9. Übung zu algebraischen Strukturen: Teilbarkeit in Integritätsbereichen

Aufgabe (9.1) Es sei R ein Integritätsbereich. Beweise die folgenden Aussagen!

(a) Es gilt $a \mid a$ für alle $a \in R$ (Reflexivität).
(b) Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$ (Transitivität).
(c) Die Assoziierungsrelation $\sim$ ist eine Äquivalenzrelation, und es gilt $a \sim b$ genau dann, wenn die Bedingungen $a \mid b$ und $b \mid a$ gelten.
(d) Die Menge $\{0\}$ und die Einheitenmenge $R^\times$ sind Äquivalenzklassen unter der Assoziierungsrelation $\sim$.
(e) Ist $u \in R^\times$ eine Einheit, so gelten für zwei beliebige Elemente $a, b \in R$ die Äquivalenzen $a \mid b \Leftrightarrow ua \mid b \Leftrightarrow a \mid ub$.
(f) Es sei $r \in R \setminus \{0\}$. Genau dann gilt $a \mid b$, wenn $ra \mid rb$ gilt.
(g) Gelten die Bedingungen $c \mid a$ und $c \mid b$, so gilt auch $c \mid ra + sb$ für alle $r, s \in R$.

Aufgabe (9.2) Es seien $a_1, \ldots, a_n$ Elemente eines Integritätsbereichs R. Beweise die folgenden Aussagen!

(a) Ist $g \neq 0$ ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$, so sind $a_1/g, \ldots, a_n/g$ teilerfremd.
(b) Sind g und g' größte gemeinsame Teiler von $a_1, \ldots, a_n$, so gilt $g' \sim g$.
(c) Ist g ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$ und gilt gilt $g' \sim g$, so ist auch g' ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$.
(d) Sind k und k' kleinste gemeinsame Vielfache von $a_1, \ldots, a_n$, so gilt $k' \sim k$.
(e) Ist k ein kleinstes gemeinsames Vielfaches von $a_1, \ldots, a_n$ und gilt gilt $k' \sim k$, so ist auch k' ein kleinstes gemeinsames Vielfaches von $a_1, \ldots, a_n$.
(f) Es seien g ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$ und $r \neq 0$ ein von Null verschiedenes Ringelement. Besitzen $ra_1, \ldots, ra_n$ überhaupt einen größten gemeinsamen Teiler, so ist rg ein solcher.

Aufgabe (9.3) Wir betrachten den Ring $R := \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Beweise die folgenden Aussagen!

(a) Definieren wir $N : R \to \mathbb{Z}$ durch $N(a + b\sqrt{-5}) := a^2 + 5b^2$, so gilt $N(xy) = N(x)N(y)$ für alle $x, y \in R$.
(b) Ist a ein gemeinsamer Teiler von x und y in R, so ist $N(a)$ ein gemeinsamer Teiler von $N(x)$ und $N(y)$ in $\mathbb{Z}$.
(c) Ist a ein gemeinsames Vielfaches von x und y in R, so ist $N(a)$ ein gemeinsames Vielfaches von $N(x)$ und $N(y)$ in $\mathbb{Z}$.
(d) Die Elemente $x := 2$ und $y := 1 + \sqrt{-5}$ besitzen einen ggT, aber kein kgV.
(e) Die Elemente $x := 6$ und $y := 2 + 2\sqrt{-5}$ besitzen weder einen ggT noch ein kgV.
(f) Die Elemente $x := 3$ und $y := 2 + \sqrt{-5}$ besitzen einen größten gemeinsamen Teiler g, aber es gibt keine lineare Darstellung dieses ggT, also keine Darstellung der Form $g = rx + sy$ mit Elementen $r, s \in R$.

Aufgabe (9.4) Gib in den folgenden Fällen jeweils an, ob das angegebene Element in dem angegebenen Ring irreduzibel ist!

(a) $X^2 + 1$ in $\mathbb{R}[X]$ bzw. in $\mathbb{C}[X]$
(b) $2X + 2$ in $\mathbb{Z}[X]$ bzw. in $\mathbb{Q}[X]$
(c) $X^2 - X - 2$ in $\mathbb{Z}[X]$ bzw. in $X^2 - X - 2$ in $\mathbb{Z}[[X]]$
(d) $X^4 + 4$ in $\mathbb{Z}[X]$ bzw. in $\mathbb{Q}[X]$ bzw. in $\mathbb{R}[X]$

Aufgabe (9.5) Charakterisiere die irreduziblen Polynome in $\mathbb{C}[X]$ und in $\mathbb{R}[X]$.

Aufgabe (9.6) Zeige, daß die Elemente $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ in $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ irreduzibel, aber nicht prim sind.

Aufgabe (9.7) Beweise Aussage (2.9)(c) im Skript: Gilt $p_1 \cdots p_m = q_1 \ldots q_n$ mit Primelementen p_i und q_j, so gilt $m = n$, und es gibt eine Permutation $\sigma \in \mathrm{Sym}_n$ derart, daß jeweils q_i mit $p_{\sigma(i)}$ assoziiert ist. (Eine Darstellung eines Elements als Produkt von Primelementen ist also immer eindeutig bis auf die Reihenfolge der Faktoren und die Multiplikation mit Einheiten.)

Aufgabe (9.8) Es sei R ein Integritätsbereich. Beweise die folgenden Aussagen!

(a) Genau dann gilt $a \mid b$, wenn $\langle\!\langle a \rangle\!\rangle \supseteq \langle\!\langle b \rangle\!\rangle$ gilt.
(b) Genau dann sind a und b assoziiert, wenn $\langle\!\langle a \rangle\!\rangle = \langle\!\langle b \rangle\!\rangle$ gilt.
(c) Genau dann gilt $x = 0$, wenn $\langle\!\langle x \rangle\!\rangle = \{0\}$ gilt.
(d) Genau dann ist x eine Einheit, wenn $\langle\!\langle x \rangle\!\rangle = R$ gilt.
(e) Genau dann ist x irreduzibel, wenn $\langle\!\langle x \rangle\!\rangle$ maximal in der Menge aller echten Hauptideale von R ist.
(f) Genau dann ist x ein gemeinsames Vielfaches von $a_1, \ldots, a_n$, wenn $\langle\!\langle x \rangle\!\rangle \subseteq \langle\!\langle a_1 \rangle\!\rangle \cap \cdots \cap \langle\!\langle a_n \rangle\!\rangle$ gilt.
(g) Genau dann ist x ein kleinstes gemeinsames Vielfaches von $a_1, \ldots, a_n$, wenn $\langle\!\langle x \rangle\!\rangle = \langle\!\langle a_1 \rangle\!\rangle \cap \cdots \cap \langle\!\langle a_n \rangle\!\rangle$ gilt.
(h) Genau dann ist x ein gemeinsamer Teiler von $a_1, \ldots, a_n$, wenn $\langle\!\langle a_1 \rangle\!\rangle + \cdots + \langle\!\langle a_n \rangle\!\rangle \subseteq \langle\!\langle x \rangle\!\rangle$ gilt.
(i) Wenn $\langle\!\langle a_1 \rangle\!\rangle + \cdots + \langle\!\langle a_n \rangle\!\rangle = \langle\!\langle x \rangle\!\rangle$ gilt, so ist x ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$.

Aufgabe (9.9) Bestimme im Ring $R = \mathbb{Z} + i\mathbb{Z}$ der Gaußschen ganzen Zahlen einen größten gemeinsamen Teiler von $a := 127 + 9i$ und $b := 19 + 113i$ und stelle ihn als R-Linearkombination von a und b dar.

Aufgabe (9.10) Wir betrachten den Ring $R = \mathbb{Z} + i\mathbb{Z}$ der Gaußschen ganzen Zahlen.

(a) Es sei $p \in \mathbb{N}$ eine Primzahl. Wann ist p nicht nur irreduzibel in $\mathbb{Z}$, sondern auch in R?
(b) Zeige, daß ein Element $z = a + ib \in R$ genau dann irreduzibel in R ist, wenn entweder $a^2 + b^2$ eine Primzahl ist oder aber wenn $z \in \{\pm p, \pm ip\}$ gilt, wobei p eine Primzahl mit $p \equiv 3$ modulo 4 ist.
(c) Zerlege in R die Elemente 30, $17 + 4i$ und $8 + 6i$ in Primfaktoren.

Aufgabe (9.x) Beweise das **Eisenstein-Kriterium**: Es seien R ein Integritätsbereich und $f(X) = \sum_{k=0}^{n} c_k X^k$ ein Polynom in $R[X]$. Es gebe ein Primelement $p \in R$ mit folgenden Eigenschaften:

- $p | c_k$ für $0 \leq k \leq n-1$,
- $p \nmid c_n$,
- $p^2 \nmid c_0$.

Dann ist f irreduzibel in $R[X]$.

Aufgabe (9.y) Beweise die Irreduzibilität der folgenden Polynome in dem jeweils angegebenen Polynomring!

(a) $p(X) = X^7 + 48X - 24$ in $\mathbb{Z}[X]$
(b) $p(X) = 2X^5 + 21X^3 + 6X + 15$ in $\mathbb{Z}[X]$
(c) $p(X) = X^4 + X^3 + X^2 + X + 1$ in $\mathbb{Z}_2[X]$
(d) $p(X) = X^4 + X^3 + X^2 + X + 1$ in $\mathbb{Z}[X]$
(e) $p(X) = X^3 + 4iX^2 - 6X - 1 + 3i$ in $(\mathbb{Z} + i\mathbb{Z})[X]$
(f) $p(X, Y, Z) = X^2 + Y^3 + Z^5$ in $K[X, Y, Z]$ (wobei K ein beliebiger Körper ist)

Aufgabe (9.z) Wir betrachten das Polynom $X_1^3 + X_2^3 + \cdots + X_n^3$ über einem Körper K. Für welche Zahlen $n \in \mathbb{N}$ und welche Körper K ist dieses Polynom irreduzibel?