9. Übungszettel zur Vorlesung „Geometrische Gruppentheorie 2“
Musterlösung

SoSe 2016
WWU Münster

Prof. Dr. Linus Kramer
Nils Leder
Antoine Beljean

Aufgabe 9.1
Sei K ein Körper mit Teilringen A, B und C so, dass $A \subseteq B \subseteq C$ gilt. Zeige: Ist C ganz über B (d.h. jedes Element in C ist ganz über B) und B ganz über A, so ist C ganz über A.

Lösung: Sei $c \in C$ beliebig. Zu zeigen: c ist ganz über A.
Wie im Hinweis zu Aufgabe 7.4 ist c genau dann ganz über A, wenn ein Teilring $S \subseteq C$ existiert, der A und c enthält und als A-Modul endlich erzeugt ist.
Da C ganz über B ist, erfüllt c eine normierte Polynomgleichung mit Koeffizienten in B, d.h. es gibt $b_0, \ldots, b_{n-1} \in B$ mit $c^n + b_{n-1}c^{n-1} + \ldots + b_1 c + b_0 = 0$.
Sei $R := A[b_0, \ldots, b_{n-1}] \subseteq B$ der von A und den b_i erzeugte Teilring.
Dann ist c offenbar auch ganz über R. (c ist Nullstelle des normierten Polynoms $X^n + b_{n-1}X^{n-1} + \ldots + b_1 X + b_0 \in R[X]$.)
Nach Vorüberlegung gibt es einen Teilring $S \subseteq C$, der R und c enthält und als R-Modul endlich erzeugt ist. Wegen $A \subseteq R \subseteq S$ genügt es zu zeigen, dass S ein endlich erzeugter A-Modul ist.
Dafür beweisen wir zuerst, dass der Ring R als A-Modul endlich erzeugt ist.
Da B ganz über A ist, ist jedes b_i ganz über A. Nach dem Beweis von Aufgabe 7.4 ist der Ring $A[b_i]$ für $i = 0, \ldots, n-1$ damit ein endlich erzeugter A-Modul.
Sei $Z_i \subseteq A[b_i]$ für $i = 0, \ldots, n-1$ eine endliche Menge, die $A[b_i]$ als A-Modul erzeugt. Nun überzeugt man sich leicht, dass $R = A[b_0, \ldots, b_{n-1}]$ als A-Modul von den Produkten $z_0 \cdot \ldots \cdot z_{n-1}$ mit $z_i \in Z_i$ erzeugt wird. (Für einen Ring der Form $A[b_0, b_1]$ haben wir das schon in der Lösung von Aufgabe 7.4 gesehen.)
Also ist R ein endlich erzeugter A-Modul.
Sei $r_1, \ldots r_l \in R$ ein endliches Erzeugendensystem für R als A-Modul. Da S ein endlich erzeugter R-Modul ist, existieren $s_1, \ldots, s_m \in S$, die S als R-Modul erzeugen.
Behauptung: Die endliche Menge $\{r_j \cdot s_i \mid 1 \leq j \leq l, 1 \leq i \leq m\}$ erzeugt S als A-Modul.
Beweis: Sei $y \in S$ beliebig. Da $\{s_1, \ldots, s_m\}$ eine Erzeugermenge von S als R-Modul ist, gibt es $\alpha_1, \ldots, \alpha_m \in R$ mit $y = \sum_{i=1}^{m} \alpha_i s_i$. Nun wird R als A-Modul von den $r_j, j = 1, \ldots, l$ erzeugt. Somit gibt es für jedes $i \in \{1, \ldots, m\}$ Elemente $a_{i1}, \ldots, a_{il} \in A$ mit $\alpha_i = \sum_{j=1}^{l} a_{ij} r_j = \alpha_i$. Insgesamt erhalten wir:

$$y = \sum_{i=1}^{m} \alpha_i s_i = \sum_{i=1}^{m} (\sum_{j=1}^{l} a_{ij} r_j) s_i = \sum_{i=1}^{m} \sum_{j=1}^{l} a_{ij} (r_j \cdot s_i)$$

Da $y \in S$ beliebig war, erzeugt die Menge $\{r_j \cdot s_i \mid 1 \leq j \leq l, 1 \leq i \leq m\}$ S als A-Modul und S ist als A-Modul endlich erzeugt.

Schließlich ist S ein Teilring von C, der A und c enthält und als A-Modul endlich erzeugt ist. Damit ist c ganz über A.

Aufgabe 9.2
Sei R ein kommutativer Ring und $G \subseteq \mathrm{Aut}(R)$ eine endliche Gruppe von Ringautomorphismen von R. Sei

$$R^G := \{x \in R \mid \sigma(x) = x \text{ für alle } \sigma \in G\}$$

der Unterring der G-Invarianten in R. Zeige: R ist ganz über R^G.

Lösung: Sei $r \in R$ beliebig. Zu zeigen: r ist ganz über R^G.
Definiere ein Polynom $p \in R[X]$ durch $p := \prod_{\sigma \in G} (X - \sigma(r))$. Da G endlich und R kommutativ ist, ist dies ein wohldefiniertes, normiertes Polynom über R. Da der Linearfaktor $X - r$ ein Teiler von p ist, gilt $p(r) = 0$.
Wir zeigen nun, dass p sogar ein Polynom in $R^G[X]$ ist, d.h. dass alle Koeffizienten in R^G liegen. Sei $n := \#G < \infty$. Dann gibt es $a_0, \ldots, a_{n-1} \in R$ mit $p = X^n + a_{n-1}X^{n-1} + \ldots a_1 X + a_0$. Die Koeffizienten in Grad 0 bzw. Grad $n-1$ lassen sich leicht ablesen. Es gilt:

$$a_0 = (-1)^n \prod_{\sigma \in G} \sigma(r) \text{ und } a_{n-1} = -\sum_{\sigma \in G} \sigma(r)$$

Durch Ausmultiplizieren von $p := \prod_{\sigma \in G} (X - \sigma(r))$ erhalten wir allgemein

$$a_k = (-1)^{n-k} \cdot \sum_{\substack{S \subseteq G, \\ \#S = n-k}} \prod_{\sigma \in S} \sigma(r).$$

Sei $k \in \{0, \ldots, n-1\}$ beliebig. Jedes $\tau \in G$ permutiert τ die Teilmengen der Kardinalität $n-k$ von G und wir erhalten:

$$\begin{aligned}
\tau(a_k) &= \tau((-1)^{n-k} \cdot \sum_{\substack{S \subseteq G, \\ \#S = n-k}} \prod_{\sigma \in S} \sigma(r)) \\
&= (-1)^{n-k} \cdot \sum_{\substack{S \subseteq G, \\ \#S = n-k}} \prod_{\sigma \in S} \tau(\sigma(r)) \\
&= (-1)^{n-k} \cdot \sum_{\substack{S \subseteq G, \\ \#S = n-k}} \prod_{\tilde{\sigma} \in \tau(S)} \tilde{\sigma}(r) \\
&= (-1)^{n-k} \cdot \sum_{\substack{S \subseteq G, \\ \#S = n-k}} \prod_{\tilde{\sigma} \in S} \tilde{\sigma}(r) = a_k
\end{aligned}$$

(Der letzte Gleichungsschritt erfolgt durch eine Umsortierung der Summanden.)
Wegen $\tau(a_k) = a_k$ für alle $\tau \in G$ gilt $a_k \in R^G$. Somit ist $p \in R^G[X]$ und r ist als Nullstelle des normierten Polynoms p ganz über dem Ring R^G.
Alternativ: Dass die Koeffizienten des oben definierten Polynoms p in R^G liegen,

lässt sich auf eine weitere (konzeptionell nützliche) Weise zeigen. Jeder Ringautomorphismus σ von R lässt sich durch die Zuordnung $X \mapsto X$ eindeutig zu einem Ringautomorphismus $\hat{\sigma} : R[X] \to R[X]$ fortsetzen. (Anschaulich wird bei $\hat{\sigma}$ auf jeden Koeffizienten eines Polynoms der Automorphismus σ angewendet, d.h. es gilt $\hat{\sigma}(\sum_{i=0}^{n} \alpha_i X^i) = \sum_{i=0}^{n} \sigma(\alpha_i) X^i$.)
Nun liegt ein Polynom q genau dann in $R^G[X]$, wenn $\hat{\sigma}(q) = q$ für alle $\sigma \in G$ gilt. Da $\hat{\sigma}$ für jedes $\sigma \in G$ die Linearfaktoren von $p = \prod_{\sigma \in G} (X - \sigma(r))$ permutiert, gilt $\hat{\sigma}(p) = p$ für alle $\sigma \in G$ und es folgt $p \in R^G[X]$.

Aufgabe 9.3
Sei R ein kommutativer Ring und $I \trianglelefteq R$ ein Ideal. Dann definieren wir das *Radikal* von I in R als $\mathrm{rad}(I) := \{x \in R \mid x^n \in I \text{ für ein } n \in \mathbb{N}\}$.
Zeige: $\mathrm{rad}(I)$ ist ein Ideal in R. Was ist das Radikal des Nullideals?

Lösung: Da I ein Ideal in R ist, gilt $0^1 = 0 \in R$. Somit gilt $0 \in \mathrm{rad}(I)$.
Seien $a, b \in \mathrm{rad}(I)$ beliebig. Dann gibt es $n, m \in \mathbb{N}$ mit $a^n \in I$ und $b^m \in I$. Da R kommutativ ist, erhalten wir mit dem binomischen Lehrsatz:

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} \cdot a^k \cdot b^{n+m-k}$$

Um zu sehen, dass $(a+b)^{n+m} \in I$ gilt, genügt es also zu zeigen, dass jeder der Summanden $\binom{n+m}{k} \cdot a^k \cdot b^{n+m-k}$ in I liegt. Gilt $k \geq n$, so haben wir wegen $a^n \in I$ auch $a^k = a^{k-n} \cdot a^n \in I$. Da das Produkt eines Elements aus I mit einem beliebigen Element in R wieder in I liegt, gilt daher $\binom{n+m}{k} \cdot a^k \cdot b^{n+m-k} \in I$. Ist $k < n$, so gilt $n + m - k > m$. Wegen $b^m \in I$ folgt $b^{n+m-k} \in I$ und somit $\binom{n+m}{k} \cdot a^k \cdot b^{n+m-k} \in I$. Da jeder der Summanden in I liegt, gilt $(a+b)^{n+m} \in I$ und nach Definition $a + b \in \mathrm{rad}(I)$.
Sei $r \in R$ beliebig. Da R kommutativ ist, gilt $(r \cdot a)^n = r^n \cdot a^n \in I$. Folglich ist $r \cdot a \in \mathrm{rad}(I)$. Insgesamt ist $\mathrm{rad}(I)$ ein Ideal.
Ein Element $x \in R$ liegt genau dann in $\mathrm{rad}(\{0\})$, wenn es ein $n \in \mathbb{N}$ mit $x^n = 0$ gibt. Das Radikal des Nullideals besteht also genau aus den nilpotenten Elementen in R.

Aufgabe 9.4
Sei K ein algebraisch abgeschlossener Körper und $f_1, \ldots, f_r \in K[X_1, \ldots, X_n]$ Polynome in n Variablen über K. Zeige, dass die folgenden Aussagen äquivalent sind:

i) Die Polynome $f_1, \ldots, f_r$ haben eine gemeinsame Nullstelle, d.h. es gibt $x = (x_1, \ldots, x_n) \in K^n$ mit $f_i(x) = 0$ für alle $i = 1, \ldots, r$.

ii) Das von den f_i erzeugte Ideal $(f_1, \ldots, f_r)$ ist ein echtes Ideal, d.h. $(f_1, \ldots, f_r) \neq K[X_1, \ldots, X_n]$.

Lösung:

i) $\Rightarrow$ *ii)* Sei $x = (x_1, \ldots, x_n) \in K^n$ eine gemeinsame Nullstelle der Polynome $f_1, \ldots, f_r$. Dann gilt $f(x) = 0$ für jedes Polynom $f \in (f_1, \ldots, f_r)$ in dem

von den f_i erzeugten Ideal. Denn: Sei $f \in (f_1, \ldots, f_r)$ beliebig. Dann gibt es $g_1, \ldots, g_r \in K[X_1, \ldots, X_n]$ mit $f = \sum_{i=1}^{r} g_i \cdot f_i$. Es folgt:

$$f(x) = (\sum_{i=1}^{r} g_i \cdot f_i)(x) = \sum_{i=1}^{r} g_i(x) \cdot f_i(x) = \sum_{i=1}^{r} g_i(x) \cdot 0 = 0$$

Betrachte nun das konstante Polynom $e = 1 \in K[X_1, \ldots, X_n]$. Dann gilt $e(x) = 1 \neq 0$ und folglich $e \notin (f_1, \ldots, f_r)$. $(f_1, \ldots, f_r)$ ist damit ein echtes Ideal in $K[X_1, \ldots, X_n]$.

ii) $\Rightarrow$ *i)* Sei $(f_1, \ldots, f_r)$ ein echtes Ideal in $K[X_1, \ldots, X_n]$. Dann gibt es ein maximales echtes Ideal $\mathfrak{m} \trianglelefteq K[X_1, \ldots, X_n]$ mit $(f_1, \ldots, f_r) \subseteq \mathfrak{m}$. Da K algebraisch abgeschlossen ist, gibt es nach dem schwachen Nullstellensatz (Theorem 12 in Kapitel 3 der Vorlesung) Elemente $\alpha_1, \ldots, \alpha_n \in K$ mit $\mathfrak{m} = (X_1 - \alpha_1, \ldots, X_n - \alpha_n)$. Setze $q_i := X_i - \alpha_i$ für $i = 1, \ldots, n$ und $x = (\alpha_1, \ldots, \alpha_n) \in K^n$. Dann gilt für $i = 1, \ldots, n$:

$$q_i(x) = (X_i - \alpha_i)(\alpha_1, \ldots, \alpha_n) = \alpha_i - \alpha_i = 0$$

Da die q_i das Ideal $\mathfrak{m}$ erzeugen, gilt mit der Argumentation in *i)* $\Rightarrow$ *ii)* schon $f(x) = 0$ für alle $f \in \mathfrak{m}$. Wegen $(f_1, \ldots, f_r) \subseteq \mathfrak{m}$ gilt insbesondere $f_i(x) = 0$ für $i = 1, \ldots, r$, d.h. die Polynome $f_1, \ldots, f_r$ haben eine gemeinsame Nullstelle.

***-Aufgabe**

Sei K ein algebraisch abgeschlossener Körper, $\mathfrak{a} \trianglelefteq K[X_1, \ldots, X_n]$ ein echtes Ideal und $X \subseteq K^n$ eine Teilmenge.

a) Setze

$$I(X) := \{p \in K[X_1, \ldots, X_n] \mid p(x) = 0 \text{ für alle } x \in X\}.$$

Zeige: $I(X)$ ist ein Ideal in $K[X_1, \ldots, X_n]$.

b) Sei $V(\mathfrak{a})$ die durch $\mathfrak{a}$ definierte *algebraische Varietät*, d.h.

$$V(\mathfrak{a}) = \{x \in K^n \mid p(x) = 0 \text{ für alle } p \in \mathfrak{a}\}.$$

Zeige: $I(V(\mathfrak{a})) = \text{rad}(\mathfrak{a})$

Lösung:

a) Das Nullpolynom $0 \in K[X_1, \ldots, X_n]$ verschwindet auf allen Punkten des K^n, insbesondere auf allen Punkten in X. Somit gilt $0 \in I(X)$.
Seien $f, g \in I(X)$ beliebig. Dann gilt für jedes $x \in X$:

$$(f + g)(x) = f(x) + g(x) = 0 + 0 = 0$$

Also ist $f + g \in I(X)$. Sei $q \in K[X_1, \ldots, X_n]$ beliebig. Für jedes $x \in X$ erhalten wir:

$$(q \cdot f)(x) = q(x) \cdot f(x) = q(x) \cdot 0 = 0$$

Es folgt $q \cdot f \in I(X)$. Insgesamt ist $I(X)$ damit ein Ideal in $K[X_1, \ldots, X_n]$.

b) Um $I(V(\mathfrak{a})) = \mathrm{rad}(\mathfrak{a})$ zu beweisen, zeigen wir beide Inklusionen.
„$\mathrm{rad}(\mathfrak{a}) \subseteq I(V(\mathfrak{a}))$“: Sei $f \in \mathrm{rad}(\mathfrak{a})$ beliebig. Dann gibt es $n \in \mathbb{N}$ mit $f^n \in \mathfrak{a}$. Sei $x \in V(\mathfrak{a})$ beliebig. Zu zeigen: $f(x) = 0$
Wegen $f^n \in \mathfrak{a}$ gilt:

$$f(x)^n = (f^n)(x) = 0 \Rightarrow f(x) = 0$$

Da $x \in V(\mathfrak{a})$ beliebig war, folgt

$$f \in \{p \in K[X_1, \ldots, X_n] \mid p(x) = 0 \text{ für alle } x \in V(\mathfrak{a})\} = I(V(\mathfrak{a})).$$

„$I(V(\mathfrak{a})) \subseteq \mathrm{rad}(\mathfrak{a})$“: Sei $f \in I(V(\mathfrak{a}))$ beliebig und o.E. $f \neq 0$.
Nach dem Korollar zu Hilberts Basissatz (Theorem 6 in Kapitel 3 der Vorlesung), ist $K[X_1, \ldots, X_n]$ noethersch und das Ideal $\mathfrak{a}$ somit endlich erzeugt. Seien $f_1, \ldots, f_r \in K[X_1, \ldots, X_r]$ mit $\mathfrak{a} = (f_1, \ldots, f_r)$. Sei T eine neue Variable (also $T \neq X_i$ für $i = 1, \ldots, n$). Betrachte den Polynomring $K[X_1, \ldots, X_n, T]$ und darin das Polynom $q = f \cdot T - 1$.
Behauptung: Die Polynome $f_1, \ldots, f_r, q \in K[X_1, \ldots, X_n, T]$ haben keine gemeinsame Nullstelle in K^{n+1}.
Beweis: Per Widerspruch: Sei $(x_1, \ldots, x_n, y) \in K^{n+1}$ eine gemeinsame Nullstelle, d.h. $q(x_1, \ldots, x_n, y) = 0 = f_i(x_1, \ldots, x_n, y)$ für $i = 1, \ldots, r$. Da die Variable T in $f_1, \ldots, f_r$ „nicht vorkommt“, gilt

$$0 = f_i(x_1, \ldots, x_n, y) = f_i(x_1, \ldots, x_n)$$

für $i = 1, \ldots, r$. Somit ist $x = (x_1, \ldots, x_n) \in K^n$ eine gemeinsame Nullstelle der Polynome $f_1, \ldots, f_r$. Da die f_i das Ideal $\mathfrak{a}$ erzeugen, gilt (wie in Aufgabe 9.4 beobachtet) $g(x) = 0$ für alle $g \in \mathfrak{a}$, d.h. $x \in V(\mathfrak{a})$. Wegen $f \in I(V(\mathfrak{a}))$ folgt $f(x) = 0$. Da die Variable T in f nicht vorkommt, gilt wie oben $f(x_1, \ldots, x_n, y) = f(x) = 0$. Somit erhalten wir:

$$\begin{aligned} 0 = q(x_1, \ldots, x_n, y) &= (f \cdot T - 1)(x_1, \ldots, x_n, y) \\ &= f(x_1, \ldots, x_n, y) \cdot T(x_1, \ldots, x_n, y) - 1 \\ &= 0 \cdot y - 1 = 0 - 1 = -1 \neq 0 \qquad \lightning \end{aligned}$$

Die Annahme, die Polynome $f_1, \ldots, f_r, q$ hätten eine gemeinsame Nullstelle in K^{n+1}, war demnach falsch.
Nach Aufgabe 9.4 ist das von $f_1, \ldots, f_r, q$ erzeugte Ideal der gesamte Ring, d.h. $(f_1, \ldots, f_r, q) = K[X_1, \ldots, X_n, T]$. Insbesondere existieren Polynome $g_1, \ldots, g_r, g \in K[X_1, \ldots, X_n, T]$ mit $1 = \sum_{i=1}^{r} g_i \cdot f_i + g \cdot q$.
Einsetzen von $T = \frac{1}{f}$ liefert $1 = \sum_{i=1}^{r} g_i(X_1, \ldots, X_n, \frac{1}{f}) \cdot f_i$. (Beachte: Diese Gleichung spielt sich im Quotientenkörper $K(X_1, \ldots X_n)$ des Polynomrings $K[X_1, \ldots, X_n]$ ab. Da die Variable T in den Polynomen f_i nicht vorkommt, gilt $f_i = f_i(X_1, \ldots, X_n) = f_i(X_1, \ldots, X_n, \frac{1}{f})$.)
Multiplizieren wir beide Seiten mit einer genügend großen Potenz f^m erhalten wir in $K[X_1, \ldots, X_r]$ eine Gleichung der Form $f^m = \sum_{i=1}^{r} h_i \cdot f_i$.
(Genauer muss m so großgewählt werden, dass

$$h_i = f^m \cdot g_i(X_1, \ldots, X_n, \frac{1}{f}) \in K[X_1, \ldots, X_n]$$

für alle $i = 1, \ldots, r$ gilt. Es genügt, wenn m mindestens der maximale „T-Grad“ der Koeffiezientenpolynome $g_i \in K[X_1, \ldots, X_n, T], 1 \leq i \leq r$ ist.)

Da die f_i das Ideal $\mathfrak{a}$ erzeugen, gilt $f^m = \sum_{i=1}^{r} h_i \cdot f_i \in \mathfrak{a}$ und somit nach Definition $f \in \mathrm{rad}(\mathfrak{a})$.