Martin Schlichenmaier

Exam, June 2011

Basic Algebraic Structures

Master in Computer Science

Attention: It is not enough to give only the results. Depending on the context, arguments, proofs, and/or calculations are necessary.

Time: **120 minutes**. (Attention the exam consists of two pages.)

The use of supporting tools is **not allowed**, e.g. neither written documents, nor computers, nor calculators, nor portables, nor other electronic devices.

Problem 1.

Let $(G, \cdot)$ be a finite group and a an element of G, $a \in G$.

(a) What is the definition of the order $ord(a)$?

(b) What is the statement of the *Little Theorem of Fermat* ?

(c) Is there any relation between the order $ord(a)$ of a and the number of elements $N = \#G$ in the group G ? If yes, give this relation (and arguments for it)?

Problem 2.

Let $(G, \cdot)$ be a group with $\#G = p$, p a prime number. Let e be the neutral element.

(a) Show that every element $a \in G$ with $a \neq e$ is a generator of G.

(b) Give all subgroups of G.

(c) Is G a commutative group?

Problem 3.

Let $\mathbb{F}_7$ be the field with exactly 7 elements. We write its elements in the standard form (mod 7) as $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$.

(a) Give for each $\bar{a}$ its additive inverse (give the result in standard form), *(without proof)*.

(b) Give for each $\bar{a} \neq \bar{0}$ its multiplicative inverse (give the result in standard form), *(without proof)* .

(c) The group $(\mathbb{F}_7, +)$ is a cyclic group. Why? Give all its generators.

(d) From the lectures it is known that $(\mathbb{F}_7 \setminus \{\bar{0}\}, \cdot)$ is a cyclic group. Give all its generators (explain why these elements are generators).

(e) An element a of a field $\mathbb{K}$ is called a square if there exists $b \in \mathbb{K}$, such that $b \cdot b = b^2 = a$. Determiner in $\mathbb{F}_7$ all squares.

Problem 4.

Consider the real polynomial ring $\mathbb{R}[X]$.

(a) Show that the polynomial $f(X) = X^2 + 1$ is irreducible over $\mathbb{R}$.

(b) What is the $gcd(X^2 + 1, X - 2)$?

(c) As known from the lectures/exercises, from f irreducible it follows that $\mathbb{K} := \mathbb{R}[X]/(f)$ is a field. What is the multiplicative inverse of $X - 2 \mod f$ considered as element in $\mathbb{K}$?

(d) Do you know to which well-known field, the constructed field $\mathbb{K}$ is isomorphic to?

Problem 5.

Let $\mathbb{F}_{2^2}$ be the unique finite field with 4 elements.

(a) Give its addition and multiplication tables.

(b) What is the characteristics ($char$) of the field $\mathbb{F}_{2^2}$?

(c) Explain how this field can be obtained starting from the polynomial ring over a suitable field. (*Hint: Have a look on Problem 4.*)

Problem 6.

The following polynomials are considered as polynomials over the real numbers $\mathbb{R}$.

(a) What is the greatest common divisor $gcd(X^4 - 1, X^2 - 1)$?

(b) What is the greatest common divisor $gcd(5X^3 + 2X^2 + X, X^2 + X)$?