Universität Mannheim, Lehrstuhl für Mathematik VI
Prof. Dr. Claus Hertling, Ralf Kurbel

Übungsaufgaben zur Kodierungstheorie

Alle Aufgaben betreffen Kapitel 6.
In Kapitel 6 ist für p eine Primzahl und $n \in \mathbb{N}$ folgende Menge definiert,

$$J_{n,p} := \{f(t) \in \mathbb{F}_p[t] \mid \deg f(t) = n,\ f(t) \text{ unitär und irreduzibel}\}.$$

In Satz 6.14 werden folgende Formeln bewiesen (die zweite verfeinert die erste),

$$\begin{aligned} p^n &= \sum_{r \text{ teilt } n} r \cdot |J_{r,p}| \\ t^{p^n} - t &= \prod_{r \text{ teilt } n} \prod_{f(t) \in J_{r,p}} f(t) \quad \text{in } \mathbb{F}_p[t] \\ &= \prod_{a \in \mathbb{F}_{p^n}} (t-a). \end{aligned}$$

Aus der ersten wird die Formel

$$|J_{n,p}| = \frac{1}{n} \sum_{r \text{ teilt } n} \mu(r) \cdot p^{\frac{n}{r}}$$

gefolgert, und aus dieser $|J_{n,p}| > 0$ und damit $J_{n,p} \neq \emptyset$. Die zweite und dritte Formel zeigen, welche irreduziblen Polynome als Minimalpolynome der Elemente von $\mathbb{F}_{p^n}$ als Körpererweiterung von $\mathbb{F}_p$ auftreten, nämlich alle in $J_{r,p}$ mit r Teiler von n.
Andererseits zeigt Satz 6.18, daß alle Minimalpolynome (von Elementen α von $\mathbb{F}_{p^n}$ als Körpererweiterung von $\mathbb{F}_p$) die spezielle Gestalt $m_{\alpha,p}$ von Satz 6.18 c) haben. Schliesslich folgt aus Satz 6.17 der Gruppenisomorphismus

$$(\mathbb{F}_{p^n} - \{0\}, \cdot) \cong (\mathbb{Z}/(p^n-1)\mathbb{Z}, +).$$

Aus der Struktur der Gruppe $(\mathbb{Z}/(p^n-1)\mathbb{Z}, +)$ kann man wie im Beispiel 6.21 relativ leicht ablesen, welche Grade die Minimalpolynome der Elemente von $\mathbb{F}_{p^n} - \{0\}$ haben und welche von ihnen primitiv (Definition 6.20) sind.

1. *(2 Punkte)* Bestimmen Sie mit der Formel

   $$|J_{n,p}| = \frac{1}{n} \sum_{r \text{ teilt } n} \mu(r) \cdot p^{\frac{n}{r}}$$

   explizitere Formeln für $|J_{n,p}|$ für $1 \leq n \leq 6$, und werten Sie diese 6 Formeln in den Fällen $p = 2$ und $p = 3$ aus.

2. *(4 Punkte)* Für $d \in \mathbb{N} \cup \{0\}$ gibt es 2^d unitäre Polynome vom Grad d in $\mathbb{F}_2[t]$. Jedes mit $d \geq 1$ lässt sich eindeutig als Produkt von unitären und irreduziblen Polynome schreiben. Listen Sie alle $30 = 2 + 4 + 8 + 16$ unitären Polynome der Grade $d \in \{1, 2, 3, 4\}$ und ihre Produkt-Zerlegungen in unitäre und irreduzible Polynome auf.

Bitte wenden!

3. *(2 Punkte)* Die Lösung von Aufgabe 1 zeigt $|J_{6,2}| = 9$, d.h. es gibt 9 unitäre und irreduzible Polynome vom Grad 6 in $\mathbb{F}_2[t]$. Wieviele von ihnen sind primitiv (Definition 6.20)?

   Hinweise: Die Lösung ist ähnlich zu Beispiel 6.21 und benutzt die Struktur der Gruppe $(\mathbb{F}_{p^n} - \{0\}, \cdot) \cong (\mathbb{Z}/(p^n - 1)\mathbb{Z}, +)$. Wieviele Einheiten hat diese Gruppe?
   (Diese Aufgabe erfordert *nicht* die Bestimmung der 9 Elemente von $J_{6,2}$, sondern ist viel einfacher.)

4. *(4 Punkte)* Nach Satz 6.14 und Beispiel 6.15 der Vorlesung ist in $\mathbb{F}_2[t]$

$$t^7 - 1 = (t+1)(t^3 + t + 1)(t^3 + t^2 + 1)$$

   die Zerlegung in irreduzible Faktoren. Weiter ist nach Satz 6.14 der Körper $\mathbb{F}_{2^3}$ konstruierbar als Quotientenring $\mathbb{F}_2[t]/(t^3 + t + 1)$. Sei $\alpha := [t] \in \mathbb{F}_2[t]/(t^3 + t + 1)$. Offenbar ist

$$\mathbb{F}_{2^3} \cong \mathbb{F}_2[t]/(t^3 + t + 1) = \mathbb{F}_2 \cdot 1 \oplus \mathbb{F}_2 \cdot \alpha \oplus \mathbb{F}_2 \cdot \alpha^2.$$

   Weiter sind nach Satz 6.14 die Nullstellen von $t^7 - 1$ genau die Elemente von $\mathbb{F}_{2^3} - \{0\}$. Natürlich ist 1 die Nullstelle von $t + 1$, und natürlich ist α eine Nullstelle von $t^3 + t + 1$.

   Bestimmen Sie die anderen beiden Nullstellen von $t^3 + t + 1$ und die drei Nullstellen von $t^3 + t^2 + 1$. Schreiben Sie sie als Linearkombinationen von $1, \alpha$ und α^2.

   Hinweis: Sie können verschieden vorgehen. Sie können direkt mit den Linearkombinationen in $\mathbb{F}_2 \cdot 1 \oplus \mathbb{F}_2 \cdot \alpha \oplus \mathbb{F}_2 \cdot \alpha^2$ rechnen und die Relation $\alpha^3 + \alpha + 1 = 0$ nutzen. Oder Sie können Satz 6.18 benutzen und erst mit Potenzen von α arbeiten und die nachher in Linearkombinationen von $1, \alpha$ und α^2 umschreiben.

5. *(4 Punkte)* Seien $K \subset L$ zwei Körper. Dann ist L ein K-Vektorraum. Ein Element $\alpha \in L$ heißt *algebraisch über* K, falls die Elemente $1, \alpha, \alpha^2, \alpha^3, ... \in L$ nicht alle linear unabhängig über K sind. Äquivalent dazu ist, dass es ein Polynom $f(t) \in K[t] - \{0\}$ gibt mit $f(\alpha) = 0$.

   In dem Fall gibt es ein solches unitäres Polynom kleinsten Grades, und es ist eindeutig. Es wird *Minimalpolynom von α über K* genannt und hier mit $f_{min,\alpha,K}(t)$ bezeichnet. Dann ist $K[\alpha] = \sum_{i \geq 0} K \cdot \alpha^i$ ein Körper zwischen K und L, und eine K-Basis von ihm ist $1, \alpha, ..., \alpha^{n-1}$ mit $n := \deg f_{min,\alpha,K}$.

   Bestimmen Sie das Minimalpolynom von $\sqrt{3} + \sqrt{5}$ über

   (a) $\mathbb{Q}$,
   (b) $\mathbb{Q}[\sqrt{5}]$.

   Hinweis: Sie dürfen ohne Beweis benutzen, daß $\mathbb{Q}[\sqrt{3} + \sqrt{5}]$ die $\mathbb{Q}$-Basis $1, \sqrt{3}, \sqrt{5}, \sqrt{15}$ hat.

Abgabe am Montag, den 16. April 2012, in der Übung.