Universität Karlsruhe (TH)
Mathematisches Institut II
Dr. W. Trinks

Karlsruhe, 24.10.1990

Algebra I — Übungsblatt 2

Aufgabe 6 (4 Punkte)

Es seien $\theta \in \mathbb{C}\backslash\mathbb{Z}$ und $R = \{a + b\theta : a, b \in \mathbb{Z}\}$. Zeigen Sie:
R ist ein Ring genau dann, wenn θ von der Form $\theta = u + v \cdot \omega$ ist, $u, v \in \mathbb{Z}$ und ω mit folgender Eigenschaft: ($\omega = \sqrt{d}$ mit $d \in \mathbb{Z}$) oder ($\omega = \frac{1+\sqrt{d}}{2}$ mit $d \in \mathbb{Z}$, $d \equiv 1 \pmod 4$).

Aufgabe 7 (6=1+1+2+2 Punkte)

Zeigen Sie, daß $\mathbb{Z}\left[\sqrt{-1}\right] := \mathbb{Z} + \mathbb{Z}\sqrt{-1}$ ein euklidischer Ring ist. Zeigen Sie dazu:

(a) $K := \mathbb{Q} + \mathbb{Q}\sqrt{-1}$ ist ein Körper, in dem für jedes Element x die Darstellung von x als $a + b\sqrt{-1}$ eindeutig ist.

(b) Auf K ist durch $N\left(a + b\sqrt{-1}\right) := \left|(a + b\sqrt{-1}) \cdot (a - b\sqrt{-1})\right|$ eine Funktion $N\colon K \to \mathbb{Q}$ definiert, die
  (i) $N(x) = 0 \iff x = 0$,
  (ii) $N(x \cdot y) = N(x) \cdot N(y)$,
  (iii) $N(x) \in \mathbb{N}$ für $x \in \mathbb{Z}\left[\sqrt{-1}\right]$
erfüllt.

(c) $\mathbb{Z}\left[\sqrt{-1}\right]$ ist ein (bezüglich N) euklidischer Ring.

Verfahren Sie analog, um zu zeigen:

(d) $\mathbb{Z}\left[\dfrac{1+\sqrt{5}}{2}\right]$ ist ein euklidischer Ring.

Aufgabe 8 (4 Punkte)

Bestimmen Sie jeweils zu $a, b \in R$ einen ggT c von a und b, und schreiben Sie c in der Form $c = x \cdot a + y \cdot b$ mit $x, y \in R$.

(a) $R = \mathbb{Z}$, $a = 3855$, $b = 5235$.
(b) $R = \mathbb{Z}[i]$ mit $i = \sqrt{-1}$, $a = -43 + 99i$, $b = 118 + 76i$.
(c) $R = \mathbb{Q}[X]$, $a = X^4 - 5X^2 + 4$, $b = X^2 - 5X + 6$.

Aufgabe 9 ($10 = \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + 1 + 1 + \frac{1}{2} + 1 + 1 + 1 + 1 + 1 + 1$ Punkte)

Sei R ein Integritätsbereich (= nullteilerfreier kommutativer Ring mit 1), in dem zu je zwei Elementen $a, b \in R$ ein $\mathrm{ggT}(a,b)$ existiert. Zeigen Sie für $a, b, \ldots \in R$:

(a) $\mathrm{ggT}(a,b) = 0 \iff a = 0 \wedge b = 0$,
(b) $a' \mid a \wedge b' \mid b \Rightarrow \mathrm{ggT}(a',b') \mid \mathrm{ggT}(a,b)$,
(c) $\mathrm{ggT}(a, b + ac) \approx \mathrm{ggT}(a,b)$,
(d) $\mathrm{ggT}(a \cdot c, b \cdot c) \approx \mathrm{ggT}(a,b) \cdot c$,
(e) $\mathrm{ggT}(a, b \cdot c) \mid \mathrm{ggT}(a,b) \cdot \mathrm{ggT}(a,c)$,
(f) Ist $d := \mathrm{ggT}(a,b)$, so gibt es $a', b' \in R$ mit $a = a' \cdot d$, $b = b' \cdot d$ und $\mathrm{ggT}(a',b') \approx 1$.
(g) $\mathrm{ggT}(\mathrm{ggT}(a,b),c) \approx \mathrm{ggT}(a, \mathrm{ggT}(b,c))$,
(h) Zu $a, b \in R$ exisiert ein $\mathrm{kgV}(a,b)$, und es gilt $\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) \approx a \cdot b$.
(i) $\mathrm{ggT}(a + b, \mathrm{kgV}(a,b)) \approx \mathrm{ggT}(a,b)$,
(j) für $m, n \in \mathbb{N}$: $\mathrm{ggT}\left(a^m - 1, a^n - 1\right) \approx a^{\mathrm{ggT}(m,n)} - 1$.
(k) $\mathrm{ggT}(\mathrm{kgV}(a,b),c) \approx \mathrm{kgV}(\mathrm{ggT}(a,c), \mathrm{ggT}(b,c))$,
(l) $\mathrm{kgV}(\mathrm{ggT}(a,b),c) \approx \mathrm{ggT}(\mathrm{kgV}(a,c), \mathrm{kgV}(b,c))$.

* **Aufgabe 10** (5 Punkte)

Der euklidische Algorithmus liefert zu $a, b \in \mathbb{N}$ den ggT $g = \mathrm{ggT}(a,b)$. Folgende Variante liefert auch eine Darstellung $g = u \cdot a + v \cdot b$ mit $u, v \in \mathbb{Z}$, und zwar fast immer mit kleinstmöglichem $|u|$ und kleinstmöglichem $|v|$:

> Seien $a, b \in \mathbb{N}$ gegeben.
> Man betrachtet Tripel (x,y,z) mit $x \cdot a + y \cdot b = z$, $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, $z \in \mathbb{N}$.
> Man startet mit $(x_1, y_1, z_1) = (1, 0, a)$ und $(x_2, y_2, z_2) = (0, 1, b)$.
> Für $n = 2, 3, \ldots$:
> Falls $z_n > 0$, dividiere man z_{n-1} durch z_n mit Rest: $z_{n-1} = q \cdot z_n + z_{n+1}$ und setze $(x_{n+1}, y_{n+1}, z_{n+1}) := (x_{n-1}, y_{n-1}, z_{n-1}) - q \cdot (x_n, y_n, z_n)$.
> Falls $z_n = 0$, breche man ab, setze $m := n$ und liefere $(x_{m-1}, y_{m-1}, z_{m-1})$ als Ergebnis.

$z_{m-1} = g$ ist aus der Vorlesung bekannt.
Zeigen Sie:
Für das Ergebnis $(u, v, g) = (x_{m-1}, y_{m-1}, z_{m-1})$ gilt $g = \mathrm{ggT}(a,b) \geq 0$, $u \cdot a + v \cdot b = g$.
Falls $b = 0$: $m = 2$, $(u, v, g) = (1, 0, a)$.
Falls $b > 0$ und $b \mid a$: $m = 3$, $(u, v, g) = (0, 1, b)$.
Falls $b > 0$ und $b \nmid a$: $m > 3$, $g > 0$, $|u| \leq \frac{b}{2g}$, $|v| \leq \frac{a}{2g}$.
(Hinweise:
Untersuchen Sie die Vorzeichen von x_n und y_n.
Was passiert mit den Ausdrücken $x_n \cdot y_{n+1} - x_{n+1} \cdot y_n$, $x_n \cdot z_{n+1} - x_{n+1} \cdot z_n$, $y_n \cdot z_{n+1} - y_{n+1} \cdot z_n$ beim Schritt von $n-1$ auf n?
Setzen Sie dann $n = m - 1$ ein.)

Abgabe: Bis spätestens Dienstag, 30.10.1990, 11.15 Uhr in den Kasten bei Zi. 308 des Mathematikgebäudes oder in der Übung im Neuen Hörsaal.