MIE-MPI: Tutorial 7

`created: November 5, 2019, 12:06`

7.1 Rings and fields

Exercise 7.1. Which of the following sets with the classical addition and multiplication are rings or fields?

(a) The set of all even numbers.

(b) The set of all odd numbers.

(c) The set of non-negative even numbers.

(d) The set of rational numbers.

Exercise 7.2. Is the set of matrices $(\mathbb{R}^{n,n}, +, \cdot)$ with matrix multiplication and addition a ring? Is it a field? If not, how can we change it to get a field?

7.2 Finite fields of order p^n

Exercise 7.3. Find the Cayley table for both operations in the field $GF(2^2)$, where the multiplication is done modulo $x^2 + x - 1$. Find neutral elements and generators in the additive group and the multiplicative group of this field. Find also the inverse elements of $x + 1$ and x.

Exercise 7.4. Find the Cayley table for $GF(3^2)$, where the multiplication is done mod $x^2 - x - 1$.

Exercise 7.5. Find all irreducible polynomials of degree less than 5 from the ring $\mathbb{Z}_2[x]$.

Exercise 7.6. Consider the field $GF(2^3)$, where the multiplication is done mod x^3+x+1.

(a) Decide whether $x^3 + x + 1$ is irreducible over $\mathbb{Z}_2$.

(b) Find the inverse of 010.

(c) Calculate

$$100 \cdot (010)^{-1} + 010 \cdot 010.$$

Exercise 7.7. In the field $GF(3^3)$ with multiplication modulo $x^3 + 2x + 1$ find

(a) the inverse of 122,

(b) all y from this field satisfying

$$211 \cdot (100 + y) = 002\,.$$

Exercise 7.8. Let $v(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ be a polynomial from $\mathbb{Z}_p[x]$ with p prime and m positive integer. Show that

$$(v(x))^p = v(x^p).$$

 © KAM FIT, CTU in Prague