WS 05/06
Priv.-Doz. Dr. S. Wewers
Andreas Martin

Algebra I

8. Übungsblatt

Aufgabe 1: (1+1+1/2+1/2+1=4 P) Sei R ein faktorieller Ring. Wir bezeichnen mit $P \subset R$ ein Vertretersystem der Assoziiertenklassen aller Primelemente (d.h. für jedes Primelement $p \in R$ existiert ein eindeutiges Element $p' \in P$ mit $p \sim p'$). Für Elemente $a, b \in R - \{0\}$ setzen wir

$$\mathrm{ggT}(a,b) := \prod_{p \in P} p^{\min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\}},$$
$$\mathrm{kgV}(a,b) := \prod_{p \in P} p^{\max\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\}}.$$

Seien $a, b, c \in R - \{0\}$. Zeigen Sie:

(a) Die Assoziiertenklassen von $\mathrm{ggT}(a,b)$ und $\mathrm{kgV}(a,b)$ hängen nicht von der Wahl des Vertretersystems P ab.

(b) $a|b \iff \mathrm{ord}_p(a) \le \mathrm{ord}_p(b) \;\; \forall\, p \in P$,

(c) $c|a$ und $c|b \iff c|\mathrm{ggT}(a,b)$,

(d) $a|c$ und $b|c \iff \mathrm{kgV}(a,b)|c$.

(e) Bestimmen Sie den ggT der Polynome

$$f = 10X - 15, \; g = 15X - 6$$

in dem Ring $\mathbb{Z}[X]$ (bis auf Assoziiertheit).

Lösung:

(b) Es seien zunächst $x, y \in R \setminus \{0\}$ beliebig. Dann gibt es Einheiten $u, v \in R^\times$ so, daß

$$x \;=\; u \cdot \prod_{p \in P} p^{\mathrm{ord}_p(x)} \;, \quad x \;=\; v \cdot \prod_{p \in P} p^{\mathrm{ord}_p(y)} \;.$$

Es folgt

$$xy \;=\; uv \cdot \prod_{p \in P} p^{\mathrm{ord}_p(x) + \mathrm{ord}_p(y)}$$

und $uv \in R^\times$. Wegen der Eindeutigkeit der Primfaktorzerlegung gilt also

$$\mathrm{ord}_p(xy) \;=\; \mathrm{ord}_p(x) + \mathrm{ord}_p(y) \;, \forall p \in P \;.$$

Es gelte nun $a|b$. Dann gibt es ein $c \in R \setminus \{0\}$ so, daß $ac = b$. Es folgt

$$\mathrm{ord}_p(b) \;=\; \mathrm{ord}_p(ac) \;=\; \mathrm{ord}_p(a) + \mathrm{ord}_p(c) \ge \mathrm{ord}_p(a) \;, \forall p \in P \;.$$

Es gelte nun umgekehrt $\mathrm{ord}_p(a) \ge \mathrm{ord}_p(b)$ für alle $p \in P$. Dann ist

$$a \cdot \prod_{p \in P} p^{\mathrm{ord}_p(b) - \mathrm{ord}_p(a)} \;\sim\; \prod_{p \in P} p^{\mathrm{ord}_p(b)} \;\sim\; b \;,$$

und daraus folgt $a|b$.

(c) Es gilt nach (b)

$$\begin{aligned} c|a \text{ und } c|b &\iff \operatorname{ord}_p(c) \le \operatorname{ord}_p(a) \text{ und } \operatorname{ord}_p(c) \le \operatorname{ord}_p(b),\ \forall p \in P \\ &\iff \operatorname{ord}_p(c) \le \min\{\operatorname{ord}_p(a), \operatorname{ord}_p(b)\},\ \forall p \in P \\ &\iff \operatorname{ord}_p(c) \le \operatorname{ord}_p(\operatorname{ggT}(a,b)),\ \forall p \in P \\ &\iff c|\operatorname{ggT}(a,b)\ . \end{aligned}$$

(d) Es gilt nach (b)

$$\begin{aligned} a|c \text{ und } b|c &\iff \operatorname{ord}_p(c) \ge \operatorname{ord}_p(a) \text{ und } \operatorname{ord}_p(c) \ge \operatorname{ord}_p(b),\ \forall p \in P \\ &\iff \operatorname{ord}_p(c) \ge \max\{\operatorname{ord}_p(a), \operatorname{ord}_p(b)\},\ \forall p \in P \\ &\iff \operatorname{ord}_p(c) \ge \operatorname{ord}_p(\operatorname{kgV}(a,b)),\ \forall p \in P \\ &\iff \operatorname{kgV}(a,b)|c\ . \end{aligned}$$

(a) Es sei P' ein weiteres Vertretersystem der Assoziiertenklassen aller Primelemente von R. Es seien $g := \operatorname{ggT}(a,b)$ und $k := \operatorname{kgV}(a,b)$ mittels P gebildet, und es seien g' und k' die entsprechenden Objekte mittels P' gebildet. Zu zeigen: $g \sim g'$ und $k \sim k'$. Nach (c) gilt $g|a$ und $g|b$. Daraus folgt nach (c) $g|g'$. Ebenso gilt nach (c) $g'|a$ und $g'|b$. Wiederum nach (c) folgt daher $g'|g$. Also gilt $g|g'$ und $g'|g$, woraus $g \sim g'$ folgt. Eine analoge Argumentation zeigt, daß $k \sim k'$ gilt.

(e) Es gilt

$$f \;=\; 5 \cdot (2X - 3)\ ,\quad g \;=\; 3 \cdot (5X - 2)\ .$$

Nun sind 5 und 3 Primelemente in $\mathbb{Z}$, also auch in $\mathbb{Z}[X]$. Ferner sind die Polynome $2X - 3$ und $5X - 2$ primitiv in $\mathbb{Z}[X]$ und irreduzibel in $\mathbb{Q}[X]$, da sie vom Grade 1 sind. Also handelt es sich jeweils um Primelemente in $\mathbb{Z}[X]$. Wegen $(\mathbb{Z}[X])^\times = \{\pm 1\}$ sind keine zwei dieser Primelement assoziiert. Daher besitzen f und g keine gemeinsamen Primfaktoren, d.h. wir können schreiben

$$\operatorname{ggT}(f,g) \;=\; 1\ .$$

Aufgabe 2: (1/2+1/2+1+1+1=4 P) Welches der folgenden Polynome ist irreduzibel in dem Ring $\mathbb{Q}[X,Y]$, und welches ist irreduzible in $\mathbb{C}[X,Y]$?

(a) $X^5 - 3$,

(b) $Y^4 - 4$,

(c) $X^2 + XY + Y^2$,

(d) $X^2 + Y^2 - 1$,

(e) $X^4 - 2X^2Y^2 + 1$.

Lösung:

Lemma *Ist R ein Integritätsring, und ist f ein normiertes reduzibles Polynom $f \in R[X]$ vom Grade ≥ 2, so läßt f stets eine Faktorisierung $f = gh$ in nicht-konstante normierte Polynome $g, h \in R[X]$ zu.*

Beweis: Es sei $f = gh$ eine Faktorisierung von f in Nicht-Einheiten $g, h \in R[X]$ mit führenden Koeffizienten a bzw. b. Dann folgt wegen der Normiertheit von f sogleich $ab = 1$, d.h. $a, b \in R^\times$. Dann ist $f = (bg)(ah)$ ein Faktorisierung in normierte Polynome, die dann notwendigerweise nicht-konstant sind. $\square$

(a)

- Wir zeigen, daß X^5-3 irreduzibel in $\mathbb{Z}[X]$ ist. Wir nehmen also an, daß X^5-3 in zwei normierte nicht-konstante Polynome $\in \mathbb{Z}[X]$ zerfällt, d.h. es gelte
$$X^5-3 \;=\; \left(\sum_{\nu=0}^{n} a_\nu X^\nu\right)\left(\sum_{\mu=0}^{m} b_\mu X^\mu\right)$$
mit Koeffizienten $a_\nu, b_\mu \in \mathbb{Z}$. Dabei gelte $a_n = b_m = 1$, $n,m \geq 2$ und $n+m=5$. Koeffizientenvergleich ergibt
$$-3 \;=\; a_0 b_0 \;.$$
Also können wir annehmen, daß $a_0 = \pm 3$ und $b_0 = \mp 1$ gilt. Wegen $a_n = 1$ gibt es ein $k \in \{0,\ldots,n\}$ so, daß
$$a_0 \equiv \ldots \equiv a_{k-1} \mod 3 \;, \quad a_k \not\equiv 3 \mod 3 \;.$$
Betrachtet man den Koeffizienten von X^k, so ergibt sich wegen $b_0 = \mp 1$
$$0 \;=\; \sum_{\nu+\mu=k} a_\nu b_\mu \;\equiv\; a_k b_0 \;\equiv\; a_k \mod 3 \;,$$
im Widerspruch zur Wahl von k.
- Nach Vorlesung folgt, daß X^5-3 auch irreduzibel in $\mathbb{Q}[X]$ ist. Dann ist nach Vorlesung X^5-3 auch irreduzibel in $\mathbb{Q}[X][Y] = \mathbb{Q}[X,Y]$, da $\mathbb{Q}[X]$ faktoriell ist.
- X^5-3 besitzt in $\mathbb{C}$ eine Nullstelle $\alpha := 3^{1/5}$. Also faktorisiert $X^5-3 = (X-\alpha)g$ mit einem Polynom $g \in \mathbb{C}[X]$ vom Grade 4. Daher ist X^5-3 nicht irreduzibel in $\mathbb{C}[X,Y]$.

(b) Es gilt $Y^4-4 = (Y^2-2)(Y^2+2)$. Daher ist Y^4-4 reduzibel in $\mathbb{Q}[X,Y]$ und in $\mathbb{C}[X,Y]$.

(c)

- Wir nehmen an, das Polynom X^2+XY+Y^2 wäre reduzibel in $\mathbb{Q}[X,Y] = \mathbb{Q}[Y][X]$. Also gilt
$$X^2+XY+Y^2 \;=\; (X+a)(X+b)$$
mit gewissen $a,b \in \mathbb{Q}[Y]$. Koeffizientenvergleich ergibt
$$ab \;=\; Y^2 \;,\;\; a+b \;=\; Y \;.$$
Daraus folgt $a\cdot(Y-a) = Y^2$. Also ist $a \in \mathbb{Q}[Y]$ ein Polynom vom Grade 1. Da Y Primelelement ist, folgt aus der Eindeutigkeit der Primfaktorzerlegung, daß $a \sim Y$, d.h. $a = eY$ für ein $e \in \mathbb{Q}^\times$, und $b = e^{-1}Y$. Aus $Y = a+b = (e+e^{-1})Y$ folgt dann aber $e+e^{-1} = 1$. Daraus folgt wiederum
$$0 \;=\; e(e+e^{-1}-1) \;=\; e^2-e+1 \;=\; \left(e-\frac{1}{2}\right)^2 + \frac{3}{4} \;\geq\; \frac{3}{4} \;,$$
ein Widerspruch. Also ist X^2+XY+Y^2 irreduzibel in $\mathbb{Q}[X,Y]$.
- Es sei $\alpha := \exp(2\pi\mathrm{i}/3)$ eine nicht-triviale dritte Einheitswurzel. Dann gilt
$$1+\alpha+\alpha^2 \;=\; \frac{1-\alpha^3}{1-\alpha} \;=\; 0 \;.$$
Folglich ist
$$X^2+XY+Y^2 \;=\; (X-\alpha Y)(X-\alpha^2 Y) \;,$$
und das Polynom X^2+XY+Y^2 ist nicht irreduzibel in $\mathbb{C}[X,Y]$.

(d) Wir zeigen, daß das Polynom $X^2 + Y^2 - 1$ irreduzibel in $K[X, Y]$ ist, wobei K ein beliebiger Körper sei, in dem $1 + 1 \neq 0$ gilt. Wir nehmen das Gegenteil an, d.h. es gilt

$$X^2 + Y^2 - 1 \;=\; (X + a)(X + b)$$

mit gewissen $a, b \in K[Y]$. Koeffizientenvergleich ergibt $a + b = 0$ und $ab = Y^2 - 1$. Daraus ergibt sich $b = -a$ und

$$a^2 \;=\; 1 - Y^2 \;=\; (1 - Y)(1 + Y)\;.$$

Also ist a ein Polynom in Y vom Grade 1, und die Eindeutigkeit der Primfaktorzerlegung ergibt $1 - Y \sim 1 + Y$ in $K[Y]$. Das ist jedoch unmöglich, da $1 \neq -1$.

(e)
- Wir nehmen an, das Polynom zerfalle in zwei Polynome in $\mathbb{C}[Y][X]$ vom Grade 2. Es gelte also

  $$X^4 - 2X^2Y^2 + 1 \;=\; (X^2 + aX + b)(X^2 + cX + d)$$

  mit gewissen $a, b, c, d \in \mathbb{C}[Y]$. Koeffizientenvergleich ergibt $a + c = 0$, $b + ac + d = -2Y^2$, $ad + bc = 0$ und $bd = 1$. Daraus folgt $c = -a$ und $a(d - b) = 0$. Also gilt $a = 0$ oder $b = d$. Im Falle $a = 0$ folgt wegen $b, d \in \mathbb{C}^\times$ sogleich $-2Y^2 = b - a^2 + d \in \mathbb{C}$, ein Widerspruch. Im Falle $b = d$ folgt aus $bd = 1$ sogleich $b = \pm 1$; und daher $-2Y^2 = \pm 2 - a^2$. Somit ist

  $$a^2 \;=\; 2Y^2 \pm 2 \;=\; \begin{cases} 2(Y + \mathrm{i})(Y - \mathrm{i}), & \text{falls } b = 1 \\ 2(Y + 1)(Y - 1), & \text{falls } b = -1\;. \end{cases}$$

  Wegen der Eindeutigkeit der Primfaktorzerlegung folgt $Y + \mathrm{i} \sim Y - \mathrm{i}$ bzw. $Y + 1 \sim Y - 1$, jeweils ein Widerspruch.
- Wir nehmen an, das Polynom zerfalle in zwei Polynome in $\mathbb{C}[Y][X]$ vom Grade 1 bzw. 3. Es gelte also

  $$X^4 - 2X^2Y^2 + 1 \;=\; (X^3 + aX^2 + bX + c)(X + d)$$

  mit gewissen $a, b, c, d \in \mathbb{C}[Y]$. Koeffizientenvergleich ergibt $a + d = 0$, $ad + b = -2Y^2$, $bd + c = 0$ und $cd = 1$. Daraus folgt $d = -a$, $c = -bd = ba$ und $1 = cd = abd$. Also sind $a, b, c, d \in \mathbb{C}^\times$, im Widerspruch zu $-2Y^2 = ad + b$.

Also ist $X^4 - 2X^2Y^2 + 1$ irreduzibel in $\mathbb{Q}[X, Y]$ und $\mathbb{C}[X, Y]$.

Aufgabe 3: (1/2+1/2+1+1+1=4 P) Sei R ein Ring und $I \lhd R$ ein Ideal, $I \neq R$. Wir bezeichnen mit $R[X] \cdot I$ das von den Elementen aus I erzeugte Ideal des Polynomringes $R[X]$.

(a) Zeigen Sie: ein Polynom $f = \sum a_i X^i$ liegt genau dann in $R[X] \cdot I$, wenn alle Koeffizienten a_i in I liegen.

(b) Konstruieren Sie einen Ringhomomorphismus

$$R[X]/R[X] \cdot I \longrightarrow (R/I)[X],$$

und zeigen Sie, dass dieser Homomorphismus ein Isomorphismus ist.

(c) Zeigen Sie: I ist genau dann ein Primideal von R, wenn $R[X] \cdot I$ ein Primideal von $R[X]$ ist. (Hinweis: benutzen Sie die Aussage von Aufgabe 1(b) vom 7. Übungsblatt.)

(d) Nun sei R ein faktorieller Ring und $f, g \in R[X]$. Folgern Sie aus (b): wenn f und g primitiv sind, dann ist auch fg primitiv. (Bem.: diese Aussage ist Teil des Lemmas von Gauß.)

(e) Zeigen Sie: $R[X] \cdot I$ ist niemals ein maximales Ideal.

Lösung:

(a) Per Definition ist $R[X] \cdot I$ das kleinste Ideal von $R[X]$, welches die Menge I enthält. Wir schreiben

$$I[X] \ := \ \left\{ \sum_{\nu=0}^{n} a_\nu X^\nu \,\middle|\, n \in \mathbb{N},\ a_\nu \in I \right\} .$$

Zu zeigen ist also $R[X] \cdot I = I[X]$. Nun ist definitionsgemäß $I \subseteq R[X] \cdot I$. Nach der Definition eines Ideals ist damit auch jedes Element von $I[X]$ in $R[X] \cdot I$ enthalten, d.h. es gilt $I[X] \subseteq R[X] \cdot I$. Umgekehrt ist $I[X]$ ein Ideal von $R[X]$, wie man leicht nachrechnet, und es gilt $I \subseteq I[X]$. Daraus folgt definitionsgemäß $R[X] \cdot I \subseteq I[X]$.

(b) Wir wollen zunächst ein Lemma formulieren.

Lemma *Es sei $\psi : R \to S$ ein Ringhomomorphismus. Dann ist die Abbildung*

$$\varphi : R[X] \to S[X] \ , \ \ \sum_\nu a_\nu X^\nu \mapsto \sum_\nu \psi(a_\nu) X^\nu$$

ein Ringhomomorphismus, und es gilt

$$\begin{aligned} \operatorname{Kern} \varphi &= R[X] \cdot (\operatorname{Kern} \psi) \\ \operatorname{Bild} \varphi &= S[X] \cdot (\operatorname{Bild} \psi) \ . \end{aligned}$$

Der Beweis ist einfach und sei dem Leser zur Übung überlassen. Wendet man dieses Lemma auf die kanonische Abbildung $R \to R/I$ an, so erhält man einen surjektiven Ringhomomorphismus

$$\varphi : R[X] \ \to \ (R/I)[X] \ , \ \ \sum_\nu a_\nu X^\nu \ \mapsto \ \sum_\nu \overline{a_\nu}\, X^\nu \ ,$$

und es gilt

$$\operatorname{Kern} \varphi \ = \ R[X] \cdot I \ .$$

Nach dem Homomorphiesatz induziert φ einen Ringisomorphismus

$$\overline{\varphi} : R[X]/R[X] \cdot I \ \to \ (R/I)[X] \ , \ \ \overline{f} \mapsto \varphi(f) \ .$$

(c) Nach Vorlesung ist I genau dann ein Primideal von R, wenn R/I ein Integritätsring ist. Nach Blatt 7, Aufgabe 1(b), ist dies genau dann der Fall, wenn $(R/I)[X]$ ein Integritätsring ist. Nach (b) gilt dies genau dann, wenn $R[X]/R[X] \cdot I$ ein Integritätsring ist. Dies ist wiederum genau dann richtig, wenn $R[X] \cdot I$ ein Primideal ist.

(d) Es seien $f, g \in R[X]$ primitiv. Es sei p ein Primelement von R. Zu zeigen: p teilt nicht alle Koeffizienten von fg. Wir nehmen das Gegenteil an. Also gilt $p | fg$ in $R[X]$. Es sei $I := pR$ und $\overline{\varphi} : R[X]/R[X] \cdot I \to (R/I)[X]$ der in (b) konstruierte Isomorphismus. Dann gilt

$$\overline{\varphi}(\overline{f}) \cdot \overline{\varphi}(\overline{g}) \ = \ \overline{\varphi}(\overline{f}\,\overline{g}) \ = \ \overline{\varphi}(\overline{fg}) \ = \ \varphi(fg) \ = \ 0 \ ,$$

da alle Koeffizienten von fg in I liegen. Nun ist $(R/I)[X]$ ein Integritätsring. Also folgt $\varphi(f) = \overline{\varphi}(\overline{f}) = 0$ oder $\varphi(g) = \overline{\varphi}(\overline{g}) = 0$. Dies bedeutet aber $f \in R[X] \cdot I$ oder $g \in R[X] \cdot I$, d.h. alle Koeffizienten von f sind durch p teilbar, oder alle Koeffizienten von g sind durch p teilbar. Dies widerspricht der Primitivität von f und g.

(e) Wäre $R[X]\cdot I$ ein maximales Ideal, so wäre $R[X]/R[X]\cdot I$ ein Körper. Nach (b) wäre dann auch $(R/I)[X]$ ein Körper. Dies widerspricht aber Blatt 7, Aufgabe 1(c).