



**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

10 / 10 BE

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

Hausaufgabe 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 $x, y \in K(\alpha)$

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

einfacher: $g = \frac{a\alpha+b}{c\alpha+d}$ nach α umstellen

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 $K(\alpha) = K(\frac{a\alpha+b}{c\alpha+d})$

Hausaufgabe 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 $f = \text{MinPol}(\zeta_5 \mid \mathbb{Q})$. Damit ist ζ_5 algebraisch über \mathbb{Q} und es gilt nach Satz 2.7 auch $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = \deg(\zeta_5 \mid \mathbb{Q}) = 4$ und dem ersten Teil der Aufgabe $[\mathbb{Q}(\zeta_5 + \zeta_5^{-1}) : \mathbb{Q}] = \deg(\zeta_5 + \zeta_5^{-1} \mid \mathbb{Q}) = 2$. Aufgrund der Multiplikativität des Körpergrades (Satz 1.12) gilt

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

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 $\mathbb{Q}(\zeta_5) \neq \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$.

Hausaufgabe 9

Sei $\alpha \in L$ algebraisch über K mit $\deg(\alpha \mid K)$ 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 $\deg(f) = \deg(\alpha \mid K) = [K(\alpha) : K] = 2k + 1$ 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 $\deg(\alpha \mid K) = 2k$ 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. $K(\alpha) = K(\alpha^2)$.

Hausaufgaben

Algebra & Zahlentheorie – Übungsblatt 2

Eric Kunze (Matr.-Nr. 4679202)

Ü-Gruppe: Freitag 2. DS

Thema: Wurzelkörper, Zerfällungskörper, algebraischer Abschluss

10/10 BE

Hausaufgabe 23

Sei $f \in K[X]$ irreduzibel und $[L : K]$ endlich und teilerfremd zu $\deg(f)$. Zeigen Sie, dass f auch in $L[X]$ irreduzibel ist.

Sei α eine Nullstelle von f in einem algebraischen Abschluss von L . Wegen Multiplikativität der Körpergrade ergibt sich $[L(\alpha) : K] = [L(\alpha) : L] \cdot [L : K] = [L(\alpha) : K(\alpha)] \cdot [K(\alpha) : K]$. Also gilt

$$[L(\alpha) : L] = \frac{[L(\alpha) : K(\alpha)] \cdot [K(\alpha) : K]}{[L : K]} = \frac{[L(\alpha) : K(\alpha)] \cdot \deg(f)}{[L : K]}$$

Da $[L : K]$ und $\deg(f)$ teilerfremd sind, ist $[L : K]$ ein Teiler von $[L(\alpha) : K(\alpha)]$. Andererseits gilt auch immer $[L(\alpha) : K(\alpha)] \leq [L : K]$ und deshalb $[L(\alpha) : K(\alpha)] = [L : K]$. Somit folgt dann daraus $[L(\alpha) : L] = \deg(\alpha|L) = \deg(f)$ und f ist als Minimalpolynom über L irreduzibel.

Hausaufgabe 24

Bestimmen Sie den Zerfällungskörper von $f = X^2 + X + 1$, $f = X^3 + X^2 + X + 1$ und $f = X^4 + X^3 + X^2 + X + 1$ über \mathbb{Q} und geben Sie jeweils den Grad an.

- Wir betrachten das Polynom $f = X^2 + X + 1$. Dies ist offensichtlich das dritte Kreisteilungspolynom Φ_3 . Somit hat es die Nullstellen ζ_3 und ζ_3^2 . Da $\zeta_3^2 \in \mathbb{Q}(\zeta_3)$ ist $\mathbb{Q}(\zeta_3, \zeta_3^2) = \mathbb{Q}(\zeta_3)$. Damit ist also $\mathbb{Q}(\zeta_3)$ der Zerfällungskörper von f . Da Φ_3 gemäß eines Satzes aus Geometrie irreduzibel ist, ist also $f = \text{MinPol}(\zeta_3 | \mathbb{Q})$ und somit ist $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$.
- Wir betrachten das Polynom $f = X^4 + X^3 + X^2 + X + 1$, welches wiederum das fünfte Kreisteilungspolynom Φ_5 ist. Somit hat es die Nullstellen ζ_5^k für $k = 1, 2, 3, 4$ und $\mathbb{Q}(\zeta_5)$ ist Zerfällungskörper von f , da wieder alle weiteren Potenzen bereits in $\mathbb{Q}(\zeta_5)$ liegen. Auch f ist als Kreisteilungspolynom wieder irreduzibel und somit $f = \text{MinPol}(\zeta_5 | \mathbb{Q})$. Also ist $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$.
- Betrachten wir nun noch das Polynom $f = X^3 + X^2 + X + 1$, so hat dieses auf jeden Fall die Nullstelle -1 . Polynomdivision mit $X + 1$ ergibt dann $f = (X + 1)(X^2 + 1)$. Aus dem zweiten Faktor ergeben sich die weiteren Nullstellen i und $-i$. Offensichtlich ist $1 \in \mathbb{Q}$ bereits enthalten und $-i$ lässt sich aus i darstellen. Damit ist also $\mathbb{Q}(i)$ als Zerfällungskörper von f ausreichend. Weiter ist $g = X^2 + 1$ irreduzibel und normiert, also ist g das Minimalpolynom von i über \mathbb{Q} . Damit ist $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

Hausaufgabe 25

Bestimmen Sie den Grad des Zerfällungskörpers von $f = X^4 + 1$ über \mathbb{Q} und über $\mathbb{Q}(\sqrt{2})$.

Erneut ist $f = X^4 + 1$ ein Kreisteilungspolynom, nämlich Φ_8 . Damit erhalten wir alle mit 8 teilerfremden Potenzen von ζ_8 als Nullstellen, d.h. f hat die Nullstellen $\zeta_8, \zeta_8^3, \zeta_8^5, \zeta_8^7$. Alternativ ist $\zeta_8 = \frac{1+i}{\sqrt{2}}$ und dies zur vierten Potenz ergibt wieder -1 , wie auch die drei weiteren Potenzen. Als Zerfällungskörper ist somit wieder $\mathbb{Q}(\zeta_8)$ ausreichend. f ist normiert und nach V18 irreduzibel, also Minimalpolynom von ζ_8 über \mathbb{Q} und somit ist $\deg(\zeta_8|\mathbb{Q}) = [\mathbb{Q}(\zeta_8) : \mathbb{Q}] = 4$.

Da $\zeta_8 = \exp\left(\frac{2\pi i}{8}\right) = \frac{1+i}{\sqrt{2}}$, ist $i = \zeta_8^2 \in \mathbb{Q}(\zeta_8)$ und auch $\zeta_8 + \zeta_8^7 = \sqrt{2} \in \mathbb{Q}(\zeta_8)$. Damit ist $\mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$. Es ist bereits bekannt, dass $[\mathbb{Q}(i) : \mathbb{Q}] = 2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ und außerdem ist klar, dass $i \notin \mathbb{Q}(\sqrt{2})$. Also folgt daraus, dass $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$, also ist $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$. Insbesondere folgt daraus nun auch, dass $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(i, \sqrt{2})$ ist.

Nach Multiplikativität der Körpergrade gilt nun $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = [\mathbb{Q}(\zeta_8) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$. Aus dem ersten Teil wissen wir, dass $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = 4$. Außerdem ist bekannt, dass $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ gilt und somit nur $[\mathbb{Q}(\zeta_8) : \mathbb{Q}(\sqrt{2})] = 2$ gelten kann.

Hausaufgaben

Algebra & Zahlentheorie – Übungsblatt 3

Eric Kunze (Matr.-Nr. 4679202)

Ü-Gruppe: Freitag 2. DS

Thema: Transzendente Erweiterungen & separable Polynome

8/12 BE

Hausaufgabe 38

Bestimmen Sie den Grad des Zerfällungskörpers des Polynoms $f = X^4 + 2X^2 - 2$ über \mathbb{Q} . Ist f separabel?

Wir betrachten das Polynom $f = X^4 + 2X^2 - 2 \in \mathbb{Q}[X]$ mit der Substitution $Y := X^2$, was uns $f = Y^2 + 2Y - 2$ liefert. Damit erhält man die Nullstellen $X_{1/2} = \pm\sqrt{-1 + \sqrt{3}}$ und $X_{3/4} = \pm\sqrt{-1 - \sqrt{3}}$. Offensichtlich sind alle vier Nullstellen voneinander verschieden und haben alle Vielfachheit eins. Damit ist also die Summe der Vielfachheiten der Nullstellen gleich dem Grad des Polynoms und f somit separabel.

Im Folgenden sei $\alpha_1 = \sqrt{-1 + \sqrt{3}}$ und $\alpha_2 = \sqrt{-1 - \sqrt{3}}$.

Da mit $a \in K$ für einen Körper K auch schon $-a \in K$ gilt, reicht als Zerfällungskörper für f auch $L := \mathbb{Q}(\alpha_1, \alpha_2)$ aus. Mit Eisenstein und $p = 2$ stellen wir fest, dass f irreduzibel ist. Damit gilt $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 4$. Um den Grad des Zerfällungskörpers zu bestimmen fehlt nun noch $[L : \mathbb{Q}(\alpha_1)]$. Man kann α_2 auch schreiben als $\alpha_2 = \sqrt{-1 - \sqrt{3}} = \sqrt{-1 \cdot (1 + \sqrt{3})} = i\sqrt{1 + \sqrt{3}} \in \mathbb{C}$. Jedoch ist mit $\alpha_1 \in \mathbb{R}$ (da $-1 + \sqrt{3} > 0$) auch $\mathbb{Q}(\alpha_1) \subseteq \mathbb{R}$ und damit auf jeden Fall $\alpha_2 \notin \mathbb{Q}(\alpha_1)$. Somit ist auch $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)] > 1$. Andererseits hat das Polynom $g = X^2 - \alpha_1^2 + 2 \in \mathbb{Q}(\alpha_1)[X]$ mit

$$g(\alpha_2) = \alpha_2^2 + \alpha_1^2 + 2 = -1 - \sqrt{3} - 1 + \sqrt{3} + 2 = 0$$

die Nullstelle α_2 . Damit ist es das Polynom kleinsten Grades, welches Minimalpolynom von α_2 über $\mathbb{Q}(\alpha_1)$ sein kann. Deshalb gilt $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)] = 2$. Da der Körpergrad multiplikativ ist, ergibt sich

$$[L : \mathbb{Q}] = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)] \cdot [\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 2 \cdot 4 = 8$$

Hausaufgabe 39

Sei $L = K(X)$ ein rationaler Funktionenkörper. Sei $\alpha = \frac{f}{g} \in L \setminus K$ mit $f, g \in K[X]$ teilerfremd. Zeigen Sie, dass $[L : K(\alpha)] = \max\{\deg(f), \deg(g)\}$.

Hausaufgabe 40

Sei $p > 0$, $a \in K$ und $f = X^p - X + a \in K[X]$. Zeigen Sie:

- (a) $f(X) = f(X + 1)$
- (b) f ist separabel
- (c) Jeder Wurzelkörper von f ist ein Zerfällungskörper von f .
- (d) Hat f keine Nullstelle in K , so ist f irreduzibel.

(zu a) Es ist $f(X + 1) = (X + 1)^p - (X + 1) + a \stackrel{V1}{=} X^p + 1^p - X - 1 + a = X^p - X + a = f(X)$.

(zu b) Sei α eine Nullstelle von f , d.h. $f(\alpha) = 0$. Wegen Teil (a) gilt dann auch $0 = f(\alpha) = f(\alpha + 1) = \dots = f(\alpha + p - 1)$. Da $\text{char}(K) = p$, sind die $\alpha, \alpha + 1, \dots, \alpha + p - 1$ paarweise verschieden. Damit hat f genau p Nullstellen. Da f auch Grad p hat, ist f damit separabel.

(zu c) Sei L ein Wurzelkörper von f , d.h. $L = K(\alpha)$ für eine Nullstelle α von f . Nach Teil (b) sind dann $\alpha, \alpha + 1, \dots, \alpha + p - 1$ die Nullstellen von f . Jedoch ist mit $i \in K$ (bzw. genauer $\iota(i)$) für alle $i \in \{0, \dots, p - 1\}$ auch $\alpha + i \in K(\alpha)$ und damit ist $K(\alpha) = K(\alpha + i)$ für alle $i \in \{0, \dots, p - 1\}$. Somit ist dann $K(\alpha) = L$ auch schon ein Zerfällungskörper, in dem $f = \prod_{i=0}^{p-1} (X - (\alpha + i))$ in Linearfaktoren zerfällt.

(zu d) Wir zeigen die Kontraposition. Angenommen f sei reduzibel, dann existiert eine Darstellung $f = \prod_{i=0}^m r_i$ mit $r_i \in K[X]$ für alle $i \in \{0, \dots, m\}$ und ein $m \geq 2$.

Wir zeigen nun, dass alle r_i den gleichen Grad haben. Sei L der Zerfällungskörper von f . Wir betrachten eine Nullstelle $\alpha \in L$ von f . Wie wir bereits gesehen haben, sind dann auch $\alpha + 1, \dots, \alpha + p - 1$ Nullstellen. Damit lässt sich f schreiben als $f = \prod_{i=0}^{p-1} (X - (\alpha + i)) =: \prod_{i=0}^{p-1} r_i(X)$. Offensichtlich ist r_i irreduzibel über K für alle $i \in \{0, \dots, p - 1\}$. Dann existiert zu jedem irreduziblen Faktor aber auch ein $s \in \{0, \dots, p - 1\}$, sodass $\bar{r}_i(X) := r_i(X + s)$ gilt und dieses \bar{r}_i ist ebenso irreduzibel. Damit hat r_i für alle $i \in \{0, \dots, p - 1\}$ den gleichen Grad wie das Minimalpolynom von α .

Da nun alle irreduziblen Faktoren den gleichen Grad besitzen, $m \geq 2$ aufgrund der Reduzibilität gilt und p prim ist, müssen alle r_i Linearfaktoren sein. Somit hat f dann schon Nullstellen in K , nämlich die Nullstellen der Linearfaktoren, also $\alpha, \alpha + 1, \dots, \alpha + p - 1$.

Hausaufgaben

Algebra & Zahlentheorie – Übungsblatt 4

Eric Kunze (Matr.-Nr. 4679202)

Ü-Gruppe: Freitag 2. DS

Thema: separable Erweiterungen, einfache Erweiterungen

Lemma 1

Sei $f \in K[X]$ separabel und $g \in K[X]$, sodass $f = g \cdot h$ für ein weiteres Polynom $h \in K[X]$. Dann ist auch g separabel.

Beweis. Angenommen g hat eine mindestens zweifache Nullstelle α , d.h. $g = (X - \alpha)^2 \cdot \bar{g}$ für ein Polynom $\bar{g} \in K[X]$. Dann ist aber auch $f = g \cdot h = (X - \alpha)^2 \cdot \bar{g} \cdot h$ und α somit eine mindestens zweifache Nullstelle von f . Dies ist jedoch im Widerspruch zur Separabilität von f , d.h. g muss schon separabel gewesen sein. \square

Hausaufgabe 54

Seien $p > 0$, $L|K$ algebraisch und $\alpha \in L$. Zeigen Sie: Genau dann ist α separabel über K , wenn $K(\alpha) = K(\alpha^p)$.

(\Leftarrow) Es gelte $K(\alpha) = K(\alpha^p)$. Dann ist insbesondere $\alpha \in K(\alpha^p)$ und wir können α als Linearkombination der Potenzen von α^p schreiben, also $\alpha = \sum_{i \geq 0} a_i \cdot (\alpha^p)^i \in K(\alpha^p)$. Nun können wir das Polynom $f = \sum_{i \geq 0} a_i \cdot (X^p)^i - X \in K[X]$ betrachten. Nach der vorherigen Überlegung ist $f(\alpha) = 0$, d.h. das Minimalpolynom $\text{MinPol}(\alpha | K) = \bar{f} \mid f$. Nun betrachten wir die formale Ableitung von f , d.h. $f' = \sum_{i \geq 0} p i \cdot a_i \cdot X^{p i - 1} - 1 = -1$, da $\text{char}(K) = p > 0$ und somit alle Koeffizienten der Summe verschwinden. Nun gilt $\text{ggT}(f, f') = 1$, was nach Satz 6.6 die Separabilität von f impliziert. Da nun \bar{f} ein Teiler von f ist, überträgt sich die Separabilität nach Lemma 1 auch auf \bar{f} . Damit ist also das Minimalpolynom von α über K separabel und nach Definition α separabel über K .

(\Rightarrow) Sei α separabel über K . Wir bezeichnen mit f das Minimalpolynom von α über K , mit h das Minimalpolynom von α über $K(\alpha^p)$. Man stellt fest, dass im Körper $K(\alpha)$ gilt $h \mid f$. Das Polynom $g = X^p - \alpha^p \in K(\alpha^p)[X]$ hat offensichtlich α als Nullstelle und ist somit ein Vielfaches von h . g lässt sich aufgrund der positiven Charakteristik (V1) auch schreiben als $g = (X - \alpha)^p$, sodass h als Teiler von der Form $h = (X - \alpha)^n$ für ein $n \leq p$ sein muss. Da α separabel ist, darf der Faktor $(X - \alpha)$ nur einmal im Minimalpolynom f vorkommen. Dies vererbt sich nun auch auf den Teiler h von f , d.h. es muss $n = 1$ gelten. Damit gilt also $h = X - \alpha \in K(\alpha^p)[X]$. Nun ist also $\alpha \in K(\alpha^p)$ und gemeinsam mit der trivialen Inklusion $K(\alpha^p) \subseteq K(\alpha)$ gilt nun schon $K(\alpha) = K(\alpha^p)$.

Hausaufgabe 55

Sei $d \in K^\times \setminus (K^\times)^2$ und $\alpha = x + y\sqrt{d} \in L = K(\sqrt{d})$. Drücken Sie $N_{L|K}(\alpha)$ und $Sp_{L|K}(\alpha)$ durch x und y aus.

Als K -Vektorraum hat L die Basis $\mathcal{B} = (1, \sqrt{d})$. Dann gilt $\mu_\alpha(1) = \alpha = x + y\sqrt{d}$, $\mu_\alpha(\sqrt{d}) = x\sqrt{d} + yd$ und damit schließlich für die darstellende Matrix

$$M_{\mathcal{B}}(\mu_\alpha) = \begin{pmatrix} x & yd \\ y & x \end{pmatrix}$$

Damit ist $N_{L|K}(\alpha) = \det(M_{\mathcal{B}}(\mu_\alpha)) = x^2 - y^2d$ und $Sp_{L|K}(\alpha) = Sp(M_{\mathcal{B}}(\mu_\alpha)) = 2x$.

Hausaufgabe 56

Sei ℓ eine Primzahl und $L = \mathbb{Q}(\zeta_\ell)$. Zeigen Sie, dass $\text{Sp}_{L|\mathbb{Q}}(1) = \ell - 1$ und $\text{Sp}_{L|\mathbb{Q}}(\zeta_\ell^j) = -1$ für jedes $j \in \{1, \dots, \ell - 1\}$. Folgern Sie, dass $\text{Sp}_{L|\mathbb{Q}}(1 - \zeta_\ell^j) = \ell$ für jedes $j \in \{1, \dots, \ell - 1\}$.

Für die ersten beiden Teile habe ich jeweils zwei Lösungen.

- Das Minimalpolynom von ζ_ℓ ist $\Phi_\ell = 1 + X + \dots + X^{\ell-1}$ mit $[\mathbb{Q}(\zeta_\ell) : \mathbb{Q}] = \deg(\Phi_\ell) = \ell - 1$. Somit hat eine Basis des K -Vektorraums L also Mächtigkeit $\ell - 1$. Eine solche Basis ist beispielsweise durch $\mathcal{B} = (1, \zeta_\ell, \zeta_\ell^2, \dots, \zeta_\ell^{\ell-2})$ gegeben. Nun suchen wir die darstellende Matrix von μ_1 bezüglich dieser Basis. Diese ergibt sich wegen $\mu_1 = \text{id}_L$ als $M_{\mathcal{B}}(\mu_1) = \mathbb{1}_{\ell-1}$. Dann ergibt sich für die Spur $\text{Sp}_{L|\mathbb{Q}}(1) = \text{Sp } M_{\mathcal{B}}(\mu_1) = \ell - 1$. Alternativ ist $1 \in \mathbb{Q}$ und damit nach Lemma 8.5 mit $n = [L : \mathbb{Q}] = \ell - 1$ schon $\text{Sp}_{L|\mathbb{Q}}(1) = n \cdot 1 = \ell - 1$.
- Betrachten wir nun die darstellende Matrix von $\mu_{\zeta_\ell^j}$ bezüglich \mathcal{B} . Es gilt $\mu_{\zeta_\ell^j}(1) = \zeta_\ell^j$, $\mu_{\zeta_\ell^j}(\zeta_\ell^k) = \zeta_\ell^j \cdot \zeta_\ell^k = \zeta_\ell^{j+k}$ für alle $k \leq \ell - j - 2$. Für alle $k \in \{\ell - j, \dots, \ell\}$ gilt $\mu_{\zeta_\ell^j}(\zeta_\ell^k) = \zeta_\ell^{j+k-\ell}$. In diesen Fällen erfolgt also nur eine Permutation der Basiselemente. Für $k = \ell - j - 1$ betrachten wir das Kreisteilungspolynom $\Phi_\ell(\zeta_\ell) = 1 + \zeta_\ell + \zeta_\ell^2 + \dots + \zeta_\ell^{\ell-2} + \zeta_\ell^{\ell-1} = 0$. Nun können wir dieses nach $\zeta_\ell^{\ell-1}$ umstellen und erhalten $\zeta_\ell^{\ell-1} = -\sum_{i=0}^{\ell-2} \zeta_\ell^i$. Nun können wir diese Informationen zur darstellenden Matrix zusammensetzen:

$$M_{\mathcal{B}}(\mu_{\zeta_\ell^j}) = \left(\begin{array}{ccc|c|ccc} 0 & \dots & 0 & -1 & 1 & \dots & 0 \\ 1 & \dots & 0 & -1 & \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots & \vdots & 0 & \dots & 1 \\ 0 & \dots & 1 & -1 & 0 & \dots & 0 \end{array} \right) = \left(\begin{array}{ccc|c|ccc} 0 & \dots & 0 & -1 & & & \\ & & & \vdots & & & \\ & & & \vdots & & \mathbb{1}_j & \\ & \mathbb{1}_{\ell-j-2} & & \vdots & & & \\ & & & -1 & 0 & \dots & 0 \end{array} \right) \in \text{Mat}_{\ell-1}(\mathbb{Q})$$

Nun stehen auf der Hauptdiagonalen nur Nullen und in der $(\ell - j - 1)$ -ten Spalte stehen in jeder Zeile eine -1 . Damit ergibt sich $\text{Sp}_{L|\mathbb{Q}} = \text{Sp } M_{\mathcal{B}}(\mu_{\zeta_\ell^j}) = -1$. Alternativ können wir wieder Lemma 8.5 (d) anwenden. Wir wissen, dass $\Phi_\ell = \text{MinPol}(\zeta_\ell | \mathbb{Q})$ ist und dann ergibt sich $m = \frac{n}{r} = \frac{n}{\deg(\Phi_\ell)} = \frac{\ell-1}{\ell-1} = 1$. Da ℓ prim ist, sind alle Koeffizienten im Kreisteilungspolynom Φ_ℓ gleich Eins und es folgt mit Lemma 8.5 (d), dass $\text{Sp}_{L|\mathbb{Q}}(\mu_{\zeta_\ell^j}) = -m \cdot 1 = -1$ für alle $j \in \{1, \dots, \ell - 1\}$.

- Für die letzte Aussage können wir die K -Linearität der Spur aus Lemma 8.5 (b) anwenden:
 $\text{Sp}_{L|\mathbb{Q}}(1 - \mu_{\zeta_\ell^j}) = \text{Sp}_{L|\mathbb{Q}}(1) - \text{Sp}_{L|\mathbb{Q}}(\mu_{\zeta_\ell^j}) = \ell - 1 - (-1) = \ell$.

Hausaufgabe 57

Seien $a, b \in \mathbb{Z}$. Bestimmen Sie ein primitives Element der Erweiterung $\mathbb{Q}(\sqrt{a}, \sqrt{b}) | \mathbb{Q}$.

Definieren wir $\alpha = \sqrt{a}$ und $\beta = \sqrt{b}$. Wir wollen zeigen, dass $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + \beta)$. Die Inklusion $\mathbb{Q}(\alpha + \beta) \subseteq \mathbb{Q}(\alpha, \beta)$ ist klar. Um die andere Inklusion zu zeigen betrachten wir einige Potenzen von $\alpha + \beta$:

$$\begin{aligned} (\alpha + \beta)^2 &= a + 2\alpha\beta + b &= (a + b) + 2\alpha\beta \\ (\alpha + \beta)^3 &= a\alpha + 2a\beta + b\alpha + a\beta + 2b\alpha + b\beta = (a + 3b)\alpha + (3a + b)\beta \\ (\alpha + \beta)^4 &= (a + b)^2 + 4(a + b)\alpha\beta + 4ab &= (a^2 + 6ab + b^2) + 4(a + b)\alpha\beta \end{aligned}$$

Schreiben wir dies nun als Gleichungssystem in Matrixform, dann ergibt sich

$$\begin{pmatrix} \alpha + \beta \\ (\alpha + \beta)^2 \\ (\alpha + \beta)^3 \\ (\alpha + \beta)^4 \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 & 1 & 0 \\ a + b & 0 & 0 & 2 \\ 0 & a + 3b & 3a + b & 0 \\ a^2 + 6ab + b^2 & 0 & 0 & 4(a + b) \end{pmatrix}}_{=:A} \cdot \begin{pmatrix} 1 \\ \alpha \\ \beta \\ \alpha\beta \end{pmatrix}$$

Es gilt $\det(A) = -4(a - b)^3 \neq 0$ für $a \neq b$. Für $a \neq b$ ist also $A \in \text{GL}_4(\mathbb{Q})$ und damit existiert $A^{-1} \in \text{GL}_4(\mathbb{Q})$ mit

$$\begin{pmatrix} 1 \\ \alpha \\ \beta \\ \alpha\beta \end{pmatrix} = A^{-1} \cdot \begin{pmatrix} \alpha + \beta \\ (\alpha + \beta)^2 \\ (\alpha + \beta)^3 \\ (\alpha + \beta)^4 \end{pmatrix}$$

Aus der zweiten und dritten Zeile folgt dann insbesondere, dass α und β mithilfe der Potenzen von $\alpha + \beta$ geschrieben werden können. Dies zeigt nun auch $\alpha, \beta \in \mathbb{Q}(\alpha + \beta)$ und somit die Inklusion $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\alpha + \beta)$. Schlussendlich folgt damit $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$, also ist $\sqrt{a} + \sqrt{b}$ primitives Element der Erweiterung $\mathbb{Q}(\sqrt{a}, \sqrt{b}) \mid \mathbb{Q}$.

Hausaufgaben

Algebra & Zahlentheorie – Übungsblatt 5

Eric Kunze (Matr.-Nr. 4679202)

Ü-Gruppe: Freitag 2. DS

Thema: Normale Erweiterungen, Galoiserweiterungen

Hausaufgabe 70

Seien $K \subseteq L_1, L_2 \subseteq \mathbb{Q}$ mit $L_1|K$ und $L_2|K$ endlich galoissch sowie $L_1 \cap L_2 = K$. Dann ist auch das Kompositum $L_1 L_2$ galoissch über K und $\text{Gal}(L_1 L_2|K) \cong \text{Gal}(L_1|K) \times \text{Gal}(L_2|K)$.

Hausaufgabe 71

Sei $L = \mathbb{Q}(i, \zeta_3, \sqrt{2})$. Zeigen Sie, dass $L|\mathbb{Q}$ galoissch ist, bestimmen Sie $\text{Gal}(L|\mathbb{Q})$ und geben Sie ein primitives Element der Erweiterung $L|\mathbb{Q}$ an.

Hausaufgabe 72

Sei $\mathbb{Q} \subseteq L \subseteq \mathbb{C}$ mit $L|\mathbb{Q}$ endlich galoissch und $\text{Gal}(L|\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. Zeigen Sie, dass es genau einen Zwischenkörper $\mathbb{Q} \subseteq M \subseteq L$ gibt und dieser erfüllt $M \subseteq \mathbb{R}$.

$G := \text{Gal}(L|\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$ ist eine zyklische Gruppe der Ordnung $\#G = 4$. Somit gibt es für jeden Teiler der Gruppenordnung genau eine Untergruppe mit entsprechender Ordnung. Sei also $U \leq G$. Dann ist $\#U \in \{1, 2, 4\}$. Für den Index gilt dann entsprechend

$$(G : U) = \frac{\#G}{\#U} \in \{4, 2, 1\}$$

Nach Theorem 2.2 kennen wir eine Bijektion $\phi: \text{Ugr}(G) \rightarrow \text{Zwk}(L|\mathbb{Q})$. Definieren wir nun $M := \phi(U)$. Da die Untergruppen U stets existieren, existiert dann auch der zugehörige Zwischenkörper. Dann gilt aufgrund der Indextreue der Bijektion $[L : M] \in \{4, 2, 1\}$. Ist nun $\#U = 1$, so ist $[L : M] = 4$ und nach dem Gradsatz ergibt sich dann

$$[M : \mathbb{Q}] = \frac{[L : \mathbb{Q}]}{[L : M]} = 1$$

Damit ist also $M = \mathbb{Q}$, was nicht möglich ist. Ist $\#U = 4$, so folgt analog, dass $[L : M] = 1$. Ist dagegen $\#U = 2$, so ist $[L : M] = 2$ und aufgrund des Gradsatzes gilt dann $[M : \mathbb{Q}] = [L : M] = 2$. Somit ist der Zwischenkörper M immer eindeutig bestimmt.

Hausaufgaben

Algebra & Zahlentheorie – Übungsblatt 6

Eric Kunze (Matr.-Nr. 4679202)

Ü-Gruppe: Freitag 2. DS

Thema: Galoisgruppe von Polynomen, endliche Körper

Hausaufgabe 86

Sei L der Zerfällungskörper von $f = X^4 + 1$ über \mathbb{Q} . Bestimmen Sie die Zwischenkörper M der Erweiterung $L|\mathbb{Q}$ und geben Sie jeweils ein primitives Element von $M|\mathbb{Q}$ an.

Sei L der Zerfällungskörper von $f = X^4 + 1$ über \mathbb{Q} . In Aufgabe H25 haben wir gezeigt, dass die Nullstellen von f gerade die ζ_8^i für $i = 1, 3, 5, 7$ sind. Damit ergibt sich $L = \mathbb{Q}(\zeta_8)$. Da f separabel ist (alle Nullstellen sind offensichtlich paarweise verschieden), ist L als Zerfällungskörper galoissch und somit ist $\# \text{Gal}(L|\mathbb{Q}) = [L : \mathbb{Q}] = \deg(f) = 4$.

Bestimmen wir nun $G := \text{Gal}(L|\mathbb{Q}) = \text{Aut}(L|\mathbb{Q})$. Dazu müssen wir jedes $\sigma \in G$ lediglich auf ζ_8 definieren, da σ als Automorphismus auf \mathbb{Q} die Identität ist. Jedes solches σ muss ζ_8 auf eines seiner Konjugierten abbilden. Die Konjugierten ergeben sich als die weiteren Nullstellen von f . Somit ergibt sich nun $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ mit $\sigma_i(\zeta_8) = \zeta_8^{2i-1}$, also

$$\sigma_1(\zeta_8) = \zeta_8 \quad \sigma_2(\zeta_8) = \zeta_8^3 \quad \sigma_3(\zeta_8) = \zeta_8^5 \quad \sigma_4(\zeta_8) = \zeta_8^7$$

Betrachten wir nun die Ordnungen der Elemente. Es ist $\sigma_2^2(\zeta_8) = \sigma_2(\zeta_8^3) = \zeta_8^9 = \zeta_8$. Somit ist $\sigma_2^2 = \text{id}_L$, d.h. $\text{ord}(\sigma_2) = 2$. Weiter ist auch $\sigma_4^2(\zeta_8) = \sigma_4(\zeta_8^7) = \zeta_8^{49} = \zeta_8$ und damit auch $\text{ord}(\sigma_4) = 2$. Nun gibt es (mindestens) zwei Elemente der gleichen Ordnung in G , sodass G nicht zyklisch sein kann. Da wir nur (bis auf Isomorphie) zwei Gruppen der Ordnung 4 kennen, muss $G \cong V_4$ gelten. Schließlich kennen wir wegen $\sigma_4 = \sigma_2 \circ \sigma_3$ auch schon die Untergruppen von G , nämlich $\text{Ugr}(G) = \{1, \langle \sigma_2 \rangle, \langle \sigma_3 \rangle, \langle \sigma_2, \sigma_3 \rangle\} =: \{U_1, U_2, U_3, U_4\}$.

Aus der Galois-Korrespondenz erhalten wir eine Abbildung $\phi: \text{Ugr}(G) \rightarrow \text{Zwk}(L|\mathbb{Q})$ mit $\phi(H) = H^\circ := L^H = \{\alpha \in L : \alpha^h = \alpha \ \forall h \in H\}$. Bestimmen wir nun $\phi(U_i)$ für $i = 1, 2, 3, 4$. Für U_1 ist $\phi(U_1) = L$ offensichtlich. Für U_2 betrachten wir, wie sich bestimmte Argumente, vor allem Potenzen von ζ_8 , unter dem Erzeuger σ_2 verhalten. Beispielsweise ist $\sigma_2(\zeta_8^2) = \zeta_8^6 \neq \zeta_8^2$. Somit kann ζ_8^2 nicht in $\phi(U_2)$ sein. Mit ζ_8^4 stellt man fest, dass $\sigma_2(\zeta_8^4) = \zeta_8^4$ gilt wegen $\text{ord}(\sigma_2) = 2$ folglich auch $\sigma_2^2(\zeta_8^4) = \zeta_8^4$. Damit gilt also für alle $u \in U_2$, dass $(\zeta_8^4)^u = \zeta_8^4$. Analog fährt man fort und erhält schließlich folgende Zwischenkörper:

$$\begin{aligned}\phi(U_1) &= L^{\text{id}} = \{\alpha \in L : \alpha^{\text{id}} = \alpha\} = L \\ \phi(U_2) &= L^{\langle \sigma_2 \rangle} = \{\alpha \in L : \alpha^u = \alpha \ \forall u \in U_2\} = \mathbb{Q}(\zeta_8^4) \\ \phi(U_3) &= L^{\langle \sigma_3 \rangle} = \{\alpha \in L : \alpha^u = \alpha \ \forall u \in U_3\} = \mathbb{Q}(\zeta_8^2) \\ \phi(U_4) &= L^{\langle \sigma_2 \rangle} = \{\alpha \in L : \alpha^u = \alpha \ \forall u \in U_4\} = \mathbb{Q}\end{aligned}$$

Damit ergibt sich die Menge der Zwischenkörper von $L|\mathbb{Q}$ als $\text{Zwk}(L|\mathbb{Q}) = \{\mathbb{Q}, \mathbb{Q}(\zeta_8^2), \mathbb{Q}(\zeta_8^4), L\}$.

Hausaufgabe 87

Bestimmen Sie die Galoisgruppe von $f = X^4 + 1$ über \mathbb{F}_p , in Abhängigkeit von $p > 2$.

Hausaufgabe 88

Sei $K = \mathbb{F}_q$ und sei ℓ eine Primzahl. Bestimmen Sie die Anzahl der primitiven Elemente der Erweiterung $\mathbb{F}_{q^\ell}|\mathbb{F}_q$. Schließen Sie, dass es $\ell^{-1}(q^\ell - q)(q - 1)$ viele irreduzible $f \in K[X]$ vom Grad $\deg(f) = \ell$ gibt.

Wir betrachten die Körpererweiterung $L := \mathbb{F}_{q^\ell}|\mathbb{F}_q =: K$ und wollen zeigen, dass alle Elemente in $L \setminus K$ primitiv sind. Dann wissen wir, dass nach Satz 3.5, dass $L|K$ einfach ist. Wählen wir nun ein $\alpha \in L \setminus K$, d.h. $[K(\alpha) : K] \neq 1$. Dann ist auf jeden Fall $K(\alpha) \subseteq L$ und somit

$$\ell = [L : K] = [L : K(\alpha)] \cdot \underbrace{[K(\alpha) : K]}_{\neq 1}$$

Folglich ist $[K(\alpha) : K] = \ell$ und somit $[L : K(\alpha)] = 1$, da ℓ prim ist. Damit ist $L = K(\alpha)$ für beliebiges $\alpha \in L \setminus K$. Nun gibt es genau $q^\ell - q$ Elemente in $L \setminus K$, die alle primitiv sind, d.h. die Anzahl der primitiven Elemente von $L|K$ ist genau $q^\ell - q$.

Betrachten wir nun die Menge $\mathcal{I}_\ell := \{f \in K[X]_{=\ell} : f \text{ irreduzibel}\}$ der irreduziblen Polynome vom Grad ℓ und die Menge $\mathcal{M}_\ell := \{f \in K[X]_{=\ell} : f = \text{MinPol}(\alpha | K) \text{ für ein } \alpha \in L\}$ der Minimalpolynome vom Grad ℓ über K . Diese sind irreduzibel und somit gilt $\mathcal{M}_\ell \subseteq \mathcal{I}_\ell$.

Wir zeigen nun, dass auch $\mathcal{I}_\ell^{\text{normiert}} = \mathcal{M}_\ell$ gilt. Sei $f \in \mathcal{I}_\ell^{\text{normiert}}$, d.h. f ist irreduzibel vom Grad ℓ und normiert. f hat eine Nullstelle α im algebraischen Abschluss \bar{K} . Dann können wir wieder $K(\alpha)|K$ betrachten. Da f irreduzibel und normiert ist, ist f das Minimalpolynom von α . Dann ist $[K(\alpha) : K] = \ell$. Da es nach Satz 3.7 nur genau eine Erweiterung von K mit Grad ℓ gibt, ist $L = K(\alpha)$, d.h. $\alpha \in L$, und damit $\mathcal{I}_\ell^{\text{normiert}} \subseteq \mathcal{M}_\ell$. Zusammen mit der Inklusion $\mathcal{M}_\ell \subseteq \mathcal{I}_\ell$ gilt dann $\mathcal{I}_\ell^{\text{normiert}} = \mathcal{M}_\ell$.

Nun hat jedes $f \in \mathcal{M}_\ell$ genau ℓ Nullstellen, d.h. es gibt zu jedem primitiven Element $\alpha \in L$ genau $\ell - 1$ Konjugierte bzw. haben ℓ primitive Elemente in L das gleiche Minimalpolynom. Damit müssen wir die Anzahl der primitiven Elemente einmal durch ℓ teilen und erhalten für die Anzahl der Minimalpolynome vom Grad ℓ genau

$$\#\mathcal{M}_\ell = \frac{q^\ell - q}{\ell}$$

Nun unterscheiden sich die Polynome in \mathcal{I}_ℓ und \mathcal{M}_ℓ lediglich um die Normierung. Machen wir die Normierung der Minimalpolynome rückgängig, so erhalten wir stets ein irreduzibles Polynom in \mathcal{I}_ℓ . Diese Umkehrung besteht aus der Multiplikation eines $f \in \mathcal{M}_\ell$ mit einem Element $c \in K^\times$, sodass $c \cdot f \in \mathcal{I}_\ell$. Somit ist $(q - 1) \cdot \#\mathcal{M}_\ell = \#\mathcal{I}_\ell$.

Somit ergibt sich schlussendlich

$$\#\mathcal{I}_\ell = \frac{(q^\ell - q)(q - 1)}{\ell}$$

für die Anzahl der irreduziblen Polynome $f \in K[X]$.

Hausaufgaben

Algebra & Zahlentheorie – Übungsblatt 7

Eric Kunze (Matr.-Nr. 4679202)

Ü-Gruppe: Freitag 2. DS

Thema: Galoistheorie, Kreisteilungskörper

Übung 101

Bestimmen Sie die Galoisgruppen der Polynome $f_1 = X^3 + X + 1$, $f_2 = X^3 - 2X - 1$, $f_3 = X^3 - 12X + 8$ und $f_4 = X^4 + 3X^2 + 2$ über \mathbb{Q} .

- Betrachten wir $f_1 = X^3 + X + 1$. Reduktion modulo 2 liefert ein Polynom $f_1^{\text{red}} = X^3 + X + 1 \in \mathbb{F}_2[X]$ und wegen $f(0) = 1$ sowie $f(1) = 1$ in \mathbb{F}_2 hat f_1^{red} keine Nullstellen in \mathbb{F}_2 . Daraus folgt die Irreduzibilität über \mathbb{F}_2 und mit dem Reduktionskriterium aus GEO schließlich auch selbige über \mathbb{Q} . Weiter gilt mit Ü98 für die Diskriminante $\text{discr}(f_1) = -4 - 27 = -31 \notin (\mathbb{Q}^\times)^2$. Somit gilt mit Beispiel 5.18 aus der Vorlesung, dass $\text{Gal}(f_1 | \mathbb{Q}) = S_3$.
- Das Polynom $f_2 = X^3 - 2X - 1$ hat die Nullstelle -1 und ist somit reduzibel. Für die Diskriminante gilt $\text{discr}(f) = -4 \cdot (-2)^3 - 27 = 5 \notin (\mathbb{Q}^\times)^2$. Somit ist wieder nach Beispiel 5.18 $\text{Gal}(f_2 | \mathbb{Q}) \cong C_2$.
- Wir betrachten das Polynom $f_3 = X^3 - 12X + 8$. Reduktion modulo 5 liefert das Polynom $f_3^{\text{red}} = X^3 + 3X + 3 \in \mathbb{F}_5[X]$. Dort lassen sich die Nullstellen schnell bestimmen, denn wegen

$$f_3^{\text{red}}(0) = 3$$

$$f_3^{\text{red}}(1) = 2$$

$$f_3^{\text{red}}(2) = 7 = 2$$

$$f_3^{\text{red}}(3) = 24 = 4$$

$$f_3^{\text{red}}(4) = 59 = 4$$

gibt es keine. Somit ist nach Reduktionskriterium dann auch f irreduzibel über \mathbb{Q} . Für die Diskriminante gilt wieder $\text{discr}(f) = -4 \cdot (-12)^3 - 27 \cdot 8^2 = 2^8 \cdot 3^3 - 3^3 \cdot 2^6 = 3^4 \cdot 2^6 \in (\mathbb{Q}^\times)^2$. Damit ist $\text{Gal}(f_3 | \mathbb{Q}) = A_3 \cong C_3$.

- Für das Polynom $f_4 = X^4 + 3X^2 + 2 = (X^2 + 2)(X^2 + 1)$ kann man die Nullstellen $\alpha_1 = i$, $\alpha_2 = -i$, $\alpha_3 = i\sqrt{2}$ und $\alpha_4 = -i\sqrt{2}$ erraten. Die Automorphismen des Zerfällungskörpers $L = \mathbb{Q}(i, \sqrt{2})$ sind auf \mathbb{Q} ohnehin die Identität und vertauschen auf L nur die beiden Nullstellenpaare $\alpha_1 \leftrightarrow \alpha_2$ und $\alpha_3 \leftrightarrow \alpha_4$. Damit lassen diese sich in Zykelschreibweise notieren als $\text{Gal}(f_4 | \mathbb{Q}) = \text{Aut}(L | \mathbb{Q}) = \{\text{id}, (1\ 2)(3\ 4), (1\ 2), (3\ 4)\}$. Damit ist $\text{Gal}(f_4 | \mathbb{Q}) = \langle (1\ 2), (3\ 4) \rangle \cong C_2 \times C_2 \cong V_4$.

Übung 102

Sei K vollkommen und $L|K$ algebraisch. Hat jedes $f \in K[X] \setminus K$ eine Nullstelle in L , so ist L ein algebraischer Abschluss von K .

Hinweis: Betrachten sie für $\alpha \in \bar{L}$ die normale Hülle M von $K(\alpha)|K$ und zeigen Sie, dass $M \subseteq L$ gilt.

Übung 103

Sei p eine ungerade Primzahl und $L = \mathbb{Q}(\zeta_p)$. Zeigen Sie: L enthält genau einen Teilkörper K der Form $K = \mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}$ kein Quadrat. Genau dann ist $K \subseteq \mathbb{R}$, wenn $p \equiv 1 \pmod{4}$.

Nach Korollar 6.9 ist $\mathbb{Q}(\zeta_p)|\mathbb{Q}$ galoissch mit $G := \text{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Damit ist $\#G = \#(\mathbb{Z}/p\mathbb{Z})^\times = p-1$. Da $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \cong C_{p-1}$ zyklisch und $p-1$ gerade ist (also $\frac{p-1}{2} \mid p-1$), gibt es genau eine Untergruppe $C_{\frac{p-1}{2}}$ mit $(C_{\frac{p-1}{2}} : C_{p-1}) = \frac{\#C_{p-1}}{\#C_{\frac{p-1}{2}}} = 2$. Nach Galois-Korrespondenz bleibt der Index erhalten, d.h. mit $K = L^{C_{\frac{p-1}{2}}}$ und $\mathbb{Q} = L^{C_{p-1}}$ ist $[K : \mathbb{Q}] = (C_{\frac{p-1}{2}} : C_{p-1}) = 2$. Nach Übung Ü20 ist nun $K = \mathbb{Q}(\sqrt{d})$ für ein $d \in \mathbb{Q}$. Dabei ist d kein Quadrat, da dann $\sqrt{d} \in \mathbb{Q}$ gelten würde und somit $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$, d.h. $[K : \mathbb{Q}] = 1$, was falsch ist. Nun müssen wir noch zeigen, dass auch $d \in \mathbb{Z}$ ist. Dazu sei d von der Form $d = \frac{a}{b}$ mit $a, b \in \mathbb{Z}$, $b \neq 0$ und $\text{ggT}(a, b) = 1$. Der Fall $a = 0$ ist klar. Wir wählen $d' = ab \in \mathbb{Z}$, dann ist zu zeigen, dass $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$.

- $\sqrt{ab} \in \mathbb{Q}(\sqrt{\frac{a}{b}})$: Mit $\sqrt{\frac{a}{b}} \in \mathbb{Q}(\sqrt{\frac{a}{b}})$ ist auch $\sqrt{\frac{b}{a}} = (\sqrt{\frac{a}{b}})^{-1} \in \mathbb{Q}(\sqrt{\frac{a}{b}})$. Wegen $a-b \in \mathbb{Q}$ ist dann

$$(a-b) \left(\sqrt{\frac{a}{b}} - \sqrt{\frac{b}{a}} \right)^{-1} = (a-b) \left(\frac{a-b}{\sqrt{ab}} \right)^{-1} = \sqrt{ab}$$

- $\sqrt{\frac{a}{b}} \in \mathbb{Q}(\sqrt{ab})$: Wegen $b \in \mathbb{Q}$ ist

$$\frac{\sqrt{ab}}{b} = \sqrt{\frac{ab}{b^2}} = \sqrt{\frac{a}{b}}$$

Somit ist $\mathbb{Q}(\sqrt{\frac{a}{b}}) = \mathbb{Q}(\sqrt{ab})$ und $K = \mathbb{Q}(\sqrt{d'})$ mit $d' \in \mathbb{Z}$ ein eindeutig bestimmter Zwischenkörper $\mathbb{Q} \subseteq K \subseteq L$.

Wir betrachten die komplexe Konjugation $\tau: \mathbb{C} \rightarrow \mathbb{C}$ mit $x+iy \mapsto x-iy$. Diese ist bekanntermaßen ein Automorphismus und wegen $\tau|_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}$ auch $\tau \in G$. Wegen $\tau \circ \tau = \text{id}_{\mathbb{C}}$ ist $\text{ord}(\tau) = 2$.

Sei nun $K \subseteq \mathbb{R}$. Dann ist $\tau|_K = \text{id}_K$, da auch $\tau|_{\mathbb{R}} = \text{id}_{\mathbb{R}}$. Somit ist $\tau \in K^\circ = C_{\frac{p-1}{2}}$. Wegen $\text{ord}(\tau) = 2$ gilt $2 \mid \#C_{\frac{p-1}{2}} = \frac{p-1}{2}$ und damit $4 \mid p-1$, was gerade $p \equiv 1 \pmod{4}$ entspricht.

Gelte $p \equiv 1 \pmod{4}$. Dann ist $4 \mid p-1$, also existiert eine eindeutig bestimmte Untergruppe $C_{\frac{p-1}{4}}$. Da $\text{ord}(\tau) = 2$ und es in C_{p-1} nur $\phi(2) = 1$ Element der Ordnung zwei gibt, muss schon $\tau|_K = \text{id}_K$ und daher $K \subseteq \mathbb{R}$ gelten.