



**TECHNISCHE
UNIVERSITÄT
DRESDEN**

Fakultät Mathematik Institut für Algebra, Professur für Algebra

ALGEBRA & ZAHLENTHEORIE

Hausaufgaben

Prof. Dr. Arno Fehm

Sommersemester 2019

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

Hausaufgaben

Algebra & Zahlentheorie – Übungsblatt 1

Eric Kunze (Matr.-Nr. 4679202)

Ü-Gruppe: Freitag 2. DS

Thema: Körpergrad, algebraische Erweiterungen

Lemma 1

Sei K ein Körper. Ist $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(K)$, so gelten folgende Eigenschaften:

- $a = 0 \Rightarrow b, c \neq 0$
- $b = 0 \Rightarrow a, d \neq 0$
- $c = 0 \Rightarrow a, d \neq 0$
- $d = 0 \Rightarrow b, c \neq 0$
- Sind $a, b, c, d \in K^\times$, so ist $a^{-1}b - c^{-1}d \neq 0$.

Beweis. Ist ein Eintrag der Matrix gleich Null, so müssen die Einträge in der gleichen Zeile und der gleichen Spalte ungleich Null sein, da sonst eine Nullspalte oder Nullzeile den Rangverlust und damit auch den Verlust der Invertierbarkeit bedeuten würde. Daraus folgen bereits die ersten vier Aussagen. Für die letzte Aussage nehmen wir an, dass $a^{-1}b - c^{-1}d = 0$ gilt. Dann gilt auch $a^{-1}b = c^{-1}d$, was sich umstellen lässt zu $ad = bc$ bzw. zu $0 = ad - bc = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ im Widerspruch zur Invertierbarkeit. \square

Übung 7

Ist $\alpha \in L \setminus K$ und $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(K)$, so ist $K(\alpha) = K\left(\frac{a\alpha+b}{c\alpha+d}\right)$.

- $K(\alpha) \subseteq K\left(\frac{a\alpha+b}{c\alpha+d}\right)$.

Wir wollen α aus $\frac{a\alpha+b}{c\alpha+d}$ darstellen. Betrachten wir dazu für $x, y \in K(\alpha)$

$$\alpha = x \cdot \frac{a\alpha + b}{c\alpha + d} + y$$

Wir müssen nun 5 verschiedene Fälle unterscheiden.

- (i) Ist $a = 0$, so sind $b, c \in K^\times$ nach Lemma 1. Dann finden wir mit $x = \frac{(c\alpha+d)^2}{bc}$ und $y = -c^{-1}d$

$$x \cdot \frac{b}{c\alpha + d} + y = \frac{(c\alpha + d)^2}{bc} \cdot \frac{b}{c\alpha + d} - \frac{d}{c} = \alpha + \frac{d}{c} - \frac{d}{c} = \alpha$$

- (ii) Ist $b = 0$, so sind nach Lemma 1 $a, d \in K^\times$. Falls $c = 0$ ist, so ist die Aussage mit $x = a^{-1}d$ klar. Sei also $0 \neq c \in K^\times$. Mit $x = -a^{-1}c^2(\alpha + c^{-1}d)^2d^{-1}$ und $y = \frac{\alpha^2 + 2\alpha c^{-1}d}{c^{-1}d}$ ist

$$x \cdot \frac{a\alpha + b}{c\alpha + d} + y = \frac{c^2(\alpha + c^{-1}d)^2}{-ad} \cdot \frac{a\alpha}{c\alpha + d} + \frac{\alpha^2 + 2\alpha c^{-1}d}{c^{-1}d} = \alpha$$

- (iii) Ist $c = 0$, so sind $a, d \in K^\times$ nach Lemma 1. Mit $x = a^{-1}d$ sowie $y = -a^{-1}b$ ist

$$x \cdot \frac{a\alpha + b}{c\alpha + d} + y = \frac{d}{a} \cdot \frac{a \cdot \alpha + b}{d} - \frac{b}{a} = \alpha + \frac{b}{a} - \frac{b}{a} = \alpha$$

- (iv) Ist $a = 0$, so sind $b, c \in K^\times$ nach Lemma 1. Dann gilt mit $x = b^{-1}c\alpha^2$ und $y = -a \cdot \alpha^2 \cdot b^{-1}$

$$x \cdot \frac{a\alpha + b}{c\alpha + d} + y = \frac{c \cdot \alpha^2}{b} \cdot \frac{a \cdot \alpha + b}{c \cdot \alpha} - \frac{a \cdot \alpha^2}{b} = \frac{a \cdot \alpha^2 + b \cdot \alpha - a \cdot \alpha^2}{b} = \alpha$$

- (v) Für den allgemeinen Fall seien $0 \neq a, b, c, d \in K^\times$. Zur besseren Nachvollziehbarkeit konstruieren

wir hier das α direkt aus $\frac{a\alpha+b}{c\alpha+d}$. Wir multiplizieren zuerst mit $a^{-1}c$, was $\frac{\alpha+a^{-1}b}{\alpha+c^{-1}d}$ ergibt. Addieren wir eine -1 , so liefert dies $\frac{a^{-1}b-c^{-1}d}{\alpha+c^{-1}d}$. Durch Multiplikation mit $\frac{(\alpha+c^{-1}d)^2}{a^{-1}b-c^{-1}d}$ (der Nenner ist wegen Lemma 1 nicht Null) erreichen wir $\alpha + c^{-1}d$. Abschließend eliminiert die Addition von $-c^{-1}a$ noch den letzten Summanden und wir erhalten α . Damit ergibt sich

$$x = \frac{c \cdot (\alpha + c^{-1}d)^2}{b - ac^{-1}d} \quad \text{und} \quad y = -\frac{(\alpha + c^{-1}d)^2}{a^{-1}b - c^{-1}d} - c^{-1}d$$

- (vi) Die zwei weiteren Fälle, dass jeweils zwei diagonal zueinander stehende Elemente gleich Null sind ergeben sich unmittelbar aus den Operationen der Fälle, dass je einer von beiden Einträgen Null sind.

Damit gilt für jedes $\xi \in K(\alpha)$ auch $\xi \in K(\frac{a\alpha+b}{c\alpha+d})$.

- $K(\frac{a\alpha+b}{c\alpha+d}) \subseteq K(\alpha)$.

Da $\alpha \in K(\alpha)$ und $a, b \in K$ ist auch $a \cdot \alpha + b \in K(\alpha)$. Analog ist für $c \in K^\times$ und $d \in K$ auch $c \cdot \alpha + d \in K(\alpha)$. Angenommen $c \cdot \alpha + d = 0$, dann gilt $\alpha = -\frac{d}{c} \in K$ im Widerspruch zu $\alpha \in L \setminus K$. Damit ist also $c \cdot \alpha + d \neq 0$, d.h. $c \cdot \alpha + d \in K^\times$. Schließlich ist dann auch $(a \cdot \alpha + b) \cdot (c \cdot \alpha + d)^{-1} = \frac{a\alpha+b}{c\alpha+d} \in K(\alpha)$. Daraus folgt nun die Inklusion $K(\frac{a\alpha+b}{c\alpha+d}) \subseteq K(\alpha)$.

Schlussendlich folgt aus beiden Inklusionen die Gleichheit der Körper, also $K(\alpha) = K(\frac{a\alpha+b}{c\alpha+d})$

Übung 8

Bestimmen Sie das Minimalpolynom von $1+\sqrt{5}/2$ und von $\zeta_5 + \zeta_5^{-1}$ jeweils über \mathbb{Q} . Ist $\mathbb{Q}(\zeta_5) = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$?

- Man stellt schnell fest, dass $\alpha = \frac{1+\sqrt{5}}{2}$ eine Nullstelle von $f = X^2 - X - 1 \in \mathbb{Q}[X]$ ist, denn

$$f(\alpha) = \frac{(1+\sqrt{5})^2}{4} - \frac{1+\sqrt{5}}{2} - 1 = \frac{1+2\sqrt{5}+5}{4} - \frac{2+2\sqrt{5}}{4} - 1 = 0$$

Dieses Polynom ist normiert und besitzt die Nullstellen

$$x_{1/2} = \frac{1}{2} \pm \sqrt{\frac{1}{4} + 1} = \frac{1 \pm \sqrt{5}}{2} \notin \mathbb{Q}$$

Somit ist f nach GEO II.7.1 irreduzibel und es gilt $f = \text{MinPol}(\alpha \mid \mathbb{Q})$.

- Betrachten wir einige Potenzen von $\alpha = \zeta_5 + \zeta_5^{-1}$.

$$\begin{aligned} \alpha^3 &= \zeta_5^3 + \zeta_5^{-3} + 3(\zeta_5 + \zeta_5^{-1}) \\ \alpha^5 &= 2 + 5(\zeta_5^3 + \zeta_5^{-3}) + 10(\zeta_5 + \zeta_5^{-1}) \end{aligned}$$

Nun ist offensichtlich, dass man eine Null aus diesen Potenzen schreiben kann, nämlich $0 = \alpha^5 - 5\alpha^3 + 5\alpha - 2$. Damit erhält man ein Polynom $f = X^5 - 5X^3 + 5X - 2 \in \mathbb{Q}[X]$, welches α als Nullstelle hat. Dieses Polynom ist allerdings nicht irreduzibel, d.h. es gibt eine Zerlegung

$$f = (X - 2)(X^2 + X - 1)^2$$

Da α keine Nullstelle von $X - 2$ ist, jedoch von f , muss also α eine Nullstelle von $\bar{f} = X^2 + X - 1$ sein. Dieses Polynom ist normiert und hat nur die Nullstellen $x_{1/2} = \frac{1 \pm \sqrt{5}}{2} \notin \mathbb{Q}$. Somit ist \bar{f} nach GEO II.7.1 irreduzibel und es gilt $\bar{f} = \text{MinPol}(\alpha \mid \mathbb{Q})$.

- Angenommen es gilt $\mathbb{Q}(\zeta_5) = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$. Ein Polynom mit Nullstelle ζ_5 ist zum Beispiel $\bar{f} = X^5 + 1 = (X-1)(X^4 - X^3 + X^2 - X + 1)$, wobei $f = X^4 - X^3 + X^2 - X + 1$ ein normierter, irreduzibler Faktor mit Nullstelle ζ_5 ist, also $f = \text{MinPol}(\zeta_5 | \mathbb{Q})$. Damit ist ζ_5 algebraisch über \mathbb{Q} und es gilt nach Satz 2.7 auch $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = \deg(\zeta_5 | \mathbb{Q}) = 4$ und dem ersten Teil der Aufgabe $[\mathbb{Q}(\zeta_5 + \zeta_5^{-1}) : \mathbb{Q}] = \deg(\zeta_5 + \zeta_5^{-1} | \mathbb{Q}) = 2$. Aufgrund der Multiplikativität des Körpergrades (Satz 1.12) gilt

$$\begin{array}{ccccc} [\mathbb{Q}(\zeta_5) : \mathbb{Q}(\zeta_5 + \zeta_5^{-1})] & \cdot & [\mathbb{Q}(\zeta_5 + \zeta_5^{-1}) : \mathbb{Q}] & = & [\mathbb{Q}(\zeta_5) : \mathbb{Q}] \\ \Rightarrow [\mathbb{Q}(\zeta_5) : \mathbb{Q}(\zeta_5 + \zeta_5^{-1})] & \cdot & 2 & = & 4 \end{array}$$

woraus also $[\mathbb{Q}(\zeta_5) : \mathbb{Q}(\zeta_5 + \zeta_5^{-1})] = 4/2 = 2$ folgt, was im Widerspruch zur Annahme steht. Somit ist $\mathbb{Q}(\zeta_5) \neq \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$.

Übung 9

Sei $\alpha \in L$ algebraisch über K mit $\deg(\alpha | K)$ ungerade. Zeigen Sie, dass $K(\alpha) = K(\alpha^2)$ gilt.

Da α algebraisch über K ist, existiert ein Polynom $f \in K[X]$, für das $f(\alpha) = 0$ gilt. Aus der Eigenschaft algebraisch zu sein folgt mit Satz 2.7 auch, dass $\deg(f) = \deg(\alpha | K) = [K(\alpha) : K] = 2k+1$ für ein $k \in \mathbb{N}_0$. Betrachte daher $f = \sum_{i=0}^{2k+1} c_i X^i$. Wir können f zerlegen in

$$f = \sum_{i=0}^k a_i X^{2i+1} + \sum_{i=0}^k b_i X^{2i} = \left(\sum_{i=0}^k a_i X^{2i} \right) \cdot X + \sum_{i=0}^k b_i X^{2i}$$

wobei $a_i = c_{2i+1}$ und $b_i = c_{2i}$ für alle $i \in \{0, \dots, k\}$. Definieren wir nun

$$\bar{f} := \left(\sum_{i=0}^k a_i (\alpha^2)^i \right) \cdot X + \sum_{i=0}^k b_i (\alpha^2)^i \in K(\alpha^2)[X]$$

Weiterhin gilt natürlich $\bar{f}(\alpha) = 0$. Der Leitkoeffizient von \bar{f} ist nicht Null, da sonst der Grad von $\sum_{i=0}^k a_i (\alpha^2)^i$ kleiner als der Grad des Minimalpolynoms von α über K wäre. Angenommen $\text{LC}(\bar{f}) = \sum_{i=0}^k a_i (\alpha^2)^i = 0$. Dann ist das Polynom $\sum_{i=0}^k a_i X^{2i} \in K[X]$ vom Grad $2k$ schon Minimalpolynom und $\deg(\alpha | K) = 2k$ gerade im Widerspruch zur Voraussetzung. Damit ist $\text{LC}(\bar{f}) \neq 0$.

Definieren wir also

$$g = X + \frac{\sum_{i=0}^k b_i \alpha^{2i}}{\sum_{i=0}^k a_i \alpha^{2i}} \in K(\alpha)[X]$$

so hat dieses Grad 1 (ist also irreduzibel), ist normiert und α ist Nullstelle davon. Damit ist $[K(\alpha) : K(\alpha^2)] = 1$ und die Körper sind gleich, d.h. $K(\alpha) = K(\alpha^2)$.