Einführung in die Algebra und Zahlentheorie
Übungsblatt 13

Abgabetermin Donnerstag, den 03.02.2010 vor der Vorlesung.

0. Wiederholen Sie Abschnitt 6 im Vorlesungsmanuskript.

1. Betrachten Sie das Polynom
$$f = x^9 - x \in \mathbb{F}_3[x]$$
mit Koeffizienten in dem Körper $\mathbb{F}_3 = \mathbb{Z}/3$ mit 3 Elementen.
   (a) Zerlegen Sie f in irreduzible Faktoren $f_i \in \mathbb{F}_3[x]$.
   (b) Bestimmen Sie zu jedem Faktor f_i die Nullstellen in $\mathbb{F}_9 \cong \mathbb{F}_3[x] / (x^2+1)$.

2. (a) Bestimmen Sie alle Unterkörper von $\mathbb{F}_{2^{36}}$ und die Inklusionsbeziehungen zwischen diesen.
   (b) Beschreiben Sie die Körpererweiterung $\mathbb{F}_4 \subset \mathbb{F}_{16}$ als
$$\mathbb{F}_{16} = \mathbb{F}_4[y] / (g)$$
mit $g \in \mathbb{F}_4[y]$ irreduzibel.

3. Seien $K \subset L \subset M$ Körpererweiterungen. Zeigen Sie
$$K \subset M \text{ algebraisch} \iff K \subset L \text{ und } L \subset M \text{ algebraisch}$$

4. Sei $K \subset L$ eine Körpererweiterung und A die Menge der über K algebraischen Elemente von L. Zeigen Sie:
   (a) A ist ein Körper und $K \subset A$ ist algebraisch.
   (b) Ist $a \in L$ algebraisch über A, dann schon über K.
   (c) War L algebraisch abgeschlossen, dann ist A der algebraische Abschluss von K.
   (d) Der Körper $A = \overline{\mathbb{Q}}$ der über $K = \mathbb{Q}$ algebraischen Elemente von $L = \mathbb{C}$ ist abzählbar.

5. (4 Zusatzpunkte) Schreiben Sie (z.B. in Maple) jeweils eine Funktion, die
   (a) alle normierten, irreduziblen Polynome vom Grad $r \in \mathbb{N}$ in $\mathbb{F}_p[x]$ aufzählt.
   (b) für ein gegebenes normiertes irreduzibles $f \in \mathbb{F}_p[x]$ vom Grad r die Elemente von $\mathbb{F}_{p^r} \cong \mathbb{F}_p[x] / (f)$ bestimmt, d.h. für jedes Element seinen Repräsentanten vom Grad $< r$.
   (c) auf der Menge dieser Repräsentanten die Addition, Multiplikation und Bildung des Inversen implementiert.
   (d) alle zyklischen Erzeuger von $\mathbb{F}_{p^r}^{\times}$ bestimmt.

   Hinweis: Maple-Funktionen `Irreduc`, `Rem`, `Gcdex`, `mod`.