D-MATH | Algebra II | FS 2016
Prof. Richard Pink

Wiederholungsserie

Körpertheorie

1. Seien K_1 und K_2 Zwischenkörper einer endlichen Körpererweiterung L/K. Zeige, dass K_1 und K_2 genau dann linear disjunkt sind über K, wenn die natürliche Abbildung $K_1 \otimes_K K_2 \to K_1 K_2$ ein K-Vektorraumisomorphismus ist.

2. 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.

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

4. Seien K ein Körper, $L = K(\alpha)$ eine endliche einfache Erweiterung und $F \subset L$ eine Zwischenerweiterung. Seien weiter $f \in K[X]$ und $f_F \in F[X]$ die Minimalpolynome von α über K, beziehungsweise über F.

   (a) Zeige, dass $f_F | f$ in $L[X]$ gilt.

   (b) Sei $f_F = X^n + \sum_{k=0}^{n-1} a_k X^k$. Zeige, dass $K(a_0, \ldots, a_{n-1}) = F$ ist.

   (c) Folgere, dass die Erweiterung L/K nur endlich viele Zwischenerweiterungen hat.

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

6. Entscheide, ob sich der Winkel $\arccos(11/16)$ mit Zirkel und Lineal dritteln lässt.

7. Zeige: Jede Körpererweiterung von $\mathbb{Q}$ vom Transzendenzgrad $\leqslant |\mathbb{R}|$ ist isomorph zu einem Unterkörper von $\mathbb{C}$.

*8. Sei F/K eine (nicht notwendigerweise algebraische) Körpererweiterung mit Zwischenkörpern K_1 und K_2, sodass F algebraische Abschlüsse $\overline{K_1}$ von K_1 sowie $\overline{K_2}$ von K_2 enthält. Zeige oder widerlege:

(*a) $\overline{K_1} \cap \overline{K_2}$ ist ein algebraischer Abschluss von $K_1 \cap K_2$.

(**b) $\overline{K_1}\,\overline{K_2}$ ist ein algebraischer Abschluss von $K_1 K_2$.

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

10. Zeige: Für endliche Körper k und ℓ existiert ein Homomorphismus $k \to \ell$ genau dann, wenn $|\ell|$ eine Potenz von $|k|$ ist.

*11. Sei p eine Primzahl und sei $q = p^n$ für eine positive ganze Zahl n.

(a) Zeige: Ein irreduzibles Polynom $f \in \mathbb{F}_p[X]$ teilt $X^q - X$ in $\mathbb{F}_p[X]$ genau dann, wenn sein Grad ein Teiler von n ist.

(b) Sei I_d die Menge der normierten, irreduziblen Polynome vom Grad d in $\mathbb{F}_p[X]$. Beweise die Gleichung
$$X^q - X = \prod_{d|n} \prod_{f \in I_d} f.$$

(c) Folgere daraus, dass gilt $\sum_{d|n} d|I_d| = q$.

(d) Bestimme die Anzahl der irreduziblen Polynome vom Grad 6, 7, 8 in $\mathbb{F}_2[X]$.

12. Der *Satz von Wilson* besagt, dass für jede Primzahl p gilt $(p-1)! \equiv -1 \mod (p)$. Beweise dies vermittels einer Rechnung in $\mathbb{F}_p^\times$.

13. Wann ist eine Körpererweiterung vom Grad 2 inseparabel?

14. Für welche Werte von k ist die Körpererweiterung $\mathbb{F}_7(X)/\mathbb{F}_7(X^k)$

(a) separabel?

(b) normal?

(c) galoissch?

15. Sei H die Gruppe aller Automorphismen von $\mathbb{C}(X)$ der Form $f(X) \mapsto f(X+a)$ für alle $a \in \mathbb{C}$. Bestimme den Fixkörper $\mathbb{C}(X)^H$.

16. Sei L/K eine endliche Galoiserweiterung mit Zwischenkörpern K_1 und K_2 und den entsprechenden Galoisgruppen $\Gamma_i := \mathrm{Gal}(L/K_i) \leqslant \Gamma := \mathrm{Gal}(L/K)$. Zeige:

(a) $K_1 K_2 = L^{\Gamma_1 \cap \Gamma_2}$,

(b) $K_1 \cap K_2 = L^{\langle \Gamma_1, \Gamma_2 \rangle}$, wobei $\langle \Gamma_1, \Gamma_2 \rangle$ die von Γ_1 und Γ_2 erzeugte Untergruppe von Γ bezeichnet.

(c) Nehme an, dass $K_1K_2 = L$ gilt, der Durchschnitt $K_1 \cap K_2 = K$ ist und dass ausserdem für $i = 1, 2$ die Erweiterung K_i/K galoissch ist. Dann ist $\mathrm{Gal}(L/K) \cong \Gamma_1 \times \Gamma_2$.

*17. Sei K ein Körper der Charakteristik 0 und sei X transzendent über K. Zeige, dass $K(X^2) \cap K(X^2 - X) = K$ ist.

18. Zeige oder widerlege: Es existiert eine Körpererweiterung mit genau $50'000$ echten Zwischenkörpern.

19. Bestimme die Galoisgruppen der folgenden Polynome über $\mathbb{Q}$:

(a) $X^3 - 2X + 1$,

(b) $X^3 + X + 1$,

(c) $X^3 - 6X + 1$,

(d) $X^3 - 12X + 8$.

*20. Sei m ungerade, und sei K ein Körper der Charakteristik 0, der alle m-ten Einheitswurzeln enthält. Sei f ein irreduzibles Polynom der Form

$$f(X) = X^{2m} - 2aX^m + 1 \in K[X].$$

Zeige:

(a) Jeder Stammkörper L von f über K ist bereits ein Zerfällungskörper.

(b) Die Galoisgruppe $\mathrm{Gal}(L/K)$ ist isomorph zur Diedergruppe D_m.

(c) Bestimme alle Zwischenkörper von L/K.

*21. In dieser Aufgabe beweisen wir den Fundamentalsatz der Algebra mit Hilfe der Galoistheorie. Sei $K/\mathbb{R}$ eine endliche Körpererweiterung.

(a) Nimm an, $K/\mathbb{R}$ sei galoissch. Zeige, dass ein Körperturm $K = K_n/\ldots/K_0/\mathbb{R}$ existiert, sodass $[K_0/\mathbb{R}]$ ungerade ist und für jedes $0 \leqslant i \leqslant n-1$ die Erweiterung K_{i+1}/K_i den Grad 2 hat.

(b) Zeige, dass $\mathbb{R}$ keine nichttriviale Erweiterung von ungeradem Grad hat.

(c) Zeige, dass jede Erweiterung von $\mathbb{R}$ vom Grad 2 isomorph zu $\mathbb{C}$ ist.

(d) Zeige, dass $\mathbb{C}$ keine Erweiterung vom Grad 2 hat.

(e) Folgere, dass K entweder $\mathbb{R}$ oder $\mathbb{C}$ ist.

22. Sei R ein Ring, und seien $f, g \in R[X]$ normierte Polynome. Zeige:

$$\mathrm{Disc}_{fg} = \mathrm{Disc}_f \cdot \mathrm{Disc}_g \cdot \mathrm{Res}^2_{f,g}\,.$$

23. Zeige: Für beliebige positive ganze Zahlen $q_1, \ldots, q_n$ gilt

$$L := \mathbb{Q}\big(\sqrt{q_1}, \ldots, \sqrt{q_n}\big) \; = \; \mathbb{Q}\big(\sqrt{q_1} + \ldots + \sqrt{q_n}\big).$$

*24. Sei L/K eine endliche Körpererweiterung vom Grad m. Für jedes $\alpha \in L$ ist die *Spur* $\mathrm{Tr}_{L/K}(\alpha)$ definiert als Spur der K-linearen Abbildung $\mu_\alpha \colon L \to L$, $x \mapsto \alpha x$. Zeige:

(a) Ist $X^n + \sum_{k=0}^{n-1} a_k X^k$ das Minimalpolynom von $\alpha \in L$ über K, so gilt für die Spur $\mathrm{Tr}_{L/K}(\alpha) = -\frac{m}{n} a_{n-1}$.

(b) Die Spur induziert eine K-lineare Abbildung $\mathrm{Tr}_{L/K} \colon L \to K$.

(c) Ist L/K separabel und $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_m\}$ für einen algebraischen Abschluss $\overline{K}$ von K, so gilt $\mathrm{Tr}_{L/K}(\alpha) = \sigma_1(\alpha) + \ldots + \sigma_m(\alpha)$.

(d) Ist L/K separabel, so ist die Spurabbildung $\mathrm{Tr}_{L/K} \colon L \to K$ surjektiv.

(e) Benutze dies um den zur Untergruppe $\{1, 2, 4\} < \mathbb{F}_7^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_7)/\mathbb{Q})$ gehörenden Zwischenkörper explizit zu konstruieren.

(*f) Zeige allgemein: Für jede Primzahl p und jede Untergruppe $H < \mathbb{F}_p^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ und jede primitive p-te Einheitswurzel ζ gilt

$$\mathbb{Q}(\mu_p)^H \; = \; \mathbb{Q}\Big(\sum_{h \in H} \zeta^h\Big).$$

Beachte: Die Spur einer quadratischen Matrix ist definiert als die Summe ihrer Diagonaleinträge. Als minus der zweithöchste Koeffizient des charakteristischen Polynoms ist sie invariant unter Ähnlichkeit. (Vergleiche Lineare Algebra I Wiederholungsserie Aufgabe 9.) Für jeden Endomorphismus φ eines endlich dimensionalen K-Vektorraums mit Basis $\mathcal{B}$ ist die Spur der Darstellungsmatrx $M_{\mathcal{B}\mathcal{B}}(\varphi)$ folglich unabhängig von $\mathcal{B}$, hängt also nur von φ ab, und heisst die *Spur von* φ, englisch trace, geschrieben $\mathrm{Tr}(\varphi)$.

25. Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom, das in $\mathbb{C}$ sowohl reelle als auch nicht-reelle Nullstellen hat. Zeige, dass Gal_f nicht abelsch ist.

**26. Konstruiere für jede natürliche Zahl $n \geqslant 1$

(a) ein Polynom vom Grad n über $\mathbb{Q}$ mit Galoisgruppe S_n.

(b) eine Erweiterung vom Grad n von $\mathbb{Q}$, die keine echten Zwischenkörper besitzt.