LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Werner Bley
Martin Hofer

Wintersemester 2018/19
5. Januar 2019

Algebra – Lösungsskizzen zu Übungsblatt 9

Aufgabe 1 (6 Punkte).

a) Nach dem Eisensteinkriterium für $p = 7$ ist $f(x)$ irreduzibel in $\mathbb{Q}[x]$. Da f primitiv ist, ist f auch irreduzibel in $\mathbb{Z}[x]$.

b) Liest man das Polynom g modulo 3 so erhält man $\bar{g}(x) = x^3 + x^2 + 2 \in \mathbb{F}_3[x]$. Falls $\bar{g}$ reduzibel wäre, so hätte $\bar{g}$ aus Gradgründen einen Linearfaktor, also eine eine Nullstelle in $\mathbb{F}_3$. Dies ist jedoch nicht der Fall. Also ist $\bar{g}$ irreduzibel und damit auch g irreduzibel in $\mathbb{Z}[x]$, denn jede Zerlegung in $\mathbb{Z}[x]$ würde ja zu einer Zerlegung in $\mathbb{F}_3[x]$ führen. Da g primitiv ist, ist g auch irreduzibel in $\mathbb{Q}[x]$.

c) Wir schreiben
$$h(x,y) = y^5 + (x-1)y^3 + (x-1)^2y + x(x-1)$$
und lesen dies in $(\mathbb{Q}[x])[y]$. Der Ring $\mathbb{Q}[x]$ ist euklidisch, insbesondere also faktoriell. Aus Gradgründen ist $p = x - 1$ ein Primelement. Das Eisensteinkriterium liefert also, das h irreduzibel in $(\mathbb{Q}[x])[y]$ ist. Also ist h irreduzibel.

Aufgabe 2 (6 Punkte).
Zuerst sollte man sich durch eine kurze Rechnung vergewissern, dass es sich bei Φ_g, wie in der Angabe behauptet, wirklich um einen Homomorphismus handelt.

a) Sei Φ_g ein Isomorphismus. Insbesondere gibt es dann ein $f \in R[X]$ mit $\Phi_g(f) = f(g) = X$. Wegen $1 = \deg(X) = \deg(f) \cdot \deg(g)$ folgt dann $\deg(f) = \deg(g) = 1$, also $g = aX + b$ und $f = cX + d$ für gewisse $a, b, c, d \in R$. Es ist aber $X = f(g) = c(aX + b) + d = acX + (cb + d)$, woraus man $ac = 1$ erhält, insbesondere ist a invertierbar.

Sei nun andererseits $g = aX + b$ mit $a \in R^\times$, $b \in R$. Man wählt sich dann $h = a^{-1}(X - b) \in R[X]$ und eine kurze Rechnung zeigt
$$\Phi_g \circ \Phi_h = id_{R[X]} = \Phi_h \circ \Phi_g \,,$$
was zeigt, dass Φ_g ein Isomorphismus ist.

b) Zuerst erkennen wir, dass aufgrund der geometrischen Reihe
$$f := X^{p-1} + X^{p-2} + \ldots + 1 = \frac{X^p - 1}{X - 1}$$
gilt. Es ist dann
$$\begin{aligned}\Phi_g\left(X^{p-1} + X^{p-2} + \ldots + 1\right) = \Phi_g\left(\frac{X^p - 1}{X - 1}\right) &= \frac{(X+1)^p - 1}{X} \\ &= X^{p-1} + \binom{p}{1} X^{p-2} + \ldots + \binom{p}{p-1},\end{aligned}$$

wobei das letzte Gleichheitszeichen aus dem binomischen Lehrsatz folgt. Eisenstein mit p liefert dann die Irreduzibilität von $\Phi_g(f)$. Nach a) ist Φ_g aber ein Isomorphismus und dieser schickt irreduzible Elemente auf irreduzible Elemente, was die Behauptung zeigt.

Aufgabe 3 (5 Punkte).

a) Sei I ein Primideal. Da $0 \in I$ gilt, bekommen wir sofort $0 \notin R \setminus I$ und $R \setminus I$ ist nichtleer, da für I als Primideal gilt $I \neq R$. Für $a, b \in R \setminus I$ ist nun zu zeigen, dass $ab \in R \setminus I$. Nehmen wir also an $ab \in I$. Da I ein Primideal ist, muss dann gelten $a \in I$ oder $b \in I$, was aber ein Widerspruch ist und somit ist $R \setminus I$ eine multiplikativ abgeschlossene Menge.
Sei $R \setminus I$ eine multiplikativ abgeschlossene Menge. Es gilt $I \neq R$ da $R \setminus I \neq \emptyset$. Sei $ab \in I$ für $a \in I$ und $b \in I$. Wenn wir annehmen, dass $a \notin I$ und $b \notin I$, bekommen wir $a \in R \setminus I$ und $b \in R \setminus I$ und da $R \setminus I$ eine multiplikative Menge ist, $ab \in R \setminus I$, was ein Widerspruch ist. Also ist I ein Primideal.

b) Wir setzen $S := R \setminus P$. Es gilt $1 \notin PS^{-1}R$, also ist $PS^{-1}R$ ein echtes Ideal.
Sei $x/y \in S^{-1}R \setminus PS^{-1}R$. Dann gilt $x \in S$ und somit $y/x \in S^{-1}R$ und somit auch $x/y \in (S^{-1}R)^\times$. Also folgt mit Aufgabe 2 von Blatt 8 die Behauptung.

Aufgabe 4 (5 Punkte).

a) Wir zeigen etwas allgemeiner, dass für $p \neq 2$ und $p \nmid a$ gilt: $p^{\alpha-1}$ die Ordnung von $1 + ap$ modulo p^α ist. Um dies zu zeigen, beweisen wir zunächst einige allgemeine Behauptungen die auch anderswo nützlich sein können:
Behauptung 1. *Sei p eine Primzahl und $1 \leq k < p$. Dann ist der Binomialkoeffizient $\binom{p}{k}$ durch p teilbar.*

Beweis. Per Definition gilt

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \text{ und somit } p! = k!(p-k)!\binom{p}{k}.$$

Es gilt nun aber $p \mid p!$ und $p \nmid k!$ und $p \nmid (p-k)!$, womit die Aussage gezeigt ist. □

Behauptung 2. *Sei $\alpha \geq 1$ und $a \equiv b \bmod p^\alpha$. Dann gilt*

$$a^p \equiv b^p \bmod p^{\alpha+1}.$$

Beweis. Wir können a schreiben als $a = b + cp^\alpha$, $c \in \mathbb{Z}$. Also gilt

$$a^p = b^p + \binom{p}{1} b^{p-1} c p^\alpha + A,$$

wobei $A \in \mathbb{Z}$ mit $p^{\alpha+2} \mid A$. Da der zweite Term durch $p^{\alpha+1}$ teilbar ist erhalten wir die Behauptung. □

Behauptung 3. *Sei $\alpha \geq 2$ und $p \neq 2$, dann gilt für alle $a \in \mathbb{Z}$:*

$$(1 + ap)^{p^{\alpha-2}} \equiv 1 + ap^{\alpha-1} \bmod p^\alpha.$$

Beweis. Wir beweisen diese Behauptung durch Induktion über n. Wenn $\alpha = 2$ ist, ist die Behauptung trivial. Wir nehmen also an die Behauptung ist wahr für ein $\alpha \geq 2$ und wollen sie für $\alpha + 1$ zeigen. Durch das Anwenden von Behauptung 2 erhalten wir

$$(1 + ap)^{p^{\alpha-1}} \equiv (1 + ap^{\alpha-1})^p \bmod p^{\alpha+1}$$

Aus der Binomischen Formel erhalten wir

$$(1 + ap^{\alpha-1})^p = 1 + \binom{p}{1} ap^{\alpha-1} + B,$$

wobei B die Summe von $p - 2$ Termen ist. Mit Behauptung 1 sieht man schnell, dass alle diese Terme durch $p^{1+2(\alpha-1)}$ teilbar sind mit Ausnahme (eventuell) des letzten Terms $a^p p^{p(\alpha-1)}$. Da $\alpha \geq 2$, $1 + 2(\alpha - 1) \geq \alpha + 1$, und da $p \geq 3$, $p(\alpha - 1) \geq \alpha + 1$. Also gilt $p^{\alpha+1} \mid B$ und

$$(1 + ap)^{p^{\alpha-1}} \equiv 1 + ap^{\alpha} \bmod p^{\alpha+1}.$$

□

Nun können wir die eigentliche Aussage zeigen:
Mit Behauptung 3 gilt

$$(1 + ap)^{p^{\alpha-1}} \equiv 1 + ap^{\alpha} \bmod p^{\alpha+1}.$$

was sofort impliziert

$$(1 + ap)^{p^{\alpha-1}} \equiv 1 \bmod p^{\alpha}$$

und somit hat $1 + ap$ eine Ordnung die $p^{\alpha-1}$ teilt. Aber

$$(1 + ap)^{p^{\alpha-2}} \equiv 1 + ap^{\alpha-1} \bmod p^{\alpha}.$$

zeigt, dass $p^{\alpha-2}$ nicht ein Vielfaches der Ordnung von $1 + ap$ ist (hier benutzen wir $p \nmid a$). Also ist $\operatorname{ord}(1 + ap) = p^{\alpha-1}$ in $(\mathbb{Z}/p^{\alpha}\mathbb{Z})^{\times}$.

b) Wir sehen, dass $(\mathbb{Z}/8\mathbb{Z})^{\times} = \{1, 3, 5, 7\}$ also eine Gruppe der Ordnung 4 ist. Da 3^2, 5^2 und 7^2 kongruent ist zu 1 modulo 8 ist, ist jedes Element selbstinvers und somit ist die Gruppe isomorph zur Kleinschen Vierergruppe. Anderseits sehen wir, dass $\langle 3 \rangle \times \langle 5 \rangle$ aus den Elementen $\{(1,1), (1,5), (3,1), (3,5)\}$ besteht. Auch hier kann man nachrechnen, dass jedes Element selbstinvers ist und somit muss die Gruppe ebenfalls isomorph zur Kleinschen Vierergruppe sein, was zu zeigen war. Hat man sich, wie oben, für Repräsentanten entschieden, ist es natürlich auch einfach, direkt eine Abbildung anzugeben:

$$\begin{aligned} 1 &\mapsto (1,1) \\ 3 &\mapsto (3,1) \\ 5 &\mapsto (1,5) \\ 7 &\mapsto (3,5) \end{aligned}$$

von der man nachrechnen kann, dass sie ein Isomorphismus ist.

Aufgabe 5 (6 Punkte).

a) Durch das Einsetzen aller Elemente aus $\mathbb{F}_3$ kann man einsehen, dass sich von $x^3 + x^2 + 2$ und $x^2 - 2$ keine Linearfaktoren in $\mathbb{F}_3[x]$ abspalten lassen und somit sind die Polynome irreduzibel in $\mathbb{F}_3[x]$. Wir sehen dadurch auch, dass die beiden Polynome teilerfremd sind. Mit dem Chinesischen Restsatz erhalten wir

$$\left(\mathbb{F}_3[x]/(x^3 + x^2 + 2)(x^2 - 2)\right)^\times \cong \left(\mathbb{F}_3[x]/(x^3 + x^2 + 2)\right)^\times \times \left(\mathbb{F}_3[x]/(x^2 - 2)\right)^\times$$

Da wir schon gezeigt haben, dass die beiden Polynome irreduzibel sind, erhalten wir $\left(\mathbb{F}_3[x]/(x^3 + x^2 + 2)\right) \cong \mathbb{F}_{3^3}$ und $\mathbb{F}_3[x]/(x^2 - 2) \cong \mathbb{F}_{3^2}$ und somit ist die Anzahl der Elemente $26 \cdot 8$.

b) Sei G eine abelsche Gruppe mit $g, h \in G$ und $m = \operatorname{ord}(g)$ sowie $n = \operatorname{ord}(h)$. Zudem setzen wir $d := \operatorname{kgV}(m, n)$.

Unter der Annahme, dass m und n teilerfremd sind, wissen wir bereits, dass gh ein Element der Ordnung mn ist und in diesem Fall gilt natürlich auch $d = mn$.

Für den allgemeinen Fall betrachten wir nun die Primfaktorenzerlegung von m und n:

$$m = \prod_i p_i^{a_i} \text{ und } n = \prod_i p_i^{b_i}.$$

Wir setzen nun

$$m' = \prod_{i:a_i \geq b_i} p_i^{a_i} \text{ sowie } n' = \prod_{i:b_i > a_i} p_i^{b_i}$$

und es gilt offensichtlich: $m' \mid m$, $n' \mid n$ und $(m', n') = 1$. Man kann nun schnell nachrechnen, dass das Element $g' := g^{m/m'}$ die Ordnung m' hat und das Element $h' := h^{n/n'}$ die Ordnung n' hat. Da die Ordnungen teilerfremd sind, folgt, dass das Element $g'h'$ die Ordnung $m'n'$ hat. Per Konstruktion von n' und m' sehen wir aber auch, dass $d = m'n'$ gilt und somit haben wir gezeigt, dass ein Element der Ordnung $\operatorname{kgV}(m, n)$ existiert.