Mathematisches Institut der Universität München
Wintersemester 2009/10

Stefan Gille
Lukas-Fabian Moser

Algebra – 8. Übungsblatt

Aufgabe 1.

i) Es sei p eine Primzahl und R ein Ring der Charakteristik p. Zeige: Die Abbildung $F : R \to R$, $a \mapsto a^p$, ist ein Ringhomomorphismus (bekannt als *Frobenius-Homomorphismus*).
ii) Ist K ein endlicher Körper der Charakteristik p, so ist jedes Element von K eine p-te Potenz. (Man könnte etwa Aufgabe 2 i) von Blatt 7 verwenden.)

Aufgabe 2.

i) Zeige durch ein Gegenbeispiel: Sind L/K und M/L normale Körpererweiterungen, so muß M/K nicht notwendig normal sein.
ii) Es sei $K \subset M$ eine algebraische Körpererweiterung mit Zwischenkörpern L und L'. Es sei $LL' := L(L') = L'(L)$ das *Kompositum* von L und L', d.h. der kleinste Unterkörper von M, der L und L' enthält. Zeige: Ist L/K normal, so auch LL'/L'.

Aufgabe 3. Es sei K ein Körper und $n \geqslant 1$. Zeige, daß folgende Aussagen äquivalent sind:

i) Das Polynom $X^n - 1 \in K[X]$ ist separabel.
ii) n ist kein Vielfaches von $\mathrm{char}(K)$.

(Tip für i) $\Longrightarrow$ ii): Kontraposition und Aufgabe 1 i). – Vorsicht: In der Literatur kursieren mindestens zwei echt verschiedene Definitionen des Begriffs „separabel". Es ist wichtig, die Definition aus der Vorlesung zu nehmen, wie sie etwa auch bei Bosch verwendet wird.)

Aufgabe 4. Es sei $q > 1$. Beweise den Satz von Moore (1903), der besagt, daß folgende Aussagen äquivalent sind:

i) Es gibt einen Körper mit q Elementen.
ii) q ist eine Primzahlpotenz.

(Starthilfen: Für i) $\Longrightarrow$ ii) betrachte den Körper als Vektorraum über seinem Primkörper. Für ii) $\Longrightarrow$ i) nehme man für $q = p^k$, p prim, einen Zerfällungskörper des Polynoms $F = X^q - X$ über $\mathbb{Z}/p\mathbb{Z}$ und zeige unter Verwendung von Aufgabe 1 i), daß die Nullstellen von F einen Körper bilden.)

Zusatzaufgabe. Beweise die folgenden Sätze von Gauß (1801):

i) Für eine n-elementige Gruppe G sind äquivalent:
   (a) G ist zyklisch.
   (b) Für jedes $d \mid n$ enthält G genau eine Untergruppe der Ordnung d.
   (c) Für jedes $d \mid n$ enthält G höchstens eine Untergruppe der Ordnung d.

   (Anleitung: Arbeiten muß man nur für die Implikation (c) $\Longrightarrow$ (a). Bezeichne dazu mit $\varphi_G(d)$ die Anzahl der Elemente der Ordnung d von G und zeige:

(a) $\sum_{d|n} \varphi_G(d) = n$.
(b) Für jedes $d \mid n$ ist $\varphi_G(d)$ entweder null oder identisch mit $\varphi_{\mathbb{Z}/d\mathbb{Z}}(d)$.
(c) Für jedes $d \mid n$ ist $\varphi_{\mathbb{Z}/d\mathbb{Z}}(d) = \varphi_{\mathbb{Z}/n\mathbb{Z}}(d)$.

Meditiere anschließend über die Gleichung $\sum_{d|n} \varphi_G(d) = n = \sum_{d|n} \varphi_{\mathbb{Z}/n\mathbb{Z}}(d)$.)

ii) Ist K ein Körper und $G \subset K^\times$ eine endliche Untergruppe, so ist G zyklisch. (Insbesondere ist also die Gruppe $\mu_n(K) := \{x \in K \mid x^n = 1\}$ der n-ten Einheitswurzeln zyklisch, und ist K endlich, so ist auch $K^\times$ zyklisch.)

Die Lösungen sind bis **Dienstag, 15. Dezember 2009, 14 Uhr** *geheftet* im Algebra-Übungskasten (im 1. Stock vor der Bibliothek) einzuwerfen. Bitte Namen und Tutoriumsgruppe $\in \{A, \ldots, G, Z, X\}$ angeben!