n_p die Kardinalität von $\text{Syl}_p(G)$. Aus den Sylow-Sätzen folgt $n_p \equiv 1 \pmod p$ und $n_p \mid m = (G : S)$ (da $|S| = p^n$ und nach Lagrange ist $(G : S) = |G| : |S| = p^n \cdot m : p^n = m$). Insbesondere gilt $n_p \leq (G : S)$ und $p \mid n_p - 1$. Ist $n_p \neq 1$, so ist $p \leq n_p - 1 \leq n_p \leq (G : S)$, was unmöglich ist. Deswegen ist $n_p = 1$, d.h. $S \trianglelefteq G$ (vgl. 8.7: $S \trianglelefteq G \Leftrightarrow \#\text{Syl}_p(G) = 1$).

Übung 49

Seien $H_1, H_2 \leq G$. Die Wirkung von $\Gamma := H_1 \times H_2$ auf $X := H_1 H_2 \subseteq G$ durch $x^{(h_1, h_2)} := h_1^{-1} \cdot x \cdot h_2$ ist transitiv. Bestimmen Sie $\Gamma_1 = \text{Stab}(1)$ und folgern Sie, dass

$$|H_1 H_2| = \frac{|H_1| \cdot |H_2|}{|H_1 \cap H_2|}$$

Lösung:

▷ Betrachte die Abbildung

$$\psi: \begin{cases} H_1 H_2 \times (H_1 \times H_2) & \rightarrow H_1 H_2 \\ (x, (h_1, h_2)) & \mapsto h_1^{-1} \cdot x \cdot h_2 \end{cases}$$

Für jedes $x \in H_1 H_2$ gilt $x = g_1 \cdot g_2$ mit $g_1 \in H_1$ und $g_2 \in H_2$. Dann gilt

$$h_1^{-1} \cdot x \cdot h_2 = \underbrace{h_1^{-1} g_1}_{\in H_1} \cdot \underbrace{g_2 h_2}_{\in H_2} \in H_1 H_2$$

Deswegen ist ψ definiert.

▷ ψ ist Wirkung.

– Für alle $x \in H_1 H_2$ ist $X^{(1,1)} = 1^{-1} \cdot x \cdot 1 = x$

– Für alle $(g_1, g_2), (h_1, h_2), (l_1, l_2) \in H_1 \times H_2$ gilt

$$\begin{aligned} ((g_1 g_2)^{(h_1, h_2)})^{(l_1, l_2)} &= (h_1^{-1} g_1 g_2 h_2)^{(l_1, l_2)} = l_1^{-1} h_1^{-1} g_1 g_2 h_2 l_2 \\ &= (h_1 l_1)^{-1} g_1 g_2 (h_2 l_2) = (g_1 g_2)^{(h_1 l_1, h_2 l_2)} \\ &= (g_1 g_2)^{(h_1, h_2) \cdot (l_1, l_2)} \end{aligned}$$

▷ ψ ist transitiv: Es seien $x, y \in H_1 H_2$. Schreibe wieder $x = g_1 g_2$ mit $g_1 \in H_1, g_2 \in H_2$ und $y = l_1 l_2$ mit $l_1 \in H_1, l_2 \in H_2$. Dann gilt

$$y = l_1 l_2 = l_1 g_1^{-1} g_1 g_2 g_2^{-1} l_2 = \underbrace{(g_1 l_1^{-1})^{-1}}_{\in H_1} \cdot x \cdot \underbrace{(g_2^{-1} l_2)}_{\in H_2}$$

▷ Es gilt:

$$\begin{aligned} \text{Stab}(1) &= \{(g_1, g_2) \in H_1 \times H_2 : 1^{(g_1, g_2)} = 1\} \\ &= \{(g_1, g_2) \in H_1 \times H_2 : g_1^{-1} \cdot 1 \cdot g_2 = 1\} \\ &= \{(g_1, g_2) \in H_1 \times H_2 : g_1 = g_2\} \\ &\cong H_1 \cap H_2 \end{aligned}$$

▷ Deswegen gilt

$$\begin{aligned} |H_1 \cdot H_2| &\stackrel{\text{transitiv}}{=} \# 1^{H_1 \times H_2} \stackrel{6.11}{=} (H_1 \times H_2 : \text{Stab}(1)) \\ &\stackrel{\text{Lagrange}}{=} \frac{|H_1 \times H_2|}{|\text{Stab}(1)|} = \frac{|H_1| \cdot |H_2|}{|H_1 \cap H_2|} \end{aligned}$$

Übung 50

Jede Gruppe der Ordnung 20 ist isomorph zu einem semidirekten Produkt $C_4 \rtimes_{\alpha} C_5$ oder $V_4 \rtimes_{\alpha} C_5$.

Lösung:

Es sein G eine endliche Gruppe und n_5 die Anzahl der 5-Sylowgruppen von G . Nach den Sylow-Sätzen ist $n_5 = 1 \pmod{5}$ und $n_5 \mid 4$. Deswegen gilt $n_5 = 1$. G hat genau eine 5-Sylowgruppe, die wir mit N_5 bezeichnen. Nach 8.7 ist $N_5 \triangleleft G$. Es sei N_2 eine 2-Sylowgruppe von G ; es gilt $|N_2| = 4$ (vgl. dazu 8.2: $\#G = p^k \cdot m$ mit $p \nmid m \Rightarrow 20 = 2^2 \cdot 5 \Rightarrow H \in \text{Syl}_2(G) \Rightarrow |H| = p^k = 4$). Da $\text{ggT}(4, 5) = 1$ gilt $|N_5 \cap N_2| = 1$, d.h. $N_5 \cap N_2 = \{1\}$. Es gilt auch

$$|N_5 \cdot N_2| = \frac{|N_5| \cdot |N_2|}{|N_5 \cap N_2|} = \frac{5 \cdot 4}{1} = 20 = |G|$$

d.h. $N_5 \cdot N_2 = G$. Mit 5.6 bekommen wir $G \cong N_2 \rtimes_{\alpha} N_5$. Aber wegen $N_5 \cong C_5$ und $N_2 \cong C_3$ oder $N_2 \cong V_4$ (vgl. dazu 7.7 und 4.8 und V4) gilt $C_4 \rtimes_{\alpha} C_5$ oder $V_4 \rtimes_{\alpha} C_5$.

Übung 63 (Präsenz)

Geben Sie ein Beispiel einer Gruppe G und einer G -Menge X mit $G_x = \text{Stab}(x) \not\triangleleft G$ für ein $x \in X$.

Lösung:

Sei $n \geq 3$. Betrachte die natürliche Wirkung von S_n auf $\{1, \dots, n\}$

$$\psi: \begin{cases} \{1, \dots, n\} \times S_n & \rightarrow S_n \\ (\sigma, i) & \mapsto i^{\sigma} = \sigma(i) \end{cases}$$

Es gilt $\text{Stab}(n) = \{\sigma \in S_n : \sigma(n) = n\}$. Aber $\text{Stab}(n) \not\trianglelefteq S_n$:

$$(1 \ n) \circ \underbrace{(1 \ 2 \cdots n-1)}_{\in \text{Stab}(n)} \circ (1 \ n) \stackrel{\text{Ü26}}{=} (n \ 2 \cdots n-1) \notin \text{Stab}(n)$$

Übung 64 (Präsenz)

Sei G eine endliche Gruppe und p eine Primzahl. Genau dann ist G eine p -Gruppe, wenn $\text{ord}(g)$ für jedes $g \in G$ eine p -Potenz ist.

Lösung:

Wir betrachten beide Richtungen der Äquivalenz.

(\Rightarrow) Ist G eine p -Gruppe, so ist $\text{ord}(p)$ Teiler der Ordnung von G für jedes $g \in G$ (Lagrange), d.h. $\text{ord}(g)$ ist eine p -Potenz für jedes $g \in G$, da $\#G$ eine p -Potenz ist.

(\Leftarrow) Umgekehrt sei G eine endliche Gruppe mit

$$\forall g \in G \ \exists n \in \mathbb{N} : \text{ord}(g) = p^n \quad (\star)$$

Es sei q eine Primzahl, die $\#G$ teilt. Nach dem Satz von Cauchy (7.3) gilt: $\exists g \in G : \text{ord}(g) = q$. Aus Gleichung (\star) folgt $\text{ord}(g) = q = p$. Deswegen ist G eine p -Gruppe.

Übung 65 (Präsenz)

Es seien G eine endliche Gruppe der Ordnung 39 und X eine G -Menge der Kardinalität 23. Zeigen Sie, dass X einen Fixpunkt unter G hat.

Lösung:

Aus $\#G = 39$ und $|X| = 23$, dem Satz von Lagrange und 6.11 gilt $\#x^G \in \{1, 3, 13, 39\}$ für alle $x \in X$. Es seien a die Anzahl der Bahnen der Kardinalität 1, b die Anzahl der Bahnen der Kardinalität 3, c die Anzahl der Bahnen der Kardinalität 13. Dann gilt $23 = a + 3b + 13c$, insbesondere gilt $c \in \{0, 1\}$ (da $13 \cdot 2 = 26 > 23$). Ist $c = 0$, so gilt $23 = a + 3b$. Ist $a = 0$, so ist $23 = 3b$, was unmöglich ist, also $a \geq 1$. Ist $c = 1$, so gilt $a + 3b = 10$. Ist $a = 0$, so gilt $3b = 10$, was unmöglich ist. Deswegen gilt $a \geq 1$.

Bemerkung: Der Stabilisator G_{x_0} besteht aus den $g \in G$, die x_0 als Fixpunkt haben.

Thema: Sylow-Sätze, einfache Gruppen, auflösbare Gruppen

Übung 66 (Vorbereitung)

Sei $\Delta := \{(g, g) : g \in G\}$. Dann ist $\Delta \leq G \times G$. Ist G abelsch, so ist $\Delta \trianglelefteq G \times G$ und $(G \times G)/\Delta \cong G$. Ist G nicht abelsch, so ist $\Delta \not\trianglelefteq G \times G$

Lösung:

Wir präsentieren hier nur die Lösung für den Teil $(G \times G)/\Delta \cong G$. Betrachte dazu die Abbildung

$$f: \begin{cases} G \times G & \rightarrow G \\ (g_1, g_2) & \mapsto f(g_1, g_2) = g_1 \cdot g_2^{-1} \end{cases}$$

Da G abelsch ist, ist f ein Gruppenhomomorphismus:

$$\begin{aligned} \forall g_1, g_2, g_3, g_4 \in G : f((g_1, g_2) \cdot (g_3, g_4)) &= f(g_1 g_3, g_2 g_4) \\ &= g_1 g_3 \cdot (g_2 g_4)^{-1} \\ &= g_1 g_2^{-1} g_3 g_4^{-1} \\ &= f(g_1, g_2) \cdot f(g_3, g_4) \end{aligned}$$

Es ist klar, dass f surjektiv ist, da alle $g \in G$ dargestellt werden können als $f(g_1, 1) = g$. Außerdem gilt

$$\begin{aligned} \text{Ker}(f) &= \{(g_1, g_2) \in G \times G : f(g_1, g_2) = 1\} \\ &= \{(g_1, g_2) \in G \times G : g_1 \cdot g_2^{-1} = 1\} \\ &= \{(g_1, g_2) \in G \times G : g_1 = g_2\} \\ &= \Delta \end{aligned}$$

Mit 3.9 aus der Vorlesung schließen wir nun $(G \times G)/\text{Ker}(f) \cong \text{Im}(f) \Leftrightarrow (G \times G)/\Delta \cong G$.

Übung 68

Bestimmen Sie die Anzahl der k -Zykel $\sigma \in S_n$ für $k \in \mathbb{N}$.

Lösung:

Es seien $n \geq 1$ und $k \geq 1$. Ist $k > n$, so gibt es keinen k -Zykel in S_n . Ist $k \leq n$, so gibt es genau

$$\frac{n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-k+1)}{k}$$

k -Zykel in S_n , bzw. in anderer Darstellungsweise ist die Anzahl der k -Zykel in S_n

$$\frac{n!}{(n-k)! \cdot k}$$

Betrachte zur Veranschaulichung

$$(a_1 a_2 \cdots a_k) = (a_2 a_3 \cdots a_k a_1) = (a_3 a_4 \cdots a_k a_1 a_2) = \cdots$$

Übung 69

Ist G endlich und einfach und $H \leq G$ mit $n = (G : H) \geq 2$, so ist $\#G \mid n!$.

Lösung:

Betrachte die folgende Abbildung

$$\psi: \begin{cases} H \backslash G \times G & \rightarrow G \\ (Hg_1, g_2) & \mapsto (Hg_1)^{g_2} = Hg_1g_2 \end{cases}$$

ψ ist eine Wirkung:

$$(i) \quad \forall g \in G: \quad (Hg)^1 = Hg \cdot 1 = Hg$$

$$(ii) \quad \forall g_1, g_2, g_3 \in G: \quad ((Hg_1)^{g_2})^{g_3} = (Hg_1g_2)^{g_3} = Hg_1g_2g_3 = (Hg_1)^{g_2 \cdot g_3}$$

Betrachte den Kern der Wirkung

$$\varphi: \begin{cases} G & \rightarrow S_{(H \backslash G)} \\ g & \mapsto \varphi(g): H \backslash G \rightarrow H \backslash G, Hl \mapsto (Hl)^g \end{cases} \quad (\text{vgl. 6.3})$$

$$\text{mit } \text{Ker}(\varphi) = \{g \in G \mid \forall l \in G: (Hl)^g = Hl\}$$

Da G einfach ist und $\text{Ker}(\varphi) \trianglelefteq G$, gilt $\text{Ker}(\varphi) = 1$ oder $\text{Ker}(\varphi) = G$. Ist $\text{Ker}(\varphi) = 1$, so ist $G \cong \text{Im}(\varphi)$ nach 3.9, insbesondere gilt $\#G = \#\text{Im}(\varphi)$ und $|S_{H \backslash G}| = (G : H)! = n!$. Ist $\text{Ker}(\varphi) = G$, so gilt $H = G$:

▷ $H \subseteq G$ ist klar

▷ $G \subseteq H$. Es reicht zu zeigen, dass $\text{Ker}(\varphi) \subseteq H$ gilt. Sei $g \in \text{Ker}(\varphi)$, d.h. für alle $l \in G$ ist $Hlg = Hl$. Insbesondere ist für $l = 1$ dann $Hg = H$, d.h. also $g \in H$.

Es ist also $G = H$, was jedoch falsch ist, da $(G : H) \geq 2$. Somit ist $\text{Ker}(\varphi) = G$ nicht möglich.

Übung 70

Keine Gruppe der Ordnung 312, 12 oder 300 ist einfach.

Lösung:

Wir zeigen die Eigenschaft nicht einfach zu sein für die entsprechenden Gruppen nacheinander.

- (1) Sei G eine Gruppe der Ordnung $312 = 2 \cdot 156 = 2 \cdot 2 \cdot 78 = 2 \cdot 2 \cdot 2 \cdot 39 = 2^3 \cdot 3 \cdot 13$. Sei n_{13} die Anzahl der 13-Sylowgruppen von G . Nach den Sylowsätzen gilt $n_{13} \equiv 1 \pmod{13}$ und $n_{13} \mid 24$. Die Teiler von 24 sind genau 1, 24, 2, 12, 3, 8, 4, 6. Deswegen ist $n_{13} = 1$, d.h. es gibt genau eine 13-Sylowgruppe N_{13} von G . Mit 8.7 ist $N_{13} \trianglelefteq G$. Da $\#G = 312$ und $\#N_{13} = 13$, ist $1 \neq N_{13} \neq G$, also ist G nicht einfach.
- (2) Ist G eine endliche Gruppe der Ordnung $12 = 2^3 \cdot 3$. Es seien n_2 die Anzahl der 2-Sylowgruppen von G und n_3 die Anzahl der 3-Sylowgruppen von G . Nach den Sylowsätzen gilt

$$\begin{cases} n_2 \equiv 1 \pmod{12} \\ n_2 \mid 3 \end{cases} \quad \text{und} \quad \begin{cases} n_3 \equiv 1 \pmod{3} \\ n_3 \mid 4 \end{cases}$$

d.h. $n_2 \in \{1, 3\}$ und $n_3 \in \{1, 4\}$. Ist $n_3 = 4$, so schreibe N_1, N_2, N_3, N_4 für die vier 3-Sylowgruppen von G . Da $|N_1| = |N_2| = |N_3| = |N_4| = 3$ und $N_i \cap N_j = 1$ für $i \neq j$ (da 3 prim ist), besitzt G mindestens acht Elemente der Ordnung 3:

- $N_1 = \{1, a_1, b_1\}$ mit $\text{ord}(a_1) = 3 = \text{ord}(b_1)$
- $N_2 = \{1, a_2, b_2\}$ mit $\text{ord}(a_2) = 3 = \text{ord}(b_2)$

Ist $a_1 = a_2$, so ist $|N_1 \cap N_2| \geq 2$, was falsch ist. Sei nun $n_2 = 3$. Schreibe K_1, K_2, K_3 für die drei 2-Sylowgruppen von G . Da $|K_1| = |K_2| = |K_3| = 4$, besitzt G mindestens vier Elemente von Ordnung 2 oder 4. Insgesamt gilt $n_3 = 4$ und $n_2 = 3 \Rightarrow 12 = \#G = 8 + 4 + 1 = 13$ (8 Elemente der Ordnung 3, 4 Elemente der Ordnung 2 oder 4 und ein neutrales Element), was falsch ist. Deswegen gilt $n_3 = 1$ oder $n_2 = 1$. In jedem Fall ist G aber nicht einfach.

- (3) Es sei G eine endliche Gruppe der Ordnung $300 = 30 \cdot 10 = 5 \cdot 6 \cdot 5 \cdot 2 = 2^2 \cdot 3 \cdot 5^2$. Es sei n_5 die Anzahl der 5-Sylowgruppen von G . Nach den Sylowsätzen gilt $n_5 \equiv 1 \pmod{5}$ und $n_5 \mid 12$, d.h. auf jeden Fall ist $n_5 \in \{1, 6\}$. Es sei N_5 eine 5-Sylowgruppe von G . Ist $n_5 = 6$, so ist $(G : N_G(N_5)) = 6$ (vgl. 8.6). Ist G auch einfach so gilt $\#G = 300 = 2^2 \cdot 3 \cdot 5^2 \mid 6! = 2^4 \cdot 3^2 \cdot 5$ (vgl. Ü49), was falsch ist (vergleiche die beiden Primfaktorenzerlegungen). Deswegen gilt $n_5 = 1$ oder G ist nicht einfach. In jedem Fall aber ist G nicht einfach.

Übung 81 (Präsenz)

Geben Sie ein Beispiel einer endlichen Gruppe G , die

- (i) einfach und auflösbar ist
- (ii) nicht einfach und auflösbar ist
- (iii) einfach und nicht auflösbar ist
- (iv) nicht einfach und nicht auflösbar ist.

Lösung:

Wir geben jeweils ein Beispiel an und zeigen, dass die entsprechenden Eigenschaften gelten.

- (i) Die Gruppe $\mathbb{Z}/2\mathbb{Z}$ ist einfach (vgl. 9.3). Dann besitzt $\mathbb{Z}/2\mathbb{Z}$ die Kompositionsreihe $1 \trianglelefteq \mathbb{Z}/2\mathbb{Z}$ und $(\mathbb{Z}/2\mathbb{Z})/1 = \mathbb{Z}/2\mathbb{Z}$ ist zyklisch. Somit ist $\mathbb{Z}/2\mathbb{Z}$ auflösbar.
- (ii) Die Gruppe $\mathbb{Z}/4\mathbb{Z}$ ist nicht einfach, da $\mathbb{Z}/4\mathbb{Z}$ einen Normalteiler der Ordnung 2 besitzt. Außerdem besitzt $\mathbb{Z}/4\mathbb{Z}$ die Normalreihe $1 \triangleleft \mathbb{Z}/2\mathbb{Z} \triangleleft \mathbb{Z}/4\mathbb{Z}$, die eine Kompositionsreihe ist, da
 - $(\mathbb{Z}/4\mathbb{Z})/(\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ ist einfach
 - $(\mathbb{Z}/2\mathbb{Z})/1 \cong \mathbb{Z}/2\mathbb{Z}$ ist einfach

Da die Faktoren dieser Kompositonsreihe zyklisch sind, ist $\mathbb{Z}/4\mathbb{Z}$ auflösbar.

- (iii) Mit 9.11 ist A_5 einfach. Deswegen besitzt A_5 *genau* eine Kompositonsreihe $1 \triangleleft A_5$. Da $A_5/1 \cong A_5$ nicht zyklisch ist, ist A_5 nicht auflösbar.
- (iv) Die Gruppe S_5 ist nicht einfach, da $(S_5 : A_5) = 2$ und $A_5 \triangleleft S_5$. Da die Normalteiler der S_5 genau 1, A_5 und S_5 sind und S_5 nicht einfach ist, besitzt die S_5 genau eine Kompositi-
onsreihe, nämlich $1 \triangleleft A_5 \triangleleft S_5$. Es gilt $S_5/A_5 \cong \mathbb{Z}/2\mathbb{Z}$ und $A_5/1 \cong A_5$ ist nicht zyklisch. Deswegen ist die S_5 nicht auflösbar.

Übung 82 (Präsenz)

Für welche $n \geq 1$ ist $S_n \cong A_n \times C_2$?

Lösung:

Leider gab es dazu keine Lösung in der Übung.

Übung 106 (Vorbereitung)

Berechnen Sie $\text{ggT}(n, 2019)$ mit dem euklidischen Algorithmus, wobei n Ihr Geburtsjahr ist.

Lösung:

Sei $n = 1999$. Dann folgt mit dem euklidischen Algorithmus:

$$2019 = 1 \cdot 1999 + 20$$

$$1999 = 99 \cdot 20 + 19$$

$$20 = 1 \cdot 19 + 1$$

$$19 = 19 \cdot 1 + 0$$

Damit ist $\text{ggT}(1999, 2019) = 1$, was bereits klar ist, da 1999 prim ist.

Übung 107 (Vorbereitung)

Bestimmen Sie $x, y \in \mathbb{Z}$ mit

$$13x + 17y = \text{ggT}(13, 17) \quad (1)$$

Bestimmen Sie außerdem $x, y \in \mathbb{Z}$ mit

$$13x + 17y = 3 \quad (2)$$

Lösung:

Mit dem euklidischen Algorithmus folgt

$$17 = 1 \cdot 13 + 4$$

$$13 = 4 \cdot 4 + 1$$

$$4 = 4 \cdot 1 + 0$$

Durch Rückwärtseinsetzen der Reste ausgehend von der vorletzten Gleichung erhalten wir

$$\begin{aligned} 1 &= 13 - 3 \cdot 4 \\ &= 13 - 3 \cdot (17 - 13) \\ &= 4 \cdot 13 - 3 \cdot 17 \end{aligned}$$

Somit ist $(x, y) = (4, -3)$ eine Lösung von Gleichung (1). Multiplizieren wir die Gleichung mit dem Faktor 3, so ist $(x, y) = (12, -9)$ eine Lösung von Gleichung (2).

Übung 108 (Vorbereitung)

$\mathbb{Z}[X]$ und $K[X, Y]$ sind keine Hauptidealringe.

Lösung:

Um zu zeigen, dass $\mathbb{Z}[X]$ kein Hauptidealring ist, betrachten wir das Ideal $(2, X)$ und zeigen, dass dies wirklich ein Ideal ist. Wir zeigen hier nur die Abgeschlossenheit unter Multiplikation mit Elementen aus $\mathbb{Z}[X]$. Sei dazu $f \in \mathbb{Z}[X]$, dann ist

$$f \cdot (a \cdot 2 + b \cdot X) = f \cdot a \cdot 2 + f \cdot b \cdot X = \underbrace{(f \cdot a)}_{\in \mathbb{Z}[X]} \cdot 2 + \underbrace{(f \cdot b)}_{\in \mathbb{Z}[X]} \cdot X \in (2, X)$$

Für $K[X, Y]$ ist beispielsweise (X, Y) ein Ideal und damit $K[X, Y]$ kein Hauptidealring.

Übung 110

Definiere $R_0 = R$ und $R_{i+1} := R_i[X_{i+1}]$. Dann ist $R_n \cong R[X_1, \dots, X_n]$.

Lösung:

Wir lösen die Aufgabe durch vollständige Induktion über $n \geq 0$. Für $n = 0$ gilt $R_0 = R$. Für $n = 1$ gilt $R_1 = R_0[X_1] = R[X_1]$. Sei daher nun $n > 1$. Wir setzen voraus, dass es Isomorphismen $\Phi_n: R_n \rightarrow R[X_1, \dots, X_n]$ sowie $\Psi_n: R[X_1, \dots, X_n] \rightarrow R_n$ gibt mit

$$\Phi_n \circ \Psi_n = \text{id}_{R[X_1, \dots, X_n]} \quad (3a)$$

$$\Psi_n \circ \Phi_n = \text{id}_{R_n}$$

$$\Phi_n|_R = \text{id}_R \quad (3b)$$

$$\Psi_n|_R = \text{id}_R$$

$$\Psi_n(X_i) = \Phi_n(X_i) = X_i \text{ für alle } i \in \{1, \dots, n\} \quad (3c)$$

Betrachte die Abbildung

$$\iota: \begin{cases} R & \rightarrow R_{n+1} \\ x & \mapsto x \end{cases} \quad (4)$$

Mit Ü89 gibt es dann $\Psi_{n+1}: R[X_1, \dots, X_{n+1}] \rightarrow R_{n+1}$ mit $\Psi_{n+1}(X_i) = X_i$ für alle $i \in \{1, \dots, n+1\}$ und $\Psi_{n+1}(x) = \iota(x) = x$ für alle $x \in R$.

Betrachte die Abbildung

$$\kappa: \begin{cases} R_n & \rightarrow R[X_1, \dots, X_{n+1}] \\ x & \mapsto \Phi_n(x) \end{cases} \quad (5)$$

Mit Ü89 gibt es $\Phi_{n+1}: R_n[X_{n+1}] \rightarrow R[X_1, \dots, X_{n+1}]$ mit

$$\Phi_{n+1}(X_{n+1}) = X_{n+1} \text{ und} \quad (6a)$$

$$\Phi_{n+1}(x) = \Phi_n(x) \text{ für alle } x \in R_n \quad (6b)$$

Da $\Psi_n(x) \stackrel{(3b)}{=} x$ für jedes $x \in R$ und $\Psi_n(X_i) \stackrel{(3c)}{=} X_i$ für jedes $i \in \{1, \dots, n\}$ gilt auch $\Psi_{n+1}|_{R[X_1, \dots, X_n]} = \Psi_n$.

Übung 111

Es sei R nullteilerfrei und $\iota: R \rightarrow K := \text{Quot}(R)$. Beweisen Sie die universelle Eigenschaft des Quotientenkörpers: Ist L ein Körper und $\varphi \in \text{Hom}(R, L)$ injektiv, so gibt es genau ein $\varphi' \in \text{Hom}(K, L)$ mit $\varphi' \circ \iota = \varphi$.

Lösung:

Es seien L ein Körper und $\varphi \in \text{Hom}(R, L)$ injektiv. Da φ injektiv ist, ist $\varphi(b) \neq 0$ für alle $b \in R \setminus \{0\}$. Betrachte die Abbildung

$$\psi: \begin{cases} K & \rightarrow L \\ \frac{a}{b} & \mapsto \varphi(\frac{a}{b}) = \varphi(a) \cdot \varphi(b)^{-1} \end{cases}$$

