Einführung in die Algebra und Diskrete Mathematik
12. Übungsblatt für den 25. Juni 2009

1. Bestimmen Sie Multiplikations- und Additionstafel für GF(8).

   Lösung: GF(8) ist isomorph zu $Z_2[x]/(f)$ für $f = x^3 + x + 1$.
   Elemente sind also von der Form $[ax^2 + bx + c]_f$ für $a, b, c \in \mathbb{Z}_2$.

2. Bestimmen Sie alle primitiven Elemente von GF(7).

   Lösung: $[3]_7, [5]_7$

3. Bestimmen Sie alle primitiven Elemente von GF(8). Wählen Sie eines aus und stellen Sie alle anderen Elemente $\neq 0$ als Potenzen davon dar.

   Lösung: Die multiplikative Gruppe von GF(8) ist isomorph zu $(\mathbb{Z}_7, +)$.
   Also ist jedes Element $\neq 1$ primitiv.

4. Finden Sie den kleinsten Erweiterungskörper von GF(3) in dem $f = x^2 + 1$ in Linearfaktoren zerfällt. Ist f primitiv?

   Lösung: f zerfällt in GF(3)/(f), aber in keinem kleineren Körper.

   f teilt $x^4 - 1$, dh. f hat Exponent $4 < 8$ und ist nicht primitiv (maximalperiodisch).

5. Sei f ein irreduzibles Polynom vom Grad n über GF(p). Zeigen Sie, dass f in GF(p^n) eine Nullstelle a hat und in folgendes Produkt von Linearfaktoren zerfällt:

   $$f = \prod_{i=0}^{n-1}(x - a^{p^i})$$

   [Hinweis: Zeigen Sie, dass f keine mehrfachen Nullstellen hat und dass mit a auch a^p eine Nullstelle von f ist.]

   Lösung: GF(p^n) ist isomorph zu $\mathbb{Z}_p[x]/(f)$.

   Sei $f = \sum_{i=0}^{n} b_i x^i$ mit $b_i \in \mathbb{Z}_p$. Wegen $\sum_{i=0}^{n} b_i [x]_f^i = [f]_f = [0]_f$, ist $a := [x]_f$ in $\mathbb{Z}_p[x]/(f)$ eine Nullstelle von f .

   Wegen

   $$0 = (\sum_{i=0}^{n} b_i a^i)^p$$

$$= \quad (\sum_{i=0}^{n} b_i^p a^{pi}) \qquad \text{Aufgabe 11.4}$$

$$= \quad (\sum_{i=0}^{n} b_i a^{pi}) \qquad \text{Satz von Fermat}$$

ist a^p ebenfalls Nullstelle von f. Genauso sind alle a^{p^i} für $i \in \mathbb{N}_0$ Nullstellen.

Es bleibt zu zeigen, dass $a, a^p, \ldots, a^{p^{n-1}}$ paarweise verschieden sind. Angenommen, $a^{p^i} = a^{p^j}$ für $0 \leq i \leq j < n$. Potenzieren mit p^{n-j} ergibt $a^{p^{n+i-j}} = a^{p^n} = a$. Also gilt $f | x^{p^{n+i-j}} - x$.

Das heisst, dass f in GF(p^{n+i-j}) in Linearfaktoren zerfällt. Insbesonders ist die Nullstelle $a \in GF(p^{n+i-j})$. Weil $GF(p^{n+i-j})$ abgeschlossen unter Addition und Multiplikation ist, ist für alle $c_0, \ldots, c_n \in \mathbb{Z}_p$ auch $\sum_{i=0}^{n} c_i a^i$ in GF(p^{n+i-j}). Damit enthält GF(p^{n+i-j}) alle Elemente aus GF(p^n) und $p^n \leq p^{n+i-j}$. Daraus folgt $i = j$. Also sind $a, a^p, \ldots, a^{p^{n-1}}$ genau n unterschiedliche Nullstellen von f und $f = \prod_{i=0}^{n-1}(x - a^{p^i})$.