D-MATH | Algebra I | HS 2015
Prof. Richard Pink

Musterlösung 3

Faktorielle Ringe, Grösster gemeinsamer Teiler, Ideale, Faktorringe

1. Sei K ein Körper. Zeige, dass $K[X^2, X^3] \subset K[X]$ ein Integritätsbereich, aber nicht faktoriell ist.

   Lösung: Wir betrachten die beiden Zerlegungen

   $$(X^2)^3 = (X^3)^2$$

   von $X^6 \in R := K[X^2, X^3]$ und zeigen, dass X^2 und X^3 irreduzible Elemente von R sind.

   Die Elemente X^2 und X^3 sind keine Einheiten von R, da alle Einheiten von R auch Einheiten in $K[X]$ sind und daher $R^\times = K^\times = K[X]^\times$ gilt. Falls $X^2 = g \cdot h$ oder $X^3 = g \cdot h$ für $g, h \in R \smallsetminus R^\times$ gilt, müssen g oder h Grad 1 haben. Jedoch sind alle Elemente von R von der Form $p(X^2, X^3)$ für ein $p \in K[X]$. Darum enthält R keine Polynome vom Grad 1 und obige Zerlegungen von X^2 und X^3 können nicht existieren. Daher sind X^2 und X^3 irreduzibel in R.

   Somit haben wir zwei Zerlegungen von X^6 in irreduzible Elemente mit einer unterschiedlichen Anzahl Faktoren gefunden. Dies ist in faktoriellen Ringen nicht möglich. Deshalb ist R nicht faktoriell.

2. Sei R ein faktorieller Ring.

   (a) Seien $a, b, c \in R$. Zeige:

   $$c|ab,\ \mathrm{ggT}(a, c) \sim 1 \Longrightarrow c|b.$$

   (b) Sei $u \in R^\times$, und seien $p_1, \ldots, p_n$ Primelemente von R. Zeige, dass die Teiler von $up_1 \cdots p_n$ genau die Elemente der Form $v \cdot \prod_{i \in I} p_i$ sind für alle $v \in R^\times$ und alle Teilmengen $I \subset \{1, \ldots, n\}$.

   Lösung:

   (a) Suppose first that $c = 0$. If $b = 0$, then $c|b$ and we are done. Otherwise $c|ab$ implies $ab = 0$, and since $b \neq 0$ and R is an integral domain, it follows that $a = 0$. But then $\mathrm{ggT}(a, c) = \mathrm{ggT}(0, 0) = 0 \neq 1$, contradiction, so the case does not occur.

   Now suppose that $c \neq 0$. We write $c = up_1 \cdots p_n$ with $u \in R^\times$ and primes $p_i \in R$ and proceed by induction on n.

If $n = 0$, then $u \cdot (u^{-1}b) = b$ shows that $c = u$ divides b, as desired. Otherwise $p_n|c|ab$ implies that $p_n|ab$ and hence $p_n|a$ or $p_n|b$. In the case $p_n|a$ it follows that $p_n| \operatorname{ggT}(a, c) \sim 1$ and hence $p_n|1$, a contradiction. Thus $p_n|b$. Write $b = b'p_n$ and $c' := up_1...p_{n-1}$. The fact that $c|ab$ means that $xc = ab$ for some $x \in R$. Thus we have $xc'p_n = ab'p_n$, and canceling the factor $p_n \neq 0$ implies that $xc' = ab'$. Therefore $c'|ab'$. Also, $\operatorname{ggT}(a, c')$ is a common divisor of a and c' and hence of c; so it is a divisor of $\operatorname{ggT}(a, c)$. Since $\operatorname{ggT}(a, c) \sim 1$, it follows that $\operatorname{ggT}(a, c') \sim 1$. The induction hypothesis for $n - 1$ in place of n thus shows that $c'|b'$. This means that $yc' = b'$ for some $y \in R$; hence $yc = yc'p_n = b'p_n = b$ and thus $c|b$, as desired.

(b) Let $a := up_1...p_n$. If $d := v \cdot \prod_{i \in I} p_i$ is as stated in the exericse, then

$$d \cdot uv^{-1} \prod_{j \in I^c} p_j = a$$

and so $d|a$.

Conversely, let d be a divisor of a. Then there exists an $x \in R$ such that $dx = a$. Since R is factorial, we can write $d = tq_1...q_r$ and $x = wq_{r+1}...q_{r+s}$, where $t, w \in R^\times$, and the q_i are primes. Thus we have

$$a = up_1...p_n = twq_1...q_{r+s}.$$

By the uniqueness of the factorization of a, we have $r + s = n$, and there exists a permutation $\sigma \in S_n$ such that $\forall i : p_{\sigma i} \sim q_i$. For each i, let $u_i \in R^\times$ be such that $u_i p_{\sigma i} = q_i$. Then, with $v := tu_1...u_r$, we have

$$d = v \cdot p_{\sigma 1}...p_{\sigma r},$$

so d is of the desired form.

3. Betrachte Elemente $a_1, \ldots, a_n$ eines faktoriellen Rings R. Ein Element $b \in R$ mit $\forall i$: $a_i|b$ heisst *gemeinsames Vielfaches von* $a_1, \ldots, a_n$.

   (a) Zeige, dass es ein gemeinsames Vielfaches b von $a_1, \ldots, a_n$ existiert, so dass für jedes gemeinsame Vielfache b' von $a_1, \ldots, a_n$ gilt $b|b'$.

   (b) Zeige, dass dieses *kleinste gemeinsame Vielfache von* $a_1, \ldots, a_n$ eindeutig bis auf Assoziiertheit ist. Wir bezeichnen jedes solche mit $\operatorname{kgV}(a_1, \ldots, a_n)$.

   (c) Zeige, dass $\operatorname{ggT}(a_1, a_2) \cdot \operatorname{kgV}(a_1, a_2) \sim a_1 \cdot a_2$ gilt.

Lösung: If there exists an i such that $a_i = 0$, then the only common multiple of $a_1, ..., a_n$ is 0, and hence everything holds with $\operatorname{kgV}(a_1, \ldots, a_n) = 0$. Thus we assume that all of the a_i are non-zero.

Choose a system of representatives $\{p_i \mid i \in I\}$ with respect to $\sim$ of the prime elements of R.

(a) Since R is factorial, we can write each a_j uniquely as a product $u_j \prod_i' p_i^{\mu_{ji}}$ with $u_j \in R^\times$ and $\mu_{ji} \geqslant 0$. For each i, set $\mu_i := \max\{\mu_{ji} \mid 1 \leqslant j \leqslant n\}$. Let $b := \prod_i' p_i^{\mu_i}$. By part (b) of the last theorem of §2.2 of the Zusammenfassung b is a multiple of each a_j.

Conversely consider any common multiple b' of the a_i. If $b' = 0$, we already have $b|b'$. Otherwise write $b' = v \prod_i' p_i^{\nu_i}$ with $v \in R^\times$. Then by the same theorem, $a_j|b$ is equivalent to $\mu_{ji} \leqslant \nu_i$ for all i. Thus $\mu_i \leqslant \nu_i$ for all i, and by the same theorem again $b|b'$. Therefore b is a least common multiple of the a_i.

(b) Let $b, b' \in R$ be least common multiples of $a_1, ..., a_n$. The fact that b' satisfies the property in (a) implies that $b'|b$. Similarly $b|b'$, and thus $b \sim b'$.

(c) Write $a_j = u_j \prod_i' p_i^{\mu_{ji}}$ as in (a). In the Vorlesung and in (a) we have seen that

$$\begin{aligned} \mathrm{ggT}(a_1, a_2) &\sim \textstyle\prod_i' p_i^{\min(\mu_{1i},\mu_{2i})}, \\ \mathrm{kgV}(a_1, a_2) &\sim \textstyle\prod_i' p_i^{\max(\mu_{1i},\mu_{2i})}. \end{aligned}$$

Thus

$$\mathrm{ggT}(a_1, a_2)\cdot\mathrm{kgV}(a_1, a_2) \sim \textstyle\prod_i' p_i^{\min(\mu_{1i},\mu_{2i})+\max(\mu_{1i},\mu_{2i})} = \prod_i' p_i^{\mu_{1i}+\mu_{2i}} \sim a_1 \cdot a_2,$$

as desired.

4. Zeige, dass für alle Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ und alle Elemente x, y eines Rings R gilt

(a) $(x)(y) = (xy)$

(b) $\mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{b})\mathfrak{c}$

(c) $(x) \cdot ((y) \cdot \mathfrak{a}) = (xy) \cdot \mathfrak{a}$

Lösung:

(a) Let $r \in (x)(y)$. Then $r = \sum_{i=1}^n x_i y_i$ with $x_i \in (x)$ and $y_i \in (y)$. Write $x_i = a_i x$ and $y_i = b_i y$ for $a_i, b_i \in R$. We have

$$r = \sum_{i=1}^n (a_i x) \cdot (b_i y) = \sum_{i=1}^n (a_i b_i) \cdot xy = (\sum_{i=1}^n a_i b_i) \cdot xy,$$

and so $r \in (xy)$. Thus the inclusion "$\subset$ " holds.

For $r \in (xy)$ we have $r = axy = ax \cdot y$ for some $a \in R$, from which we see that $r \in (x)(y)$, and the inclusion " $\supset$ " holds.

(b) Let $x \in \mathfrak{a}(\mathfrak{b}\mathfrak{c})$. Then $x = \sum_{i=1}^n a_i d_i$ where $a_i \in \mathfrak{a}$ and $d_i \in \mathfrak{b}\mathfrak{c}$. Similarly each $d_i = \sum_{j=1}^{m_i} b_{i,j} c_{i,j}$ with $b_{i,j} \in \mathfrak{b}$ and $c_{i,j} \in \mathfrak{c}$. Hence we have

$$x = \sum_{i=1}^n a_i d_i = \sum_{i=1}^n a_i (\sum_{j=1}^{m_i} b_{i,j} c_{i,j}) = \sum_{i=1}^n \sum_{j=1}^{m_i} (a_i b_{i,j}) c_{i,j}.$$

Now $(a_i b_{i,j})c_{i,j} \in (\mathfrak{a}\mathfrak{b})\mathfrak{c}$ for each i. Since ideals are closed under addition, we see that $x \in (\mathfrak{a}\mathfrak{b})\mathfrak{c}$. We have thus shown the inclusion "$\subset$." The argument for "$\supset$ " is analogous.

(c) Using first (b) and then (a) implies $(x) \cdot ((y) \cdot \mathfrak{a}) = ((x) \cdot (y)) \cdot \mathfrak{a} = (xy) \cdot \mathfrak{a}$.

5. Sei R ein Ring. Ein Element $x \in R$ heisst *nilpotent*, falls ein $n \geqslant 1$ mit $x^n = 0$ existiert. Beweise oder widerlege:

(a) Die Menge der Nullteiler von R zusammen mit 0 ist ein Ideal von R.

(b) Die Menge I der nilpotenten Elemente von R ist ein Ideal von R.

*(c) Zeige: Für I wie in (b) enthält der Faktorring R/I ausser 0 keine nilpotenten Elemente.

Lösung:

(a) Im Ring $R := \mathbb{Z} \times \mathbb{Z}$ gilt $(1,0) \cdot (0,1) = (0,0) = 0_R$. Deshalb sind $(1,0)$ und $(0,1)$ Nullteiler von R. Jedoch ist $1_R = (1,1) = (1,0) + (0,1)$ als Einselement kein Nullteiler von R. Darum ist die Menge der Nullteiler von R zusammen mit 0 nicht additiv abgeschlossen. Sie ist also kein Ideal von R und die Aussage ist widerlegt.

(b) Seien $a, b \in R$ nilpotent. Dafür gibt es $n, m \geqslant 1$ mit $a^n = b^m = 0$. Da R kommutativ ist, gilt

$$(a-b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} (-1)^{n+m-k} a^k b^{n+m-k}.$$

Nach Voraussetzung ist aber $a^k = 0$ für $n \leqslant k \leqslant n+m$ und $b^{n+m-k} = 0$ für $0 \leqslant k \leqslant n$. Deshalb ist $(a-b)^{n+m} = 0$ und $a - b$ nilpotent. Somit ist die Menge I der nilpotenten Elemente von R eine additive Untergruppe von R. Weiter ist für $r \in R$ und $a \in I$ mit $a^n = 0$

$$(ra)^n = r^n a^n = 0,$$

also $ra \in I$. Somit ist I ein Ideal von R und die Aussage bewiesen.

(c) Da I ein Ideal von R ist, existiert der Faktorring R/I. Sei $x + I$ ein nilpotentes Element von R/I. Dafür gibt es ein $n \geqslant 1$ mit

$$(x + I)^n = x^n + I = I.$$

Deshalb ist $x^n \in I$, es gibt also ein $m \geqslant 1$ mit $(x^n)^m = x^{nm} = 0$. Es folgt, dass x als nilpotentes Element von R in I liegt. Somit ist $x + I = I = 0_{R/I}$ das einzige nilpotente Element von R/I.

6. Betrachte einen Ringhomomorphismus $\varphi\colon R \to S$ und ein Ideal $\mathfrak{b} \subset S$. Zeige, dass $\mathfrak{a} := \varphi^{-1}(\mathfrak{b}) := \{a \in R \mid \varphi(a) \in \mathfrak{b}\}$ ein Ideal von R ist und dass φ einen injektiven Ringhomomorphismus $R/\mathfrak{a} \hookrightarrow S/\mathfrak{b}$ induziert.

   Lösung: Since $0 \in \mathfrak{b}$ and $\varphi(0) = 0$, we have $0 \in \mathfrak{a}$, and it follows that $\mathfrak{a} \neq \varnothing$.

   Let $a_1, a_2 \in \mathfrak{a}$. Then there exist $b_1, b_2 \in \mathfrak{b}$ such that $\varphi(a_1) = b_1$ and $\varphi(a_2) = b_2$. Since φ is a homomorphism and $\mathfrak{b}$ is an ideal, we have $\varphi(a_1+a_2) = \varphi(a_1)+\varphi(a_2) = b_1 + b_2 \in \mathfrak{b}$. Therefore $a_1 + a_2 \in \mathfrak{a}$, and $\mathfrak{a}$ is closed under addition.

   The fact that φ is a homomorphism also implies that for all $x \in R$ and $a \in \mathfrak{a}$, we have $\varphi(xa) = \varphi(x)\varphi(a) \in \mathfrak{b}$, since $\varphi(a) \in \mathfrak{b}$ and $\mathfrak{b}$ is an ideal. We have thus shown that $\mathfrak{a}$ is an ideal in R.

   Let ψ denote the composite of φ with the factor map $S \to S/\mathfrak{b}$. Then for any $x \in R$ we have $\psi(x) = \varphi(x) + \mathfrak{b} = 0 + \mathfrak{b} = \mathfrak{b}$ if and only if $\varphi(x) \in \mathfrak{b}$, that is, if and only if $x \in \mathfrak{a}$. Thus $\ker(\psi) = \mathfrak{a}$. By the universal property of $R/\mathfrak{a}$ the homomorphism ψ factors through a unique homomorphism $\bar{\psi}\colon R/\mathfrak{a} \to S/\mathfrak{b}$.

$$
\begin{tikzcd}
\mathfrak{a} \arrow[d, phantom, "\cap"] & \mathfrak{b} \arrow[d, phantom, "\cap"] \\
R \arrow[r, "\varphi"] \arrow[d] \arrow[dr, "\psi"] & S \arrow[d] \\
R/\mathfrak{a} \arrow[r, "\bar{\psi}"] & S/\mathfrak{b}
\end{tikzcd}
$$

   For any $x \in R$ we have $x + \mathfrak{a} \in \ker(\bar{\psi})$ if and only if $\bar{\psi}(x + \mathfrak{a}) = \psi(x) = 0$ if and only if $x \in \ker(\psi) = \mathfrak{a}$ if and only if $x + \mathfrak{a} = 0 + \mathfrak{a}$. Thus $\ker(\bar{\psi}) = 0$ and hence $\bar{\psi}$ is injective.