Mathematisches Institut der Universität München
Wintersemester 2009/10

Stefan Gille
Lukas-Fabian Moser

Algebra – Lösungsideen zum 8. Übungsblatt

Aufgabe 1.

i) In der Vorlesung wurde gezeigt, daß $(a+b)^p = a^p + b^p$ gilt (der Grund war, daß die beim Ausmultiplizieren nach der binomischen Formel auftretenden Binomialkoeffizienten fast alle durch p teilbar sind, denn es ist

$$\binom{p}{i} = \frac{p!}{i! \cdot (p-i)!},$$

und der Zähler enthält den Primfaktor p, der Nenner nicht, wenn $i < p$ und $p - i < p$, also $0 < i < p$ ist.) Das ist aber der einzige problematische Teil, denn $1^p = 1$ und $(ab)^p = a^p b^p$ gelten immer und überall.

ii) Die Frobeniusabbildung $F : K \to K$, $a \mapsto a^p$, ist nach i) ein Körperhomomorphismus, nach Aufgabe 2 i) von Blatt 7 deswegen injektiv und damit, da K eine endliche Menge ist, automatisch surjektiv.

Aufgabe 2.

i) Betrachte beispielsweise den Körperturm $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. Die erste Erweiterung ist normal, denn sie entsteht durch Adjunktion *aller* Lösungen von $X^2 - 2 = 0$ zu $\mathbb{Q}$ (denn beide Lösungen unterscheiden sich nur durchs Vorzeichen; adjungiert man also die eine, bekommt man automatisch beide). Genauso sieht man, daß die zweite Erweiterung normal ist (sie Entsteht durch Adjunktion aller Lösungen von $X^2 - \sqrt{2} = 0$). Die Gesamterweiterung $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ ist aber nicht normal: denn das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}$ ist $X^4 - 2$ (irreduzibel nach Eisenstein), es zerfällt aber nicht in Linearfaktoren: denn es zerfällt nicht einmal über $\mathbb{R}$ (zwei der Nullstellen sind echt komplex), aber es ist ja $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$.

ii) Ist L/K normal, so gibt es nach einem Satz der Vorlesung eine Menge $S \subset K[X]$ von Polynomen, die alle über L zerfallen, und deren Nullstellen L über K erzeugen. Diese Nullstellen erzeugen dann aber auch LL' über L', und damit ist (nach der anderen Richtung im gleichen Satz der Vorlesung) diese Erweiterung normal.

Aufgabe 3.

i) $\Longrightarrow$ ii). Ist $\mathrm{char}(k) = 0$, so ist nichts zu zeigen; wir können also $\mathrm{char}(k) = p > 0$ annehmen. Ist nun $n = p \cdot m$ ein Vielfaches von p, so ist $X^n - 1 = (X^m)^p - 1^p = (X^m - 1)^p$ nach Aufgabe 1 i), und ein Polynom der Form F^ℓ für $\ell > 1$ kann niemals separabel sein, da jede Nullstelle mindestens ℓ-mal auftritt. (Man kann auch anders argumentieren: die Ableitung von $X^n - 1$ ist $nX^{n-1} = 0$ wegen $p \mid n$, also ist jede Nullstelle von f (die nicht unbedingt in k zu liegen braucht) mehrfach, und da das Polynom Grad > 1 hat, kann es damit nicht separabel sein.)

ii) $\Longrightarrow$ i). Die formale Ableitung des Polynoms ist nX^{n-1}, also (da $n \neq 0$ in K gilt) bis auf eine Einheit identisch mit X^{n-1}. Aber X^{n-1} und $X^n - 1$ sind teilerfremd in $K[X]$ (das erste der beiden Polynome hat X als einzigen Primteiler, und der teilt das zweite offensichtlich nicht), also hat $X^n - 1$ keine mehrfachen Nullstellen in irgendeinem Erweiterungskörper.

Aufgabe 4.
i) $\Longrightarrow$ ii). Es sei K ein Körper mit q Elementen. Sei p die Charakteristik von K; dann ist p eine Primzahl, und K enthält einen p-elementigen Unterkörper $K_0 \cong \mathbb{Z}/p\mathbb{Z}$ (als Bild des einzigen Ringhomomorphismus $\mathbb{Z} \to K$). Insbesondere ist K ein – sicherlich endlichdimensionaler – Vektorraum über K_0 und als solcher Isomorph zu K_0^n für irgendein $n \geqslant 1$ (genauer ist $n = [K : K_0]$), d.h. K hat $|K_0^n| = |K_0|^n = p^n$ Elemente.
ii) $\Longrightarrow$ i). Es sei $q = p^n$ mit $n \geqslant 1$. Wie im Hinweis vorgeschlagen, sei L ein Zerfällungskörper von $F = X^q - X$ über $K_0 := \mathbb{Z}/p\mathbb{Z}$. Es sei $K \subset L$ die Menge der Nullstellen von F. Tatsächlich ist K ein Körper: Bezeichnen wir nämlich mit $f : L \to L$ den Frobeniushomomorphismus $a \mapsto a^p$, so ist $K = \{a \in L \,|\, f^n(a) = a\}$, und allgemein kann man ziemlich schnell nachrechnen: Die Menge aller Elemente, auf denen zwei Körperhomomorphismen (hier f^n und id) übereinstimmen, bildet wieder einen Körper. – Außerdem hat K genau q Elemente, denn F kann keine mehrfachen Nullstellen haben wegen $F' = qX^{q-1} - 1 = -1$. (Insbesondere folgt im übrigen $K = L$.)
Bemerkung: Die Motivation, gerade das Polynom $X^q - X$ zu nehmen, liefert der Satz von Euler-Fermat aus der Gruppentheorie, der ja insbesondere besagt: Ist K ein Körper mit n Elementen, so ist $a^{n-1} = 1$ für alle $0 \neq a \in K$ und damit $a^n = a$ für alle $a \in K$, d.h. K ist Zerfällungskörper von $X^n - X$ über irgendeinem Unterkörper.

Zusatzaufgabe.

i) (a) $\Longrightarrow$ (b) ist wohlbekannt und (b) $\Longrightarrow$ (c) trivial (sorry für den Ausdruck, aber hier stimmt's ausnahmsweise wirklich). Für (c) $\Longrightarrow$ (a) sei $\varphi_G(d)$ die Anzahl der Elemente der Ordnung d von G. Da die Ordnung jedes Elementes die Gruppenordnung teilt, folgt $\sum_{d|n} \varphi_G(d) = n$. Gibt es nun ein Element g der Ordnung d von G, so ist $\langle g \rangle$ isomorph zu $\mathbb{Z}/d\mathbb{Z}$, also folgt $\varphi_G(d) \geqslant \varphi_{\mathbb{Z}/d\mathbb{Z}}(d)$. Jedes Element der Ordnung d von G muß aber in $\langle g \rangle$ liegen (hier geht die Voraussetzung (c) ein), also folgt $\varphi_G(d) = \varphi_{\mathbb{Z}/d\mathbb{Z}}(d)$. – Angewandt auf die Gruppe $\mathbb{Z}/n\mathbb{Z}$ anstelle von G folgt insbesondere $\varphi_{\mathbb{Z}/n\mathbb{Z}}(d) = \varphi_{\mathbb{Z}/d\mathbb{Z}}(d)$, denn wegen $d \mid n$ gibt es ja Elemente der Ordnung d in $\mathbb{Z}/n\mathbb{Z}$. Also haben wir insgesamt $\sum_{d|n} \varphi_G(d) = n = \sum_{d|n} \varphi_{\mathbb{Z}/n\mathbb{Z}}(d)$. Wegen $\varphi_G(d) \leqslant \varphi_{\mathbb{Z}/d\mathbb{Z}}(d) = \varphi_{\mathbb{Z}/n\mathbb{Z}}(d)$ für alle d müssen dann aber alle Summanden auf der linken und der rechten Seite übereinstimmen, also $\varphi_G(d) = \varphi_{\mathbb{Z}/n\mathbb{Z}}(d)$ für alle $d \mid n$, und insbesondere (für $d = n$) enthält G ein Element der Ordnung n und ist damit zyklisch.
ii) Es sei $n = |G|$. Nach i) genügt es zu zeigen, daß G für jedes $d \mid n$ höchstens eine d-elementige Untergruppe besitzt. Ist aber $U \subset G$ eine solche, so gilt $x^d = 1$ für alle $x \in U$ nach Euler–Fermat, und da die Polynomgleichung $X^d - 1 = 0$ in einem Körper nur höchstens d Lösungen haben kann, folgt $U = \{x \in G \,|\, x^d = 1\}$. Das zeigt, daß U eindeutig bestimmt ist, wie behauptet.