Technische Universität Berlin
Fakultät II, Institut für Mathematik
Paul Breiding
Sekretariat MA 3-2

Algebra I

Wintersemester 2015/2016

Blatt 9 - Musterlösung

Für die Korrektheit der Lösungen wird keine Gewähr übernommen.

Aufgabe 1 (10 Punkte). Es seien n, m ganze Zahlen mit $\mathrm{ggT}(n, m) = 1$. Sei weiterhin R ein Integritätsbereich und $a, b \in R$. Zeige: Falls $a^n = b^n$ und $a^m = b^m$, so gilt $a = b$.

Lösung. Sei F der Quotientenkörper von R. Wir interpretieren R als Unterring von F via der Inklusion $R \hookrightarrow F, a \mapsto a$. Seien $a, b \in R$. Seien weiterhin $n, m \in \mathbb{Z}$ mit $\mathrm{ggT}(n, m) = 1$. Angenommen $a^n = b^n$ sowie $a^m = b^m$. Falls $a = 0$, dann gilt $b = 0$. Wir nehmen an, dass $a \neq 0$. Nach dem Lemma von Bezout existieren $r, s \in \mathbb{Z}$ mit $rn + sm = 1$. Daher gilt $a = a^{rn+sm} = (a^n)^r (a^m)^s = (b^n)^r (b^m)^s = b^{rn+sm} = b$. ∎

Bemerkung: In einer früheren Version war R nur als Ring gefordert. Dann ist die Aussage aber falsch wie folgendes Beispiel zeigt: In $\mathbb{Z}/8\mathbb{Z}$ gilt $2^3 = 4^2 = 0$. Aber $\mathrm{ggT}(2, 3) = 1$ und $2 \neq 4$.

Aufgabe 2 (10 Punkte). Es sei R ein kommutativer Ring und

$$N := \{x \in R \mid \exists n \in \mathbb{N} : x^n = 0\},$$

die Menge der nilpotenten Elemente. Zeige:

(1) N ist ein Ideal in R.

(2) Für alle $z \in R/N$ und $n \in \mathbb{N}$ gilt: Falls $z^n = 0$, dann ist $z = 0$.

Lösung. Zu (1): Wir zeigen zunächst mit Hilfe des Untegruppenkriteriums, dass N eine Untegruppe von R bzgl. $+$ ist. Seien $a, b \in N$. Dann existieren $n, m \in \mathbb{N}$ mit $a^n = b^m = 0$. Betrachte

$$\begin{aligned}
(a-b)^{n+m} &\overset{R \text{ komm.}}{=} \sum_{i=0}^{n+m} \binom{n+m}{i} a^i (-b)^{n+m-i} \\
&= \sum_{i=0}^{n-1} \binom{n+m}{i} a^i \underbrace{(-b)^{n+m-i}}_{=0} + \sum_{i=n}^{n+m} \binom{n+m}{i} \underbrace{a^i}_{=0} (-b)^{n+m-i} \\
&= 0.
\end{aligned}$$

Technische Universität Berlin
Fakultät II, Institut für Mathematik
Paul Breiding
Sekretariat MA 3-2

Also ist $a - b \in N$. Sei nun $x \in R$ und $a \in N$, $n \in \mathbb{N}$ mit $a^n = 0$. Dann gilt $(ax)^n \overset{R \text{ komm.}}{=} a^n x^n = 0$, also $ax \in N$. Dies zeigt, dass N ein Ideal ist.

Zu (2): Sei $z \in R/N$ und $n \in \mathbb{N}$ mit $z^n = 0$. Sei $\pi : R \to R/N$ der kanonische Homomorphismus. Da π surjektiv ist, existiert ein $a \in R$ mit $\pi(a) = z$. Wegen $\pi(a^n) = z^n = 0$, gilt $a^n \in N$. Daher existiert $m \in \mathbb{N}$ mit $(a^n)^m = a^{nm} = 0$. Dies zeigt, dass $a \in N$ und $z = \pi(a) = 0$. ∎

Aufgabe 3 (10 Punkte). Es sei $p > 2$ eine Primzahl. Wir werden in der Vorlesung zeigen, dass die Gruppe $\mathbb{F}_p^\times$ zyklisch ist. Dies darf im Folgenden verwendet werden.

(1) Zeige: $[\mathbb{F}_p^\times : (\mathbb{F}_p^\times)^2] = 2$, wobei $(\mathbb{F}_p^\times)^2 := \left\{ a^2 \,\middle|\, a \in \mathbb{F}_p^\times \right\}$.

(2) Zeige, dass $-1 \in (\mathbb{F}_p^\times)^2$ genau dann gilt, wenn $4 \mid (p-1)$.

(3) Zeige: Falls eine Primzahl p Summe von zwei Quadraten ist, so ist $p - 1$ durch 4 teilbar.

(4) Zeige, dass das Ideal $(3, 1 + \sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}]$ kein Hauptideal ist.
Hinweis: Verwende Überlegungen von Blatt 8, Aufgabe 5.

Lösung. Zu (1): Wir benutzen, dass $\mathbb{F}_p^\times$ zyklisch ist. Sei $\mathbb{F}_p^\times = \langle g \rangle$, so dass

$$\mathbb{F}_p^\times = \left\{ g^1, \dots, g^{p-1} \right\}.$$

Da $\mathbb{F}_p^\times$ abelsch ist, ist $(\mathbb{F}_p^\times)^2$ eine Gruppe und $\phi : \mathbb{F}_p^\times \to (\mathbb{F}_p^\times)^2,\ x \mapsto x^2$ ein Homomorphismus. Wir berechnen $\ker \phi$. Es ist $\phi(g^i) = g^{2i} = 1$ genau dann, wenn $2i$ von $p-1$ geteilt wird. Da $p > 2$, ist $p - 1$ gerade. Somit wird $2i$ genau dann von $p-1$ geteilt, wenn i von $\frac{p-1}{2}$ geteilt wird. Dies zeigt, dass $\ker \phi = \left\{ g^i \in \mathbb{F}_p^\times \,\middle|\, g^{2i} = 1 \right\} = \left\{ 1, g^{\frac{p-1}{2}} \right\}$ und daher $[\mathbb{F}_p^\times : (\mathbb{F}_p^\times)^2] = |\ker \phi| = 2$.

Bemerkung: In einer früheren Version des Zettels sollte die Aussage für einen beliebigen Körper gezeigt werden. Diese Aussage wäre falsch, wie das folgende Beispiel zeigt: Wir wissen, dass $\mathbb{C}$ algebraisch abgeschlossen ist. Insbesondere hat die Gleichung $X^2 - a = 0$ für alle $a \in \mathbb{C}$ eine Lösung. Das heißt, dass alle Elemente in $\mathbb{C}^\times$ Quadrate sind. Also $\mathbb{C}^\times = (\mathbb{C}^\times)^2$ und daher $[\mathbb{C}^\times : (\mathbb{C}^\times)^2] = 1$.

Zu (2): Es ist $(-1)^2 = 1$. Mit der Notation von (1) sehen wir, dass $-1 \in \ker \phi$ und daher $-1 = g^{\frac{p-1}{2}}$. Sei nun $-1 \in (\mathbb{F}_p^\times)^2$. Dann existiert ein $k \in \{1, \dots, p-1\}$ mit

$$g^{2k} = g^{\frac{p-1}{2}}. \tag{0.1}$$

Wir können $k \in \left\{1, \ldots, \frac{p-1}{2}\right\}$ annehmen: Falls $k > \frac{p-1}{2}$, so ist $g^{2(k-\frac{p-1}{2})} = g^{2k}$. Nach Annahme sind $2k, \frac{p-1}{2} \in \{1, \ldots, p-1\}$. Aus (0.1) folgern wir $2k = \frac{p-1}{2}$, in anderen Worten $4 \mid (p-1)$. Gilt andererseits, dass $4 \mid (p-1)$, so gilt $(g^{\frac{p-1}{4}})^2 = g^{\frac{p-1}{2}} = -1$, also $-1 \in \mathbb{F}_p^\times$.

Zu (3): Sei $p = x^2 + y^2$, $x, y \in \mathbb{Z}$. Wir schreiben X, Y für die Restklassen von x, y mod p. Nach Voraussetzung gilt, $X^2 = -Y^2$. Da p prim ist, gilt $\mathrm{ggT}(y, p) = 1$ und somit $Y \in \mathbb{F}_p^\times$. Wir folgern, dass $-1 = (XY^{-1})^2$. Nach (2) gilt, dass $4 \mid (p-1)$.

Zu (4): Angenommen $(3, 1+\sqrt{-5})$ ist ein Hauptideal, etwa $(3, 1+\sqrt{-5}) = (x)$, $x \in \mathbb{Z}[\sqrt{-5}]$. Dann existieren $a, b \in \mathbb{Z}[\sqrt{-5}]$ mit $3 = ax$ und $1+\sqrt{-5} = bx$. Beachte, dass $|3|^2 = 9$ und $|1+\sqrt{-5}|^2 = 6$. Es folgt, dass $|x|^2 = 3$. Sei nun $x = x_1 + x_2\sqrt{-5}$, $x_1, x_2 \in \mathbb{Z}$, so dass $|x|^2 = x_1^2 + 5x_2^2$. Da die Gleichung $3 = x_1^2 + 5x_2^2$ in den ganzen Zahlen nicht lösbar ist, muss die Annahme falsch sein und $(3, 1+\sqrt{-5})$ ist kein Hauptideal. ∎

Aufgabe 4 (10 Punkte). Zerlege $X^8 + X^6 - X^5 - X^2 - X - 1 \in \mathbb{F}_3[X]$ in quadratfreie Faktoren.

Lösung. Aus der Vorlesung wissen wir, dass $f = X^8 + X^6 - X^5 - X^2 - X - 1 \in \mathbb{F}_3[X]$ genau dann quadratfrei ist, wenn $\mathrm{ggT}(f, f') = 1$ gilt. Wir berechnen mit Polynomdivision, dass $\mathrm{ggT}(f, f') = 1$. Also ist f bereits quadratfrei. ∎

Aufgabe 5 (10 Punkte). Zeige jeweils, dass das Polynom quadratfrei ist und berechne seine irreduziblen Faktoren mit Berlekamps Algorithmus.

(1) $X^4 - X^2 + X + 1 \in \mathbb{F}_3[X]$.

(2) $X^3 - 2X^2 - X - 2 \in \mathbb{F}_5[X]$.

Lösung. Zu (1): Sei $f = X^4 - X^2 + X + 1 \in \mathbb{F}_3[X]$. Wir berechnen $\mathrm{ggT}(f, f') = 1$. Also ist f quadratfrei. Nun wollen wir Berlekamps Algorithmus anwenden. Nach Vorlesung müssen wir folgende Schritte ausführen.

(1) *Berechne die Matrix* $(\beta_{ik})_{0 \le i,k \le n-1} \in \mathbb{F}_p^{n \times n}$ *mit* $x^{pk} = \sum_{i=0}^{n-1} \beta_{ik} x^i \bmod f$ *(dies ist die Darstellungsmatrix von* $\Phi : \mathbb{F}_p[X]/(f) \to \mathbb{F}_p[X]/(f)$, $a \mapsto a^p$*).*

(2) *Berechne eine Basis von* $B = \ker((\beta_{ik}) - I_{n\times n})$*. Setze* $t = \dim B$*.*

(3) (1) *Falls* $t = 1$*:* **Ausgabe:** *f ist irreduzibel.*

(2) *Falls* $t > 1$*: Für alle Basiselemente* $a \notin \mathbb{F}_p$ *von* B *berechne* $d = \mathrm{ggT}(a - s, f)$*,* $s \in \mathbb{F}_p$*, bis* $d \neq 1$*.* **Ausgabe:** *t ist die Anzahl irreduzibler Faktoren von f und d ist ein nichttrivialer Faktor von f.*

Technische Universität Berlin
Fakultät II, Institut für Mathematik
Paul Breiding
Sekretariat MA 3-2

In unserem Fall ist $n = 4$ und $p = 3$. Die Darstellungen von x^{3k} in der Basis $\{1, x, x^2, x^3\}$ lässt sich mit Hilfe von Polynomdivision der x^{3k} durch f berechnen. Wir erhalten

$$(\beta_{ik}) = \begin{bmatrix} 1 & 0 & -1 & -1 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{bmatrix}.$$

Mittels Gauss Elimination berechnen wir

$$B = \ker \begin{bmatrix} 0 & 0 & -1 & -1 \\ 0 & -1 & -1 & -1 \\ 0 & 0 & -1 & -1 \\ 0 & 1 & -1 & -1 \end{bmatrix} = \operatorname{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \\ 1 \end{pmatrix} \right\}.$$

Es ist $t = \dim B = 2$. Wir schreiben die zwei Basiselemente von B zur Übersicht als Polynome: $B = \{1, X^3 - X^2\}$. Es gilt $\mathrm{ggT}(X^3 - X^2 - 1, f) = X + 1$. Daher ist

$$f = (X+1)\frac{f}{X+1} = (X+1)(X^3 - X^2 + 1)$$

eine nichttriviale Zerlegung von f. Da die Anzahl der irreduziblen Faktoren von f gleich $t = 2$ ist, ist dies bereits die Zerlegung von f in irreduzible Faktoren.

Zu (2): Sei $f = X^3 - 2X^2 - X - 2 \in \mathbb{F}_5[X]$. Wir berechnen $\mathrm{ggT}(f, f') = 1$. Also ist f quadratfrei. Wir verfahren wie oben und erhalten

$$(\beta_{ik}) = \begin{bmatrix} 1 & 0 & -2 \\ 0 & -1 & 1 \\ 0 & -1 & 0 \end{bmatrix}.$$

Mittels Gauss Elimination berechnen wir

$$B = \ker \begin{bmatrix} 0 & 0 & -2 \\ 0 & -2 & 1 \\ 0 & -1 & -1 \end{bmatrix} = \operatorname{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\}.$$

■

Ausgabe: f ist irreduzibel.