Institut für Mathematische Optimierung
TU Braunschweig

SS 2006

Prof. Dr. Sándor Fekete
Nils Schweer

Coding Theory / Discrete Mathematics II
Assignment 3 (May 11, 2006)

(This assignment is due on May 18, 2006, 1.00 p.m., by dropping it into the wooden box **in front of** F 310)

Exercise 1 (Field):
Show that $\mathbb{Q}(\sqrt[3]{2}) = \{a + b \cdot \sqrt[3]{2} + c \cdot (\sqrt[3]{2})^2 : a, b, c \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$.
(Hint: In order to prove the existence of a unique inverse element you can do the following: Consider the equation $s \cdot r = 1$ with $r = r_1 + r_2 \cdot \sqrt[3]{2} + r_3 \cdot (\sqrt[3]{2})^2$ and $s = s_1 + s_2 \cdot \sqrt[3]{2} + s_3 \cdot (\sqrt[3]{2})^2$. Multiply r and s and compare the coefficients on both sides of the equation. Show that the resulting system of linear equations has a unique solution.)

(40 Points)

Exercise 2 (Squares):
Consider $\mathbb{Z}_p$ with p being an odd prime number. Let $h \leq \lfloor \frac{p}{2} \rfloor$. Show that the squares $0^2, 1^2, \ldots, h^2$ are pairwise different modulo p.

(20 Points)