26.11.2008

I. Bouw
L. Brewis und D.Ufer

Übungen zur Algebra I - WS08/09
Blatt 7

Abgabe ist Mittwoch, den 03.12.2008, vor der Vorlesung (**zu zweit!**)

Aufgabe 1: Euklidischer Algorithmus (2+2+2)

Bemerkung 1 *Seien p_1, p_2 Polynome über einem Körper K mit $0 < \deg p_2 < \deg p_1$. In der Vorlesung haben wir den $\mathrm{ggT}(p_1, p_2)$ als das bis auf Einheiten eindeutige Polynom minimalen Grades $s_1 \cdot p_1 + s_2 \cdot p_2 \neq 0$ über alle Polynome s_1, s_2 definiert.Den ggT liefert uns der Euklidische Algorithmus. Dieser geht wie folgt:*
Zu einem Paar von Polynomen f, g mit $0 < \deg f < \deg g$ existieren eindeutige Polynome q, r mit $g = fq + r$, wobei $0 \leq \deg r < \deg f$. Diese r, q liefert uns die Polynomdivision. Schreibt man $r_{-1} = p_1$, $r_0 = p_2$ und definiert man q_i, r_i rekursiv durch

$$r_{n-2} = q_n \cdot r_{n-1} + r_n \tag{1}$$

mit $0 \leq \deg r_n < \deg r_{n-1}$, wählt man m minimal so, dass $r_m = 0$ dann ist $\mathrm{ggT}(a, b) = r_{m-1}$.

(a) Bestimmen Sie das Polynom $d = \mathrm{ggT}(f, g)$ für $f = x^3 + x^2 + x - 3$ und $g = x^6 - x^5 + 6x^2 - 13x + 7$.

(b) Finden Sie $s_1, s_2 \in K[x]$ mit $s_1 \cdot f + s_2 \cdot g = d$ für f, g aus (a) mittels Rücksubstitution von (1).

(c) Zeigen Sie, dass g in $K[x]/(f)$ genau dann invertierbar ist, wenn $\mathrm{ggT}(f, g) = 1$.

Aufgabe 2: Minimalpolynome (1+2+2)

Sei $\zeta_{12} = \cos\frac{\pi}{6} + i \sin\frac{\pi}{6}$ eine primitive 12. Einheitswurzel.

(a) Bestimmen Sie die Ordnung für die Elemente ζ_{12}^j in $\mu_{12} = \{x \in \mathbb{C} : x^{12} = 1\}$ für $j = 1, \ldots, 11$.

(b) Faktorisieren Sie $x^{12} - 1$ über $\mathbb{C}$ und über $\mathbb{Q}$.

(c) Bestimmen Sie das Minimalpolynom von ζ_{12} über $\mathbb{Q}$ und über $\mathbb{Q}(i)$.

Aufgabe 3: Endliche Körper (1+2+2)

(a) Zeigen Sie, dass die Polynome $x^2 - 2$ und $x^2 - 3$ irreduzibel über $\mathbb{F}_5$ sind.

(b) Zeigen Sie, dass $\mathbb{F}_5[x]/(x^2 - 2)$ isomorph ist zu $\mathbb{F}_5[x]/(x^2 - 3)$.

(c) Zeigen Sie, dass $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ und schließen Sie daraus, dass $\mathbb{Q}(\sqrt{2})$ nicht isomorph ist zu $\mathbb{Q}(\sqrt{3})$.

Bemerkung 2 *Allgemeiner kann man zeigen, dass für alle Primzahlen p und alle natürlichen Zahlen $n \geq 1$ genau ein Körper mit p^n Elementen existiert.*