LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Werner Bley
Martin Hofer

Wintersemester 2018/19
28. Januar 2019

Algebra – Lösungsskizzen zu Übungsblatt 11

Aufgabe 1 (6 Punkte).

a) Es ist $E = \mathbb{Q}(\omega, \zeta)$ mit $\omega := \sqrt[p]{m} \in \mathbb{R}$ und $\zeta := \exp(2\pi i/p)$. Betrachte den Körperturm $E/F/\mathbb{Q}$ mit $F := \mathbb{Q}(\omega)$. Die $\mathbb{Q}$-Homomorphismen von $F/\mathbb{Q}$ sind gegeben durch

$$\sigma_i(\omega) = \zeta^i\omega, \quad i = 0, \ldots, p-1.$$

Es gilt $\mathrm{Mipo}_{\zeta,F} \mid \mathrm{Mipo}_{\zeta,\mathbb{Q}}$ und $\mathrm{Mipo}_{\zeta,\mathbb{Q}} = x^{p-1} + x^{p-2} + \ldots + x + 1$. Ferner ist $[F : \mathbb{Q}] = p$ und $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. Wegen $\mathrm{ggT}([F : \mathbb{Q}], [\mathbb{Q}(\zeta) : \mathbb{Q}]) = 1$ folgt $[E : F] = p - 1$ und daher auch $\mathrm{Mipo}_{\zeta,F} = x^{p-1} + x^{p-2} + \ldots + x + 1 =: g$.
Die Fortsetzungen der σ_i werden parametrisiert durch die Nullstellen von $\sigma_i g = g$. Also erhalten wir

$$G := G(E/\mathbb{Q}) = \{\sigma_{ij} \mid 0 \le i \le p-1, 1 \le j \le p-1\},$$

wobei

$$\sigma_{ij}(\zeta) = \zeta^j \text{ und } \sigma_{ij}|_F = \sigma_i$$

gilt.

b) Sei

$$H := \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \mid \alpha \in \mathbb{F}_p^\times, \beta \in \mathbb{F}_p \right\}$$

Betrachte die Abbildung

$$\psi\colon H \longrightarrow G, \quad \begin{pmatrix} j & i \\ 0 & 1 \end{pmatrix} \mapsto \sigma_{ij}.$$

Es gilt:

$$\begin{pmatrix} j & i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} l & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} jl & jk+i \\ 0 & 1 \end{pmatrix}.$$

Wegen

$$\sigma_{ij}\sigma_{kl}(\omega) = \sigma_{ij}(\zeta^k\omega) = \zeta^{jk+i}\omega,$$
$$\sigma_{ij}\sigma_{kl}(\zeta) = \sigma_{ij}(\zeta^l) = \zeta^{jl}.$$

gilt

$$\psi\left(\begin{pmatrix} j & i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} l & k \\ 0 & 1 \end{pmatrix}\right) = \psi\left(\begin{pmatrix} j & i \\ 0 & 1 \end{pmatrix}\right) \psi\left(\begin{pmatrix} l & k \\ 0 & 1 \end{pmatrix}\right),$$

d.h. ψ ist ein Homomorphismus.
ψ ist offensichtlich surjektiv und wegen $|G| = |H| = p(p-1)$ auch injektiv.

c) Da $|\mathbb{F}_3^\times| = 2$ und $|\mathbb{F}_3| = 3$ kann man direkt ablesen, dass die Gruppe sechs Elemente haben muss. Zudem gilt über $\mathbb{F}_3$

$$\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$$

also ist G eine nicht-abelsche Gruppe der Ordnung 6 und somit wissen wir das diese isomorph zur Gruppe S_3 sein muss.

Aufgabe 2 (6 Punkte).

a) Wir betrachten den Körperturm $K/F/\mathbb{Q}$ mit $K = \mathbb{Q}(\sqrt{1+i})$ und $F := \mathbb{Q}(i)$. Es gilt: $G(F/\mathbb{Q}) = \{id, \tau\}$ mit $\tau(i) = -i$. Das Minimalpolynom von $\alpha := \sqrt{1+i}$ über F ist gegeben durch $g := x^2 - (1+i)$. Also sind die Fortsetzungen von id gegeben durch

$$\sigma_1(\alpha) = \sqrt{1+i}, \quad \sigma_2(\alpha) = -\sqrt{1+i}.$$

Die Fortsetzungen von τ sind parametrisiert durch die Nullstellen von $\tau g = x^2 - (1-i)$ und daher gegeben durch

$$\sigma_3(\alpha) = \sqrt{1-i}, \quad \sigma_4(\alpha) = -\sqrt{1-i}.$$

Die normale Hülle ist also gegeben durch

$$E = \mathbb{Q}(\sqrt{1+i}, \sqrt{1-i}).$$

Aus

$$\frac{\sqrt{1+i}}{\sqrt{1-i}} = \frac{1+i}{\sqrt{2}}$$

folgert man leicht $E = \mathbb{Q}(\sqrt{1+i}, \sqrt{2})$.

b) Wegen $\sqrt{2} \notin K$ ist das Minimalpolynom von $\sqrt{2}$ über K gegeben durch $x^2 - 2$. Damit besteht $G(E/\mathbb{Q})$ aus den folgenden 8 Elementen

$$\sigma_{ik}(\sqrt{2}) = (-1)^k\sqrt{2}, \quad \sigma_{ik}|_K = \sigma_i, \quad i = 1,2,3,4, \quad k = 0,1.$$

Aufgabe 3 (6 Punkte).

a) Sei K ein endlicher Körper, also gilt $|K| = p^n$ für eine Primzahl p und ein $n \in \mathbb{N}$. Somit gibt es eine kanonische Einbettung $\mathbb{F}_p \hookrightarrow K$. Wir wissen außerdem mit Satz 3.2.1, dass $K^\times$ zyklisch ist. Sei σ ein Erzeuger von $K^\times$. Wir betrachten nun den Ringhomomorphismus

$$\begin{aligned} \mathrm{ev}_\sigma : \mathbb{F}_p[X] &\to K \\ g(X) &\mapsto g(\sigma) \end{aligned}$$

Da jedes Element von K entweder 0 oder eine Potenz von σ ist, ist ev_σ wegen $0 = \mathrm{ev}_\sigma(0)$ und $\sigma^n = \mathrm{ev}_\sigma(X^n)$ für jedes $n \geq 0$. Also gilt $\mathbb{F}_p[X]/\ker(\mathrm{ev}_\sigma) \cong K$. Der Kern von ev_σ ist damit ein maximales Ideal in $\mathbb{F}_p[X]$ und muss somit erzeugt werden von einem normierten, irreduziblen Polynom $f(X)$, was zu zeigen war.

b) Wir wissen bereits, dass für jedes p^n ein Körper K exisitert mit $|K| = p^n$. Mit Teilaufgabe a) sehen wir, dass für einen solchen Körper ein irreduzibles, normiertes Polynom $f(X)$ gibt mit $K \cong \mathbb{F}_p[X]/(f(X))$. Wir können also folgern $n = [K : \mathbb{F}_p] = \deg(f)$, was zu zeigen war.

Aufgabe 4 (6 Punkte).

a) Sei α eine Nullstelle von $f := X^p - b$ in einem Zerfällungskörper L. Dann gilt offenbar $\alpha^p = b$. Somit können wir schreiben: $X^p - \alpha^p = (X - \alpha)^p$, wobei die letzte Gleichheit natürlich nur gilt wegen $\mathrm{char}(K) = p$ ('Freshman's dream'). Also ist α eine p-fache Nullstelle und somit liegen alle Nullstellen von $X^p - b$ in $K(\alpha)$ und $L = K(\alpha)$ ist somit der Zerfällungskörper von f und deswegen ist die Erweiterung L/K normal.

b) Zu irreduzibel: Wir wollen zuerst untersuchen, wie wir f zerlegen können. Ist α eine Nullstelle von f in einem Zerfällungskörper L, so gilt offensichtlich wie oben: $f = X^p - b = X^p - \alpha^p = (X - \alpha)^p$ ist eine Faktorisierung von f in L. Ist $g \in K[X]$ ein normierter Faktor von f, so muss wegen der Eindeutigkeit der Primfaktorzerlegung $g = (X - \alpha)^d$ für ein $0 \leq d \leq p$ gelten. Der zweithöchste Koeffizient von g ist aber $(\pm)d \cdot \alpha$ und dieser muss in K liegen. Wegen $\alpha \notin K$ muss also $d \cdot 1_K = 0$ gelten, was $p \mid d$ impliziert. Insbesondere hat man $d = 0$ oder $d = p$ und f ist irreduzibel.
Zu nicht separabel: Ganz offensichtlich ist $f' = 0$ und nach Vorlesung ist f nicht separabel.

c) Zuerst sehen wir ein, dass der Frobenius-Homomorphismus als Körperhomomorphismus immer injektiv ist.
Sei nun zunächst K perfekt. Offensichtlich ist jedes irreduzible Polynom g über K separabel (man kann immer einen Zerfällungskörper von g über K betrachten. Dort hat g eine Nullstelle und diese ist nach Voraussetzung separabel, also ist g separabel). Gibt es nun ein $b \in K$, das keine p-te Potenz ist, so ist nach b) das Polynom $X^p - b$ irreduzibel und nicht separabel, Widerspruch. Jedes $b \in K$ ist also p-te Potenz und der Frobenius ist surjektiv, also ein Automorphismus.
Sei nun F surjektiv, L/K eine algebraische Erweiterung und $a \in L$. Wir zeigen, dass das Minimalpolynom g von a über K separabel ist. Nach Voraussetzung ist g irreduzibel. Ist g nicht separabel, so hat g eine mehrfache Nullstelle (in $\overline{K}$) und es gilt $g' = 0$. Dann gibt es aber ein $h = \sum_{i=0}^{d} a_i X^i \in K[X]$ mit $g = h(X^p)$. Da der Frobenius surjektiv ist, existieren allerdings $b_i \in K$ mit $b_i^p = a_i$ und es folgt $g = h(X^p) = \sum_{i=0}^{d} a_i X^{ip} = \sum_{i=0}^{d} b_i^p X^{ip} = \sum_{i=0}^{d} (b_i X^i)^p = \left(\sum_{i=0}^{d} b_i X^i\right)^p$. Das ist ein Widerspruch zur Irreduzibilität von g und somit muss g separabel sein. Insbesondere ist auch a separabel und wir haben alles gezeigt.