D-MATH Algebra I HS 2015
Prof. Richard Pink

Musterlösung 4

Ideale, Primideale, Hauptidealringe

1. Sei $a \in \mathbb{R}$. Untersuche, wann der Ring $\mathbb{R}[X]/(X^2+a)$ isomorph zu $\mathbb{R}\times\mathbb{R}$, beziehungsweise zu $\mathbb{C}$, beziehungsweise zu keinem der beiden ist.

   Lösung: Definiere für $a<0$

$$\varphi: \begin{array}{ccc} \mathbb{R}[X] & \longrightarrow & \mathbb{R}\times\mathbb{R} \\ f & \longmapsto & (f(\sqrt{-a}), f(-\sqrt{-a})) \end{array}$$

   und für $a>0$

$$\varphi: \begin{array}{ccc} \mathbb{R}[X] & \longrightarrow & \mathbb{C} \\ f & \longmapsto & f(\sqrt{a}i) \end{array}.$$

   In beiden Fällen ist φ eine $\mathbb{R}$-lineare Abbildung und nach der universellen Eigenschaft des Polynomrings $\mathbb{R}[X]$ ein Ringhomomorphismus. Zudem ist φ surjektiv, da es im Fall $a<0$ für alle $c,d\in\mathbb{R}$ ein Polynom $f\in\mathbb{R}[X]$ mit $f(\sqrt{-a})=c$ und $f(-\sqrt{-a})=d$ gibt (z.B. lineares Polynom wählen) und im Fall $a>0$ klarerweise die Elemente 1 und $\sqrt{a}i$ im Bild von φ liegen, die $\mathbb{C}$ als $\mathbb{R}$-Vektorraum erzeugen.

   Da $\ker\varphi$ in beiden Fällen das Ideal (X^2+a) enthält, induziert φ nach der universellen Eigenschaft des Faktorrings einen surjektiven $\mathbb{R}$-linearen Ringhomomorphismus $\overline{\varphi}:\mathbb{R}[X]/(X^2+a)\to\mathbb{R}\times\mathbb{R}$ bzw. $\overline{\varphi}:\mathbb{R}[X]/(X^2+a)\to\mathbb{C}$.

   Wir beschreiben nun die Elemente des Faktorrings $\mathbb{R}[X]/(X^2+a)$ explizit: Für ein beliebiges $f\in\mathbb{R}[X]$ gibt es nach Division mit Rest eindeutige $q,r\in\mathbb{R}[X]$ mit

$$f(X)=q(X)(X^2+a)+r(X)$$

   und $\deg(r)\leqslant 1$. Es gilt also $f(X)+(X^2+a)=aX+b+(X^2+a)$ in $\mathbb{R}[X]/(X^2+a)$ für eindeutige $a,b\in\mathbb{R}$. Somit ist $\mathbb{R}[X]/(X^2+a)$ ein zweidimensionaler $\mathbb{R}$-Vektorraum. Da $\mathbb{R}\times\mathbb{R}$ und $\mathbb{C}$ auch Dimension 2 über $\mathbb{R}$ haben, ist daher $\overline{\varphi}$ als surjektive $\mathbb{R}$-lineare Abbildung in beiden Fällen ein Isomorphismus.

   Im Fall $a=0$ hat der Ring $\mathbb{R}[X]/(X^2+a)=\mathbb{R}[X]/(X^2)$ mit $\alpha:=X+(X^2)$ ein von Null verschiedenes nilpotentes Element mit $\alpha^2=0$. Die Ringe $\mathbb{R}\times\mathbb{R}$ und $\mathbb{C}$ haben keine solchen Elemente und sind daher nicht zu $\mathbb{R}[X]/(X^2)$ isomorph.

*2. Zeige, dass ein echtes Ideal $\mathfrak{p}\subsetneqq R$ dann und nur dann ein Primideal ist, wenn für beliebige Ideale $\mathfrak{a},\mathfrak{b}\subset R$ gilt

$$\mathfrak{ab}\subset\mathfrak{p} \implies (\mathfrak{a}\subset\mathfrak{p} \text{ oder } \mathfrak{b}\subset\mathfrak{p}).$$

Lösung: „nur dann“: Sei $\mathfrak{p}$ ein solches Ideal. Für alle $a, b \in R$ mit $ab \in \mathfrak{p}$ gilt dann $(a)(b) = (ab) \subset \mathfrak{p}$ und folglich $(a) \subset \mathfrak{p}$ oder $(b) \subset \mathfrak{p}$, also $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Somit ist $\mathfrak{p}$ ein Primideal.

„dann“: Sei $\mathfrak{p}$ ein Primideal. Betrachte Ideale $\mathfrak{a}, \mathfrak{b} \subset R$ mit $\mathfrak{ab} \subset \mathfrak{p}$ und $\mathfrak{a} \not\subset \mathfrak{p}$ und $\mathfrak{b} \not\subset \mathfrak{p}$. Wähle $a \in \mathfrak{a} \setminus \mathfrak{p}$ und $b \in \mathfrak{b} \setminus \mathfrak{p}$. Dann ist $ab \in \mathfrak{ab} \subset \mathfrak{p}$ mit $a, b \notin \mathfrak{p}$, was der Definition von Primideal widerspricht.

3. (a) Zeige, dass jeder endliche Integritätsbereich ein Körper ist.

   (b) Sei R ein Ring und I ein Primideal von R mit endlichem Faktorring R/I. Folgere aus (a), dass I ein maximales Ideal von R ist.

   Lösung:

   (a) Sei R ein endlicher Integritätsbereich. Wir beweisen, dass jedes Element $a \in R \setminus \{0\}$ ein multiplikatives Inverses hat. Betrachte dazu die Abbildung

   $$r_a : \begin{array}{ccc} R & \longrightarrow & R \\ x & \longmapsto & xa \end{array} .$$

   Sie ist injektiv, denn aus $x_1 a = x_2 a$ folgt $x_1 = x_2$, da R ein Integritätsbereich ist. Wegen der Endlichkeit von R ist darum r_a auch surjektiv. Deshalb finden wir ein $b \in R$ mit $ba = ab = 1$. Somit hat jedes $0 \neq a \in R$ ein multiplikatives Inverses. Zudem ist $1 \neq 0$, da dies in Integritätsbereichen vorausgesetzt ist. Daher ist R ist ein Körper.

   (b) Da I ein Primideal von R ist, ist R/I ein Integritätsbereich, der nach Voraussetzung endlich ist. Nach (a) ist darum R/I ein Körper, also ist I ein maximales Ideal von R.

4. Sei R der Ring der stetigen Funktionen $f : [0, 1] \to \mathbb{R}$.

   (a) Hat R Nullteiler?

   (b) Zeige, dass R überabzählbar viele maximale Ideale hat.

   *(c) Bestimme alle maximale Ideale von R.

   **(d) Sind die maximale Ideale von R Hauptideale? Sind sie endlich erzeugt?

Lösung:

(a) Der Ring R enthält Nullteiler; zum Beispiel ist das Produkt der beiden von Null verschiedenen stetigen Funktionen

$$f(x) = \begin{cases} \frac{1}{2} - x\,, & 0 \leqslant x \leqslant \frac{1}{2} \\ 0\,, & \frac{1}{2} \leqslant x \leqslant 1 \end{cases}$$
$$g(x) = \begin{cases} 0\,, & 0 \leqslant x \leqslant \frac{1}{2} \\ \frac{1}{2} - x\,, & \frac{1}{2} \leqslant x \leqslant 1 \end{cases}$$

gleich 0.

(b) Wir zeigen, dass für jedes $a \in [0,1]$ die Teilmenge $\mathfrak{m}_a = \{f \in R \mid f(a) = 0\}$ von R ein maximales Ideal ist. Betrachte dazu die Abbildung

$$\varphi_a : \begin{array}{ccc} R & \longrightarrow & \mathbb{R} \\ f & \longmapsto & f(a) \end{array}.$$

Sie ist ein Ringhomomorphismus und klarerweise surjektiv, da für jedes $y \in \mathbb{R}$ eine stetige Funktion $f : [0,1] \to \mathbb{R}$ mit $f(a) = y$ existiert, nämlich zum Beispiel die konstante Funktion. Weiter gilt $\ker \varphi_a = \mathfrak{m}_a$ nach Definition von $\mathfrak{m}_a$. Nach dem Homomorphiesatz ist darum $\mathfrak{m}_a$ ein Ideal mit $R/\mathfrak{m}_a \cong \mathbb{R}$. Da $\mathbb{R}$ ein Körper ist, folgt daraus, dass $\mathfrak{m}_a$ ein maximales Ideal von R ist.

Für $a \neq b$ in $[0,1]$ ist $\mathfrak{m}_a \neq \mathfrak{m}_b$, da eine stetige Funktion $f : [0,1] \to \mathbb{R}$ mit $f(a) = 0$ und $f(b) \neq 0$ existiert, die also in $\mathfrak{m}_a$ und nicht in $\mathfrak{m}_b$ liegt. Somit bilden die $\mathfrak{m}_a$ für $a \in [0,1]$ überabzählbar viele maximale Ideale von R.

(c) Sei $\mathfrak{m} \subset R$ ein von allen $\mathfrak{m}_a$ verschiedenes maximales Ideal. Für jedes $a \in [0,1]$ gilt dann $\mathfrak{m} \not\subset \mathfrak{m}_a$, denn sonst würde $\mathfrak{m} \subsetneqq \mathfrak{m}_a \subsetneqq (1)$ der Maximalität von $\mathfrak{m}$ widersprechen. Also existiert eine stetige Funktion $f_a \in \mathfrak{m}$ mit $f_a(a) \neq 0$. Wegen der Stetigkeit existiert eine Umgebung $a \in U_a \subset [0,1]$ mit $\forall x \in U_a \colon f_a(x) \neq 0$. Diese U_a für alle $a \in [0,1]$ bilden eine offene Überdeckung von $[0,1]$. Wegen der Kompaktheit existiert eine endliche Teilüberdeckung $[0,1] = \bigcup_{i=1}^{n} U_{a_i}$. Setze $f := \sum_{i=1}^{n} f_{a_i}^2$. Diese Funktion ist wieder stetig, also ein Element von R. Ausserdem ist $f(x) > 0$ für alle $x \in [0,1]$. Somit ist die Funktion $x \mapsto \frac{1}{f(x)}$ wohldefiniert und stetig; also ist $f \in R^\times$. Nach Konstruktion ist aber $f \in \mathfrak{m}$, also auch $1 \in \mathfrak{m}$, was der Voraussetzung an $\mathfrak{m}$ widerspricht. Somit sind die Ideale $\mathfrak{m}_a$ für alle $a \in [0,1]$ genau die maximalen Ideale von R.

5. Sei R ein Hauptidealring. Zeige, dass jedes von Null verschiedene Primideal in R maximal ist.

Lösing: Let $(\pi) \subset R$ be a non-zero prime ideal, and let $(a) \subset R$ be an ideal containing (π). Then $\pi \in (a)$ implies that $\pi = xa$ for some $x \in R$. From the Vorlesung we know that π is a prime element in R. Since PIDs are factorial, this

means that π is irreducible. Therefore we have $x \in R^\times$ or $a \in R^\times$. In the first case, we have $p \sim a$ and hence $(\pi) = (a)$. Otherwise we have $(a) = (1) = R$. Therefore every ideal containing (π) is equal to (π) or all of R, and we've shown that (π) is maximal.

6. Im Ring $R := \mathbb{Z}[i\sqrt{5}] \subset \mathbb{C}$ gilt die Gleichheit

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Zeige:

(a) Die Funktion $N\colon R \to \mathbb{Z}^{\geqslant 0}, z = a + bi\sqrt{5} \mapsto |z|^2 = a^2 + 5b^2$ ist multiplikativ (das heisst, $\forall \alpha, \beta \in R : N(\alpha\beta) = N(\alpha)N(\beta)$).

(b) $R^\times = \{u \in R \mid N(u) = 1\} = \{\pm 1\}$.

(c) Die Elemente $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ sind unzerlegbar in R.

(d) Die Elemente $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ sind keine Primelemente in R.

(e) Für das Ideal $I = (2, 1 + i\sqrt{5})$ gilt $I \cdot I = (2)$.

(f) I ist kein Hauptideal von R.

(g) I ist ein maximales Ideal von R.

(h) R ist nicht faktoriell.

Lösung:

(a) Für alle $\alpha \in R$ gilt $N(\alpha) = |\alpha|^2$, wobei $|\ |$ den gewöhnlichen komplexen Absolutbetrag bezeichnet. Für alle $\alpha, \beta \in R$ folgt daraus $N(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2|\beta|^2 = N(\alpha)N(\beta)$, wie gewünscht.
Variante: Seien $\alpha = a_1 + a_2 i\sqrt{5}$ und $\beta = b_1 + b_2 i\sqrt{5} \in R$. Dann ist

$$\begin{aligned} N(\alpha\beta) &= N(a_1b_1 - 5a_2b_2 + (a_1b_2 + a_2b_1)i\sqrt{5}) \\ &= (a_1b_1 - 5a_2b_2)^2 + 5(a_1b_2 + a_2b_1)^2 \\ &= a_1^2b_1^2 + 25a_2^2b_2^2 + 5a_1^2b_2^2 + 5a_2^2b_1^2 \\ &= (a_1^2 + 5b_1^2)(b_1^2 + 5b_2^2) \\ &= N(a_1 + a_2 i\sqrt{5})N(b_1 + b_2 i\sqrt{5}) = N(\alpha)N(\beta). \end{aligned}$$

(b) Betrachte eine Einheit $u = a + bi\sqrt{5} \in R$. Da N multiplikativ ist, gilt $N(u^{-1}) \cdot N(u) = N(u^{-1}u) = N(1) = 1$. Wegen $N(u^{-1}), N(u) \in \mathbb{Z}^{\geqslant 0}$ muss daher $N(u) = a^2 + 5b^2 = 1$ sein. Daraus folgt sofort $b = 0$ und $a^2 = 1$, also $u = a = \pm 1$. Umgekehrt gilt für jedes Element $u = a + bi\sqrt{5} \in R$ mit $a^2 + 5b^2 = 1$ auch $(a + bi\sqrt{5})(a - bi\sqrt{5}) = 1$, also ist u eine Einheit in R.

(c) Falls $2 = \alpha\beta$ mit $\alpha, \beta \in R$ ist, folgt $4 = N(2) = N(\alpha)N(\beta)$. Wenn α und β keine Einheiten sind, ist $N(\alpha), N(\beta) > 1$ nach (b). Es gibt dann nur die Möglichkeit $N(\alpha) = N(\beta) = 2$. Diese kann aber nicht auftreten, da 2 wegen $a^2+5b^2 \neq 2$ für alle $a, b \in \mathbb{Z}$ nicht im Bild von N liegt. Somit ist 2 unzerlegbar in R.

Wegen $a^2 + 5b^2 \neq 3$ für alle $a, b \in \mathbb{Z}$ liegt auch 3 nicht im Bild von N. Wegen $N(3) = 9 = 3 \cdot 3$ folgt darum analog, dass 3 unzerlegbar in R ist.

Falls $1 + i\sqrt{5} = \alpha\beta$ mit $\alpha, \beta \in R$ ist, folgt $6 = N(1 + i\sqrt{5}) = N(\alpha)N(\beta)$. Wenn α und β keine Einheiten sind, dann müssen $N(\alpha), N(\beta) \in \{2, 3\}$ sein. Dies ist wiederum nicht möglich, da 2 und 3 nicht im Bild von N liegen. Daher ist $1 + i\sqrt{5}$ unzerlegbar. Mit der gleichen Argumentation folgt auch die Unzerlegbarkeit von $1 - i\sqrt{5}$.

(d) Wegen der Gleichheit $6 = 2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$ sind 2 und 3 Teiler von $(1+i\sqrt{5}) \cdot (1-i\sqrt{5})$ und $1+i\sqrt{5}$ und $1-i\sqrt{5}$ Teiler von $2 \cdot 3$. Keines der vier Elemente ist aber ein Teiler eines anderen, weil sie nach (c) unzerlegbar sind, sich aber nach (b) nicht um Einheiten unterscheiden, da sie vershiedene Bilder unter N haben.

(e) Durch Multiplikation der Erzeuger erhalten wir

$$I \cdot I = (2, 1 + i\sqrt{5})(2, 1 + i\sqrt{5}) = (4, 2 + 2i\sqrt{5}, -4 + 2i\sqrt{5}).$$

Da $(2) = \{2a + 2bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ ist, haben wir $4, 2 + 2i\sqrt{5}, -4 + 2i\sqrt{5} \in (2)$ und daher $I \cdot I \subset (2)$. Umgekehrt ist

$$2 = (2 + 2i\sqrt{5}) - (-4 + 2i\sqrt{5}) - 4 \in I \cdot I.$$

Somit gilt $(2) = I \cdot I$.

(f) Wir nehmen an, dass I ein Hauptideal ist, d.h. $I = (2, 1 + i\sqrt{5}) = (\alpha)$ für ein $\alpha \in R$. Dann ist $2 = x\alpha$ für ein $x \in R$. Wegen der Unzerlegbarkeit von 2 ist entweder $x \in R^\times$ oder $\alpha \in R^\times$. Im ersten Fall ist 2 assoziiert zu α, also $(2) = (\alpha) = (2, 1 + i\sqrt{5})$. Dies ist ein Widerspruch, da $1 + i\sqrt{5}$ nicht in (2) liegt.

Es bleibt nur der Fall $\alpha \in R^\times$ übrig, in dem $I = (\alpha) = R$ ist. Auch dieser Fall kann nach (e) wegen des Widerspruchs

$$R = R \cdot R = I \cdot I = (2) \neq R$$

nicht auftreten. Somit ist I kein Hauptideal.

(g) Aus (f) folgt bereits, dass $I \neq (1)$, also ein echtes Ideal ist. Betrachte ein echt grösseres Ideal $I \subsetneq I' \subset R$ und wähle ein Element $a + bi\sqrt{5} \in I' \setminus I$. Die Rechnung $a + bi\sqrt{5} = (a - b) + b \cdot (1 + i\sqrt{5})$ zeigt dann, dass $a - b \notin I$ ist. Wegen $\mathbb{Z} \cap I = 2\mathbb{Z}$ bedeutet dies, dass $a - b$ ungerade ist. Also ist

$$1 = (a + bi\sqrt{5}) - \tfrac{a-b-1}{2} \cdot 2 - b \cdot (1 + i\sqrt{5}) \in (a + bi\sqrt{5}) + I \subset I'.$$

Somit ist $I' = (1)$; und deshalb ist I maximal.

(h) Mögliche Lösungen sind:

- Aus (c) und (d) folgt, dass in R unzerlegbare Elemente existieren, die nicht prim sind. Daher ist R nicht faktoriell.
- Die Gleichung $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ ergibt nach (c) zwei Zerlegungen von 6 in unzerlegbare Elemente. Bei (d) haben wir festgestellt, dass $2, 3 \nmid 1 \pm i\sqrt{5}$ und $1 \pm i\sqrt{5} \nmid 2, 3$ gilt. Daher sind $2, 3$ nicht zu $1 \pm i\sqrt{5}$ assoziiert und die beiden obigen Zerlegungen sind nicht zueinander assoziiert. Deshalb kann R nicht faktoriell sein.

7. Die Brüder Dmitrij, Iwan und Alexej Karamasow leben in einem Studentenwohnheim. Dmitrij hat sich angewöhnt alle 5, Iwan alle 7 und Alexej alle 11 Tage eine Pizza zu essen. Die erste Pizza des Jahres 2015 essen Dmitrij und Alexej am 3.1. und Iwan am 4.1. An welchem Tag werden sie erstmals alle drei gemeinsam eine Pizza essen?

   Lösung: Sei $x \in \mathbb{Z}^{\geqslant 0}$ die Anzahl Tage, die seit dem 3. Januar vergangen sind, wenn erstmals alle drei gemeinsam eine Pizza essen. Nach Aufgabenstellung ist x die kleinste nicht-negative ganze Zahl, die das folgende Restsystem löst:

$$\begin{aligned} x &\equiv 0 \pmod 5 \\ x &\equiv 0 \pmod{11} \\ x &\equiv 1 \pmod 7 \end{aligned}$$

   Da 5, 7 und 11 paarweise teilerfremd sind, wissen wir nach dem Chinesischen Restsatz, dass dieses System genau eine Lösung x modulo $5 \cdot 7 \cdot 11 = 385$ hat. Nach den ersten beiden Gleichungen ist diese durch 5 und 11 teilbar, also ein Vielfaches von 55. Von den Vielfachen k von 55 mit $0 \leqslant k < 385$ ist 330 auch Lösung der dritten Gleichung. Somit essen erstmals am 330. Tag nach dem 3. Januar, also am 29. November 2015, alle drei zusammen eine Pizza.

**8. Bestimme die Anzahl der irreduziblen normierten Polynome vom Grad n in $\mathbb{F}_p[X]$.