Codierungstheorie (Sommersemester 2014)

Irene Bouw, Michel Börner

Blatt: 05
Punkte: 10

Abgabe zu zweit vor der Vorlesung am Di., **27.05.14** um 10:15 Uhr im Raum E 20. Die **Übung** findet nicht am Fr., 30.5., sondern am Mittwoch, 28.5. um 16:00 Uhr im E18 in der Helmholtzstraße 22 statt.

Aufgabe 11 (Existenz und Eindeutigkeit von $\mathbb{F}_8$)

Dies ist eine Fortsetzung von Aufgabe 10, d.h. die Ergebnisse von Blatt 4 dürfen verwendet werden. Es ist $K := \mathbb{F}_2[x]/(x^3+x+1)$ ein Körper und $\alpha \in K$ eine Nullstelle von $f(x) = x^3+x+1$.

a) Finde alle Nullstellen von $f(x)$ in K und schreibe f als Produkt von Linearfaktoren.

b) Zeige, dass $g(x) = x^3+x^2+1 \in \mathbb{F}_2[x]$ ebenfalls irreduzibel ist und zerlege $g \in K[x]$ in Linearfaktoren.

c) Benutze b), um einen expliziten Körperisomorphismus $\varphi : K \xrightarrow{\sim} \mathbb{F}_2[x]/(g) =: K'$ zu konstruieren.

d) Benutze a) und b), um $x^8 - x \in \mathbb{F}_2[x]$ in irreduzible Faktoren zu zerlegen und begründe deine Vorgehensweise. (1+1,5+1,5+1 = **5 P**)

Aufgabe 12 (Minimalpolynome)

a) Zeige, dass $f(x) = x^5+x^2+1 \in \mathbb{F}_2[x]$ irreduzibel ist. Damit ist $\mathbb{F}_{32} := \mathbb{F}_2[x]/(f)$ ein Körper.

b) Sei $\alpha \in \mathbb{F}_{32}$ ein Element mit Minimalpolynom $\min_{\mathbb{F}_2}(\alpha) = x^5+x^2+1$. Berechne die Ordnung von α.

c) Bestimme $\min_{\mathbb{F}_2}(\alpha^2+1)$.

d) Bestimme $s \in \mathbb{N}$ minimal, so dass $h(x) = (x^2+x+1)\cdot(x^3+x+1) \in \mathbb{F}_{2^s}[x]$ in Linearfaktoren zerfällt. (1+0,5+2+1,5 = **5 P**)

Endliche Körper in Maple

Folgende Befehle sollten sich als nützlich erweisen für die gesamte Vorlesung, dürfen aber **nicht** die von Hand gerechnete und begründete Lösung ersetzen.

```
> expand((x-1)*(x-2));
> quo(x^2+3, x+1, x);
> rem(x^2+3, x+1, x);
> gcd(x^3+2*x^2+x+2, x^2+5*x+6);
> factor(x^3+2*x^2+x+2);
> Factor(x^3+x^2+1) mod 3;
```

Maple ist in den kiz-Pools verfügbar, einfach 'maple kiz ulm' googeln für eine Anleitung.
Oder von einem beliebigen Rechner ssh aufrufen:

```
ssh benutzername@giessen.rz.uni-ulm.de     # oder gera, fulda, erfurt, aachen, ...
Password: ...
giessen$ module load math/maple
giessen$ maple
...
> Factor(x^4+x+1) mod 2;
...
> quit;
```