LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Werner Bley
Martin Hofer

Wintersemester 2018/19
1. Februar 2019

Algebra – Lösungsskizzen zu Übungsblatt 12

Aufgabe 1 (8 Punkte).

a) Sei $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ und somit $f' = \sum_{i=1}^{n} i a_i X^{i-1}$. Wir haben bereits gezeigt, dass ein Polynom genau dann separabel ist, wenn $f' \neq 0$ gilt. Wenn also $f \in K[X^p]$ gilt, folgt sofort dass $f' = 0$ ist, also ist f nicht separabel. Andererseits, sei f nicht separabel und somit $f' = 0$, dann gilt für alle $i \in \{1, \ldots, n\}$ mit $a_i \neq 0 \in \mathbb{F}_p$ dass $p \mid i$, also muss $f \in K[X^p]$ gelten.

b) Sei K vollkommen. Für gegebenes $\alpha \in K$ sei E Zerfällungskörper des Polynoms $f = X^p - \alpha$ über K. In E besitzt f eine Nullstelle, d.h. es gibt ein $\beta \in E^p$ mit $\beta^p = \alpha$. Da die Abbildung $x \mapsto x^p$ von E in sich als Homomorphismus von Körpern injektiv ist, besitzt f in E nur die eine Nullstelle β. Es folgt $f = (X - \beta)^p$. Sei $g = \mathrm{Mipo}_K(\beta)$. Nach Voraussetzung ist g separabel. Als Teiler von f kann dann g nur die Gestalt $g = X - \beta$ besitzen, also ist $\beta \in K$.

   Sei umgekehrt $K = K^p$ vorausgesetzt. Wir nehmen an, es gebe ein irreduzibles Polynom $f \in K[X]$ welches nicht separabel ist. Nach Teilaufgabe a) hat dieses die Gestalt $f(X) = g(X^p)$ mit $g \in K[X]$. Wegen $K = K^p$ gilt, $g(X) = \sum b_i^p X^i$ mit $b_i \in K$. Es folgt $f(X) = g(X^p) = \sum b_i^p X^{pi} = \left(\sum b_i X^i\right)^p$.

c) Man sieht schnell das in einem endlichen Körper der Charakteristik $p > 0$ gilt $K = K^p$. Dann können wir die Aussage aus Teilaufgabe b) folgern.

Aufgabe 2 (12 Punkte).

a) Die Nullstellen von f berechnen sich (mittels Substitution und Mitternachtsformel) zu

$$\sqrt{a + \sqrt{a^2 - b}}, \quad -\sqrt{a + \sqrt{a^2 - b}}, \quad \sqrt{a - \sqrt{a^2 - b}}, \quad -\sqrt{a - \sqrt{a^2 - b}}.$$

   Sei $\xi = \sqrt{a + \sqrt{a^2 - b}}$ und $\omega = \sqrt{a - \sqrt{a^2 - b}}$, dann ist f sowohl das Minimalpolynom von ξ als auch von ω, da f nach Voraussetzung irreduzibel ist. Es folgt

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = 4 \quad \text{und} \quad [\mathbb{Q}(\omega) : \mathbb{Q}] = 4.$$

   Wegen $\omega, \xi \in L$ ist $\mathbb{Q}(\xi) \subseteq L$ und $\mathbb{Q}(\omega) \subseteq L$. Zusammen mit $[L : \mathbb{Q}] = 4$ und obigen Erweiterungsgraden liefert die Gradformel $[L : \mathbb{Q}(\xi)] = 1 = [L : \mathbb{Q}(\omega)]$, d. h. $L = \mathbb{Q}(\xi) = \mathbb{Q}(\omega)$.

   Wegen $\xi^2 - a = \sqrt{a^2 - b} \in L$ ist auf jeden Fall $K \subseteq L$. Weiter ist

$$\xi^2 \omega^2 = (a + \sqrt{a^2 - b})(a - \sqrt{a^2 - b}) = a^2 - (a^2 - b) = b,$$

sodass $\xi\omega = \pm\sqrt{b}$ in L liegt. Um $\sqrt{b} \in K$ zu zeigen, zeigen wir, dass jedes $\sigma \in G(L/K)$ auch $\sqrt{b}$ fixiert. Sei also $\sigma \in G(L/K)$, d. h. es gelte $\sigma(\sqrt{a^2-b}) = \sqrt{a^2-b}$. Dann folgt

$$\sigma(\xi)^2 = \sigma(\xi^2) = \sigma(a + \sqrt{a^2-b}) = a + \sqrt{a^2-b} = \xi^2$$

und analog

$$\sigma(\omega)^2 = \sigma(\omega^2) = \sigma(a - \sqrt{a^2-b}) = a - \sqrt{a^2-b} = \omega^2.$$

Also ist $\sigma(\xi) = \pm\xi$. und $\sigma(\omega) = \pm\omega$. Da ξ die Erweiterung $L|\mathbb{Q}$ erzeugt, ist σ durch Angabe von $\sigma(\xi)$ bereits eindeutig festgelegt, sprich: Ist $\sigma(\xi) = \xi$, so ist $\sigma = \mathrm{id}_L$. Ist andererseits $\sigma(\xi) = -\xi$, so kann nicht $\sigma(\omega) = \omega$ gelten, denn ω erzeugt ebenfalls die Erweiterung $L|\mathbb{Q}$, sodass aus $\sigma(\omega) = \omega$ ebenfalls $\sigma = \mathrm{id}_L$ folgen würde. Es muss daher $\sigma(\omega) = -\omega$ sein. In beiden Fällen folgt

$$\sigma(\sqrt{b}) = \sigma(\pm\xi\omega) = \pm\sigma(\xi)\sigma(\omega) = \pm\xi\omega = \sqrt{b}.$$

Also liegt $\sqrt{b}$ im Fixkörper $L^{G(L/K)} = K$.

Gilt $\sqrt{b} \in K$, so ist

$$\xi\omega = \pm\sqrt{b} \iff \omega = \pm\sqrt{b}\xi^{-1} \quad \in \mathbb{Q}(\xi).$$

Also wird auch in diesem Fall L bereits von ξ allein erzeugt und es gilt $[L : \mathbb{Q}] = [\mathbb{Q}(\xi) : \mathbb{Q}] = \mathrm{grad} f = 4$.

b) Sei $\sigma \in G(L/\mathbb{Q})$. Wir zeigen $\sigma^2 = \mathrm{id}_L$, denn das bedeutet, dass jedes Element in $G(L/\mathbb{Q})$ höchstens Ordnung 2 hat. Da wir in Teil a) bereits gesehen haben, dass

$$|G(L/\mathbb{Q})| = [L : \mathbb{Q}] = 4$$

beträgt und es nur zwei Gruppen der Ordnung 4, nämlich $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, gibt, muss dann $G(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sein.
Da σ eine Nullstelle von f wieder auf eine Nullstelle abbilden muss, ist $\sigma(\xi) \in \{\xi, -\xi, \omega, -\omega\}$. Durch Angabe von $\sigma(\xi)$ wird σ bereits eindeutig festgelegt, also folgt aus $\sigma(\xi) = \xi$ und $\sigma(\xi) = -\xi$ jeweils, dass $\sigma^2 = \mathrm{id}_L$ erfüllt ist.
Nach Voraussetzung ist $\sqrt{b} \in \mathbb{Q}$, also ist $\sigma(\sqrt{b}) = \sqrt{b}$ und es folgt

$$\omega\xi = \pm\sqrt{b} = \sigma(\pm\sqrt{b}) = \sigma(\omega\xi) = \sigma(\omega)\sigma(\xi)$$

Falls $\sigma(\xi) = \omega$, so muss also $\sigma(\omega) = \xi$ sein, sodass

$$\sigma^2(\xi) = \sigma(\omega) = \xi \quad \Rightarrow \quad \sigma^2 = \mathrm{id}_L\,.$$

Vollkommen analog folgt aus $\sigma(\xi) = -\omega$, dass $\sigma(\omega) = -\xi$ und

$$\sigma^2(\xi) = \sigma(-\omega) = -\sigma(\omega) = \xi \quad \Rightarrow \quad \sigma^2 = \mathrm{id}_L\,.$$

Es gibt daher kein Element der Ordnung 4 in $G(L/\mathbb{Q})$, weshalb diese nicht zyklisch sein kann.

c) Falls $\sqrt{b} \notin \mathbb{Q}$, so muss es ein $\sigma \in G(L/\mathbb{Q})$ geben mit $\sigma(\sqrt{b}) \neq \sqrt{b}$. Wir haben bereits gesehen, dass sowohl aus $\sigma(\xi) = \xi$ als auch aus $\sigma(\xi) = -\xi$ folgt, dass $\sigma(\sqrt{b}) = \sqrt{b}$. Die verbleibenden Möglichkeiten für $\sigma(\xi)$ sind $\pm\omega$. Sei also $\varepsilon \in \{+1, -1\}$ mit $\sigma(\xi) = \varepsilon\omega$. Dann folgt aus

$$\xi\omega = \pm\sqrt{b} \neq \sigma(\pm\sqrt{b}) = \sigma(\xi)\sigma(\omega) = \varepsilon\omega\sigma(\omega),$$

dass $\sigma(\omega) \neq \varepsilon\xi$. Andererseits ist $\sigma(\omega) \neq \omega$ und $\sigma(\omega) \neq -\omega$, denn da auch ω die Erweiterung $L|\mathbb{Q}$ erzeugt, würde sonst wie in Teil a) $\sigma(\xi) = \xi$ bzw. $\sigma(\xi) = -\xi$ folgen. Es bleibt also nur noch $\sigma(\omega) = -\varepsilon\xi$. Dies bedeutet

$$\sigma(\xi) = \varepsilon\omega, \quad \sigma^2(\xi) = -\varepsilon^2\xi = -\xi, \quad \sigma^3(\xi) = -\varepsilon\omega, \quad \sigma^4(\xi) = \varepsilon^2\xi = \xi$$

und somit beträgt die Ordnung von σ vier. Da dies der Gruppenordnung von $G(L/\mathbb{Q})$ entspricht, ist σ ein Erzeuger von $G(L/\mathbb{Q})$ und es folgt $G(L/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.

d) Die Inklusion $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ ist klar. Für die umgekehrte Inklusion bemerken wir, dass

$$\tfrac{1}{2}[(\sqrt{2}+\sqrt{3})^2 - 5] = \tfrac{1}{2}[(2+2\sqrt{6}+3) - 5] = \sqrt{6} \quad \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$$

und somit

$$\sqrt{6}\cdot(\sqrt{2}+\sqrt{3}) - 2(\sqrt{2}+\sqrt{3}) = 2\sqrt{3}+3\sqrt{2}-2(\sqrt{2}+\sqrt{3}) = \sqrt{2} \quad \in \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

Es folgt $\sqrt{3} = (\sqrt{2}+\sqrt{3}) - \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Dies zeigt $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$, insgesamt also Gleichheit.

e) Sei $\alpha = \sqrt{2}+\sqrt{3}$. Wir berechnen das Minimalpolynom von α:

$$\begin{aligned}\alpha^2 = 2+2\sqrt{6}+3 \Rightarrow (\alpha^2-5)^2 = 4\cdot 6 &\iff \alpha^4 - 10\alpha^2 + 25 = 24\\ &\iff \alpha^4 - 10\alpha^2 + 1 = 0\end{aligned}$$

Also ist $f = X^4 - 10X^2 + 1$ zumindest ein normiertes Polynom mit Nullstelle α. Um zu zeigen, dass f das Minimalpolynom von α ist, weisen wir $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4 = \operatorname{grad} f$ nach. Die Abschätzung „$\leq$“ folgt daraus, dass das Minimalpolynom von α ein Teiler von f ist, also höchstens Grad 4 hat. Unter Verwendung von Teil d) gilt

$$\mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\alpha) \quad \text{und} \quad \mathbb{Q}(\sqrt{3}) \subsetneq \mathbb{Q}(\alpha).$$

Da $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{3})$ quadratische Erweiterungen von $\mathbb{Q}$ sind, ist $[\mathbb{Q}(\alpha):\mathbb{Q}] > 2$. Außerdem ist $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ nach der Gradformel sogar ein Teiler von $[\mathbb{Q}(\alpha):\mathbb{Q}]$. Dies zeigt $[\mathbb{Q}(\alpha):\mathbb{Q}] \geq 4$. Somit ist f tatsächlich das Minimalpolynom von α.
Zu zeigen bleibt, dass $\mathbb{Q}(\sqrt{2},\sqrt{3})$ der Zerfällungskörper von f ist. Es ist $\mathbb{Q}(\sqrt{2},\sqrt{3})$ auf jeden Fall der Zerfällungskörper von $(X^2-2)(X^3-2)$, also ist die Erweiterung $\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q}$ normal. Da f eine Nullstelle in $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ besitzt, müssen dort schon alle Nullstellen liegen. Daraus folgt bereits, dass $\mathbb{Q}(\sqrt{2},\sqrt{3})$ der Zerfällungskörper von f über $\mathbb{Q}$ ist.

Es sind nun alle Voraussetzungen von Teil a) erfüllt. Wegen $\sqrt{1} = 1 \in \mathbb{Q}$, folgt also aus Teil b), dass $G(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Aufgabe 3 (4 Punkte).
Sei E/K eine endliche galoissche Körpererweiterung und C der algebraische Abschluss von E. Da E/K separabel ist gilt $[E : K] = [E : K]_s = |G(E/K, C/K)|$. Weil E/K normal ist, können wir $G(E/K, C/K)$ mit $G(E/K)$ identifizieren. Also gilt insgesamt $[E : K] = |G(E/K)|$.
Sei nun E/K eine endliche Körpererweiterung mit $[E : K] = |G(E/K)|$ und C der algebraische Abschluss von E. Die Bedingung $[E : K] = |G(E/K)|$ impliziert aber, dass für jeden Homomorphismus $\sigma : E/K \to C/K$ gilt $\sigma(E) = E$ und für diese Bedingung haben wir wiederum gezeigt, das sie die Normalität der Erweiterung impliziert. Ebenso liefert uns der Fortsetzungssatz für die $[E : K]$ Homomorphismen $\sigma : E/K \to E/K$ wiederum $[E : K]$ verschiedene Homomorphismen $\sigma' : E/K \to C/K$ mit $\sigma(E) = E$ und somit folgt $[E : K]_s = [E : K]$. Aus der Vorlesung wissen wir nun, dass das die Separabilität der Erweiterung impliziert, also ist die Erweiterung E/K insgesamt galoissch.

Aufgabe 4 (4 Punkte).
Sei L/K eine endliche Körpererweiterung vom Grad n, C der algebraische Abschluss von K und sei $\alpha \in L$. Wir nehmen an, dass gilt: $L = K(\alpha)$ und L/K separabel. Aus $K(\alpha)/K$ separabel folgt dass α separabel ist über K, das heißt das Minimalpolynom $\mathrm{Mipo}_K(\alpha)$ hat n verschiedenen Nullstellen. Wir wissen aber auch, das ein β genau dann eine Nullstelle von $\mathrm{Mipo}_K(\alpha)$ ist, wenn β konjugiert ist zu α in C. Also gibt es genau n paarweise verschiedene Konjugierte zu α.
Wir nehmen nun an es gibt n verschiedene Konjugierte von α. Wie oben wissen wir aber, dass somit das Minimalpolynom $\mathrm{Mipo}_K(\alpha)$ n verschiedene Nullstellen hat. Somit gilt mit einem Satz der Vorlesung $[K(\alpha) : K]_s = n$. Wegen $n = [K(\alpha) : K]_s \leq [K(\alpha) : K] \leq [L : K] = n$ muss gelten, $[K(\alpha) : K] = n$. Da zudem $K(\alpha) \subseteq L$ wegen $\alpha \in L$ gilt, folgt $L = K(\alpha)$. Somit folgt aber sofort $[L : K]_s = [L : K]$ und mit einem Satz aus der Vorlesung ist L/K auch separabel.