Einführung in die Algebra — Übungsblatt 6

Prof. Dr. Catharina Stroppel, Dr. Martin Palmer-Anghel (Assistent) // Wintersemester 17/18

[**Abgabe**: 23. November 2017, **vor** der Vorlesung, 10:00 – 10:15]

Aufgabe 1. (3 Punkte)

Geben Sie einen Beweis für das Lemma 7.16 der Vorlesung:
Lemma 7.16. Seien S ein kommutativer Ring, $R \subseteq S$ ein Unterring und $a_1, \dots, a_n \in S$. Dann:

(1) $a_1, \dots, a_n$ sind algebraisch abhängig genau dann, wenn es $p(t_1, \dots, t_n) \in R[t_1, \dots, t_n] \smallsetminus \{0\}$ gibt, so dass $p(a_1, \dots, a_n) = 0$.
(2) Diese Aussage ist äquivalent zur folgenden:
$a_1, \dots, a_n$ sind algebraisch *un*abhängig $\Leftrightarrow$ Ist für ein Polynom $p(t_1, \dots, t_n) \in R[t_1, \dots, t_n]$ das Element $p(a_1, \dots, a_n) \in S$ null, dann muss $p(t_1, \dots, t_n) = 0$ sein.

Aufgabe 2. (6 Punkte)

Sei $R = \mathbb{Z}[\mathrm{i}\sqrt{5}] = \{a + b\mathrm{i}\sqrt{5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

(a) Zeigen Sie, dass R der von $\mathrm{i}\sqrt{5}$ erzeugte Unterring über $\mathbb{Z}$ in $\mathbb{C}$ ist.
(b) Mithilfe der Betragsfunktion $|\;| \colon \mathbb{C} \to \mathbb{R}$ (*cf.* Blatt 5 Aufgabe 2) zeigen Sie, dass $R^\times = \{\pm 1\}$.
(c) Zeigen Sie, dass die Elemente $2, 3, 1 + \mathrm{i}\sqrt{5}, 1 - \mathrm{i}\sqrt{5} \in R$ irreduzibel sind.
(d) Folgern Sie, dass R kein faktorieller Ring ist.
(e) Deshalb ist R auch kein Hauptidealring. Geben Sie mit Begründung ein Ideal in R an, das kein Hauptideal ist.
Hinweis: benutzen Sie dafür wieder die Betragsfunktion.

Aufgabe 3. (6 Punkte)

(a) Seien $n_1, n_2, \dots, n_k \in \mathbb{N}$ paarweise teilerfremd — das heißt, es gibt keine Primzahl p mit $p \mid n_i$ und $p \mid n_j$ für zwei verschiedene i, j — und sei $N = n_1 n_2 \cdots n_k$. Zeigen Sie, dass

$$\mathbb{Z}/N\mathbb{Z} \;\cong\; \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \tag{1}$$

als Ringe.
(b) Zeigen Sie, dass (1) *nicht* wahr ist, sogar nicht einmal als Gruppen, wenn $n_1, n_2, \dots, n_k \in \mathbb{N}$ *nicht* paarweise teilerfremd sind.
Hinweis: was ist die größte Ordnung eines Elements der rechten Seite?
(c) Finden Sie alle $x \in \mathbb{Z}$, so dass $x \equiv 4 \pmod 7$ und $x \equiv 7 \pmod{12}$.
Hinweis: finden Sie zuerst eine Lösung, dann benutzen Sie den Isomorphismus (1), um alle anderen zu finden. Um die erste Lösung zu finden, könnten Sie z.B. zuerst ganze Zahlen a, b finden, so dass $7a + 12b = 1$.
(d) Finden Sie alle $x \in \mathbb{Z}$, so dass $x \equiv 4 \pmod 6$, $x \equiv 33 \pmod{35}$ und $x \equiv 10 \pmod{11}$.
(e) Finden Sie alle $x \in \mathbb{Z}$, so dass $x \equiv p - 2 \pmod p$ für alle Primzahlen $p < 100$.

Aufgabe 4. (5 Punkte)

Sei $(X, \leqslant)$ eine partiell geordnete Menge. Man sagt, dass eine aufsteigende Kette $x_0 \leqslant x_1 \leqslant \cdots$ in X *stationär* wird, wenn ein $n_0 \in \mathbb{N}$ existiert mit $x_m = x_{n_0}$ für alle $m \geqslant n_0$.

Sei jetzt R ein Integritätsbereich und $\mathrm{HI}(R)$ die partiell geordnete Menge aller Hauptideale von R.

Zeigen Sie:

(a) Wenn R ein faktorieller Ring ist, dann gilt:
  (i) Jedes irreduzible Element von R ist prim.
  (ii) Jede aufsteigende Kette in $\mathrm{HI}(R)$ wird stationär.

(b) Wenn (i) und (ii) für R gelten, dann ist R ein faktorieller Ring.

Zur Information. Nach der Vorlesung gilt

$$\{\text{euklidische Ringe}\} \subseteq \{\text{Hauptidealringe}\} \subseteq \{\text{faktorielle Ringe}\}.$$

Allerdings sind die beiden Inklusionen jeweils echt. Für die zweite Inklusion werden wir in der Vorlesung sehen, dass $\mathbb{Z}[t]$ und $\mathbb{C}[t_1, t_2]$ faktorielle Ringe sind, aber nach Aufgabe 1 von Übungsblatt 5 wissen wir, dass sie keine Hauptidealringe sind. Für die erste Inklusion gilt das Folgende.

Sei $d \in \mathbb{Z}$ eine quadratfreie ganze Zahl und definiere $\mathcal{O}_d = \mathbb{Z}[\sqrt{d}]$ wenn $d \equiv 2$ oder $3 \pmod 4$ und $\mathcal{O}_d = \mathbb{Z}\big[\frac{1}{2}(1+\sqrt{d})\big]$ wenn $d \equiv 1 \pmod 4$, wobei für $z \in \mathbb{C}$ bedeutet $\mathbb{Z}[z]$ den von z erzeugten Unterring über $\mathbb{Z}$ in $\mathbb{C}$, anders gesagt: $\mathbb{Z}[z] = \{a + bz \mid a, b \in \mathbb{Z}\}$. Wenn d positiv ist, bezeichnet $\sqrt{d}$ die positive Wurzel, wie üblich, und wenn d negativ ist, definieren wir $\sqrt{d} = \mathrm{i}\sqrt{-d}$. Zum Beispiel ist $\mathcal{O}_{-1} = \mathbb{Z}[\mathrm{i}]$ der Ring der Gaußschen Zahlen. Wir haben in Aufgabe 2 oben gesehen, dass $\mathcal{O}_{-5}$ kein faktorieller Ring ist. Andererseits haben wir in Aufgabe 2 auf Übungsblatt 5 gezeigt, dass $\mathcal{O}_{-1}$ ein Hauptidealring, und deshalb insbesondere ein faktorieller Ring, ist. Es gibt tatsächlich nur endlich viele negative d, so dass $\mathcal{O}_d$ ein faktorieller Ring ist, nämlich:

$$d \in \{-163, -67, -43, -19, -11, -7, -3, -2, -1\}.$$

Für positive d kennt man die entsprechende Liste noch nicht, und nicht einmal ob die Liste endlich ist. Für alle Ringe der Form $\mathcal{O}_d$ gilt die Äquivalenz: Hauptidealring $\Leftrightarrow$ faktorieller Ring (was im allgemeinen bestimmt nicht gilt, wie oben schon bemerkt), also die Frage, wann $\mathcal{O}_d$ ein Hauptidealring ist, hat dieselbe (unvollständige) Lösung. Es gibt aber eine komplette Lösung zur Frage, wann $\mathcal{O}_d$ ein *euklidischer* Ring ist. Dies gilt nämlich genau dann, wenn:

$$d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Also insbesondere ist $\mathcal{O}_{-19} = \mathbb{Z}\big[\frac{1}{2}(1+\mathrm{i}\sqrt{19})\big]$ ein Hauptidealring, der kein euklidischer Ring ist. Dazu vergleiche man die Abschnitte 14.7–9 und die zugehörigen "Notes" in:
G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, fifth ed., 1979 (OUP).

NB: Wenn ein Teil einer Aufgabe mit dem Symbol $*$ versehen wird, zeigt dies, dass dieser Teil etwas anspruchsvoller sein sollte.

Allgemeine Instruktionen.

- Die Abgabe ist in Gruppen von zwei oder drei Personen erlaubt; allerdings muss ersichtlich sein, dass jedes Mitglied der Gruppe die Lösung von mindestens einer Aufgabe aufgeschrieben hat. Bitte geben Sie immer Name und Tutorium von jedem Gruppenmitglied an.
- Wenn nicht explizit ausgeschlossen, dürfen Sie Resultate aus der Vorlesung ohne Beweis verwenden, müssen aber dabei immer die Nummer oder den Namen des Satzes, oder aber die Aussage des Satzes, angeben, sodass klar ist, welches Resultat Sie verwenden möchten.
- Die neuen Übungsblätter können immer Donnerstags ab spätestens 12 Uhr von der Homepage der Vorlesung (math.uni-bonn.de/people/palmer/A1.html) heruntergeladen werden.
- Lösungen zu den Übungszettel müssen Donnerstags **vor** der Vorlesung, d.h. 10:00 – 10:15 Uhr, eingereicht werden. Die korrigierten Übungszettel bekommen Sie in Ihrem Tutorium zurück; dort werden auch die Lösungen zu den Aufgaben besprochen.
- Für die Zulassung zur Klausur sind mindestens 50% der Übungspunkte erforderlich.
- Bei Fragen zu diesem Übungszettel, wenden Sie sich bitte an Ihren Tutor, oder an den Assistenten. Mehr Details zur Vorlesung finden Sie auf der oben genannten Homepage.