7. Übungszettel zur Vorlesung „Geometrische Gruppentheorie 2“
Musterlösung

SoSe 2016
WWU Münster

Prof. Dr. Linus Kramer
Nils Leder
Antoine Beljean

Aufgabe 7.1
Sei A ein kommutativer Ring und $n \in \mathbb{N}, n \geq 1$. Zeige:

$$\mathrm{GL}_n(A) \cong \mathrm{SL}_n(A) \rtimes A^*$$

Lösung: Wir betten zunächst A^* via $a \mapsto \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}$ als Untergruppe in $\mathrm{GL}_n(A)$ ein. Nach Vorlesung ist $\mathrm{SL}_n(A)$ ein Normalteiler in $\mathrm{GL}_n(A)$.
Weiter gilt $\det \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} = a$ und somit $\mathrm{SL}_n(A) \cap A^* = \{1\}$.
Wir zeigen nun, dass $\mathrm{SL}_n(A) \cdot A^* = \mathrm{GL}_n(A)$ gilt.
Sei $S \in \mathrm{GL}_n(A)$ beliebig und $a := \det S \in A^*$. Schreibe $S = (s_1, \dots, s_n)$ als Spaltenmatrix. Dann hat die Matrix $S' = (a^{-1}s_1, s_2, \dots, s_n)$ die Determinante 1, also $S' \in \mathrm{SL}_n(A)$ und es gilt: $S = S' \cdot \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} \in \mathrm{SL}_n(A) \cdot A^*$
Wegen $\mathrm{SL}_n(A) \trianglelefteq \mathrm{GL}_n(A)$, $\mathrm{SL}_n(A) \cdot A^* = \mathrm{GL}_n(A)$ und $\mathrm{SL}_n(A) \cap A^* = \{1\}$ ist $\mathrm{GL}_n(A)$ nach Aufgabe 6.4 b) isomorph zu einem semi-direkten Produkt $\mathrm{SL}_n(A) \rtimes A^*$.

Aufgabe 7.2
Sei A ein kommutativer Ring, $n \in \mathbb{N}$ und $S, T \in A^{n \times n}$. Zeige: Gilt $ST = 1$, so gilt auch $TS = 1$.

Lösung: Es gilt nach Lemma 1 in Kapitel 3 der Vorlesung:

$$\det S \cdot \det T = \det ST = \det 1 = 1$$

Somit ist $\det S \in A^*$ und S invertierbar. Es gibt also eine Matrix $U \in A^{n \times n}$ mit $US = 1 = SU$. Nun folgt:

$$T = 1 \cdot T = (US) \cdot T = U \cdot (ST) = U \cdot 1 = U$$

Somit gilt $T = U$ und daher $TS = 1$.

Aufgabe 7.3
Sei R ein Ring, $I \trianglelefteq R$ ein Ideal und K ein Körper. Zeige:

a) I ist genau dann ein maximales Ideal, wenn R/I ein Körper ist.

b) I ist genau dann ein Primideal, wenn R/I ein Integritätsbereich ist.

c) Ist $z \in R$ nilpotent (d.h. es gibt $n \in \mathbb{N}$ mit $z^n = 0$), so ist $1-z$ invertierbar.

d) K ist genau dann algebraisch abgeschlossen, wenn K keine echte, endliche Körpererweiterung besitzt.

Lösung:

a) Sei I ein maximales Ideal und $r + I \in R/I$ mit $r + I \neq 0 + I$, d.h. $r \notin I$. Da r nicht in I liegt und I maximal ist, erzeugen r und I den ganzen Ring. Somit gibt es $s \in R$ und $i \in I$ mit $1 = r \cdot s + i$. Es folgt $(r+I)\cdot(s+I) = rs + I = 1 + I = 1_{R/I}$. Also ist $r + I$ in R/I invertierbar und R/I ist ein Körper.
Sei umgekehrt R/I ein Körper und $r \in R \setminus I$. Dann ist $r + I \neq 0 + I$ und folglich invertierbar. Sei $s \in R$ mit $(r + I) \cdot (s + I) = 1 + I$. Nun gilt $rs+I = 1+I$, also $1-rs \in I$. Damit liegt 1 in dem von I und r erzeugten Ideal. Das von I und r erzeugte Ideal ist damit schon der gesamte Ring R. Da $r \in R \setminus I$ beliebig war, ist I ein maximales Ideal.

b) Sei I ein Primideal. Seien $r+I, s+I \in R/I$ mit $(r+I)\cdot(s+I) = 0+I$, d.h. $rs \in I$. Da I ein Primideal ist, gilt nun $r \in I$ oder $s \in I$. Dies bedeutet $r + I = 0 + I$ oder $s + I = 0 + I$. Damit ist R/I nullteilerfrei, also ein Integritätsbereich.
Sei umgekehrt R/I ein Integritätsbereich. Seien $r, s \in R$ mit $rs \in I$. Dann gilt $(r + I) \cdot (s + I) = rs + I = 0 + I$. Da R/I nullteilerfrei ist, folgt $r + I = 0 + I$ oder $s + I = 0 + I$, also $r \in R$ oder $s \in R$. Damit ist I ein Primideal.

c) Sei $z \in R$ nilpotent und $n \in \mathbb{N}$ mit $z^n = 0$. Setze $y := \sum_{i=0}^{n-1} z^i \in R$. Offenbar kommutiert y mit $1 - z$. Weiter gilt:

$$(1-z)\cdot y = (1-z)\cdot\sum_{i=0}^{n-1} z^i = \sum_{i=0}^{n-1} z^i - \sum_{i=1}^{n} z^i = 1 - z^n = 1 - 0 = 1$$

Folglich ist y invers zu $1 - z$ und $1 - z$ ist invertierbar.

d) Sei K algebraisch abgeschlossen und E eine endliche Körpererweiterung von K. Sei $x \in E$ beliebig. Als endliche Körpererweiterung ist E insbesondere algebraisch über K. Sei $p \in K[X]$ das Minimalpolynom von x über K. Da K algebraisch abgeschlossen ist, zerfällt p über K in (normierte) Linearfaktoren. Da $x \in E$ eine Nullstelle von p ist, gilt $x \in K$. Da $x \in E$ beliebig war, ist $E = K$ und E/K ist keine echte Körpererweiterung.
Die umgekehrte Richtung zeigen wir durch Kontraposition:
Sei K nicht algebraisch abgeschlossen. Dann gibt es ein irreduzibles Polynom $p \in K[X]$, das über K keine Nullstelle besitzt. Nun ist aus der

Algebra bekannt, dass p in $K[X]$ ein maximales Ideal (p) erzeugt. Nach Teil a) ist damit $E := K[X]/(p)$ ein Körper. Wegen $\deg p \geq 2$ beträgt die Dimension von E als K-Vektorraum mindestens 2 und E/K ist eine echte, endliche Körpererweiterung.

Aufgabe 7.4
Sei K ein Körper und $R \subseteq K$ ein Teilring. Dann bilden die über R ganzen Elemente in K einen Teilring.

Lösung: Wir beweisen zunächst die Hilfsbehauptung, dass $x \in K$ genau dann ganz über R ist, wenn es einen Teilring $C \subseteq K$ gibt, welcher R und x enthält und als R-Modul endlich erzeugt ist.
Sei $x \in K$ ganz über R. Sei $R[x] \subseteq K$ der von R und x erzeugte Teilring in K. Zu zeigen: $R[x]$ ist als R-Modul endlich erzeugt.
Es gilt $R[x] = \{\sum_{i=0}^{n} a_i \cdot x^i \mid a_i \in R\}$. Somit wird $R[x]$ als R-Modul von den x-Potenzen $1, x, x^2, \ldots$ erzeugt. Da $x \in K$ ganz über R ist, gibt es ein normiertes Polynom $p \in R[X]$ mit $p(x) = 0$. Seien $b_1, \ldots, b_n \in R$ mit $p = \sum_{i=0}^{n} b_i \cdot X^i$, also $b_i \in R$ und insbesondere $b_n = 1$. Dann gilt $0 = p(x) = \sum_{i=0}^{n} b_i \cdot x^i$ und somit:

$$x^n = 1 \cdot x^n = b_n \cdot x^n = -\sum_{i=0}^{n-1} b_i \cdot x^i$$

Daraus folgt, dass x^n in dem von $1, x, \ldots, x^{n-1}$ erzeugten R-Modul liegt. Induktiv zeigt man, dass x^k für alle $k \geq n$ in diesem Modul enthalten ist. $R[x]$ wird also von $1, x, \ldots, x^{n-1}$ erzeugt. $R[x]$ ist damit ein Teilring, der R und x enthält und als R-Modul endlich erzeugt ist.
Sei umgekehrt $C \subseteq K$ ein Teilring, der R und x enthält und als R-Modul endlich erzeugt ist. Sei $z_1, \ldots, z_n$ ein endliches Erzeugendensystem von C als R-Modul. Dann gibt es $a_{ij} \in R$ für $1 \leq i, j \leq n$ so, dass $x \cdot z_i = \sum_{i=1}^{n} a_{ij} \cdot z_j$ für alle $i = 1, \ldots, n$ gilt. Sei $A \in R^{n \times n}$ die Matrix mit den Einträgen a_{ij}. Betrachte nun die Matrix $M := x \cdot 1_n - A \in C^{n \times n}$. Nach Konstruktion von A gilt $M \cdot \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = 0$. Wegen $M^* \cdot M = \det M \cdot 1_n$ gilt daher auch $\det M \cdot \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = 0$, d.h. $\det M \cdot z_i = 0$ für alle $i = 1, \ldots, n$. Da $1 \in C$ eine R-Linearkombination der z_i ist, folgt $\det M = \det M \cdot 1 = 0$. Nun ist $p := \det(X \cdot 1_n - A) \in R[X]$ ein normiertes Polynom mit $p(x) = 0$. Nach Definition ist x damit ganz über R.
Nun können wir die eigentliche Aussage, dass die über R ganzen Elemente einen Teilring bilden, beweisen:
Offenbar sind 0 und 1 Nullstellen der Polynome X bzw. $X - 1 \in R[X]$ und somit ganz über R. Seien $a, b \in K$ ganz über R. Nach Hilfsbehauptung existieren dann Teilringe $C_1, C_2 \subseteq K$ mit $a \in C_1, b \in C_2$ und $R \subseteq C_1 \cap C_2$, sodass C_1 und C_2 als R-Moduln endlich erzeugt sind. Da $-a \in C_1$ gilt, ist $-a$ nach Hilfsbehauptung ganz über R.
Seien $\{x_1, \ldots, x_n\} \subseteq C_1$ und $\{y_1, \ldots, y_m\} \subseteq C_2$ Erzeugendensysteme von C_1

bzw. C_2 als R-Moduln.
Sei C der von $C_1 \cup C_2$ erzeugte Teilring. Dann enthält C die Elemente a und b sowie den Teilring R. Man rechnet leicht nach, dass C als R-Modul von den Elementen $x_i \cdot y_j$ mit $i = 1, \ldots, n$, $j = 1, \ldots, m$ erzeugt wird. Also ist C als R-Modul endlich erzeugt.
Da $C \subseteq K$ ein Teilring ist, enthält C mit a, b auch die Verknüpfungen $a+b$ und $a \cdot b$. Nach der Hilfsbehauptung sind $a + b$ und $a \cdot b$ damit ganz über R.
Insgesamt bilden die über R ganzen Elemente in K somit einen Teilring.

***-Aufgabe**
Sei A ein kommutativer Ring. Zeige: A hat invariante Basislänge.

Lösung: Per Widerspruch: Angenommen, A habe keine invariante Basislänge, dann gibt es $n, m \in \mathbb{N}$ mit $n < m$ und $A^n \cong A^m$. Sei $\varphi : A^n \to A^m$ ein Isomorphismus mit Inversem $\psi : A^m \to A^n$. Dann gilt $\varphi \circ \psi = \mathrm{id}_{A^m}$ und $\psi \circ \varphi = \mathrm{id}_{A^n}$. Durch Entwickeln bzgl. der Standardbasen des A^n bzw. A^m können wir die Abbildungen φ und ψ als Matrizen $a \in A^{m \times n}$ und $b \in A^{n \times m}$ schreiben.
Dann gilt $a \cdot b = 1_m$ und $b \cdot a = 1_n$. Nun ergänzen wir a und b zu $(m \times m)$-Matrizen. Sei $a' \in A^{m \times m}$ die Matrix, die aus a entsteht, indem rechts $m - n$ 0-Spalten hinzugefügt werden und $b' \in A^{m \times m}$ die Matrix, die man aus b durch Hinzufügen von $m - n$ unteren 0-Zeilen erhält. Dann gilt weiterhin $a' \cdot b' = 1_m$. Jedoch enthält $b' \cdot a'$ eine Nullzeile und es gilt somit $b' \cdot a' \neq 1_m$. $\lightning$
Dies ist ein Widerspruch zu Aufgabe 7.2.
Somit war die Annahme, A^n sei isomorph zu A^m für $n < m$ falsch. A hat damit invariante Basislänge.