Eberhard-Karls-Universität Tübingen
Prof. Hannah Markwig
Alheydis Geiger

Sommersemester 2020
24. Juni 2020

Algebra
Lösung Übungsblatt 9

Aufgabe 1 (4+4 Punkte).
Bestimmen Sie den Zerfällungskörper L sowie den Grad $[L:\mathbb{Q}]$ für folgende Polynome:

a) **Gesucht:** Der Zerfällungskörper L von X^6-1 und $[L:\mathbb{Q}]$.

Lösung: Nach 4.2.2 ist der Zerfällungskörper eines Polynoms die Körpererweiterung, die durch seine Nullstellen erzeugt wird. Zuerst bestimmen wir also alle Nullstellen von X^6-1. Polynomdivision liefert uns:

$$X^6-1=(X-1)(X+1)(X^4+X^2+1)$$

Wir können X^4+X^2+1 zerlegen in:

$$X^4+X^2+1=(X^2+X+1)(X^2-X+1)$$

Wir berechnen die Nullstellen von X^2+X+1 und X^2-X+1:

$$\begin{aligned}X^2+X+1=0 \Leftrightarrow X_{1/2}&=-\frac{1}{2}\pm\sqrt{\frac{1}{4}-1}=-\frac{1}{2}\pm\frac{1}{2}i\sqrt{3}\\&=e^{\frac{4\pi i}{3}},e^{\frac{2\pi i}{3}}\\X^2-X+1=0 \Leftrightarrow X_{1/2}&=\frac{1}{2}\pm\sqrt{\frac{1}{4}-1}=\frac{1}{2}\pm\frac{1}{2}i\sqrt{3}\\&=e^{\frac{\pi i}{3}},e^{\frac{5\pi i}{3}}\end{aligned}$$

Sei $w:=e^{\frac{\pi i}{3}}$. Dann folgt (da $w^3=-1$):

$$X^6-1=(X-1)(X-w)(X-w^2)(X-w^3)(X-w^4)(X-w^5)$$

Damit ist $L:=\mathbb{Q}(w)$ der Zerfällungskörper.
Da $w\notin\mathbb{Q}$ und w von X^2-X+1 annulliert wird, ist $[L:\mathbb{Q}]=2$. (Gäbe es einen kleineren Körper über dem X^6-1 zerfällt, so wäre er $\mathbb{Q}$, und darüber ist X^2-X+1 irreduzibel).

b) **Gesucht:** Der Zerfällungskörper L von X^6+1 und $[L:\mathbb{Q}]$.

Lösung: Nach 4.2.2 ist der Zerfällungskörper eines Polynoms die Körpererweiterung, die durch seine Nullstellen erzeugt wird. Zuerst bestimmen wir also alle Nullstellen von X^6+1. Wir sehen, dass $\pm i$ Nullstelle von X^6-1 ist. Polynomdivision liefert uns:

$$X^6+1=(X-i)(X+i)(X^4-X^2+1)$$

Wir können X^4-X^2+1 zerlegen in:

$$X^4-X^2+1=(X^2+iX-1)(X^2-iX-1)$$

Wir berechnen die Nullstellen von X^2+iX-1 und X^2-iX-1:

$$\begin{aligned}X^2+iX-1=0 \Leftrightarrow X_{1/2}&=-\frac{i}{2}\pm\sqrt{\frac{-1}{4}+1}=-\frac{i}{2}\pm\frac{1}{2}\sqrt{3}\\&=ie^{\frac{4\pi i}{3}},ie^{\frac{2\pi i}{3}}\\&=e^{\frac{11\pi i}{6}},e^{\frac{7\pi i}{6}}\\X^2-iX-1=0 \Leftrightarrow X_{1/2}&=\frac{i}{2}\pm\sqrt{\frac{-1}{4}+1}=\frac{i}{2}\pm\frac{1}{2}\sqrt{3}\\&=ie^{\frac{\pi i}{3}},ie^{\frac{5\pi i}{3}}\\&=e^{\frac{5\pi i}{6}},e^{\frac{\pi i}{6}}\end{aligned}$$

Eberhard-Karls-Universität Tübingen
Prof. Hannah Markwig
Alheydis Geiger

Sommersemester 2020
24. Juni 2020

Algebra
Lösung Übungsblatt 9

Mit $w := e^{\frac{\pi i}{6}}$ gilt: Die Nullstellen von X^6+1 sind $w, w^3, w^5, w^7, w^9, w^{11}$ (da $w^3 = i, w^9 = -i$). Also

$$X^6 + 1 = (X-w)(X-w^3)(X-w^5)(X-w^7)(X-w^9)(X-w^{11})$$

Es ist $\mathbb{Q}(w)$ der Zerfällungskörper von X^6+1 und $[\mathbb{Q}(w):\mathbb{Q}] = 4$, **denn**: w wird von $X^4+X^2+1 \in \mathbb{Q}[X]$ annuliert, und dieses Polynom ist irreduzibel über $\mathbb{Q}$, was wir daran sehen, das wir die Nullstellen kennen und damit sehen, dass es keine Zerlegung in zwei Polynome vom Grad 2 über $\mathbb{Q}$ gibt (Für einen Faktor vom Grad 2 ist der Koeffizient von X immer die Summe zweier Nullstellen: $e^{\frac{i\pi}{6}} + e^{\frac{5i\pi}{6}} = i \notin \mathbb{Q}$, $e^{\frac{i\pi}{6}} + e^{\frac{11i\pi}{6}} = \sqrt{3} \notin \mathbb{Q}$, als letztes bleibt $e^{\frac{i\pi}{6}} + e^{\frac{7i\pi}{6}} = 0 \in \mathbb{Q}$ aber hier ist der konstante Koeffizient das Produkt der Nullstellen: $e^{\frac{i\pi}{6}} \cdot e^{\frac{7i\pi}{6}} = e^{\frac{4\pi i}{3}} \notin \mathbb{Q}$). Damit ist X^4+X^2+1 das Minimalpolynom von w über $\mathbb{Q}$ und es folgt die Behauptung. □

Aufgabe 2 (6 Punkte).
Vor: Sei L/K eine Körpererweiterung mit $[L:K] = 2$, $\mathrm{char}(K) \neq 2$.

Beh: L ist eine Quadratwurzelerweiterung der Form $L = K(a)$ von K (eine einfache Quadratwurzelerweiterung).

Bew: Wähle $\alpha \in L \setminus K$. Se $m_\alpha \in K[X]$ das Minimalpolynom von α über K. Da $\alpha \notin K$ ist $\deg(m_\alpha) \geq 2$.
$\Rightarrow 2 = [L:K] \geq [K(\alpha):K] = \deg(m_\alpha) \geq 2$
$\Rightarrow L = K(\alpha)$
Wir müssen zeigen, dass diese Körpererweiterung von einem Quadratwurzelausdruck erzeugt wird.
Dazu betrachten wir die Nullstellen von m_α die ja die Körpererweiterung erzeugen. Wir können m_α schreiben als

$$m_\alpha(X) = X^2 + pX + q$$

mit $p, q \in K$. Die Nullstellen von m_α sind

$$-\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}.$$

Sei ohne Einschränkung $\alpha = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}$. Setze $b := \sqrt{\frac{p^2}{4} - q}$. Dann gilt $b \notin K$ (da sonst insbesondere $\alpha \in K$, Widerspruch) und $b^2 \in K$.
Zudem können wir α schreiben als: $\alpha = b - \frac{p}{2}$ und b schreiben als $b = \alpha + \frac{p}{2}$.
Es gilt also $b \in K(\alpha)$ und $\alpha \in K(b)$.
$\Rightarrow K(b) = K(\alpha) = L$.
$\Rightarrow L$ ist eine einfache Quadratwurzelerweiterung. □

Aufgabe 3 (6 Punkte).
Vor: Sei L/K eine Körpererweiterung vom Grad m ($L \subset \mathbb{C}$), $f \in K[X]$ ein irreduzibles Polynom vom Grad $\deg(f) = n$ und $\mathrm{ggT}(m,n) = 1$.

Beh: $f \in L[X]$ irreduzibel.

Beweis: Sei α eine Nullstelle von f in $\mathbb{C}$. Wir betrachten die Körpererweiterung $L(\alpha)$:

$$\begin{aligned}[L(\alpha):K] &= [L(\alpha):K(\alpha)] \cdot [K(\alpha):K] \\ &= [L(\alpha):L] \cdot [L:K]\end{aligned}$$

Da $f \in K[X]$ irreduzibel ist und $f(\alpha) = 0$ folgt: $[K(\alpha):K] = \deg(f) = n$.
$\Rightarrow n | [L(\alpha):L] \cdot [L:K]$
$\Rightarrow n | [L(\alpha):L] \cdot m$
$\Rightarrow n | [L(\alpha):L]$ (da $\mathrm{ggT}(n,m) = 1$.
Das Minimalpolynom $m_\alpha \in L[X]$ von α über L muss in $L[X]$ das Polynom f teilen, da $f(\alpha) = 0$. Es folgt also $n = \deg(f) \geq \deg(m_\alpha) = [L(\alpha):L]$. Da $n | [L(\alpha):L]$ folgt dann aber schon $n = [L(\alpha):L]$.

Eberhard-Karls-Universität Tübingen
Prof. Hannah Markwig
Alheydis Geiger

Sommersemester 2020
24. Juni 2020

Algebra
Lösung Übungsblatt 9

$\Rightarrow$ Es gibt kein Polynom über L vom Grad $< n$ das α annulliert.
$\Rightarrow$ f ist Minimalpolynom von α über L
$\Rightarrow$ f ist irreduzibel über L $\square$

Aufgabe 4 (3+4+3+1 Punkte).
Vor: Es sei K ein Körper.

a) **Beh:** Polynome vom Grad 2 und 3 in $K[X]$ sind genau dann irreduzibel, wenn sie keine Nullstelle in K haben.

Bew: Ein Element $f \in K[X]$ heißt irreduzibel, falls für $f = g \cdot h$ gilt $g \in K[X]^\times = K \setminus \{0\}$ oder $h \in K[X]^\times = K \setminus \{0\}$.
D.h. f ist irreduzibel $\Leftrightarrow$ f lässt sich nicht als Produkt von zwei Polynomen g und h darstellen, sodass $\deg(g) \geq 1$ und $\deg(h) \geq 1$.

Wir kennen die Gradformel für Polynome $g, h \in K[X]$: $\deg(g \cdot h) = \deg(g) + \deg(h)$.

Mögliche Zerlegungen von Grad 2 und 3:

$\deg(f) = \deg(g \cdot h)$	$\deg(g)$	$\deg(h)$
2	2	0
	1	1
	0	2
3	3	0
	2	1
	1	2
	0	3

Sei $f \in K[X]$ mit $\deg(f) = 2$ reduzibel, dann gibt es Polynome $g, h \in K[X] \setminus K^\times$, sodass $f = g \cdot h$. Da g, h keine Einheiten, haben sie beide Grad 1 (siehe Tabelle).
Ein Polynom von Grad 1 über K hat eine Nullstelle in K, d.h. f hat eine Nullstelle über K.
Sei umgekehrt f vom Grad 2 irreduzibeel über K, so kann f nach obigem Argument keine Nullstellen haben (da es sonst als Produkt von zwei Grad 1 Polynomen geschrieben werden könnte und damit über K reduzibel wäre).

Ist f vom Grad 3 über K reduzibel, so gibt es zwei Polynome g, h beide von Grad mindestens 1, sodass $3 = \deg(f) = \deg(g \cdot h) = \deg(g) + \deg(h)$.
Wir sehen, an der Tabelle, dass eines der Polynome Grad 1 haben muss und damit f eine Nullstelle über K hat. Umgekehrt folgt damit auch, dass falls f irreduzibel ist, f keine Nullstellen haben kann, da es sonst zerlegt werden könnte. $\square$

Beachte: Für Polynome vom Grad ≥ 4 ist die Behauptung nicht mehr richtig, siehe Aufgabe 1 d).
Die Aussage ist außerdem für einen Polynomring $R[X]$ über einem Ring R, der kein Körper ist, nicht mehr richtig. Bsp: $R = \mathbb{Z}$ und $f = 3X$. Dann ist f vom Grad 1 mit Nullstelle über $\mathbb{Z}$ aber reduzibel, da 3 und X beides keine Einheiten in $\mathbb{Z}[X]$ sind. ($\mathbb{Z}[X]^\times = \{\pm 1\}$)

b) **Frage:** Sind die Polynome $X^2 + X + 1$, $X^3 + X^2 + 1$, $X^3 + X^2 + X + 1$ und $X^4 + X^3 + X + 1$ über $\mathbb{Z}_2[X]$ irreduzibel? Bestimmen Sie ggf. ihre Zerlegung in irreduzible Polynome.

Lösung: Es ist $\mathbb{Z}_2$ ein Körper, d.h. wir können wir die Polynome $X^2 + X + 1$, $X^3 + X^2 + 1$, $X^3 + X^2 + X + 1$ Aufgabe 1a) anwenden. Falls wir für $X^4 + X^3 + X + 1$ eine Nullstelle über $\mathbb{Z}_2$ finden, können wir ebenfalls so verfahren, ansonsten müssen wir eine Zerlegung in zwei Grad 2 Polynome finden.

- $f_1 := X^2 + X + 1$ ist irreduzibel, da es über $\mathbb{Z}_2$ keine Nullstelle hat: $f_1(0) = 1, f_1(1) = 1$.
- $f_2 := X^3 + X^2 + 1$ ist irreduzibel, da es über $\mathbb{Z}_2$ keine Nullstelle hat: $f_2(0) = 1, f_2(1) = 1$.

Eberhard-Karls-Universität Tübingen
Prof. Hannah Markwig
Alheydis Geiger

Sommersemester 2020
24. Juni 2020

Algebra
Lösung Übungsblatt 9

- $f_3 := X^3 + X^2 + X + 1$ ist reduzibel, da es über $\mathbb{Z}_2$ eine Nullstelle hat: $f_3(0) = 1, f_3(1) = 0$.
  Wir suchen eine Zerlegung von f_3 in irreduzible Polynome. Da 1 eine Nullstelle von f_3 ist, wissen wir, dass $X - 1 = X + 1 \in \mathbb{Z}_2[X]$ ein irreduzibler Teiler von f_3 ist. Mit Polynomdivision folgt:

  $$f_3 = X^3 + X^2 + X + 1 = (X + 1) \cdot (X^2 + 1)$$

  Es hat X^2+1 eine Nullstelle in $\mathbb{Z}_2$, nämlich 1, daher können wir es weiter zerlegen: $X^2+1 = (X+1)\cdot(X+1)$. Insgesamt folgt:

  $$f_3 = X^3 + X^2 + X + 1 = (X + 1) \cdot (X + 1) \cdot (X + 1).$$

- $f_4 := X^4 + X^3 + X + 1$ hat mit $f_4(1) = 0$ eine Nullstelle über $\mathbb{Z}_2$, d.h. wir können einen Linearfaktor $X + 1$ abspalten - das Polyom ist also reduzibel.

  $$f_4 := X^4 + X^3 + X + 1 = (X + 1) \cdot (X^3 + 1)$$

  Da $X^3 + 1$ immer noch eine Nullstelle über $\mathbb{Z}_2$ hat, können wir es weiter zerlegen: $X^3 + 1 = (X + 1) \cdot (X^2 + X + 1)$. Dies ist nun eine Zerlegung in irreduzible Polynome. Wir haben also:

  $$f_4 := X^4 + X^3 + X + 1 = (X + 1) \cdot (X + 1) \cdot (X^2 + X + 1)$$

c) **Beh:** $f := X^5 + 2X^3 + 2$ ist irreduzibel über $\mathbb{Z}[X]$ und über $\mathbb{Q}[X]$.

Bew: Da $\mathbb{Z}$ ein faktorieller Ring ist, können wir das das Eisensteinkriterium (Satz 4.3.9) verwenden. Dazu müssen wir zeigen, dass f primitiv ist, d.h. ggT$(a_0, ..., a_5) = 1$. f hat die Koeffizienten: $a_5 = 1, a_4 = 0, a_3 = 2, a_2 = 0, a_1 = 0, a_0 = 2$.
Damit folgt ggT$(a_0, ..., a_5) =$ ggT$(1, 2) = 1$, also ist f primitiv.
Wir wählen $p = 2$ als Primzahl für das Eisensteinkriterium und sehen, dass $p|a_i$ für $i = 0, ..., 4$ und zudem dass für $p^2 = 4$ gilt $p^2 \nmid a_0$.
Nach Eisenstein ist also f irreduzibel über $\mathbb{Z}[X]$.

Nach Satz 4.3.10 impliziert f irreduzibel über $\mathbb{Z}[X]$, dass f irreduzibel ist über Quot$(\mathbb{Z})[X] = \mathbb{Q}[X]$. □

d) **Beh:** $X^4 + 2X^2 + 1$ ist ein Polynom in $\mathbb{R}[X]$ von Grad 4, dass keine Nullstellen in $\mathbb{R}$ hat, aber reduzibel ist.

Bew: Es ist deg$(X^4 + 2X^2 + 1) = 4$ und $X^4 + 2X^2 + 1 = (X^2 + 1)^2$ also ist das Polynom reduzibel vom Grad 4.
Zudem hat $X^2 + 1$ keine Nullstelle über $\mathbb{R}$, also hat auch $X^4 + 2X^2 + 1 = (X^2 + 1)^2$ keine Nullstelle über $\mathbb{R}$, wie behauptet. □

Zusatzaufgabe 5 (4 Zusatzpunkte).
Vor. Sei $K := \mathbb{Q}(\sqrt[3]{\sqrt{5}+2} - \sqrt[3]{\sqrt{5}-2})$.

Beh. $[K : \mathbf{Q}] = 1$.

Bew: Wir bestimmen zu erst ein Polynom, welches $\alpha := \sqrt[3]{\sqrt{5}+2} - \sqrt[3]{\sqrt{5}-2}$ annuliert. Dafür rechnen wir:

$$\begin{aligned}
\alpha^3 &= \sqrt{5} + 2 - 3((\sqrt[3]{\sqrt{5}+2})^2 \sqrt[3]{\sqrt{5}-2}) + 3((\sqrt[3]{\sqrt{5}+2})(\sqrt[3]{\sqrt{5}-2})^2) - (\sqrt{5}-2) \\
&= 4 - 3(\sqrt[3]{(\sqrt{5}+2)^2(\sqrt{5}-2)}) + 3(\sqrt[3]{(\sqrt{5}+2)(\sqrt{5}-2)^2}) \\
&= 4 - 3(\sqrt{5}+2) + 3(\sqrt{5}-2) \\
&= 4 - 3\alpha
\end{aligned}$$

(Nebenrechnung: $(\sqrt{5}+2)(\sqrt{5}-2) = 5 - 4 = 1$)

Eberhard-Karls-Universität Tübingen
Prof. Hannah Markwig
Alheydis Geiger

Sommersemester 2020
24. Juni 2020

Algebra
Lösung Übungsblatt 9

Damit folgt also $\alpha^3 = 4 - 3\alpha$, also insbesondere $\alpha^3 + 3\alpha - 4 = 0$. D.h. $g := x^3 + 3x - 4$ ist ein Polynom, welches α annuliert.
Das Minimalpolynom von α muss nun g teilen.
Es ist $g = (x-1)(x^2+x+4)$. Das Polynom x^2+x+4 hat nur komplexe Nullstellen, aber α ist nicht komplex. (Alternativ: setze α in x^2+x+4 ein, es kommt nicht Null heraus).
Daraus folgt, dass $x-1$ das Minimalpolynom von α ist.
$\Rightarrow \alpha = 1$
$\Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}$ also $[K : \mathbb{Q}] = 1$. □