TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Mathematik Institut für Algebra, Professur für Algebra

GEOMETRIE

Übungen

Prof. Dr. Arno Fehm

Wintersemester 2018/19

Autor : Eric Kunze
E-Mail : eric.kunze@mailbox.tu-dresden.de

Übungsblatt 1

Eric Kunze
Übungsleiter: Dr. Legrand
Wintersemester 2018/19

Geometrie

Thema: Gruppen, Ordnung und Index, symmetrische Gruppe

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

Übung 7

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

Lösung. Es sei $h \in H$.
f surjektiv $\quad \Rightarrow \quad \exists\, g_0 \in G : f(g_0) = h$
Für $g \in \operatorname{Ker}(f)$ gilt

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

d.h. die Abbildung $\varphi : \operatorname{Ker}(f) \to f^{-1}(h), g \mapsto \varphi(g) := g \cdot g_0$ 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. $g \cdot g_0^{-1} \in \operatorname{Ker}(f)$ und $\varphi(g \cdot g_0^{-1}) = g \cdot g_0^{-1} \cdot g_0 = g$.
- φ ist injektiv: Es seien $g_1, g_2 \in \operatorname{Ker}(f)$ mit $\varphi(g_1) = \varphi(g_2)$, d.h. $g_1 \cdot g_0 = g_2 \cdot g_0$
  $\Rightarrow \quad g_1 = g_2$.
- Dann ist φ bijektiv, d.h. $\left|f^{-1}(h)\right| = |\operatorname{Ker}(f)|$.

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

  $$|G| = \left| \biguplus_{h \in H} f^{-1}(h) \right| = \sum_{h \in H} \left|f^{-1}(h)\right| = \sum_{h \in H} |\operatorname{Ker}(f)| = |\operatorname{Ker}(f)| \cdot |H|$$

Übung 8
Zeigen Sie: Für $k, n \in \mathbb{N}$ ist $\operatorname{ord}(k + n\mathbb{Z}) = \frac{\operatorname{kgV}(k,n)}{k} = \frac{n}{\operatorname{ggT}(k,n)}$.

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

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

Für $m \in \mathbb{N}\backslash\{0\}$ 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 $\operatorname{ord}(k + n\mathbb{Z}) = n_1 = \frac{n}{\operatorname{ggT}(k,n)}$. □

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:

(1) Sind $K, N \leq G$, so ist $K \cup N \leq G$.

(2) Sind $K, N \leq G$, so ist $K \cdot N \leq G$.

Lösung. (1) 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.

(2) Auch diese Aussage ist falsch. Betrachte dazu $K := \{\mathrm{id}, (1\,2)\} \leq S_3$ und $N := \{\mathrm{id}, (1\,3)\} \leq S_3$. Dann ist $K \cdot N = \{\mathrm{id}, (1\,2), (1\,2), (1\,2)(1\,3) = (1\,3\,2)\} \not\leq S_3$ nach dem Satz von Lagrange, da $|KN| = 4 \nmid 6 = \#S_3$. □

Übungsblatt 2

Eric Kunze
Übungsleiter: Dr. Legrand
Wintersemester 2018/19

Geometrie

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 $S_n = \langle (1\,2) \rangle \ltimes A_n$.

Lösung. Es sei $n \in \mathbb{N}$ mit $n \geq 2$. Nach 5.6 ist zu zeigen, dass $A_n \trianglelefteq S_n$, $A_n \cap \langle (1\,2) \rangle = \{\mathrm{id}\}$ und $\langle (1\,2) \rangle \cdot A_n = S_n$ gelten. Da A_n der Kern des Homomorphismus $\mathrm{sgn}\colon S_n \to \mu_2$ ist, gilt $A_n \trianglelefteq S_n$ (vgl. 3.5). Aus $(1\,2) \notin A_n$ folgt $A_n \cap \langle (1\,2) \rangle = \{\mathrm{id}\}$. Dann zeigen wir, dass $H = \langle (1\,2) \rangle \cdot A_n = S_n$ gilt. Es sei $\sigma \in S_n$. Ist $\sigma \in A_n$, so gilt $\sigma = \mathrm{id} \cdot \sigma \in H$. Ist $\sigma \notin A_n$, so gelten $(1\,2) \cdot \sigma \in A_n$ und $\sigma = (1\,2) \cdot ((1\,2) \cdot \sigma) \in H$.

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

Übung 26

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 $\mathrm{ord}(g) \in \{1, 2, 3, 6\}$ für jedes $g \in G$.

- Ist $\mathrm{ord}(g) \in \{1, 2\}$ 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 $\mathrm{ord}(g) \in \{3, 6\}$. In beiden Fällen, gibt es ein $g_1 \in G$ mit $\mathrm{ord}(g_1) = 3$ (ist $\mathrm{ord}(g) = 6$, so ist $\mathrm{ord}(g^2) = 3$). Außerdem gibt es $g_2 \in G$ mit $\mathrm{ord}(g_2) = 2$ (vgl. H10). Dann bekommen wir: $\langle g_1 \rangle \trianglelefteq G$ (vgl. P41), $\langle g_1 \rangle \cap \langle g_2 \rangle = \{1\}$ (da $\mathrm{ggT}(2, 3) = 1$) und $\langle g_1 \rangle \cdot \langle g_2 \rangle = G$ mit dem selben Argument wie in Ü25. Somit ist $G = \langle g_2 \rangle \ltimes \langle g_1 \rangle$ (vgl. 5.6). Aus 5.12 folgt dann $G \cong C_6$ oder $G \cong S_3$. □

Übung 27
Zu welcher Ihnen bekannten Gruppe ist $\mathrm{Aut}(V_4)$ isomorph?

Lösung. Aus W4 ergibt sich $\mathrm{Aut}(V_4) \cong \mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^2) = \mathrm{Aut}(\mathbb{F}_2^2)$ (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 $\mathrm{Aut}(V_4) \cong \mathrm{GL}_2(\mathbb{F}_2)$, die eine nicht abelsche Gruppe der Ordnung 6 ist (zählen Sie einfach die Elemente der $\mathrm{GL}(\mathbb{F}_2)$ auf). Mit Ü27 schließen wir, dass $\mathrm{Aut}(V_4) \cong S_3$.

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 $\sigma : V_4 \to V_4$ auch tatsächlich ein Gruppenhomomorphismus ist. $\square$

Übung 41 (Präsenz)
Sei $H \leq G$. Zeige oder widerlege:

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

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

Lösung. a) richtig. Angenommen $H \ntrianglelefteq G$. Sei $h \in H$ mit $hH = H = Hh$ und $g \in G \setminus H$ mit $gH \neq Hg$. Wegen $(G\colon H) = 2$ gilt $gH = H$, das heißt $\exists H \in H$ mit $gh \in H$. Dann folgt

$$\underbrace{gh}_{\in H} \cdot \underbrace{h^{-1}}_{\in H} = g \in H \tag{2.1}$$ $\square$

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

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

$$(1\,3)\langle(1\,2)\rangle) = \{(1\,3), (1\,3\,2)\} \text{ und } \langle(1\,2)\rangle)(1\,3) = \{(1\,3), (1\,2\,3)\}$$

Übungsblatt 3

Eric Kunze
Übungsleiter: Dr. Legrand
Wintersemester 2018/19

Geometrie

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 $S \in \mathrm{Syl}_p(G)$. 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 $\mathrm{Syl}_p(G)$. Aus den Sylow-Sätzen folgt $n_p = 1 \mod p$ 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: $S \trianglelefteq G \;\;\Leftrightarrow\;\; \#\mathrm{Syl}_p(G) = 1$) □

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 $\Gamma_1 = \mathrm{Stab}(1)$ und folgern Sie, dass

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

Lösung. ▪ Betrachte die Abbildung

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

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 $x \in H_1H_2$ 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

$$\begin{aligned} ((g_1g_2)^{(h_1,h_2)})^{(l_1,l_2)} &= (h_1^{-1}g_1g_2h_2)^{(l_1,l_2)} = l_1^{-1}h_1^{-1}g_1g_2h_2l_2 \\ &= (h_1l_1)^{-1}g_1g_2(h_2l_2) = (g_1g_2)^{(h_1l_1,h_2l_2)} \\ &= (g_1g_2)^{(h_1,h_2)\cdot(l_1,l_2)} \end{aligned}$$

- ψ ist transitiv: Es seien $x, y \in H_1H_2$. Schreibe wieder $x = g_1g_2$ mit $g_1 \in H_1, g_2 \in H_2$ und $y = l_1l_2$ mit $l_1 \in H_1, l_2 \in H_2$. Dann gilt

$$y = l_1l_2 = l_1g_1^{-1}g_1g_2g_2^{-1}l_2 = \underbrace{(g_1l_1^{-1})^{-1}}_{\in H_1} \cdot x \cdot \underbrace{(g_2^{-1}l_2)}_{\in H_2}$$

- Es gilt:

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

- Deswegen gilt

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

Übung 50

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

Lösung. Es sein G eine endliche Gruppe und n_5 die Anzahl der 5-Sylowgruppen von G. Nach den Sylow-Sätzen ist $n_5 = 1 \mod 5$ 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 $N_5 \trianglelefteq G$. Es sei N_2 eine 2-Sylowgruppe von G; es gilt $|N_2| = 4$ (vgl. dazu 8.2: $\#G = p^k \cdot m$ mit $p \nmid m \Rightarrow 20 = 2^2 \cdot 5 \Rightarrow H \in \mathrm{Syl}_2(G) \Rightarrow |H| = p^k = 4$). Da $\mathrm{ggT}(4, 5) = 1$ 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 $G \cong N_2 \ltimes_\alpha N_5$. 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 $C_4 \ltimes_\alpha C_5$ oder $V_4 \ltimes_\alpha C_5$. □

Übung 63 (Präsenz)
Geben Sie ein Beispiel einer Gruppe G und einer G-Menge X mit $G_x = \mathrm{Stab}(x) \ntrianglelefteq G$ für ein $x \in X$.

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

$$\psi \colon \begin{cases} \{1, \ldots, n\} \times S_n & \to & S_n \\ (\sigma, i) & \mapsto & i^\sigma = \sigma(i) \end{cases}$$

Es gilt $\mathrm{Stab}(n) = \{\sigma \in S_n : \sigma(n) = n\}$. Aber $\mathrm{Stab}(n) \ntrianglelefteq S_n$:

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

Übung 64 (Präsenz)
Sei G eine endliche Gruppe und p eine Primzahl. Genau dann ist G eine p-Gruppe, wenn $\mathrm{ord}(g)$ für jedes $g \in G$ eine p-Potenz ist.

Lösung. Wir betrachten beide Richtungen der Äquivalenz.

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

($\Leftarrow$) Umgekehrt sei G eine endliche Gruppe mit

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

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

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 $a \geq 1$. $\square$

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

Übungsblatt 4

Geometrie

Eric Kunze
Übungsleiter: Dr. Legrand
Wintersemester 2018/19

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 $\Delta \ntrianglelefteq G \times G$

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

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

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

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

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

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

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

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

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

ψ ist eine Wirkung:

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

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

Betrachte den Kern der Wirkung

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

mit $\operatorname{Ker}(\varphi) = \{g \in G \mid \forall l \in G : (Hl)^g = Hl\}$
Da G einfach ist und $\operatorname{Ker}(\varphi) \trianglelefteq G$, gilt $\operatorname{Ker}(\varphi) = 1$ oder $\operatorname{Ker}(\varphi) = G$. Ist $\operatorname{Ker}(\varphi) = 1$, so ist $G \cong \operatorname{Im}(G)$ nach 3.9, insbesondere gilt $\#G = \#\operatorname{Im}(\varphi)$ und $\left|S_{H\backslash G}\right| = (G : H)! = n!$. Ist $\operatorname{Ker}(\varphi) = G$, so gilt $H = G$:

- $H \subseteq G$ ist klar
- $G \subseteq H$. Es reicht zu zeigen, dass $\operatorname{Ker}(\varphi) \subseteq H$ gilt. Sei $g \in \operatorname{Ker}(\varphi)$, 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 $\operatorname{Ker}(\varphi) = G$ 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 $n_{13} \equiv 1 \mod 13$ 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

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

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

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 $n_5 \equiv 1 \mod 5$ 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 $(G : \mathbb{N}_G(N_5)) = 6$ (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 $1 \lhd \mathbb{Z}/2\mathbb{Z} \lhd \mathbb{Z}/4\mathbb{Z}$, 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 $1 \lhd A_5$. 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 $A_5 \lhd S_5$. 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 Kompositionsreihe, nämlich $1 \lhd A_5 \lhd S_5$. 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. □

Übungsblatt 5

Geometrie

Eric Kunze
Übungsleiter: Dr. Legrand
Wintersemester 2018/19

Thema: auflösbare Gruppen, Ringe und Ideale

Lemma 1

Die Normalteiler der A_4 sind genau 1, V_4 und A_4.

Beweis. Dass alle drei Untergruppen Normalteiler sind, ist klar. Betrachten wir die Umkehrung. Sei dazu $N \trianglelefteq A_4$. Mit dem Satz von Lagrange gilt $\#N \in \{1, 2, 3, 4, 6, 12\}$. Ist $\#N = 1$, so ist $N = 1$, insbesondere ist $N \trianglelefteq A_4$.
Ist $\#N = 12$, so ist $N = A_4$. Deswegen ist $N \trianglelefteq A_4$.
Ist $\#N = 6$, so gibt es einen Widerspruch zu H11.
Ist $\#N = 4$, so ist $N = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(3\,2)\} = V_4$.
Ist $\#N = 2$, so gibt es $(a\,b)(c\,d)$ mit $N = \{\mathrm{id}, (a\,b)(c\,d)\}$. Da $(a\,b\,c) \circ (a\,b) \circ (c\,d) \circ (a\,c\,b) = (a\,d)(b\,c) \notin N$, ist $N \ntrianglelefteq A_4$.
Ist $\#N = 3$, so gibt es einen Widerspruch (wie im Fall $\#N = 2$). □

Übung 84 (Vorbereitung)

Ist $\#G \leq 9$, so ist G auflösbar.

Lösung.
- Für $\#G = 1$ ist die Auflösbarkeit klar.
- Für $\#G \in \{2, 3, 5, 7\}$ ist G zyklisch und damit auflösbar.
- Für $\#G \in \{4, 9\}$ ist G abelsch und somit auflösbar.
- Für $\#G = 8 = 2^3$ ist G eine p-Gruppe und damit auflösbar.
- Ist $\#G = 6$, so ist $G \cong C_6$, welche abelsch ist, oder $G \cong S_3$, die nach Beispiel der Vorlesung auflösbar ist (vgl. auch Ü27).

In jedem Fall ist G also auflösbar. □

Übung 85 (Vorbereitung)

Prüfen Sie nach, dass die Abbildung im Beweis von II.1.12 tatsächlich ein Ringhomomorphismus ist. Für $\varphi \in \mathrm{Hom}(R, S)$ ist diese definiert als

$$\varphi_s : \begin{cases} R\,[X] & \to & S \\ \sum_{i\geq 0} a_i X^i & \mapsto & \sum_{i \geq 0} \varphi(a_i) s^i \end{cases}$$

Lösung. Seien $f = \sum_{i\geq 0} a_i X^i, g = \sum_{i\geq 0} b_i X^i \in R[X]$. Dann ist

$$\begin{aligned}
\varphi_s(f+g) &= \varphi_s\left(\sum_{i\geq 0} a_i X^i + \sum_{i\geq 0} b_i X^i\right) \\
&= \varphi_s\left(\sum_{i\geq 0} (a_i + b_i) X^i\right) \\
&= \sum_{i\geq 0} \varphi(a_i + b_i) s^i \\
&\overset{\varphi\in\mathrm{Hom}}{=} \sum_{i\geq 0} \left(\varphi(a_i) + \varphi(b_i)\right) s^i \\
&= \sum_{i\geq 0} \varphi(a_i) s^i + \sum_{i\geq 0} \varphi(b_i) s^i \\
&= \varphi_s(f) + \varphi(s(g)
\end{aligned}$$

Die Multiplikativität folgt dann analog. □

Übung 86

Ist $\#G = pq$ mit Primzahlen p und q, so ist G auflösbar.

Lösung. Es seien p und q Primzahlen und G eine Gruppe mit $\#G = p \cdot q$.

- Ist $p = q$, so ist $\#G = p^2$ und G deswegen abelsch. Insbesondere ist G auflösbar.
- Ist $p \neq q$, so gilt $G \cong C_p \ltimes_\alpha C_q$ oder $G \cong C_q \ltimes_\alpha C_p$ (vgl. 8.9). Mit 10.7 schließen wir, dass G auflösbar ist. □

Übung 87

Bestimmen Sie die Kommutatorgruppen S_n' und A_n' für $n \geq 2$.

Lösung.
- Sei $n \geq 5$. Da $S_n' \trianglelefteq S_n$ und die Normalteiler von S_n sind $1, A_n, S_n$. Damit ist $S_n' \in \{1, A_n, S_n\}$. Ist $S_n' = 1$, so ist S_n abelsch, was falsch ist. Es gilt $S_n' \subseteq A_n$. Deswegen ist $S_n' = A_n$. Da $n \geq 5$ gilt, ist A_n einfach. Deswegen gilt $A_n' \in \{1, A_n\}$. Ist $A_n' = 1$, so ist A_n abelsch, was falsch ist. Deswegen gilt $A_n' = A_n$.
- Ist $n = 2$, so gelten $S_2 \cong C_2$ und $A_2 = 1$. Insbesondere sind S_2 und A_2 abelsch, d.h. $S_n' = A_n' = 1$.
- Ist $n = 3$, so gilt $S_3' = A_3$ (analog zum ersten Fall). Außerdem ist $A_3 \cong C_3$. Insbesondere ist A_3 abelsch, also $A_3' = 1$.
- Ist $n = 4$, so ist $S_4' \in \{1, V_4, A_4, S_4\}$ (vgl. H72). Da S_4 auflösbar ist, aber nicht abelsch, gilt $S_4' \in \{V_4, A_4\}$. Aber es ist

  $$[(3\,4),(1\,3\,2)] = (3\,4)(1\,2\,3)(3\,4)(1\,3\,2) = (1\,3\,2) \circ (3\,4) \circ (1\,2\,3) \circ (3\,4) = (1)(2\,4\,3) \in S_4' \setminus V_4$$

  Deswegen gilt $S_4' = A_4$.
  Mit Lemma 1 ist $A_4' \in \{1, V_4, A_4\}$. Da A_4 auflösbar, aber nicht abelsch ist, gilt $A_4' = V_4$. □

Übung 88

Die Gruppe $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ ist auflösbar.

Lösung. ■ Wir zeigen, dass jede Gruppe der Ordnung 12 auflösbar ist. Es sei G eine endliche Gruppe der Ordnung 12. Mit Ü70 folgt, dass G nicht einfach ist, d.h. G besitzt einen Normalteiler $N \trianglelefteq G$ mit $\#N \in \{2,3,4,6\}$. Mit V84 sind alle N auflösbar und ${}^{G}\!/\!_{N}$ auflösbar. Mit 10.7 schließen wir, dass auch G auflösbar ist.

■ Die Gruppe $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$besitzt Ordnung $(3^2-1)\cdot(3^2-3) = 8\cdot 6 = 48$. Betrachte die Determinante $\det\colon \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \to (\mathbb{Z}/3\mathbb{Z})^\times$, die Gruppenhomomorphismus ist. Da $\det(\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})) = (\mathbb{Z}/3\mathbb{Z})^\times$, gilt $\#\operatorname{Ker}(\det) = 24$. Es ist klar, dass

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \text{ und } \begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}$$

Elemente von $\mathrm{Z}\operatorname{Ker}(\det)$ sind. Außerdem ist $\operatorname{Ker}(\det)$ nicht abelsch, weil

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} = \begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}$$
$$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}$$

Deswegen gilt $\#\,\mathrm{Z}(\operatorname{Ker}(\det)) \in \{2,3,4,6,8,12\}$. Mit V84 und dem ersten Punkt oben folgt, dass $\mathrm{Z}(\operatorname{Ker}(\det))$ auflösbar ist. Deswegen ist ${}^{\operatorname{Ker}(\det)}\!/\!_{\mathrm{Z}(\operatorname{Ker}(\det))}$ auflösbar. Mit 10.7 bekommen wir, dass $\operatorname{Ker}(\det)$ auflösbar ist. Aber ${}^{\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})}\!/\!_{\operatorname{Ker}(\det)}$ hat Ordnung 2 und ist somit auflösbar. Mit 10.7 schließen wir erneut, dass $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$auflösbar ist.

Bemerkung zur Gruppenordnung: Betrachtet man $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$, dann hat man sowohl für a und c je drei Möglichkeiten, muss aber eine davon wieder abziehen, da $\left(\begin{smallmatrix}0\\ 0\end{smallmatrix}\right)$ keine zulässige Spalte ist. Für b und d muss man schließlich noch die linear abhängigen Möglichkeiten abziehen. □

Übung 89

Formulieren und beweisen Sie die universelle Eigenschaft des Polynomrings $R[X_i : i \in I]$.

Lösung. Es seien R ein Ring und $I \neq \emptyset$ eine Menge. Betrachte den Polynomring $R[X_i : I]$. Weiter Seien S ein Ring und $\varphi\colon R \to S$ ein Ringhomomorphismus sowie $s_i \in S$ für jedes $i \in I$.

zu zeigen: Es gibt genau einen Ringhomomorphismus $\varphi_{(s_i)}\colon R[X_i : I] \to S$, der sowohl $\varphi_{(s_i)}|_R = \varphi$ als auch $\varphi_{(s_i)}(X_i) = s_i$ für jedes $i \in I$ erfüllt.

Beweis: Betrachte die folgende Abbildung

$$\varphi_{(s_i)}\colon \begin{cases} R[X_i : I] & \to & S \\ \sum_\mu a_\mu X^\mu & \mapsto & \sum_\mu \varphi(a_\mu)\prod_i s_i^{\mu_i}\end{cases}$$

Für jedes $r \in R$ gilt $\varphi_{(s_i)}(r) = \varphi(r)$ (klar), d.h. $\varphi_{(s_i)}|_R = \varphi$. Insbesondere gilt $\varphi_{(s_i)}(1) = 1$. Seien $\sum_\mu a_\mu X^\mu, \sum_\mu b_\mu X^\mu \in R[X_i : i \in I]$.

Dann gilt

$$\begin{aligned}\varphi_{(s_i)}\left(\sum_\mu a_\mu X^\mu + \sum_\mu b_\mu X^\mu\right) &= \varphi_{(s_i)}\left(\sum_\mu (a_\mu + b_\mu) X^\mu\right)\\ &= \sum_\mu \varphi(a_\mu + b_\mu)\cdot \prod_i s_i^{\mu_i}\\ &= \sum_\mu \varphi(a_\mu) + \varphi(b_\mu)\cdot \prod_i s_i^{\mu_i}\\ &= \left(\sum_\mu \varphi(a_\mu)\prod_i s_i^{\mu_i}\right) + \left(\sum_\mu \varphi(b_\mu)\prod_i s_i^{\mu_i}\right)\\ &= \varphi_{(s_i)}\left(\sum_\mu a_\mu X^\mu\right) + \varphi_{(s_i)}\left(\sum_\mu b_\mu X^\mu\right)\end{aligned}$$

Analog zeigen wir die Multiplikativität, d.h.

$$\varphi_{(s_i)}\left(\sum_\mu a_\mu X^\mu \cdot \sum_\mu b_\mu X^\mu\right) = \varphi_{(s_i)}\left(\sum_\mu a_\mu X^\mu\right)\cdot \varphi_{(s_i)}\left(\sum_\mu b_\mu X^\mu\right)$$

Deswegen ist $\varphi_{(s_i)}$ ein Ringhomomorphismus. Für jedes $i \in I$ gilt $\varphi_{(s_i)}(X_i) = \varphi(1)\cdot s_i^1 = s_i$. Für die Eindeutigkeit sei $\psi\colon R[X_i\colon i\in I] \to S$ ein Ringhomomorphismus mit $\psi|_R = \varphi$ und $\psi(X_i) = s_i$ für jedes $i \in I$. Für jedes $\sum_\mu a_\mu X^\mu \in R[X_i\colon i \in I]$ gilt

$$\begin{aligned}\psi\left(\sum_\mu a_\mu X^\mu\right) &= \sum_\mu \psi(a_\mu)\cdot\psi\left(X^\mu\right)\\ &= \sum_\mu \varphi(a_\mu)\cdot\psi\left(\prod_i X_i^{\mu_i}\right)\\ &= \sum_\mu \varphi(a_\mu)\cdot\prod_i \psi(X_i)^{\mu_i}\\ &= \sum_\mu \varphi(a_\mu)\cdot\prod_i x_i^{\mu_i}\\ &= \varphi_{(s_i)}\left(\sum_\mu a_\mu X^\mu\right)\end{aligned}$$

Übung 104 (Präsenz)

Sei $R = \mathbb{Z}[X]$. Geben Sie ein Beispiel eines maximalen Ideals und ein Beispiel eines Primideals $(0) \neq \mathfrak{p} \trianglelefteq R$, das nicht maximal ist.

Lösung. ▪ Betrachte das Ideal I von $\mathbb{Z}[X]$, das von X und 2 erzeugt wird (d.h. $I = (2, X)$), sowie die Abbildung

$$\varphi\colon \begin{cases} \mathbb{Z}[X] & \to \quad \mathbb{Z}/2\mathbb{Z} \\ \sum_{i=0}^m a_i X^i & \mapsto \quad a_0 \mod 2 \end{cases}$$

Es ist klar, dass φ Ringhomomorphismus ist und surjektiv. Bestimme den Kern. Sei $\sum_{i=0}^m a_i X^i \in$

$\mathrm{Ker}(\varphi)$. Dann gibt es $b_0 \in \mathbb{Z}$ mit $a_0 = 2b_0$. Dann gilt

$$\sum_{i=0}^{m} a_i X^i = a_0 + \sum_{i=1}^{m} a_i X^i = 2b_0 + X \cdot \sum_{i=1}^{m} a_i X^{i-1} \quad \in I$$

Umgekehrt seien $P(X), Q(X) \in \mathbb{Z}[X]$. Dann gilt

$$\varphi\left(2 \cdot P(X) + X \cdot Q(X)\right) = \varphi(2) \cdot \varphi(P(X)) + \varphi(X) \cdot \varphi(Q(X)) = 0 + 0 = 0$$

Deswegen ist $\mathrm{Ker}(\varphi) = I$. Mit 2.8 bekommen wir ${}^{\mathbb{Z}[X]}/_{I} = \mathbb{Z}/2\mathbb{Z}$, was ein Körper ist. Deswegen ist I maximal (vgl. 2.11).

- Analog zeigen wir, dass $\mathfrak{p} = X \cdot \mathbb{Z}[X]$ prim, aber nicht maximal ist. □

Übung 105 (Präsenz)

Beweisen oder widerlegen Sie: Ist I ein Ideal / Primideal / maximales Ideal von R, so ist $I \cap R_0$ ein Ideal / Primideal / maximales Ideal von R_0

Lösung. Dazu gab es leider keine Lösung in der Übung. □

Übungsblatt 6

Eric Kunze
Übungsleiter: Dr. Legrand
Wintersemester 2018/19

Geometrie

Thema: Kongruenzen, Einheitengruppen, Teilbarkeit

Lemma 1

Sei $x \in \mathbb{Z}[\sqrt{-5}]$. Genau dann ist x eine Einheit, wenn $N(x) = 1$ (vgl. Gleichung (6.7)).

Beweis. Schreibe $x = a + b \cdot \sqrt{-5}$ mit $a, b \in \mathbb{Z}$.

($\Rightarrow$) Ist x eine Einheit, so gibt es $y \in \mathbb{Z}[\sqrt{-5}]$ mit $xy = 1$. Dann gilt $1 = N(1) = N(xy) = N(x) \cdot N(y)$ (Multiplikativität von N ist noch zu zeigen). Da $N(x) \in \mathbb{N}$ gilt $N(x) = 1$.

($\Leftarrow$) Ist $N(x) = 1$, so ist $a^2 + 5b^2 = 1$. Ist $b \neq 0$, so gilt $a^2 + 5b^2 \geq 5$, was falsch ist. Deswegen gilt $b = 0$ und $a^2 = 1$, d.h. $x = \pm 1$. In jedem Fall ist x eine Einheit. □

Lemma 2

$\xi = 1 + \sqrt{-5}$ ist irreduzibel in $\mathbb{Z}[\sqrt{-5}]$.

Beweis. Es ist $N(\xi) = 6 \neq 1$. Deswegen ist ξ keine Einheit nach Lemma 1. Schreibe $\xi = 1 + \sqrt{-5} = xy$ mit $x, y \in \mathbb{Z}[\sqrt{-5}]$ und $x = a + ib, y = c + id$ mit $a, b, c, d \in \mathbb{Z}$. Dann gilt

$$6 = N(\xi) = N(xy) = N(x) \cdot N(y) = (a^2 + 5b^2)(c^2 + 5d^2)$$

Deswegen gilt $a^2 + 5b^2 \in \{1, 2, 3, 6\}$. Ist $b \neq 0$, so gilt $a^2 + 5b^2 \geq 5$, d.h. $a^2 + 5b^2 = 6$ und damit $y = c^2 + 5d^2 = 1$, also y eine Einheit. Ist $b = 0$, so ist $a^2 + 5b^2 = a^2 \in \{0, 1, 4, 9, \ldots\}$. Deswegen ist $a = 1$ und x somit eine Einheit. In jedem Fall ist $\xi = 1 + \sqrt{-5}$ irreduzibel. □

Übung 106 (Vorbereitung)

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

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

$$\begin{aligned} 2019 &= 1 \cdot 1999 + 20 \\ 1999 &= 99 \cdot 20 + 19 \\ 20 &= 1 \cdot 19 + 1 \\ 19 &= 19 \cdot 1 + 0 \end{aligned}$$

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

Übung 107 (Vorbereitung)
Bestimmen Sie $x, y \in \mathbb{Z}$ mit

$$13x + 17y = \operatorname{ggT}(13, 17) \tag{6.1}$$

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

$$13x + 17y = 3 \tag{6.2}$$

Lösung. Mit dem euklidischen Algorithmus folgt

$$\begin{aligned} 17 &= 1 \cdot 13 + 4 \\ 13 &= 4 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0 \end{aligned}$$

Durch Rückwärtseinsetzen der Reste ausgehend von der vorletzten Gleichung erhalte 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 (6.1). Multiplizieren wir die Gleichung mit dem Faktor 3, so ist $(x, y) = (12, -9)$ eine Lösung von Gleichung (6.2). □

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 $\Phi_n \colon R_n \to R[X_1, \dots, X_n]$ sowie $\Psi_n \colon R[X_1, \dots, X_n] \to R_n$ gibt mit

$$\begin{aligned} \Phi_n \circ \Psi_n &= \mathrm{id}_{R[X_1,\dots,X_n]} \\ \Psi_n \circ \Phi_n &= \mathrm{id}_{R_n} \end{aligned} \tag{6.3a}$$

$$\begin{aligned} \Phi_n|_R &= \mathrm{id}_R \\ \Psi_n|_R &= \mathrm{id}_R \end{aligned} \tag{6.3b}$$

$$\Psi_n(X_i) = \Phi_n(X_i) = X_i \text{ für alle } i \in \{1, \dots, n\} \tag{6.3c}$$

Betrachte die Abbildung $\iota \colon R \to R_{n+1}, x \mapsto x$. Mit Ü89 gibt es dann $\Psi_{n+1} \colon R[X_1, \dots X_{n+1}] \to R_{n+1}$ 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

$$\kappa \colon \begin{cases} R_n & \to \quad R[X_1, \dots, X_{n+1}] \\ x & \mapsto \quad \Phi_n(x) \end{cases} \tag{6.4}$$

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

$$\Phi_{n+1}(X_{n+1}) = X_{n+1} \text{ und} \tag{6.5a}$$

$$\Phi_{n+1}(x) = \Phi_n(x) \text{ für alle } x \in R_n \tag{6.5b}$$

Da $\Psi_n(x) \overset{(6.3b)}{=} x$ für jedes $x \in R$ und $\Psi_n(X_i) \overset{(6.3c)}{=} X_i$ für jedes $i \in \{1, \dots, n\}$ gilt auch $\Psi_{n+1}|_{R[X_1,\dots,X_n]} = \Psi_n$. Für jedes $x \in R_n$ gilt

$$(\Psi_{n+1} \circ \Phi_{n+1})(x) = (\Psi_{n+1} \circ \Phi_n)(x) = (\Psi_n \circ \Phi_n)(x) = x \tag{6.6}$$

Es gilt auch

$$(\Psi_{n+1} \circ \Phi_{n+1})(X_{n+1}) = \Psi_{n+1}(X_{n+1}) = X_{n+1}$$

Deswegen gilt $\Psi_{n+1} \circ \Phi_{n+1} = \mathrm{id}_{R_n[X_n]} = \mathrm{id}_{R_{n+1}}$. Für jedes $x \in R$ gilt

$$(\Phi_{n+1} \circ \Psi_{n+1})(x) = \Phi_{n+1}(x) = \Phi_n(x) = x$$

und für jedes $i \in \{1, \dots, n+1\}$

$$(\Phi_{n+1} \circ \Psi_{n+1})(X_i) = \Phi_{n+1}(X_i) = \Phi_n(X_i) = X_i$$

Deswegen gilt $\Phi_{n+1} \circ \Psi_{n+1} = \mathrm{id}_{R[X_1,\dots,X_n]}$. □

Übung 111

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

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

$$\psi\colon \begin{cases} K & \to \quad L \\ \frac{a}{b} & \mapsto \quad \psi\left(\frac{a}{b}\right) = \varphi(a)\cdot\varphi(b)^{-1} \end{cases}$$

- *Die Abbildung ψ ist wohldefiniert.*
  Ist $a/b = c/d \in K$ mit $a, c \in R$ und $b, d \in R \setminus \{0\}$, so gilt $ad = bc$ in R. Dann gilt $\varphi(a)\cdot\varphi(d) = \varphi(ad) = \varphi(bc) = \varphi(b)\cdot\varphi(c)$, d.h. $\varphi(a)\cdot\varphi(b)^{-1} = \varphi(c)\cdot\varphi(d)^{-1}$. Damit ist φ wohldefiniert.
- *ψ ist Ringhomomorphismus.*
  (a) Für $a, c \in R$ und $b, d \in R \setminus \{0\}$ gilt

$$\begin{aligned}\psi\left(\frac{a}{b}+\frac{c}{d}\right) = \psi\left(\frac{ad+bc}{bd}\right) &= \varphi(ad+bc)\cdot\varphi(bd)^{-1}\\ &= (\varphi(a)\varphi(d)+\varphi(b)\varphi(c))\cdot\varphi(d)^{-1}\varphi(b)^{1}\\ &= \varphi(a)\varphi(d)\cdot\varphi(d)^{-1}\varphi(b)^{-1}+\varphi(b)\varphi(c)\cdot\varphi(d)^{-1}\varphi(b)^{1}\\ &= \varphi(a)\cdot\varphi(b)^{-1}+\varphi(c)\cdot\varphi(d)^{-1}\\ &= \psi\left(\frac{a}{b}\right)+\psi\left(\frac{c}{d}\right)\end{aligned}$$

  (b) Es gilt $\psi(1) = \psi\left(\frac{1}{1}\right) = \varphi(1)\cdot\varphi(1)^{-1} = 1$.

  (c) Für $a, c \in R$ und $b, d \in R \setminus \{0\}$ gilt

$$\begin{aligned}\psi\left(\frac{a}{b}\cdot\frac{c}{d}\right) = \psi\left(\frac{ac}{bd}\right) = \varphi(ac)\cdot\varphi(bd)^{-1} = \varphi(a)\varphi(c)\cdot\varphi(d)^{-1}\varphi(b)^{1} &= \varphi(a)\varphi(b)^{-1}\cdot\varphi(c)\cdot\varphi(d)^{-1}\\ &= \psi\left(\frac{a}{b}\right)\cdot\psi\left(\frac{c}{d}\right)\end{aligned}$$

- Für jedes $a \in R$ gilt $(\varphi\circ\iota)(a) = \psi(\frac{a}{1}) = \varphi(a)\cdot\varphi(1)^{-1} = \varphi(a)$.
- *ψ ist eindeutig bestimmt.*
  Es sei $\psi_1 \in \mathrm{Hom}(K, L)$ mit $\psi_1 \circ \iota = \varphi$. Für jedes $a \in R$ gilt dann

$$\psi_1\left(\frac{a}{1}\right) = (\psi_1\circ\iota)(a) = \varphi(a) = (\psi\circ\iota)(a) = \psi\left(\frac{a}{1}\right)$$

  Ist $a \neq 0$, so gilt

$$\psi_1\left(\frac{1}{a}\right) = \psi_1\left(\left(\frac{a}{1}\right)^{-1}\right) = \psi_1\left(\frac{a}{1}\right)^{-1} = \psi\left(\frac{a}{1}\right)^{-1} = \psi\left(\left(\frac{a}{1}\right)^{-1}\right) = \psi\left(\frac{1}{a}\right)$$

  Da ψ_1 und ψ Homomorphismen sind, gilt $\psi_1 = \psi$. □

Übung 112

$\mathbb{Z}[i] := \{x + iy \colon x, y \in \mathbb{Z}\}$ ist ein Teilring von $\mathbb{C}$, der euklidisch ist.

Lösung. ■ Es ist einfach zu zeigen, dass $\mathbb{Z}[i]$ ein Teilring von $\mathbb{C}$ ist.

■ Betrachte die Abbildung

$$N \colon \begin{cases} \mathbb{Z}[i] \setminus \{0\} & \to & \mathbb{N} \\ a + ib & \mapsto & a^2 + b^2 \end{cases}$$

Es seien $z_1 \in \mathbb{Z}[i]$ und $z_2 \in Z[i] \setminus \{0\}$. Betrachte $\frac{z_1}{z_2} \in \mathbb{C}$ und schreibe $\frac{z_1}{z_2} = x + iy$ mit $x, y \in \mathbb{R}$. Aber es gibt $a, b \in Z$ mit $-1/2 \leq x - a \leq 1/2$ und $-1/2 \leq y - b \leq 1/2$. Schreibe $q = a + ib \in \mathbb{Z}[i]$ und $r = z_1 - qz_2 \in \mathbb{Z}[i]$ (da $\mathbb{Z}[i]$ Teilring von $\mathbb{C}$ ist). Ist $r \neq 0$, so gilt

$$\begin{aligned} N(r) = r \cdot \overline{r} &= (z_1 - qz_2)\left(\overline{z_1} - \overline{qz_2}\right) \\ &= z_2\overline{z_2} \cdot \left(\frac{z_1}{z_2} - q\right)\left(\frac{\overline{z_1}}{\overline{z_2}} - \overline{q}\right) \\ &= N(z_2)(x + iy - a - ib)(x - iy + a + ib) \\ &= N(z_2)\left((x-a) + i(y-b)\right)\left((x-a) - i(y-b)\right) \\ &= N(z_2)\left((x-a)^2 + (y-b)^2\right) \\ &\leq N(z_2)\left(\frac{1}{4} + \frac{1}{4}\right) \\ &= 1/2 N(z_2) \\ &< N(z_2) \qquad (\text{da } N(z_2) \neq 0) \end{aligned}$$

Deswegen ist $\mathbb{Z}[i]$ euklidisch. □

Übung 113

$\mathbb{Z}[\sqrt{-5}] := \left\{x + y\sqrt{-5} \colon x, y \in \mathbb{Z}\right\}$ ist ein Teilring von $\mathbb{C}$, der nicht faktoriell ist.

Lösung. ■ Es ist einfach zu zeigen, dass $\mathbb{Z}[\sqrt{-5}]$ ein Teilring von $\mathbb{C}$ ist.

■ Betrachte die Abbildung

$$N \colon \begin{cases} \mathbb{Z}[\sqrt{-5}] & \to & \mathbb{N} \\ a + b\sqrt{-5} & \mapsto & a^2 + 5b^2 \end{cases} \tag{6.7}$$

Ist $\mathbb{Z}[\sqrt{-5}]$ faktoriell, so ist $1 + \sqrt{-5}$ prim nach Lemma 2. Da $\left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right) = 6 = 2 \cdot 3$, gilt $1 + \sqrt{-5} \mid 2$ oder $1 + \sqrt{-5} \mid 3$. Gilt $1 + \sqrt{-5} \mid 2$, so gibt es $x \in \mathbb{Z}[\sqrt{-5}]$ mit $2 = x\left(1 + \sqrt{-5}\right)$. Insbesondere ist $4 = N(2) = N(x) \cdot N\left(1 + \sqrt{-5}\right) = 6 \cdot N(x)$, d.h. $2 = 3 \cdot N(x)$, was falsch ist, da $N(x) \in \mathbb{N}$. Der andere Fall ist analog. Deswegen ist $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell. □

Übung 114 (Präsenz)

Bestimmen Sie die Lösungen der folgenden Kongruenzen in $\mathbb{Z}$:

$$\begin{array}{lll} x \equiv 1 \mod 3 & y \equiv 1 \mod 2 & z \equiv 1 \mod 4 \\ x \equiv 2 \mod 5 & y \equiv 2 \mod 3 & z \equiv 2 \mod 6 \\ x \equiv 3 \mod 7 & y \equiv 3 \mod 4 & z \equiv 3 \mod 9 \end{array}$$

Lösung. Wir lösen nur das erste System von Kongruenzen:
Es gilt $3 \cdot 5 \cdot 7 = 105$. Bestimme $u, v \in \mathbb{Z}$ mit $3u + {}^{105}/_{3} \cdot v = 1$, d.h. $3u + 35v = 1$. Es ist klar, dass $u = 12$ und $v = -1$ eine Lösung ist. Dann ist $-35 \equiv 1 \mod 3$, $-35 \equiv 0 \mod 5$ und $-35 \equiv 0 \mod 7$. Analog bestimmen wir $21 \equiv 1 \mod 5$, $21 \equiv 0 \mod 3$, $21 \equiv 0 \mod 7$, sowie $15 \equiv 1 \mod 7$, $15 \equiv 0 \mod 3$, $15 \equiv 0 \mod 5$. Betrachte $(-35) \cdot 1 + 2 \cdot 21 + 3 \cdot 15 = 52$. Dann gilt $52 + 105m \equiv 1 \mod 3$, $52 + 105m \equiv 2 \mod 5$ und $52 + 105m \equiv 3 \mod 7$ für jedes $m \in \mathbb{Z}$.
Umgekehrt sei $x \in \mathbb{Z}$ mit $x \equiv 1 \mod 3$, $x \equiv 2 \mod 5$ und $x \equiv 3 \mod 7$. Da 52 Lösung ist, gilt $x = 52 \mod 3$, $x = 52 \mod 5$ und $x = 52 \mod 7$, sowie $\operatorname{kgV}(3, 5, 7) = 105$, d.h. es gilt $x \mid 52$, somit existiert $n \in \mathbb{Z}$ mit $x = 52 + 105n$. □

Übung 115 (Präsenz)

Für jedes $n \geq 1$ gibt es $x \in \mathbb{N}$, für das keine der Zahlen $x + 1, \ldots, x + n$ prim ist.

Beweis. Sei $y = (n+1)!$. Dann gilt für $y + i$ mit $i \in \{2, \ldots, n+1\}$, dass

$$i \mid (n+1)! \tag{6.8}$$

Somit gilt auch $i \mid y + i$ für alle $i \in \{2, \ldots, n+1\}$ wegen (6.8) und $i \mid i$. Da $n \geq 1$ vorausgesetzt war, ist auch stets $y + 1 > i$ und i somit ein echter Teiler von y. Damit sind die Zahlen $y + i$ für $i \in \{2, \ldots, n+1\}$ nicht prim. Dann erfüllt $x := y + 1$ die Anforderungen. □

Übungsblatt 7

Eric Kunze
Übungsleiter: Dr. Legrand
Geometrie
Wintersemester 2018/19

Thema: Bruchringe, Irreduzibilität

Lemma 1

Es seien $a, b, c \in \mathbb{Z}$ mit $a \neq 0$, $a \mid bc$ und $\operatorname{ggT}(a, b) = 1$. Dann gilt $a \mid c$.

Beweis. Da $\operatorname{ggT}(a, b) = 1$, gibt es $u, b \in \mathbb{Z}$ mit $au + bv = 1$. Dann gilt $c = c \cdot 1 = c \cdot (au + bv) = cau + cbv \equiv cbv \equiv 0 \mod a$. □

Lemma 2

Sei $f \in \mathbb{R}[X]$. Dann gilt für alle $z \in \mathbb{C}$: $\quad f(z) = 0 \iff f(\overline{z}) = 0$

Beweis. Es seien $f \in \mathbb{R}[X]$ und $z \in \mathbb{C}$ mit $f(z) = 0$. Schreibe $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ mit $a_n, \ldots, a_0 \in \mathbb{R}$. Da $f(z) = 0$ gilt

$$\begin{aligned} 0 &= a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 \\ &= a_n \overline{z}^n + a_{n-1} \overline{z}^{n-1} + \cdots + a_1 \overline{z} + a_0 \\ &= f(\overline{z}) \end{aligned}$$

Deswegen ist $\overline{z}$ Nullstelle von f. □

Übung 131 (Vorbereitung)

Bestimmen Sie die Lösungen der folgenden Kongruenzen in $\mathbb{Z}$:

$$\begin{aligned} x &\equiv 1 \mod 3 & y &\equiv 1 \mod 2 & z &\equiv 1 \mod 4 & u &\equiv 1 \mod 4 \\ x &\equiv 2 \mod 5 & y &\equiv 2 \mod 3 & z &\equiv 2 \mod 6 & u &\equiv 1 \mod 6 \\ x &\equiv 3 \mod 7 & y &\equiv 3 \mod 4 & z &\equiv 3 \mod 9 & u &\equiv 1 \mod 9 \end{aligned}$$

Übung 133 (Vorbereitung)

Zerlegen Sie $X^4 - 2 \in \mathbb{R}[X]$ in seine Primfaktoren.

Lösung. *Wiederholung:* $f \in \mathbb{R}[X]$ *prim* $\;:\Leftrightarrow\; f \in \mathbb{R}[X]^\times$ *und* $f \mid ab \to f \mid a \vee f \mid b$

$$f = X^4 - 2 = \left(X^2 + \sqrt{2}\right)\left(X^2 - \sqrt{2}\right) = \left(X^2 + \sqrt{2}\right)\left(X - \sqrt[4]{2}\right)\left(X + \sqrt[4]{2}\right)$$

Übung 134

Ist $x = \frac{a}{b} \in \mathbb{Q}$ eine Nullstelle von $f = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$ mit $\operatorname{ggT}(a, b) = 1$, so gelten $a \mid a_0$ und $b \mid a_n$.

Lösung. Es seien $a, b \in \mathbb{Z}$ mit $b \neq 0$, $\operatorname{ggT}(a, b) = 1$ und $f\left(\frac{a}{b}\right) = 0$. Dann ist

$$0 = f\left(\frac{a}{b}\right) = \sum_{i=0}^n a_i \cdot \frac{a^i}{b^i} \quad \Leftrightarrow \quad 0 = b^n \cdot f\left(\frac{a}{b}\right) = \sum_{i=0}^n a_i \cdot a^i \cdot b^{n-i}$$

Insbesondere gelten $a \mid a_0 b^n$ und $b \mid a_n a^n$. Mit Lemma 1 folgt $a \mid a_0 b^{n-1}$ und $b \mid a_n a^{n-1}$. Per Induktion zeigt man nun noch. dass $a \mid a_0$ und $b \mid a_n$. □

Übung 135
Die folgenden Polynome sind in den jeweiligen Ringen irreduzibel:

(a) $X^3 + 39X^2 - 4X + 8 \in \mathbb{Q}[X]$
(b) $2X^4 + 200X^3 + 2000X^2 + 20000X + 20 \in \mathbb{Q}[X]$
(c) $X^5 - 64 \in \mathbb{Q}[X]$
(d) $X^2Y + XY^2 - X - Y + 1 \in \mathbb{Q}[X,Y]$

Lösung. (a) Ist das Poylnom irreduzibel über $\mathbb{Q}$, so besitzt es eine Nullstelle $x \in \mathbb{Q}$. Schreibe $x = {}^a\!/_b$ mit $a, b \in \mathbb{Z}$, $b \neq 0$ und $\operatorname{ggT}(a,b) = 1$. Mit Ü134 gilt $a \mid 8$ und $b \mid 1$, dh. $x \in \{8, -8, 4, -4, 2, -2, 1, -1\}$. Aber man zeigt leicht, dass

$$\begin{array}{cccc} f(8) \neq 0 & f(4) \neq 0 & f(2) \neq 0 & f(1) \neq 0 \\ f(-8) \neq 0 & f(-4) \neq 0 & f(-2) \neq 0 & f(-1) \neq 0 \end{array}$$

Deswegen ist f irreduzibel über $\mathbb{Q}$.

(b) Sei $f(X) = 2X^4 + 200X^3 + 2000X^2 + 20000X + 20 \in \mathbb{Q}[X]$. Da $2 \in \mathbb{Q}[X]^\times$, gilt:

$$f \text{ irreduzibel über } \mathbb{Q} \quad \Leftrightarrow \quad {}^1\!/_2\, f = X^4 + 100X^3 + 1000X^2 + 10000X + 10 \text{ irreduzibel über } \mathbb{Q}$$

Mit dem Satz von Eisenstein ($p = 2$) ist ${}^1\!/_2 f$ irreduzibel über $\mathbb{Q}$, also auch f irreduzibel über $\mathbb{Q}$.

(c) Sei $f(X) = X^5 - 64 \in \mathbb{Q}[X]$. Da $64 \neq x^5$ für alle $x \in \mathbb{Q}$, besitzt f keine Nullstelle in $\mathbb{Q}$. Deswegen gilt: Ist f irreduzibel über $\mathbb{Q}$, so gibt es $a, b, c, d, e \in \mathbb{Q}$ mit $X^5 - 64 = (X^2 + aX + b)(X^3 + cX + dX + e)$. Jetzt gilt

$$\begin{aligned} X^5 - 2 = \frac{(X^5 - 2) \cdot 32}{32} &= \frac{(2X)^5 - 64}{32} \\ &= \frac{1}{32}\big((2X)^2 - a \cdot (2X) - b\big)\big((2X)^3 + c(2X)^2 + d \cdot (2X) + e\big) \\ &= \left(\frac{4X^2 + 2aX + b}{4}\right)\left(\frac{8X^3 + 4cX^2 + 2dX + e}{8}\right) \\ &= \left(X^2 + \frac{a}{2}X + \frac{b}{4}\right)\left(X^3 + \frac{c}{2}X^2 + \frac{d}{4}X + \frac{e}{8}\right) \end{aligned}$$

Insbesondere ist $X^5 - 2$ reduzibel über $\mathbb{Q}$. Mit dem Satz von Eisenstein ($p = 2$) ist $X^5 - 2$ irreduzibel über $\mathbb{Q}$, ein Widerspruch. Deswegen ist $f(X) = X^5 - 64$ irreduzibel über $\mathbb{Q}$.

(d) Sei $f(X,Y)X^2Y + XY^2 - X - Y + 1 \in \mathbb{Q}[X,Y]$

(i) Zeige, dass $X^2 + X(Y^2 - 1) + (-Y + 1) \in \mathbb{Q}[Y][X]$ irreduzibel ist. Benutze den Satz von Eisenstein (mit dem Primelement $Y - 1$). Deswegen ist $X^2 + X(Y^2 - 1) + (-Y + 1)$ irreduzibel über $\mathbb{Q}[X]$.

(ii) Analog ist $Y^2 + Y(X^2 - 1) + (1 - X)$ irreduzibel über $\mathbb{Q}[X]$.

(iii) Zeige, dass $X^2Y + XY^2 - X - Y + 1$ irreduzibel über $\mathbb{Q}[X,Y]$ ist. Dazu schreiben wir $f(X,Y) = A(X,Y) \cdot B(X,Y)$ mit $A, B \in \mathbb{Q}[X,Y]$. Aus (i) und (ii) folgt

$$\deg_X(A) = 2 \text{ und } \deg_X(B) = 0 \quad \text{oder} \quad \deg_X(A) = 0 \text{ und } \deg_X(B) = 2$$

und

$$\deg_Y(A) = 2 \text{ und } \deg_Y(B) = 0 \quad \text{oder} \quad \deg_Y(A) = 0 \text{ und } \deg_Y(B) = 2$$

- $\deg_X(A) = 2$, $\deg_X(B) = 0$, $\deg_Y(A) = 2$, $\deg_Y(B) = 0$. Dann ist $B(X,Y) \in \mathbb{Q}$. Deswegen ist f irreduzibel über $\mathbb{Q}[X,Y]$.
- $\deg_X(A) = 0$, $\deg_X(B) = 2$, $\deg_Y(A) = 0$, $\deg_Y(B) = 2$. $\rightsquigarrow$ analog zum ersten Fall
- $\deg_X(A) = 2 = \deg_Y(B)$, $\deg_Y(A) = 0 = \deg_X(B)$. Dann ist $f(X,Y) = A(X) \cdot B(Y)$. Schreibe $A(X) = X^2 + aX + b$ und $B(Y) = Y^2 + cY + d$. Dann gilt $A(X) \cdot B(Y) = X^2Y^2 + \cdots$, ein Widerspruch. Deswegen ist dieser Fall unmöglich.
- $\deg_X(A) = 0 = \deg_Y(B)$, $\deg_Y(A) = 2 = \deg_X(B)$. $\rightsquigarrow$ analog zum dritten Fall $\square$

Übung 136

Ist $f \in \mathbb{R}[X]$ und $z \in \mathbb{C}$ mit $f(z) = 0$, so ist auch $f(\overline{z}) = 0$. Nutzen Sie dies sowie den Fundamentalsatz der Algebra, um zu zeigen, dass alle irreduziblen $f \in \mathbb{R}[X]$ Grad 1 oder 2 haben.

Lösung. Wir zeigen die folgende Aussage: f irreduzibel in $\Leftrightarrow \deg(f) \in \{1,2\}$. Es sei $f \in \mathbb{R}[X]$ irreduzibel über $\mathbb{R}$. Weiter sei $\lambda \in \mathbb{C}$ mit $f(\lambda) = 0$ nach dem Fundamentalsatz der Algebra.

- Ist $\lambda \in \mathbb{R}$, so gilt $(X - \lambda) \mid f(X)$. Da f irreduzibel ist, folgt, dass $\deg(f) = 1$.
- Ist $\lambda \in \mathbb{C} \setminus \mathbb{R}$, so ist mit Lemma 2 auch $f(\overline{\lambda}) = 0$. Schreibe $f(X) = (X - \lambda) \cdot g(X)$ mit $g \in \mathbb{C}[X]$. Da $(X - \overline{\lambda}) \mid f(X)$ und $\mathrm{ggT}(X - \lambda, X - \overline{\lambda}) = 1$ gilt: $(X - \overline{\lambda}) \mid g(X)$, d.h. es gibt $q \in \mathbb{C}[X]$ mit $g(x) = (X - \overline{\lambda}) \cdot q(X)$. Somit ist also $f(X) = (X - \lambda)(X - \overline{\lambda}) \cdot q(X) = X^2 - \underbrace{(\lambda + \overline{\lambda})}_{\in \mathbb{R}} \cdot X + \underbrace{\lambda\overline{\lambda}}_{\in \mathbb{R}} \in \mathbb{R}[X]$.

  Mit der Eindeutigkeit der Polynomdivision folgt schlussendlich, dass $q(X) \in \mathbb{R}[X]$. Da f irreduzibel in $\mathbb{R}[X]$ ist, schließen wir, dass $\deg(f) = 2$ gilt. $\square$

Übung 145 (Präsenz)

Finden Sie eine Primfaktorenzerlegung von $X^4 + 1$ in $\mathbb{C}[X]$, $\mathbb{R}[X]$ und $\mathbb{Q}[X]$.

Lösung. ▪ in $\mathbb{C}[X]$: X^4+1 hat vier Nullstellen, also $f(X) = (X-\lambda_1)(X-\lambda_2)(X-\lambda_3)(X-\lambda_4)$, wobei $(X-\lambda_i)$ stets irreduzibel ist für alle $i \in \{1,2,3,4\}$.

$$X^4 + 1 = \left(X + e^{1/4 i\pi}\right)\left(X - e^{3/4 i\pi}\right)\left(X - e^{5/4 i\pi}\right)\left(X - e^{7/4 i\pi}\right)$$

- in $\mathbb{R}[X]$: Es gilt

$$X^4 + 2 = X^4 + 1 - 2X^2 + 2X^2 = (X^2-1)^2 + 2X^2 = \left(X^2 - \sqrt{2}X + 1\right)\left(X^2 + \sqrt{2}X + 1\right)$$

  Für jedes $x \in \mathbb{R}$ gilt

$$x^2 - \sqrt{2}x + 1 = \left(x - \frac{1}{\sqrt{2}}\right)^2 + \frac{1}{2} > 0$$
$$x^2 + \sqrt{2}x + 1 = \left(x + \frac{1}{\sqrt{2}}\right)^2 + \frac{1}{2} > 0$$

  Deswegen sind $X^2 \pm \sqrt{2}X + 1$ irreduzibel über $\mathbb{R}$.

- in $Q[X]$: Ist X^4+1 irreduzibel über $\mathbb{Q}$, so gibt es normierte Polynome $A(X), B(X) \in \mathbb{Q}[X]$ mit Grad 2 und $X^4+1 = A(X)B(X)$ (da $X^4+1 \neq 0$ für alle $x \in \mathbb{Q}$). Da $x^4 \neq -1$ für alle $x \in \mathbb{R}$, sind $A(X)$ und $B(X)$ irreduzibel über $\mathbb{R}$. Aus der Eindeutigkeit der Primfaktorenzerlegung über $\mathbb{R}[X]$ folgt

$$A(X) = X^2 \pm \sqrt{2}\cdot X + 1 \text{ und } B(X) = X^2 \mp \sqrt{2}\cdot X + 1$$

  In jedem Fall bekommen wir einen Widerspruch, da $\sqrt{2} \notin \mathbb{Q}$. Deswegen ist X^4+1 irreduzibel über $\mathbb{Q}[X]$. □