Algebra I 21.6.2004
SoSe 2004
Schmale

Aufgabenblatt 10

(39) Beim Beweis von Satz 16.2 wurde stillschweigend folgendes Ergebnis benutzt: Seien p eine Primzahl, h ein Primpolynom in $\mathbb{Z}_p[x]$, $\alpha \in \mathbb{N}_+$, $d = \deg h$ $V = (\mathbb{Z}_p[x])_{d\alpha,h^\alpha}$, der zu $\mathbb{Z}_p[x]/h^\alpha\mathbb{Z}_p[x]$ isomorphe Restring und $W = \{g \in V : g^{\textcircled{p}} = g\}$. Dann ist $W = \mathbb{Z}_p$.

Leiten Sie dieses Ergebnis her.

Anleitung: $g^{\textcircled{p}} = g \Leftrightarrow h^\alpha \mid g^p - g$; $g^p - g = \prod_{r\in\mathbb{Z}_p} (g - r)$ (siehe Vorlesung).

Warum folgt: $h^\alpha \mid g - r$ für genau ein $r \in \mathbb{Z}_p$? Was besagt der chinesische Restsatz über die Lösungsmenge der einzelnen Kongruenz $g \equiv r \mod h^\alpha$; wie viele der Lösungen liegen in W?

(40) Berechnen Sie die quadratfreie Zerlegung der Polynome

(a) $x^7 + 8x^6 + 39x^5 + 163x^4 + 383x^3 + 987x^2 + 1078x + 1715$ modulo 2 und modulo 3 .

(b) $f := x^4 - 10x^2 + 1$ in $\mathbb{Q}[x]$ und modulo $2, 3, 5$. Ist f unzerlegbar?

(41) Zur diskreten Fourier-Transformation (DFT)$^{(*)}$: Sei $n \in \mathbb{N}_{\geq 2}$. Der Körper K enthalte eine sogenannte **primitive n-te Einheitswurzel** w. Das heißt nichts anderes als dass es in $G(K) = K\backslash\{0\}$ ein Element w gibt, dessen Ordnung genau n ist. Bekanntestes Beispiel ist. $K = \mathbb{C}$, $w = e^{\frac{2\pi i}{n}}$.

Sei $V := (K[x])_{n,\, x^n-1}$. Betrachtet wird die Abbildung

$\prod_w : K[x] \to K^n$ mit $\prod_w(f) = (f(1), f(w), \ldots, f(w^{n-1}))$ für $f \in K[x]$.

Die Einschränkung $\Delta_w := \pi\,|_V$ von $\prod_w$ auf V heißt **diskrete Fouriertransformation.** In dieser Aufgabe können einige für die DFT grundlegende Eigenschaften hergeleitet werden. Zeigen Sie:

(a) $x^n - 1 = (x - 1)(x^{n-1} + \cdots + x + 1) = \prod_{i=0}^{n-1} (x - w^i)$

(b) char $K \nmid n$
[$(x^{\frac{n}{p}} - 1)^p =$? falls $p =$ char K und $p \mid n$, Nullstellenanzahl?]

(c) $\sum_{j=0}^{n-1} w^{kj} = 0$ für $1 \leq k \leq n - 1$

(d) Δ_w ist ein K-linearer Ringisomorphismus, wenn im K-Vektorraum K^n komponentenweise multipliziert wird (vgl. u. A. §14).

(e) Sei D_w die Matrix von Δ_w bezüglich der kanonischen Basen in V und K^n. Bestimmen Sie D_w und bestätigen Sie die Invertierbarkeit.

(f) $D_w \cdot D_{w^{-1}} = n \cdot E_n$ mit der $n \times n$ Einheitsmatrix E_n.

(g) Was besagt (f) für die Berechung von Δ_w^{-1}?

(42) Leiten Sie die Kettenregel in Satz 17.2(b) her.

$^{(*)}$Wenn $R = \mathbb{C}$ und $w = e^{\frac{2\pi i}{n}}$ entsteht die diskrete Fouriertransformation bei Abtastvorgängen kontinuierlicher Signale. Gute Algorithmen zur schnellen Berechnung der diskreten Fouriertransformation (FFT, F für 'fast') gehören zu den praktisch bedeutsamsten Algorithmen überhaupt, siehe etwa: von zur Gathen und Gerhard, Moderne Computer Algebra, Cambrigde University Press, 2. Auflage, 2003. Die Aufgabe ist größtenteils orientiert an diesem Buch.