10. Übungszettel zur Vorlesung „Geometrische Gruppentheorie 2“
Musterlösung

SoSe 2016
WWU Münster

Prof. Dr. Linus Kramer
Nils Leder
Antoine Beljean

Aufgabe 10.1
Sei R ein Ring, $I \trianglelefteq R$ ein beidseitiges Ideal und $U := R^*$ die Einheitengruppe. Definiere

$$U_1 := \{u \in U \mid u - 1 \in I\}.$$

Zeige, dass U_1 ein Normalteiler in U ist.

Lösung: Wir zeigen zunächst, dass U_1 eine Untergruppe von U ist.
Wegen $1-1 = 0 \in I$ gilt $1 \in U_1$. Seien $u, v \in U_1$ beliebig. Dann gilt $u-1, v-1 \in I$. Somit erhalten wir für das Produkt uv:

$$uv - 1 = uv - v + v - 1 = (u-1) \cdot v + (v-1)$$

Da I ein Ideal ist, enthält I mit $u-1$ auch $(u-1) \cdot v$ und ist unter Addition abgeschlossen. Damit folgt $uv - 1 = (u-1) \cdot v + (v-1) \in I$, d.h. $uv \in U_1$.
Weiter gilt für das Inverse von u

$$u^{-1} - 1 = u^{-1} \cdot (1-u) = -u^{-1} \cdot (u-1) \in I$$

und folglich $u^{-1} \in U_1$. Insgesamt ist U_1 damit eine Untergruppe von U.
Für $U_1 \trianglelefteq U$ seien $u \in U_1, v \in U$ beliebig. Dann gilt:

$$vuv^{-1} - 1 = vuv^{-1} - v1v^{-1} = v \cdot (u-1) \cdot v^{-1} \in I$$

Dies zeigt, dass $vuv^{-1} \in U_1$ gilt und U_1 somit normal in U ist.
Alternativ: Betrachte die kanonische Projektion $R \mapsto R/I$. Dieser Ringhomomorphismus induziert (wie in Aufgabe 8.1 a) gesehen) einen Gruppenhomomorphismus $\pi : U = R^* \to (R/I)^*$ zwischen den jeweiligen Einheitengruppen. Nach Definition gilt $U_1 = \ker(\pi)$ und als Kern eines Gruppenhomomorphismus ist U_1 ein Normalteiler in U.

Aufgabe 10.2
Betrachte in den komplexen Zahlen $\mathbb{C}$ den Teilring $\mathbb{Z}[i] = \{a+b\cdot i \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. Zeige: $\mathbb{Z}[i]$ ist ein euklidischer Ring.

Lösung: Wir definieren für $z = a + bi \in \mathbb{Z}[i]$ durch $N(z) = a^2 + b^2 = |z|^2$ eine Gradfunktion $N : \mathbb{Z}[i] \to \mathbb{N}$ auf $\mathbb{Z}[i]$. Seien $z', z \in \mathbb{Z}[i]$ beliebig mit $z \neq 0$.
Zu zeigen: Es gibt $r, s \in \mathbb{Z}[i]$ mit $z' = s \cdot z + r$ und $N(r) < N(z)$.
Da $z \neq 0$ ist, können wir $\frac{z'}{z}$ im Quotientenkörper $\mathbb{Q}(i)$ von $\mathbb{Z}[i]$ betrachten. Seien $q, q' \in \mathbb{Q}$ mit $\frac{z'}{z} = q + q' \cdot i$. Durch Auf- oder Abrunden finden wir nun $n, m \in \mathbb{Z}$ mit $|q - n| \leq \frac{1}{2}$ und $|q' - m| \leq \frac{1}{2}$. Setze $s := n + m \cdot i \in \mathbb{Z}[i]$ und $r := z' - s \cdot z \in \mathbb{Z}[i]$. Nach Wahl gilt $z' = s \cdot z + r$.

Weiter gilt $(q-n)^2 \leq \frac{1}{4}$ und $(q'-m)^2 \leq \frac{1}{4}$. Damit erhalten wir wegen der Multiplikativität des Absolutbetrags auf $\mathbb{C}$:

$$\begin{aligned} N(r) = |r|^2 = |z' - s \cdot z|^2 &= |\frac{z'}{z} \cdot z - s \cdot z|^2 \\ &= |(\frac{z'}{z} - s) \cdot z|^2 = |(\frac{z'}{z} - s)|^2 \cdot |z|^2 \\ &= |(q + q' \cdot i) - (n + m \cdot i)|^2 \cdot |z|^2 \\ &= |(q-n) + (q'-m) \cdot i|^2 \cdot N(z) \\ &= ((q-n)^2 + (q'-m)^2) \cdot N(z) \\ &\leq (\frac{1}{4} + \frac{1}{4}) \cdot N(z) = \frac{1}{2} \cdot N(z) < N(z) \end{aligned}$$

Somit erfüllen $r, s \in \mathbb{Z}[i]$ die Bedingungen $z' = s \cdot z + r$ und $N(r) < N(z)$. Daher ist $\mathbb{Z}[i]$ ein euklidischer Ring.

Aufgabe 10.3
Betrachte die spezielle orthogonale Gruppe $\mathrm{SO}(2) = \{A \in \mathrm{SL}_2(\mathbb{R}) \mid A^T \cdot A = 1\}$. Sei $G \subseteq \mathrm{SO}(2)$ eine endliche Untergruppe. Zeige: G ist zyklisch.

Lösung: Die spezielle orthogonale Gruppe $\mathrm{SO}(2)$ besteht genau aus den Drehungen um den Ursprung in $\mathbb{R}^2$. Wir können jedes $a \in \mathrm{SO}(2)$ in der Form $a = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$ für einen geeigneten Winkel $\varphi \in [0, 2\pi)$ schreiben. Dann entspricht a der Drehung gegen den Uhrzeigersinn mit Drehwinkel φ.
Da $G \subseteq \mathrm{SO}(2)$ endlich ist, hat jedes Element in G endliche Ordnung. Der Drehwinkel eines jeden Elements in G ist damit ein rationales Vielfaches von 2π. Wähle $q \in \mathbb{Q}, 0 < q$ minimal, sodass die Drehung gegen den Uhrzeigersinn mit Drehwinkel $q \cdot 2\pi$ in G liegt. (Wir nehmen hierfür ohne Einschränkung $G \neq \{1\}$ an.) Diese Drehung bezeichnen wir mit β. Zu zeigen: β erzeugt G.
Sei $\alpha \in G, \alpha \neq 1$ beliebig. Dann gibt es $r \in \mathbb{Q} \cap (0,1)$, sodass α die Drehung gegen den Uhrzeigersinn mit Drehwinkel $r \cdot 2\pi$ ist. Sei $n \in \mathbb{N}$ maximal mit $n \cdot q \leq r$. Dann gilt offenbar $q > r - n \cdot q \geq 0$. Weiter ist $(r - n \cdot q) \cdot 2\pi$ der Drehwinkel von $\alpha \cdot \beta^{-n} \in G$. Ist nun $r - n \cdot q > 0$, so erhalten wir einen Widerspruch zur Minimalität von q. Somit folgt $r - n \cdot q = 0$, d.h. $r = n \cdot q$ und es gilt $\alpha = \beta^n$.
Da β die Gruppe G erzeugt, ist G zyklisch.
Alternativ: Man kann sich leicht überlegen, dass für $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SO}(2)$ die Abbildung $A \mapsto a + ci$ einen injektiven Gruppenhomomorphismus $\mathrm{SO}(2) \to \mathbb{C}^*$ (mit Bild $S^1 \subseteq \mathbb{C}^*$) definiert. (Hierfür verwendet man, dass für die Matrix A die Gleichungen $a^2 + c^2 = 1, a = d$ und $b = -c$ gelten.)
Somit ist jede endliche Untergruppe von $\mathrm{SO}(2)$ isomorph zu einer endlichen Untergruppe von $\mathbb{C}^*$. Da $\mathbb{C}$ ein Körper ist, ist nach Aufgabe 4.4 jede solche Gruppe zyklisch.

Aufgabe 10.4
Bestimme alle Primzahlen, die als Ordnung eines Elements in $\mathrm{SL}_3(\mathbb{Z})$ vorkommen.

Lösung: Wir zeigen, dass 2 und 3 die einzigen Primzahlen sind, die als Ordnung

eines Elements in $\mathrm{SL}_3(\mathbb{Z})$ vorkommen.
1. Schritt: Ist p eine Primzahl mit $p \notin \{2, 3, 7\}$, so gibt es in $\mathrm{SL}_3(\mathbb{Z})$ kein Element der Ordnung p.
Sei $a \in \mathrm{SL}_3(\mathbb{Z})$ beliebig mit $o(a) < \infty$. Gilt $a \in \Gamma_3(2)$, so hat a nach einem Lemma aus Kapitel 3 der Vorlesung entweder Ordnung 1 oder 2.
Andernfalls gilt $a \notin \Gamma_3(2)$ und wir können wie im Beweis von Satz 23 in Kapitel 3 der Vorlesung vorgehen:
Sei $\pi : \mathrm{SL}_3(\mathbb{Z}) \to \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ der von der kanonischen Projektion induzierte Gruppenhomomorphismus. Wegen $a \notin \Gamma_3(2) = \ker(\pi)$ hat a ein nicht-triviales Bild $\pi(a) \in \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$. Da $\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ in Bijektion zu der Menge der geordneten Basen des $\mathbb{Z}/2\mathbb{Z}$-Vektorraums $(\mathbb{Z}/2\mathbb{Z})^3$ steht, gilt:

$$\#\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z}) = (8-1) \cdot (8-2) \cdot (8-4) = 7 \cdot 6 \cdot 4 = 168$$

Nun teilt $o(\pi(a))$ die Gruppenordnung $\#\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z}) = 168 = 2^3 \cdot 3 \cdot 7$.
Wegen $\#(\langle a \rangle \cap \Gamma_3(2)) \in \{1, 2\}$ folgt $o(a) = k$ oder $o(a) = 2 \cdot k$ für einen geeigneten Teiler k von 168. Die einzigen Primzahlen, die als Ordnung eines Elements in $\mathrm{SL}_3(\mathbb{Z})$ auftreten können, sind daher die Primteiler von 168, also $2, 3$ und 7.
2. Schritt: $\mathrm{SL}_3(\mathbb{Z})$ enthält Elemente der Ordnung 2 und 3.
Betrachte die Matrizen $a = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in \mathrm{SL}_3(\mathbb{Z})$.
Dann gilt $o(a) = 2$ und $o(b) = 3$.
3. Schritt: $\mathrm{SL}_3(\mathbb{Z})$ enthält kein Element der Ordnung 7.
Per Widerspruch: Angenommen, es gibt $a \in \mathrm{SL}_3(\mathbb{Z})$ mit $o(a) = 7$. Aus der Theorie der Jordan'schen Normalform ist bekannt, dass a konjugiert ist zu einer oberen Dreickecksmatrix über $\mathbb{C}$ mit den Eigenwerten λ_1, λ_2 und λ_3 von a auf der Diagonale.
Wegen $o(a) = 7$ gilt $a^7 = 1$, d.h. $a^7 - 1 = 0$ und a ist Nullstelle des Polynoms $X^7 - 1 \in \mathbb{Z}[X]$. Die Eigenwerte λ_i sind folglich siebte Einheitswurzeln in $\mathbb{C}$.
Gilt $\lambda_i = 1$ für $i = 1, 2, 3$, so ist a konjugiert zu einem Element in der Heisenberggruppe über $\mathbb{C}$. Diese ist aber torsionsfrei. Dies widerspricht $o(a) = 7$. $\lightning$
Somit kann ohne Einschränkung $\lambda_1 \neq 1$ angenommen werden, d.h. λ_1 ist eine primitive siebte Einheitswurzel in $\mathbb{C}$. Nach Übergang zu einer geeigneten Potenz von a dürfen wir voraussetzen, dass

$$\lambda_1 = \zeta_7 := \exp(\frac{2\pi i}{7}) = \cos(\frac{2\pi}{7}) + \sin(\frac{2\pi}{7}) \cdot i$$

gilt. Weiter gilt $\lambda_1 \cdot \lambda_2 \cdot \lambda_3 = \det a = 1$ und $\lambda_1 + \lambda_2 + \lambda_3 = \operatorname{tr} a \in \mathbb{Z}$. Damit erhalten wir:

$$\lambda_3 = (\lambda_1 \cdot \lambda_2)^{-1} = \lambda_1^{-1} \cdot \lambda_2^{-1} = \zeta_7^{-1} \cdot \lambda_2^{-1}$$

Und somit:

$$\zeta_7 + \lambda_2 + \zeta_7^{-1} \cdot \lambda_2^{-1} \in \mathbb{Z}$$

Da λ_2 eine siebte Einheitswurzel ist, gibt es für den Ausdruck $\zeta_7 + \lambda_2 + \zeta_7^{-1} \cdot \lambda_2^{-1}$ höchstens sieben verschiedene Werte. Diese sind aber nur für $\lambda_2 = 1$ bzw. $\lambda_2 = \zeta_7^{-1}$ reell-wertig und es gilt:

$$\zeta_7 + 1 + \zeta_7^{-1} \approx 2.247 \notin \mathbb{Z} \quad \lightning$$

Folglich war die Annahme, es gebe ein Element der Ordnung 7 in $\mathrm{SL}_3(\mathbb{Z})$, falsch.

***-Aufgabe**
Sei G eine endliche Gruppe und V ein endlich-dimensionaler $\mathbb{R}$-Vektorraum, auf dem G durch lineare Transformationen wirkt. Sei $U \subseteq V$ ein G-invarianter Unterraum, d.h. ein Untervektorraum mit $g(U) = U$ für alle $g \in G$.
Zeige: U hat ein G-invariantes Komplement, d.h. es gibt einen G-invarianten Unterraum $W \subseteq V$ mit $V = U \oplus W$.
Man sagt dann, die Darstellung von G auf V ist *vollständig reduzibel*.

Lösung: Wir zeigen zuerst, dass es ein G-invariantes Skalarprodukt $(\,,\,)$ auf V gibt. Sei $\langle\,,\,\rangle$ ein beliebiges Skalarprodukt auf V. (Ein solches existiert, da wir V mit $\mathbb{R}^n$ für $n = \dim V < \infty$ identifizieren und dann das Standardskalarprodukt wählen können.)
Nun definiere $(v, w) := \frac{1}{\#G} \cdot \sum\limits_{g \in G} \langle g(v), g(w)\rangle$ für $v, w \in V$.
Behauptung: $(\,,\,)$ ist ein G-invariantes Skalarprodukt auf V.
Beweis: Da G auf V durch lineare Abbildungen wirkt und $\langle\,,\,\rangle$ bilinear ist, kann man leicht nachrechnen, dass $(\,,\,)$ eine $\mathbb{R}$-Bilinearform ist. Da $\langle\,,\,\rangle$ symmetrisch ist, ist $(\,,\,)$ offenbar ebenfalls symmetrisch. Zu zeigen: $(\,,\,)$ ist positiv definit.
Sei $v \in V$ beliebig. Dann gilt wegen $\langle g(v), g(v)\rangle \geq 0$ für alle $g \in G$ auch

$$(v, v) = \frac{1}{\#G} \cdot \sum_{g \in G} \langle g(v), g(v)\rangle \geq 0.$$

Weiter folgt aus $(v, v) = 0$ schon $\langle g(v), g(v)\rangle = 0$ für alle $g \in G$. Insbesondere gilt dann $\langle v, v\rangle = 0$, also $v = 0$. Somit ist $(\,,\,)$ positiv definit.
Insgesamt ist $(\,,\,)$ eine symmetrische, positiv definite Bilinearform, also ein Skalarprodukt auf V. Es bleibt zu zeigen: $(\,,\,)$ ist G-invariant.
Seien $v, w \in V$ und $\tilde{g} \in G$ beliebig. Da die Rechtsmultiplikation mit $\tilde{g}$ eine Bijektion $G \to G$ darstellt, erhalten wir:

$$\begin{aligned}(\tilde{g}(v), \tilde{g}(w)) &= \frac{1}{\#G} \cdot \sum_{g \in G} \langle g(\tilde{g}(v)), g(\tilde{g}(w))\rangle \\ &= \frac{1}{\#G} \cdot \sum_{g \in G} \langle g\tilde{g}(v), g\tilde{g}(w)\rangle \\ &= \frac{1}{\#G} \cdot \sum_{g' \in G} \langle g'(v), g'(w)\rangle = (v, w)\end{aligned}$$

$(\,,\,)$ ist damit G-invariant.
Wähle nun W als das orthogonale Komplement von U bgzl. $(\,,\,)$, d.h.
$W := U^\perp = \{v \in V \mid (u, v) = 0 \text{ für alle } u \in U\}$. Aus der linearen Algebra ist bekannt, dass $U \oplus W = V$ gilt, W also ein Komplement zu U ist. Wir zeigen nun, dass W ein G-invarianter Unterraum von V ist.
Seien $w \in W$ und $g \in G$ beliebig. Zu zeigen: $g(w) \in W$
Sei $u \in U$ beliebig. Da U ein G-invarianter Unterraum ist, folgt $g^{-1}(u) \in U$ und somit $(g^{-1}(u), w) = 0$. Mit der G-Invarianz von $(\,,\,)$ erhalten wir nun:

$$(u, g(w)) = (g^{-1}(u), g^{-1}(g(w)) = (g^{-1}(u), w) = 0$$

Da $u \in U$ beliebig war, folgt $g(w) \in U^\perp = W$. Folglich ist W ein G-invarianter Unterraum.