Algebra I

Musterlösung 19

Galoisgruppen und Repetitionsaufgaben

---

110. Sei α algebraisch über K und sei $\varphi\colon K \to L'$ ein Körperhomomorphismus. Dann gibt es höchstens $[K(\alpha) : K]$ verschiedene Körperhomomorphismen $\tilde{\varphi} : K(\alpha) \to L'$ mit $\tilde{\varphi}|_K = \varphi$.

Lösung: Sei $f = \sum_{i=0}^{n} a_i X^n$ das Minimalpolynom von α über K. Sei $\tilde{\varphi}$ wie in der Aufgabenstellung. Es gilt $[K(\alpha) : K] = \deg(f) = n$. Sei $\tilde{f} := \sum_{i=0}^{n} \varphi(a_i) X^n \in L'[X]$. Es gilt $\tilde{f}(\tilde{\varphi}(a)) = \varphi(f(a)) = 0$, also wird a von $\tilde{\varphi}$ auf eine Nullstelle von $\tilde{f}$ abgebildet. Da $\tilde{f}$ höchstens n Nullstellen hat, gibt es somit höchstens n Elemente in L', auf die a von $\tilde{\varphi}$ abgebildet werden kann. Andererseits ist $\tilde{\varphi}$ nach Aufgabe 105 (bzw. der Bemerkung am Ende ihrer Lösung) eindeutig durch das Bild von α bestimmt. Daher gibt es höchstens $[K(\alpha) : K]$ Möglichkeiten für $\tilde{\varphi}$.

111. Sei p prim und $m, n \geq 1$ mit $m \mid n$.

(a) Zeige, dass der m-fache Frobeniushomomorphismus

$$\begin{array}{rccc} \sigma\colon & \mathbb{F}_{p^n} & \longrightarrow & \mathbb{F}_{p^n} \\ & a & \longmapsto & a^{p^m} \end{array}$$

ein $\mathbb{F}_{p^m}$-Automorphismus von $\mathbb{F}_{p^n}$ ist.

(b) Zeige, dass $\mathrm{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_{p^m})$ von σ erzeugt wird und somit zyklisch ist.

(c) Bestimme die Zwischenkörper $\mathbb{F}$ der Körpererweiterung $\mathbb{F}_{p^n} : \mathbb{F}_{p^m}$ sowie die Galoisgruppen $\mathrm{Gal}(\mathbb{F}_{p^n} : \mathbb{F})$ und $\mathrm{Gal}(\mathbb{F} : \mathbb{F}_{p^m})$.

Lösung: (a) Da σ der Frobeniushomomorphismus m-mal mit sich selbst verknüpft ist, ist er ein Körperhomomorphismus. Da $\mathbb{F}_{p^n}$ endlich ist, ist σ somit automatisch ein Automorphismus. Die Elemente von $\mathbb{F}_{p^m}$ sind genau die Nullstellen des Polynoms $X^{p^m} - X$, d.h. genau die Elemente, die unter σ fest bleiben.

(b) Wir wissen, dass $\mathbb{F}_{p^n} = \mathbb{F}_{p^m}(b)$ ist für ein $b \in \mathbb{F}_{p^n}$, z.B. dem Erzeuger der multiplikativen Gruppe. Sei f das Minimalpolynom von b über $\mathbb{F}_{p^m}$. Dann ist für jedes $i = 0, \ldots, \frac{n}{m} - 1$ auch $\sigma^i(b)$ eine Nullstelle von f. Diese sind alle verschieden, denn wäre $\sigma^i(b) = \sigma^j(b)$ für $i > j$, dann impliziert dies $b^{p^{(i-j)m}} = \sigma^{i-j}(b) = b$, also $b \in \mathbb{F}_{p^{(i-j)m}}$, was ein Widerspruch dazu ist, dass b ein Erzeuger von $\mathbb{F}_{p^n}$ sein soll. Ausserdem hat f den Grad $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = \frac{n}{m}$, somit sind $\sigma^i(b)$ mit $i = 0, \ldots, \frac{n}{m} - 1$ alle Nullstellen von f. Nach Aufgabe 105 ist jedes Element aus $\mathrm{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_{p^m})$ eindeutig durch das Bild von b bestimmt. Weiter sind die σ^i Elemente der Galoisgruppe, denn σ ist ein solches. Deshalb ist $\mathrm{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_{p^m})$ zyklisch und von σ erzeugt.

(c) Nach dem Hauptsatz der Galoistheorie sind die Zwischenkörper der Erweiterung genau die Fixkörper der Untergruppen der Galoisgruppe. Aus der Algebra I wissen wir, dass

Untergruppen von zyklischen Gruppen stets zyklisch sind und zu den Teilern der Gruppenordnung korrespondieren. Sie sind also genau der Form $\langle\sigma^i\rangle$ mit $i|\frac{n}{m}$. Da $\sigma^i(a) = a^{p^{im}}$ ist, ist der Fixkörper von $\langle\sigma^i\rangle$ der Körper $\mathbb{F} = \mathbb{F}_{p^{im}}$. Nach Teil (b) ist $\mathrm{Gal}(\mathbb{F}_{p^n} : \mathbb{F}) = \langle\sigma^i\rangle$ und $\mathrm{Gal}(\mathbb{F} : \mathbb{F}_{p^m}) = \langle\sigma|_{\mathbb{F}}\rangle$. Beachte, dass $\sigma|_{\mathbb{F}}$ kleinere Ordnung hat als σ.

112. Sei K ein Körper und $f \in K[X]$ ein separables Polynom. Seien $a_1, \ldots, a_n$ die Nullstelle von f in einem algebraischen Abschluss von K. In Aufgabe 108 haben wir gesehen, dass $\mathrm{Gal}(f)$ in die symmetrische Gruppe $S(a_1, \ldots, a_n)$ eingebettet werden kann. Das bedeutet, dass $\mathrm{Gal}(f)$ auf den Nullstellen von f operiert.

Zeige: Für jedes $i = 1, \ldots, n$ ist die Bahn von a_i dieser Operation genau die Menge der Nullstellen des irreduziblen Faktors von f, dessen Nullstelle a_i ist.

Lösung: Sei a_i eine Nullstelle von f und sei g der irreduzible Faktor von f, dessen Nullstelle a_i ist. Sei $\sigma \in \mathrm{Gal}(f)$. Nach Korollar 19.3 ist $\sigma(a)$ ebenfalls eine Nullstelle von g, d.h. die Bahn von a_i ist in der Menge der Nullstellen von g enthalten. Sei andererseits a_j eine weitere Nullstelle von g und sei L der Zerfällungskörper von f. Nach Satz 14.4 existiert ein Körperhomomorphismus $K(a_i) \to K(a_j)$, der a_i auf a_j abbildet und auf K die Identität ist. Nach Satz 17.5 lässt sich dieser zu einem K-Automorphismus $L \to L$, einem Element aus $\mathrm{Gal}(f)$, erweitern. Somit liegen a_i und a_j in derselben Bahn und wir sind fertig.

113. Sei L der Zerfällungskörper von $X^4 - 4$ über $\mathbb{Q}$.

Bestimme alle Zwischenkörper K mit $\mathbb{Q} \subsetneq K \subsetneq L$.

Lösung: Es ist $X^4 - 4 = (X^2 - 2)(X^2 + 2)$, und daher $L = \mathbb{Q}(\sqrt{2}, i)$. Nach Aufgabe 112 ist $\mathrm{Gal}(L : \mathbb{Q}) \leq S_2 \times S_2$. Wegen $|\mathrm{Gal}(L : \mathbb{Q})| = [L : \mathbb{Q}] = 4$ folgern wir $\mathrm{Gal}(L : \mathbb{Q}) \cong S_2 \times S_2 \cong C_2 \times C_2$. Die Klein'sche Vierergruppe hat genau drei nichttriviale Untergruppen. Die Erweiterung hat also nach dem Hauptsatz der Galoistheorie genau drei echte Zwischenkörper. Es sind dies $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}i)$ und $\mathbb{Q}(i)$.

114. Sei $f \in K[X]$ irreduzibel und separabel und sei L ein Zerfällungskörper von f über K. Zeige: Ist $\mathrm{Gal}(L : K)$ abelsch, so ist $L = K(a)$ für eine beliebige Nullstelle $a \in L$ von f.

Lösung: Wir stellen zunächst fest, dass $L : K$ galoissch ist, da L ein Zerfällungskörper eines separablen Polynoms über K ist. Aus dem gleichen Grund ist $L : K(a)$ galoissch. Nach Definition ist $\mathrm{Gal}(L : K(a))$ die Untergruppe aller $\gamma \in \mathrm{Gal}(L : K)$ mit $\gamma|_{K(a)} = id_{K(a)}$, oder äquivalent $\gamma(a) = a$.

Sei $a' \in L$ eine zweite Nullstelle von f. Nach Aufgabe 112 existiert ein $\delta \in \mathrm{Gal}(L : K)$ mit $\delta(a) = a'$. Für jedes $\gamma \in \mathrm{Gal}(L : K(a))$ gilt nun $\gamma(a) = a$. Da $\mathrm{Gal}(L : K)$ abelsch ist, gilt ausserdem $\gamma \circ \delta = \delta \circ \gamma$ und folglich $\gamma(a') = \gamma(\delta(a)) = \delta(\gamma(a)) = \delta(a) = a'$. Variieren wir a', so sehen wir, dass γ jede Nullstelle von f auf sich abbildet. Da L von diesen Nullstellen über K erzeugt wird, ist γ auf ganz L die Identität. Also ist $\mathrm{Gal}(L : K(a))$ die triviale Untergruppe von $\mathrm{Gal}(L : K)$. Wegen $|\mathrm{Gal}(L : K(a))| = [L : K(a)]$ folgt also $[L : K(a)] = 1$ und somit $L = K(a)$.

115. Sei $L : K$ eine endliche Körpererweiterung und $f \in K[X]$ irreduzibel.

(a) Zeige: Falls $\deg(f)$ und $[L : K]$ teilerfremd sind, ist f irreduzibel über L.

(b) Gib Beispiele von irreduziblen Polynomen in $K[X]$ an, deren Grad nicht teilerfremd zu $[L : K]$ ist und die über L reduzibel sind.

Lösung: (a) Sei a eine Nullstelle von f in einem algebraischen Abschluss von L. Multiplikativität der Körpergrade ergibt

$$[L(a) : K] = [L(a) : L] \cdot [L : K] = [L(a) : K(a)] \cdot [K(a) : K].$$

Also gilt

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

Da $[L : K]$ und $\deg(f)$ teilerfremd sind, ist also $[L : K]$ ein Teiler von $[L(a) : K(a)]$. Andererseits gilt immer $[L(a) : K(a)] \leq [L : K]$, und deshalb hier Gleichheit. Insgesamt folgt $[L(a) : L] = \deg(f)$; somit ist f irreduzibel über L.

(b) Sei zum Beispiel $a \in L \setminus K$ und nimm f das Minimalpolynom von a über K.

116. Finde für folgende Werte von x ein annullierendes Polynom von x über $\mathbb{Q}$ und folgere daraus eine einfachere Darstellung von x.

(a) $x = \sqrt{4 + \sqrt{7}} + \sqrt{4 - \sqrt{7}}$.

(b) $x = \sqrt[3]{2 + \sqrt{5}} + \sqrt[3]{2 - \sqrt{5}}$.

Lösung: (a) Wir rechnen mit der binomischen Formel

$$x^2 \;=\; (4 + \sqrt{7}) + 2\sqrt{16 - 7} + (4 - \sqrt{7}) \;=\; 4 + 2 \cdot 3 + 4 \;=\; 14.$$

Wegen $4 \pm \sqrt{7} > 0$ ist auch $x > 0$; somit folgt $x = \sqrt{14}$.

(b) Wir rechnen

$$\begin{aligned} x^3 &= 2 + \sqrt{5} + 3\sqrt[3]{4 - 5}\left(\sqrt[3]{2 + \sqrt{5}} + \sqrt[3]{2 - \sqrt{5}}\right) + 2 - \sqrt{5} \\ 0 &= x^3 + 3x - 4. \end{aligned}$$

Also ist $X^3 + 3X - 4$ ein annullierendes Polynom für x. Dieses hat Nullstelle 1. Ausserdem zerlegen wir $X^3 + 3X - 4 = (X - 1)(X^2 + X + 4)$. Die weiteren Nullstellen sind nicht reell, aber x schon; also gilt $x = 1$.

117. Sind die folgenden Körper isomorph?

(a) $\mathbb{Q}[X]/(X^2 - 2)$ und $\mathbb{Q}[X]/(X^2 + 2)$;

(b) $\mathbb{Q}[X]/(X^2 + 1)$ und $\mathbb{Q}[X]/(X^2 + 2)$;

(c) $\mathbb{R}[X]/(X^2 + 1)$ und $\mathbb{R}[X]/(X^2 + 2)$;

(d) $\mathbb{Q}[X]/(X^3 - 2)$ und $\mathbb{Q}[X]/(X^3 + 2)$.

Lösung: (a) Wir können beide Körper in $\mathbb{C}$ einbetten via $\mathbb{Q}[X]/(X^2 - 2) \cong \mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}[X]/(X^2 + 2) \cong \mathbb{Q}(\sqrt{2}i)$. Ein Isomorphismus $\mathbb{Q}[X]/(X^2 + 2) \to \mathbb{Q}[X]/(X^2 - 2)$ entspricht damit einem Isomorphismus $\sigma\colon \mathbb{Q}(\sqrt{2}i) \to \mathbb{Q}(\sqrt{2})$. Dieser ist auf dem Primkörper $\mathbb{Q}$ die Identität; also ist $-2 = \sigma(-2) = \sigma((\sqrt{2}i)^2) = \sigma(\sqrt{2}i)^2$ ein Quadrat in $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$; Widerspruch. Somit sind die beiden Körper nicht isomorph.

(b) Wie in (a) bekommen wir $\sigma(\sqrt{2}i)^2 = -2$. Das ist in $\mathbb{Q}(i) \cong \mathbb{Q}[X]/(X^2 + 1)$ nicht möglich. Sei nämlich $(a + ib)^2 = -2$ mit $a, b \in \mathbb{Q}$. Dann ist $a^2 - b^2 + 2abi = -2$, also

$a^2 - b^2 = -2$ und $2ab = 0$. Die erste Gleichung impliziert $b \neq 0$, was mit der zweiten $a = 0$ impliziert. In die erste Gleichung eingesetzt folgt daraus $b^2 = 2$. Aber in $\mathbb{Q}$ gibt es keine Quadratwurzel aus 2, Widerspruch.

Aliter: Wir können via $\mathbb{Q}[X]/(X^2+1) \cong \mathbb{Q}(i)$ und $\mathbb{Q}[X]/(X^2+2) \cong \mathbb{Q}(\sqrt{2}i)$ beide Körper mit Unterkörpern von $\mathbb{C}$ identifizieren. Ihr Kompositum ist dann $\mathbb{Q}(\sqrt{2}, i)$ und hat Grad 4 über $\mathbb{Q}$; insbesondere sind sie verschieden. Nach einer Aufgabe auf Serie 20 sind diese beiden Körper genau dann isomorph über $\mathbb{Q}$, wenn die Galoisgruppen $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}(i))$ und $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}(\sqrt{2}i))$ in $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ konjugiert sind. Allerdings ist $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ isomorph zur Kleinschen Vierergruppe, also kommutativ, und hat keine verschiedenen zueinander konjugierten Untergruppen.

(c) Wegen $\sqrt{2} \in \mathbb{R}$ induziert die Substitution $X \mapsto X/\sqrt{2}$ einen Isomorphismus.

(d) Ja, via der von $X \mapsto -X$ induzierten Abbildung.

Aliter: $\mathbb{Q}[X]/(X^3 - 2) \cong \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(-\sqrt[3]{2}) \cong \mathbb{Q}[X]/(X^3 + 2)$.

118. (a) Seien $\alpha_1, \ldots, \alpha_n$ algebraisch über dem Körper K.
Zeige, dass dann gilt

$$\big[K(\alpha_1, \ldots, \alpha_n) : K\big] \leq \prod_{i=1}^{n} \big[K(\alpha_i) : K\big] .$$

(b) Zeige am Beispiel $\mathbb{Q}\big(\sqrt[4]{2}, \sqrt[4]{18}\big) : \mathbb{Q}$, dass die Ungleichung in (a) auch strikt sein kann.

(c) Ist die Körpererweiterung $\mathbb{Q}\big(\sqrt[4]{2}, \sqrt[4]{18}\big) : \mathbb{Q}$ normal?

Lösung: (a) Sei $K_i = K(\alpha_1, \ldots, \alpha_i)$ für $i = 1, \ldots, n$. Nach der Multiplikativität des Körpergrades gilt

$$[K(\alpha_1, \ldots, \alpha_n) : K] = [K_n : K_{n-1}] \cdot [K_{n-1} : K_{n-2}] \ldots [K_1 : K].$$

Ausserdem gilt $[K_i : K_{i-1}] = [K_{i-1}(\alpha_i) : K_{i-1}] \leq [K(\alpha_i) : K]$ nach Aufgabe 82. Damit folgt die Aussage.

(b) Offensichtlich ist $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) = \mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{2}\sqrt[4]{9}) = \mathbb{Q}(\sqrt[4]{2}, \sqrt[2]{3})$. Also ist

$$[\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, \sqrt[2]{3}) : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] \leq 2 \cdot 4 = 8.$$

Andererseits ist $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ und $[\mathbb{Q}(\sqrt[4]{18}) : \mathbb{Q}] = 4$ und somit

$$[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt[4]{18}) : \mathbb{Q}] = 16.$$

(c) Nein, denn $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) \subset \mathbb{R}$, aber das Minimalpolynom von $\sqrt[4]{2}$ ist $X^4 - 2$ und hat auch nicht-reelle Nullstellen.

119. Finde alle Körperhomomorphismen $K = \mathbb{Q}(\sqrt[4]{2}, e^{\frac{\pi i}{4}}) \to \mathbb{C}$.

Ist die Körpererweiterung $K : \mathbb{Q}$ normal?

Lösung: Wegen $e^{\frac{\pi i}{4}} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$ gilt $\mathbb{Q}(\sqrt[4]{2}, e^{\frac{\pi i}{4}}) = \mathbb{Q}(\sqrt[4]{2}, i)$. Die Erweiterung $K : \mathbb{Q}$ ist also normal, da K der Zerfällungskörper des Polynoms $X^4 - 2$ ist. Weiter gilt wegen der Normalität $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8 = |\,\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q})| = |\,\mathrm{Hom}(\mathbb{Q}(\sqrt[4]{2}, i), \mathbb{C})|$, wobei wir in der letzten Gleichheit noch benutzt haben, dass $\mathbb{Q}$ der Primkörper von K ist.

Die Körperhomomorphismen $\mathbb{Q}(i) \to \mathbb{C}$ sind die Identität und die komplexe Konjugation $\sigma\colon \mathbb{C} \to \mathbb{C}$ eingeschränkt auf $\mathbb{Q}(i)$.

Das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}(i)$ ist X^4-2 und hat die vier Nullstellen $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. Für jede Nullstelle α von X^4-2 gibt es einen Isomorphismus $\mathbb{Q}(i)[X]/(X^4-2) \to \mathbb{Q}(\alpha)$ über $\mathbb{Q}(i)$, der die Restklasse von X auf α abbildet. Daher gibt es für jedes α einen Homomorphismus $\tau_\alpha\colon \mathbb{Q}(i)(\sqrt[4]{2}) \to \mathbb{C}$ über $\mathbb{Q}(i)$, der $\sqrt[4]{2}$ auf α abbildet. Dieser ist eindeutig, da die Elemente in $\mathbb{Q}(i)(\sqrt[4]{2})$ als Polynome in $\sqrt[4]{2}$ mit Koeffizienten in $\mathbb{Q}(i)$ dargestellt werden können und der Homomorphismus auf $\mathbb{Q}(i)$ die Identität sein muss.

Die acht Homomorphismen $\{\tau_\alpha, \tau_\alpha \circ \sigma : \alpha \in \mathbb{C}, \alpha^4 = 2\}$ sind die gesuchten acht Homomorphismen $K \to \mathbb{C}$.