Anmerkungen und Lösungen zu

Einführung in die Algebra

Blatt 8

Jendrik Stelzner

Letzte Änderung: 16. Dezember 2017

Aufgabe 3

(d)

Lemma 1. *Es sei R ein kommutativer Ring von Charakteristik $\operatorname{char}(R) = p$ prim. Dann ist die Abbildung*

$$\sigma\colon R \to R, \quad x \mapsto x^p$$

ein Ringhomomorphismus.

Beweis. Es gilt $\sigma(1) = 1^p = 1$, und für alle $x, y \in R$ gilt

$$\sigma(xy) = (xy)^p = x^p y^p = \sigma(x)\sigma(y)\,,$$

da R kommutativ ist. Für alle $x, y \in R$ folgt aus der Kommutativität von R, dass

$$\sigma(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \tag{1}$$

gilt. Für alle $0 < k < p$ gelten dabei $p \nmid k!$ und $p \nmid (p-k)!$, und somit gilt

$$p \,\Big|\, \frac{p!}{k!(p-k)!} = \binom{p}{k}\,.$$

Damit folgt aus (1) die behauptete Gleichheit

$$\sigma(x+y) = (x+y)^p = x^p + y^p = \sigma(x) + \sigma(y)\,. \qquad \square$$

Bemerkung 2. Man bezeichnet den Ringhomomorphismus σ aus Lemma 1 als den *Frobenius-Homomorphismus*. Ist etwa K ein endlicher Körper und $p \coloneqq \operatorname{char}(K)$, so ist der Frobenius-Homomorphismus $\sigma\colon K \to K$, $x \mapsto x^p$ bereits ein Automorphismus: Als

Körperhomomorphismus ist σ injektiv, und wegen der Endlichkeit von K damit auch schon surjektiv.

Wir werden sehen, dass die Automorphismengruppe $\mathrm{Aut}(K)$ zyklisch ist, und von σ erzeugt wird. Gilt $|K| = p^n$, so hat σ Ordnung p, so dass $\mathrm{Aut}(K) \cong \mathbb{Z}/n$ gilt.

Wir bemerken, dass $\zeta = e^{2\pi i/p^2}$ eine p^2-te primitive Einheitswurzel ist, und somit eine Nullstelle des Kreisteilungspolynoms $\Phi_{p^2}(t) \in \mathbb{Z}[t] \subseteq \mathbb{Q}[t]$. Das Polynom $\Phi_{p^2}(t)$ ist normiert, und wir zeigen im Folgenden, dass es irreduzibel ist; dann ist $\Phi_{p^2}(t)$ bereits das Minimalpolynom von ζ über $\mathbb{Q}$.

In der Vorlesung haben wir die Irreduziblität von $\Phi_p(t)$ gezeigt, indem wir das Einstein-Kriterium für $\Phi_p(t+1)$ bezüglich der Primzahl p angewendet haben. Auf die gleiche Weise zeigen wir, dass auch $\Phi_{p^2}(t)$ irreduzibel ist, d.h. wir zeigen, dass sich auf $\Phi_{p^2}(t+1)$ das Eisenstein-Kriterium mit der Primzahl p anwenden lässt. Hierfür nutzen wir, dass $\Phi_{p^2}(t) = \Phi_p(t^p)$ gilt.

- Das Kreisteilungspolynom $\Phi_{p^2}(t)$ ist normiert, also ist auch $\Phi_{p^2}(t+1)$ normiert. Insbesondere ist der Leitkoeffizient von f nicht durch p teilbar.
- Wir müssen zeigen, dass alle anderen Koeffizienten von $\Phi_{p^2}(t)$ durch p teilbar sind. Hierfür betrachten wir den Ringhomomorphismus

$$\mathbb{Z}[t] \to \mathbb{F}_p[t], \quad g = \sum_i a_i t^i \mapsto \sum_i \overline{a_i} t^i = \overline{g}\,.$$

  Für $g_1, g_2 \in \mathbb{Z}[t]$ schreiben wir im Folgenden

$$g_1 \equiv g_2 \mod p$$

  falls $\overline{g_1} = \overline{g_2}$ gilt.

  Wir wissen bereits, dass das Polynom $\Phi_p(t+1)$ mit $\deg \Phi_p(t+1) = \deg \Phi(t) = p-1$ das Eisenstein-Kriterium erfüllt, weshalb

$$\Phi_p(t+1) \equiv t^{p-1} \mod p$$

  gilt. Indem wir für die Variable t das Polynom t^p einsetzen, erhalten wir, dass

$$\Phi_p(t^p+1) \equiv (t^p)^{p-1} = t^{p(p-1)} \mod p$$

  gilt.

  Wir möchten zeigen, dass bis auf den Leitkoeffizienten von $\Phi_{p^2}(t+1)$ alle Koeffizienten dieses Polynoms durch p teilbar sind. Da

$$\deg \Phi_{p^2}(t+1) = \deg \Phi_{p^2}(t) = \deg \Phi_p(t^p) = p \deg \Phi_p(t) = p(p-1)$$

  gilt, müssen wir also zeigen, dass

$$\Phi_{p^2}(t+1) \equiv t^{p(p-1)} \mod p\,.$$

Wir zeigen im Folgenden, dass

$$\Phi_{p^2}(t+1) \equiv \Phi_p(t^p+1) \mod p$$

gilt. Hierfür setzen wir in der Gleichung $\Phi_{p^2}(t) = \Phi_p(t^p)$ für die Variable t das Polynom $t+1$ ein, und erhalten so, dass

$$\Phi_{p^2}(t+1) = \Phi_p((t+1)^p)$$

gilt. Wir müssen also zeigen, dass

$$\Phi_p((t+1)^p) \equiv \Phi_p(t^p+1) \mod p$$

gilt. Dies ergibt sich daraus, dass nach Lemma 1 bereits

$$(t+1)^p \equiv t^p + 1^p = t^p + 1 \mod p\,,$$

gilt.

Wir haben also ingesamt gezeigt, dass

$$\Phi_{p^2}(t+1) = \Phi_p((t+1)^p) \equiv \Phi_p(t^p+1) \equiv t^{p(p-1)} \mod p$$

gilt. Das zeigt, dass alle Koeffizienten von $\Phi_{p^2}(t+1)$, bis auf den Leitkoeffizienten, durch p teilbar sind.

- Wir müssen noch zeigen, dass der konstante Term von $\Phi_{p^2}(t+1)$ nicht durch p^2 teilbar ist. Dieser konstante Teil lässt sich dadurch bestimmen, dass wir für die Variable t die Zahl $0 \in \mathbb{Z}$ einsetzen. Wir erhalten dabei, dass

  $$\Phi_{p^2}(0+1) = \Phi_{p^2}(1) = \Phi_p(1^p) = \Phi_p(1) = 1^{p-1} + 1^{p-2} + \cdots + 1^1 + 1^0 = p\,.$$

  Der konstante Koeffizient von $\Phi_{p^2}(t+1)$ ist also p, und somit nicht durch p^2 teilbar.

Bemerkung 3. Es lässt sich allgemeiner zeigen, dass das Kreisteilungspolynom $\Phi_n(t)$ für jedes $n \geq 1$ irreduzibel ist. Beim Erstellen des Übungszettels wurde davon ausgegangen, dass dies in der Vorlesung gezeigt wurde. Hierdurch würde dieser Aufgabenteil einen deutlich geringeren Arbeitsaufwand benötigen.

Aufgabe 4

(a)

Die Idee hinter der Aussage ist, dass $\phi(1) = 1$ gilt, und sich alle Elemente des Primkörpers P durch iteratives Anwenden der Körperoperationen (Addition, Subtraktion, Multiplikation, Division) aus 1 ergeben. Da ϕ mit diesen Operationen verträglich ist, sollte deshalb bereits $\phi(x) = x$ für alle $x \in P$ gelten.

Um diese Anschauung zu formalisieren, zeigen wir, dass die Menge

$$K^\phi = \{x \in K \mid \phi(x) = x\}$$

ein Unterkörper von K ist. Dann gilt $P \subseteq K$, da P in jedem Unterkörper von K enthalten ist.

Es gelten $\phi(0) = 0$ und $\phi(1) = 1$ und somit $0, 1 \in K$. Für alle $x, y \in K$ gelten auch

$$\phi(x + y) = \phi(x) + \phi(y) = x + y \quad \text{und} \quad \phi(xy) = \phi(x)\phi(y) = xy\,,$$

und somit $x + y, xy \in K$. Für jedes $x \in K$ gilt

$$\phi(-x) = -\phi(x) = -x\,,$$

und somit $-x \in K$, und falls zusätzlich $x \neq 0$ gilt, dann gilt auch

$$\phi(x^{-1}) = \phi(x)^{-1} = x^{-1}\,,$$

und somit $x^{-1} \in K$. Ingesamt zeigt dies, dass K^ϕ ein Unterkörper von K ist.

(b)

Die Abbildung $\phi\colon K \to K$ ist nach Annahme bijektiv und additiv. Für alle $\lambda \in P$ und $x \in K$ gilt nach dem vorherigen Aufgabenteil, dass

$$\phi(\lambda x) = \phi(\lambda)\phi(x) = \lambda\phi(x)\,.$$

Das zeigt insgesamt, dass ϕ ein K-Vektorraum-Automorphismus ist.