Universität Mannheim, Lehrstuhl für Mathematik VI
Christian Sevenheck

Übungsaufgaben zur Algebra

1. *(2 Punkte)* Führen Sie den erweiterten Euklidischen Algorithmus für die Zahlen $r_0 = 14372$ und $r_1 = 1236$ durch, mit den gleichen Notationen und analogen Ergebnissen wie im Beispiel 7.6 der Vorlesung.

   Geben Sie die Ergebnisse (die Anzahl n der Schritte und alle r_i, q_i, x_i, y_i für $i = 0, ..., n+1$, außer q_0 und q_{n+1} (die existieren nicht)) in einer Tabelle wie im Beispiel 7.6 an.

2. *(2 Punkte)* Führen Sie den erweiterten Euklidischen Algorithmus mit den Polynomen $r_0 = x^4 + x^3 + x + 1$ und $r_1 = x^3 + x^2 - x \in \mathbb{Q}[x]$ durch. Geben Sie die Ergebnisse (die Anzahl n der Schritte und alle r_i, q_i, x_i, y_i) in einer Tabelle wie in den Beispielen 7.6 und 7.7 der Vorlesung an.

3. *(2+1+1 Punkte)*

   (a) Aus dem erweiterten Euklidischen Algorithmus folgt, daß für zwei Zahlen $a, b \in \mathbb{Z}$ gilt:

   $$\exists\, c, d \in \mathbb{Z} \text{ mit } \operatorname{ggT}(a, b) = ca + db.$$

   Folgern Sie daraus

   $$(\mathbb{Z}/m\mathbb{Z})^* = \{[a] \mid 0 < a < m, \operatorname{ggT}(a, m) = 1\}.$$

   (b) Listen Sie in den beiden Fällen $m = 15$ und $m = 28$ jeweils die Elemente von $(\mathbb{Z}/m\mathbb{Z})^*$ und ihre Inversen auf (am besten in Tabellen mit den Inversen der Elemente unter den Elementen).

4. *(3 Punkte)* Zeigen Sie, daß der Ring $\mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ mit der Gradfunktion

   $$w : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}, \quad a + ib \mapsto |a + ib|^2 = a^2 + b^2,$$

   ein Euklidischer Ring ist.

5. *(4 Punkte)* Nach Aufgabe 4 ist der Ring $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z} \cdot i \subset \mathbb{C}$ ein Euklidischer Ring, also (Satz 7.14 der Vorlesung) auch ein Hauptidealring. Daher sind die folgenden 6 Ideale Hauptideale. Finden Sie je ein Erzeugendes (mit Beweis).

   $$(3, i), \quad (4 + 4i, 8i), \quad (2 - i, 2 + i), \quad (1 + i, 1 - i), \quad (5, 3 + 4i), \quad (10, 7 + i).$$

6. *(3 Punkte)* Für $m \in \mathbb{N} \cup \{0\}$ gibt es 2^m unitäre Polynome vom Grad m im Polynomring $\mathbb{F}_2[x]$. Weil $\mathbb{F}_2[x]$ ein Euklidischer Ring und damit ein faktorieller Ring ist, läßt sich jedes unitäre Polynom vom Grad ≥ 1 eindeutig als Produkt von unitären und irreduziblen Polynomen schreiben. Listen Sie alle $30 = 2 + 4 + 8 + 16$ unitären Polynome vom Grad $d \in \{1, 2, 3, 4\}$ und ihre Produkt-Zerlegungen in unitäre und irreduzible Polynome auf.

   Hinweis: Beachten Sie Aussage (d) in der Liste in Aufgabe 9.

7. *(2 Punkte)* Die Eulersche phi-Funktion $\varphi : \mathbb{N} - \{1\} \to \mathbb{N}$ ist definiert durch

   $$\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|.$$

   (a) Zeigen Sie folgende Verallgemeinerung des kleinen Satzes von Fermat:

   Seien $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\operatorname{ggT}(a, m) = 1$. Dann ist

   $$a^{\varphi(m)} \equiv 1 \mod m.$$

   Hinweise: Benutzen Sie Aufgabe 3 (a) und den Satz von Lagrange oder eine Folgerung davon.

   (b) Folgern Sie: *Es seien p und q zwei verschiedene Primzahlen, $a \in \mathbb{Z}$ und $r \in \mathbb{N} \cup \{0\}$. Dann gilt*

   $$a^{1 + r(p-1)(q-1)} \equiv a \mod pq.$$

Bitte wenden !!!

8. *(2+2+2 Punkte)* Für $m \in \mathbb{N}$ ist das m-te Kreisteilungspolynom $\Phi_m(x) \in \mathbb{C}[x]$ definiert durch

$$\Phi_m(x) := \prod_{a \text{ mit } 0<a<m, \mathrm{ggT}(a,m)=1} \left(x - e^{2\pi i \frac{a}{m}}\right).$$

(a) Zeigen Sie

$$x^m - 1 = \prod_{d|m} \Phi_d(x).$$

(b) Zeigen Sie $\Phi_m(x) \in \mathbb{Z}[x]$. Sie dürfen folgende Aussage benutzen:

(Polynomdivision mit Rest) Ist R ein Integritätsring und sind $f(x), g(x) \in R[x] - \{0\}$ und ist $g(x)$ unitär, so gibt es eindeutige $q(x), r(x) \in R[x]$ mit $\deg r(x) < \deg g(x)$ und $f(x) = q(x) \cdot g(x) + r(x)$.

(c) Es ist offenbar $\Phi_1(x) = x - 1$ und $\Phi_2(x) = x + 1$. Berechnen Sie $\Phi_m(x)$ für $m \in \{3, 4, 6, 12\}$.

9. *(6 Punkte)* Ist R ein Integritätsring, so auch $R[x]$ (Beweis leicht, aber nicht Teil der Aufgabenstellung). Daher ist der Begriff "irreduzibel" (Definition 7.17 (a) der Vorlesung) wohldefiniert für Polynome in $R[x]$. Bei Irreduzibilitätsuntersuchungen von Polynomen gibt es ganz verschiedene nützliche Kriterien und Aussagen. Einige sind hier aufgelistet:

(a) Eisenstein-Kriterium (7.25 (c) in der Vorlesung): Sei R ein faktorieller Ring (z.B. $R = \mathbb{Z}$) und $f(x) = a_n x^n + ... + a_1 x + a_0 \in R[x]$ mit $n \geq 1$, $a_n \neq 0$. Sei $p \in R$ ein Primelement mit

$$p \,|\, a_j \text{ für } j \leq n-1,\ p \not| a_n,\ p^2 \not| a_0.$$

Dann ist $f(x)$ irreduzibel in $R[x]$.

(b) Die Projektion $\mathbb{Z} \to \mathbb{F}_p$ (p eine Primzahl) induziert einen Ringhomomorphismus $\pi_p : \mathbb{Z}[x] \to \mathbb{F}_p[x]$. Sei $f(x) \in \mathbb{Z}[x]$. Dann gilt: $\pi_p(f(x))$ ist irreduzibel in $\mathbb{F}_p[x] \Rightarrow f(x)$ ist irreduzibel in $\mathbb{Z}[x]$.

(c) Sei R ein faktorieller Ring, K sein Quotientenkörper (z.B. $R = \mathbb{Z}$ und $K = \mathbb{Q}$) und $f(x) = a_n x^n + ... + a_1 x + a_0 \in R[x]$. Dann gilt (7.25 (b) in der Vorlesung):
$f(x)$ ist irreduzibel in $R[x] \Rightarrow f(x)$ ist irreduzibel in $K[x]$.
Ist $\mathrm{ggT}(a_n, ..., a_0) = 1$, so gilt $\iff$.

(d) Sei R ein Integritätsring (z.B. $R = \mathbb{Z}$ oder R ein Körper) und $f(x) \in R[x]$ unitär mit $\deg f(x) \in \{2, 3\}$. Dann gilt:

$$f(x) \text{ ist irreduzibel in } R[x] \iff f(x) \text{ hat keine Nullstelle in } R.$$

Für $\deg f(x) \geq 4$ gilt nur noch $\Rightarrow$. (Verallgemeinerung von 7.23 (b) auf R statt K)

(e) Ist $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 \in \mathbb{Z}[x]$ unitär mit einer Nullstelle $b \in \mathbb{Z}$, so ist b ein Teiler von a_0.

(f) Sei R ein Integritätsring, $f \in R[x]$ und $\alpha \in R$ beliebig. Dann gilt: $f(x)$ ist irreduzibel in $R[x] \iff f(x + \alpha)$ ist irreduzibel in $R[x]$.

Zeigen Sie, daß die folgenden 12 Polynome irreduzibel in $\mathbb{Z}[x]$ sind. Sie dürfen die Aussagen in der Liste oben benutzen. Sie dürfen auch die Resultate von Aufgabe 6 benutzen.

$$\begin{array}{rcl}
x^2 - x + 1 & , & x^2 - x - 1, \\
x^3 + x^2 - 2x - 1 & , & x^3 + 10x^2 + 9x - 15, \\
x^3 + 3x^2 - x - 1 & , & x^3 + 12x^2 + 24x + 48, \\
x^4 + x^3 + 16x + 17 & , & 3x^4 + 5x^3 - 10x^2 - 5x + 15, \\
7x^3 - 8x^2 + 17x - 135 & , & x^6 + 17, \\
x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 18 & , & x^8 + 2x^7 + 2x^6 + 4x^5 + 6x^4 + 10x^3 + 16x^2 + 26x + 42.
\end{array}$$

Alle Informationen zur Vorlesung (Termine, Übungsblätter etc.) sind unter

`http://hilbert.math.uni-mannheim.de/~sevenhec/Algebra12.html`

zu finden.