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

Karlsruhe, 23.1.1991

Algebra I — Übungsblatt 13

Aufgabe 66 (2 Punkte)
Bestimmen Sie den Zerfällungskörper von $X^6 + 1$ über $\mathbb{F}_2$.

Aufgabe 67 (4 Punkte)
Sei K der Zerfällungskörper des Polynoms $X^4 - 2$ über $\mathbb{Q}$. Zeigen Sie, daß $K/\mathbb{Q}$ galoissch ist. Bestimmen Sie $G = \mathrm{Gal}\,(K/\mathbb{Q})$, alle Untergruppen H von G und jeweils den Fixkörper K^H.

Aufgabe 68 (4 Punkte)
(Zum Faktorisierungsalgorithmus von *Cantor, Zassenhaus*)

(a) Sei q eine ungerade Primzahlpotenz, $f \in \mathbb{F}_q[X]$ vom Grad d. Es sei bekannt, daß f das Produkt von j verschiedenen (normierten) Primpolynomen vom Grad i ist, $d = i \cdot j$, $j > 1$.
Zeigen Sie, daß bei gleichverteilter zufälliger Auswahl von $b(X) = b_0 + b_1 X + \cdots + b_{d-1} X^{d-1} \in \mathbb{F}_q[X]$ für $c(X) := b(X)^{\frac{q^i-1}{2}}$

$$f(X) \approx \mathrm{ggT}(c(X) - 1, f(X)) \cdot \mathrm{ggT}(c(X), f(X)) \cdot \mathrm{ggT}(c(X) + 1, f(X))$$

mit Wahrscheinlichkeit $> \frac{1}{2}$ eine *nichttriviale* Faktorisierung von $f(X)$ ist.

(b) Wie berechnet man $\mathrm{ggT}\left(f(X), X^{q^n} - X\right)$ $(\mathrm{grad}(f) = d \leq n)$ mit höchstens $O\left(n \cdot d^2 \cdot (\log q)^2\right)$ Bitoperationen?

(c) Bestimmen Sie eine Quadratwurzel von $122 \in \mathbb{F}_{257}$.

Aufgabe 69 (3 Punkte)
(„Hauptsatz über symmetrische Polynome“)
Ist R ein kommutativer Ring mit 1 und sind in $R[X_1, \ldots, X_n]$

$$\begin{aligned} S_1 &= X_1 + \cdots + X_n \\ S_k &= \sum_{1 \leq i_1 < \ldots < i_k \leq n} X_{i_1} \cdots X_{i_k} \qquad (1 \leq k \leq n) \\ S_n &= X_1 \cdots X_n \end{aligned}$$

die *elementarsymmetrischen Polynome* in $X_1, \ldots, X_n$, so sind die Polynome $\in R[X_1, \ldots, X_n]$, die unter allen Permutationen der $X_1, \ldots, X_n$ invariant sind, genau die Polynome $\in R[S_1, \ldots, S_n]$.
(Hinweis zu „$\Rightarrow$“: Versuchen Sie den „Grad“ des Polynoms $\in R[X_1, \ldots, X_n]$ zu verringern, wobei der „Grad“ von ${X_1}^{m_1} \cdots {X_n}^{m_n}$ zu $(m_1, \ldots, m_n)$ festgelegt sei und Grade $\in {\mathbb{N}_0}^n$ mit der lexikographischen Ordnung verglichen werden.)

Aufgabe 70 (7 Punkte)
Für $n \in \mathbb{N}$, $n > 0$ sei das n-te *Kreisteilungspolynom* Φ_n definiert durch

$$\Phi_n(X) := \prod_{k \in \left(\mathbb{Z}/_{n\mathbb{Z}}\right)^\times} \left(X - e^{\frac{2k\pi i}{n}}\right) \in \mathbb{C}[X]$$

Zeigen Sie:

(a) Die Nullstellen von Φ_n in $\mathbb{C}$ sind genau die primitiven n-ten Einheitswurzeln, und $\operatorname{grad}(\Phi_n) = \varphi(n)$.
(b) $\prod_{d \mid n} \Phi_d(X) = X^n - 1$.
(c) $\Phi_n(X) \in \mathbb{Z}[X]$.
(d) Ist p eine Primzahl, so gilt $\Phi_{np}(X) = \left\{\begin{array}{ll} \Phi_n(X^p) & \text{falls } p \mid n \\ \frac{\Phi_n(X^p)}{\Phi_n(X)} & \text{falls } p \nmid n \end{array}\right\}$. Berechnen Sie $\Phi_n(X)$ für $1 \leq n \leq 12$.
* (e) $\Phi_n(X)$ ist in $\mathbb{Q}[X]$ irreduzibel.
(Hinweis: Benutzen Sie, daß für Primzahlen $p \nmid n$ gilt $\Phi_n(X) \mid \Phi_n(X^p)$.)
(f) $\mathbb{Q}(\zeta_n)$ mit $\zeta_n = e^{\frac{2\pi i}{n}}$ ist eine galoissche Körpererweiterung von $\mathbb{Q}$, und $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \left(\mathbb{Z}/_{n\mathbb{Z}}\right)^\times$.

Aufgabe 71 (4 Punkte)
Für $n \in \mathbb{N}$, $n > 0$ sei

$$F_n := \prod_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \left(3 + 2\cos\frac{2k\pi}{n}\right)$$

(a) $F_n \in \mathbb{Q}$.
(b) $F_n \in \mathbb{Z}$.
* (c) Können Sie eine „geschlossene Formel“ für die F_n angeben?

Abgabe: Bis spätestens Dienstag, 29.1.1991, 11.15 Uhr in den Kasten bei Zi. 308 des Mathematikgebäudes oder in der Übung im Neuen Hörsaal.