



Prof. Dr. Werner Bley
Martin Hofer

Wintersemester 2018/19

25. Januar 2019

Algebra – Lösungsskizzen zum Ferienblatt

Aufgabe 1 (3 Punkte).

Sei p eine Primzahl, $|G| = p^n$, $N \triangleleft G$ und $|N| = p$.

Wir können folgenden Homomorphismus von Gruppen definieren:

$$\begin{aligned}\alpha : G &\rightarrow \text{Aut}(N) \\ g &\mapsto (n \mapsto g^{-1}ng).\end{aligned}$$

Da $|N| = p$ gilt, folgt $N \cong \mathbb{Z}/p\mathbb{Z}$, also auch $\text{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ und somit $|\text{Aut}(N)| = p - 1$.

Das Bild von α ist isomorph zu einem Quotienten von G also gilt $|\text{im}(\alpha)| = p^m$; außerdem gilt $\text{im}(\alpha) \leq \text{Aut}(N)$. Also muss Bild von α trivial sein und α ist der triviale Gruppenhomomorphismus. Daraus folgt wieder um, dass für alle $g \in G$ und für alle $n \in N$ gilt $gn = ng$ und somit gilt auch $N \subseteq Z(G)$, was zu zeigen war.

Aufgabe 2 (3 Punkte).

Aus den Sylowsätzen und den zugehörigen Korollaren wissen wir, dass für die Anzahl der 7-Sylowuntergruppen n_7 gilt: $n_7 \equiv 1 \pmod{7}$ und $n_7 \mid 24$. Daraus können wir folgern, dass $n_7 \in \{1, 8\}$ gelten muss.

Der Fall $n_7 = 1$ ist aber nicht möglich, da die Gruppe in diesem Fall einen nicht-trivialen Normalteiler hätte (nämlich diese 7-Sylowgruppe), aber dies der Definition einer einfachen Gruppe widerspricht.

Also betrachten wir den Fall $n_7 = 8$. Jede 7-Sylowuntergruppe hat 6 Elemente der Ordnung 7 (zyklische Gruppe von Primordnung). Diese zyklischen Gruppen sind bis auf das neutrale Element disjunkt, denn ansonsten wären sie gleich. Also gibt es genau $8 \cdot 6 = 48$ Elemente der Ordnung 7.

Aufgabe 3 (3 Punkte).

- Eine Matrix ist genau dann invertierbar, wenn die Spaltenvektoren linear unabhängig sind. Für den ersten Vektor aus $\mathbb{F}_p^2$ haben wir $p^2 - 1$ Möglichkeiten (alle außer den Nullvektor). Der erste Vektor hat nun $(p - 1)$ nicht-triviale Vielfache. Das heißt für den zweiten Vektor gibt es $p^2 - 1 - (p - 1) = p^2 - p$ Möglichkeiten. Also gibt es insgesamt $(p^2 - 1)(p^2 - p)$ invertierbare 2×2 -Matrizen über $\mathbb{F}_p$.
- Die Menge der invertierbaren 2×2 -Matrizen $\mathfrak{A}$ mit Determinante t ist unabhängig von der Wahl der $t \in \mathbb{F}_p^\times$, da sie in 1-1 Beziehung mit der Menge der invertierbaren

2×2 -Matrizen $\mathfrak{B}$ mit Determinante 1 steht durch die Abbildung:

$$\begin{aligned}\mathfrak{B} &\rightarrow \mathfrak{A} \\ B &\mapsto \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} B \\ \begin{pmatrix} t^{-1} & 0 \\ 0 & 1 \end{pmatrix} A &\mapsto A.\end{aligned}$$

Da aber $|\mathbb{F}_p^\times| = p - 1$ gilt, gibt es $\frac{(p^2-1)(p^2-p)}{(p-1)}$ invertierbare 2×2 -Matrizen über $\mathbb{F}_p$ mit Determinante $t \in \mathbb{F}_p^\times$.

Aufgabe 4 (3 Punkte).

Wir betrachten den nicht-trivialen Gruppenhomomorphismus $\varphi : A_n \rightarrow H$, wobei $n \geq 5$ und A_n die alternierende Gruppe ist. Es gilt also $\ker(\varphi) \triangleleft A_n$ und da wir aus der Vorlesung wissen, dass A_n für $n \geq 5$ einfach ist und der Homomorphismus nicht-trivial ist, folgt dass $\ker(\varphi) = \{0\}$ gilt, φ also injektiv ist. Somit gilt $|A_n| \mid |H|$. Die Ordnung von A_n ist aber $n!/2$, also $n \mid |A_n|$. Daraus folgt aber sofort $n \mid |H|$.

Aufgabe 5 (3 Punkte).

Wir wollen zeigen, dass alle Gruppen G der Ordnung $|G| = 242 = 2 \cdot 11^2$ auflösbar sind. Aus der Vorlesung wissen wir, dass für die Anzahl der 11-Sylowuntergruppen gilt: $n_{11} \equiv 1 \pmod{11}$ und $n_{11} \mid 2$. Also kann es nur eine 11-Sylowuntergruppe geben und diese ist somit ein Normalteiler. Da $[G : N] = 2$, ist G/N abelsch und somit auch auflösbar. Andererseits ist auch N auflösbar, da $|N| = 11^2$ und somit eine p -Gruppe ist. Also folgt mit Satz 1.6.2, dass G auflösbar ist.

Aufgabe 6 (2 Punkte).

Da 2 in $\mathbb{Q}$ eine Einheit ist, reicht es zu zeigen, dass $g := x^4 + 3x^3 + 5x^2 + 7x + 9$ irreduzibel über $\mathbb{Q}[x]$ ist. Wir reduzieren modulo 2 und erhalten $\bar{g} = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$. Dies ist das Minimalpolynom der 5-ten Einheitswurzel also wissen wir aus der Vorlesung (5 ist eine Primzahl), dass dieses irreduzibel ist, also auch über $\mathbb{F}_2$. Somit ist g irreduzibel über $\mathbb{Z}[x]$ ist und da g zudem primitiv ist, auch über $\mathbb{Q}[x]$, was zu zeigen war.

Aufgabe 7 (2 Punkte).

Wir wissen aus der Angabe, dass für alle $a \in R$ ein $n > 1$ existiert, mit $a^n = a$. Wir nehmen uns ein Primideal $\mathfrak{p} \triangleleft R$. Sei $\mathfrak{b}$ nun ein Ideal von R das echt über $\mathfrak{p}$ liegt, i.e. $\mathfrak{p} \subsetneq \mathfrak{b}$ und sei $a \in \mathfrak{b} \setminus \mathfrak{p}$. Es gilt dann

$$0 = a^n - a = a(a^{n-1} - 1) \in \mathfrak{p}.$$

Aus der Primidealeigenschaft folgt, dass $a \in \mathfrak{p}$ oder $a^{n-1} - 1 \in \mathfrak{p} \subset \mathfrak{b}$ und somit $1 \in \mathfrak{b}$. Jedes Ideal das echt über einen Primideal $\mathfrak{p}$ liegt ist also schon der gesamte Ring R , also ist $\mathfrak{p}$ ein maximales Ideal.

Aufgabe 8 (4 Punkte).

- a) Wir erinnern uns, dass ein Primkörper P von K der Durchschnitt aller Teilkörper von K ist und somit der kleinste Teilkörper von K . Des weiteren wissen wir, dass wenn die Charakteristik eine Primzahl p ist, dass dann der Primkörper P von K isomorph zu $\mathbb{F}_p$ ist.

Sei K ein endlicher Körper mit Charakteristik p , also gilt für den Primkörper $P \cong \mathbb{F}_p$. Der Körper K ist eine Erweiterung seines Primkörpers P . Da K endlich ist, kann es nur endlich viele über P linear unabhängige Element geben; also ist $[K : P] = n \in \mathbb{N}$. Ist $(b_1, \dots, b_n)$ eine Basis von K über P , so lässt sich jedes $a \in K$ eindeutig darstellen als $a = \lambda_1 b_1 + \dots + \lambda_n b_n$ mit $\lambda_1, \dots, \lambda_n \in P$, und es ist $a \mapsto (\lambda_1, \dots, \lambda_n)$ ein P -Vektorraumisomorphismus von K nach P^n . Also gilt $|K| = |P^n| = |P|^n = p^n$.

- b) Sei K ein Körper der Charakteristik p . Die Körper E und K haben den gleichen Primkörper P . Wir können also die Körpergrade $[E : P]$ und $[K : P]$ betrachten. Nun gilt $[K : P] = n$ für ein $n \in \mathbb{N}$. Mit der Gradformel erhalten wir $[E : P] = mn$ und mit Teilaufgabe a) $|E| = p^{mn}$ sowie $|K| = p^n$, was zu zeigen war.

Aufgabe 9 (3 Punkte).

Sei E/K eine Erweiterung von Grad 2 und $\alpha \in E \setminus K$ ein beliebiges Element. Dann ist $K(\alpha)$ ein Zwischenkörper von E/K und aufgrund der Gradformel $[E : K(\alpha)] \cdot [K(\alpha) : K] = [E : K] = 2$. Wegen $\alpha \notin K$ ist $K(\alpha) \neq K$ und somit $[K(\alpha) : K] > 1$. Weil $[K(\alpha) : K]$ zugleich Teiler von 2 ist, muss $[K(\alpha) : K] = 2$ und $[E : K(\alpha)] = 1$, also $E = K(\alpha)$ gelten.

Sei f das Minimalpolynom von α über K . Wegen $\deg(f) = 2$ gibt es $p, q \in K$ mit $f = X^2 + pX + q$. Wegen $\text{char}(K) \neq 2$ existiert ein multiplikatives Inverses der 2 im Körper das wir mit $\frac{1}{2}$ bezeichnen. Ebenso schreiben wir $\frac{1}{4}$ für $\frac{1}{2} \cdot \frac{1}{2}$. Es gilt nun

$$f(\alpha) = 0 \Leftrightarrow \alpha^2 + p\alpha + q = 0 \Leftrightarrow \alpha^2 + p\alpha + \frac{1}{4}p^2 = \frac{1}{4}p^2 - q \Leftrightarrow (\alpha + \frac{1}{2}p)^2 = \frac{1}{4}d$$

wobei $d = p^2 - 4q$. Setzen wir nun $\beta = \alpha + \frac{1}{2}p$, dann gilt $K(\alpha) = K(\beta)$, denn offenbar ist $\beta = \alpha + \frac{1}{2}p \in K(\alpha)$ und $\alpha = \beta - \frac{1}{2}p \in K(\beta)$. Daraus folgt $E = K(\beta)$. Außerdem gilt $\beta^2 = \frac{1}{4}d \in K$.

Sei andererseits $\alpha \in E \setminus K$ und $\alpha^2 \in K$. Sei $\alpha^2 = \lambda \in K$. Es gilt dann $[K(\alpha) : K] = 2$, da $X^2 - \lambda$ wegen den Voraussetzungen irreduzibel ist ($\text{char}(K) \neq 2$ und $\alpha \notin K$) und somit das Minimalpolynom der Erweiterung.

Aufgabe 10 (4 Punkte).

- a) Wir bezeichnen mit U die Vereinigung von allen endlichen Körpererweiterungen von K in E . Wir wollen nun zeigen, dass $K^c = U$ gilt. Sei $\alpha \in K^c$, dann ist α per Definition algebraisch und mit einem Satz aus der Vorlesung erhalten wir, dass $K(\alpha)/K$ eine endliche Körpererweiterung von K in E ist und somit gilt $\alpha \in U$.

Andererseits, sei $\alpha \in U$. Also liegt α in einem Körper F der eine endliche Körpererweiterung von K ist. Ein Satz der Vorlesung sagt nun, dass jede endliche Körpererweiterung algebraisch ist, insbesondere gilt also $\alpha \in K^c$.

- b) Wiederum bezeichnen wir die in der Angabe definierte Vereinigung mit U .

Wir nehmen zuerst an E/K ist algebraisch. Sei $\alpha \in E$. Mit einem Satz aus der Vorlesung folgt $K(\alpha)/K$ ist endlich und somit gilt $E \subseteq U$. Die andere Inklusion ist klar.

Wir nehmen nun an $E = U$. Sei $\alpha \in E$. Nach Annahme ist dann aber auch $\alpha \in U$ und α ist somit in einer endlichen Erweiterung enthalten. Mit einem Satz der Vorlesung wissen wir, dass diese Erweiterung algebraisch ist, also ist auch α algebraisch und somit E/K eine algebraische Erweiterung.