Практикум - први час

Никола Велов

Прва недеља

1 Теоријски увод

Поље је уређена тројка $(F, +, \cdot)$ где су $+ : F \times F \to F$ и $\cdot : F \times F \to F$ бинарне операције, при чему важе следећа својства:

1° (**асоцијативност** за $+$) За све x, y, z из F је: $x + (y + z) = (x + y) + z$
2° (**комутативност** за $+$) За све x, y из F је: $x + y = y + x$
3° (**јединични елемент** за $+$) Постоји 0 из F такво да је за свако x из F: $x + 0 = 0 + x = x$
4° (**инверзни елемент** за $+$) За свако x из F постоји $-x$ из F такво да је: $x + (-x) = (-x) + x = 0$
5° (**асоцијативност** за $\cdot$) За све x, y, z из F је: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6° (**комутативност** за $\cdot$) За све x, y из F је: $x \cdot y = y \cdot x$
7° (**јединични елемент** за $\cdot$) Постоји 1 из F такво да је за свако x из F: $x \cdot 1 = 1 \cdot x = x$
8° (**инверзни елемент** за $\cdot$) За свако $x \neq 0$ из F постоји x^{-1} из F такво да је: $x \cdot x^{-1} = x^{-1} \cdot x = 1$
9° (**дистрибутивност** $\cdot$ према $+$) За све x, y, z из F важи:
$x \cdot (y + z) = x \cdot y + x \cdot z$.

Примери поља са којима смо навикли да радимо: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$.

2 Задаци

1. Нека је $m \in \mathbb{N}$ природан број. Кажемо за целе $m > 1$ бројеве $a, b \in \mathbb{Z}$ да су конгруентни по модулу m ако $m \mid a - b$ односно постоји цео број k такав да је $a - b = m \cdot k$.

   a) Доказати да је конгруенција по модулу m релација еквиваленције.

   b) Доказати за $a, b, c, d \in \mathbb{Z}$ да важи
   $a \equiv b \pmod{m}$, $c \equiv d \pmod{m} \implies$
   $a + c \equiv b + d \pmod{m}$; $a \cdot c \equiv b \cdot d \pmod{m}$.

   c) Доказати $3^6 \equiv 4 \pmod{5}$, $10^7 \equiv 1 \pmod{9}$, $-2 \equiv 8 \pmod{10}$.

2. Нека је p прост број и $\mathbb{F}_p = \{0, 1, \dots, p-1\}$. Дефинишемо $+_p : \mathbb{F}_p \times \mathbb{F}_p \to F_p$ са $a +_p b := (a + b) \pmod{p}$, односно $a +_p b$ је остатак који $a + b$ даје при дељењу са p и $a \cdot_p b := (a \cdot b) \pmod{p}$, односно односно $a \cdot_p b$ је остатак који $a \cdot b$ даје при дељењу са p.

   a) Доказати да је $\mathbb{F}_p$ поље.

   b) Израчунати 5^{-1} у $\mathbb{F}_7$, $\mathbb{F}_{13}$ и $\mathbb{F}_{17}$.

   c) Израчунати $6 \cdot 3$ у $\mathbb{F}_7$, $\mathbb{F}_{13}$ и $\mathbb{F}_{17}$.

3. Посматрајмо систем $\begin{cases} 3\mathrm{x} + 2\mathrm{y} = 0 \\ 2\mathrm{x} + 3\mathrm{y} = 0 \end{cases}$

   a) Доказати да постоје јединствени реални бројеви (x_0, y_0) који задовољавају систем.

   b) Посматрајмо овај систем у $\mathbb{F}_5$. Показати да решење у $\mathbb{F}_5$ није јединствено.

   c) Нека је $p \neq 5$ прост број. Да ли је тада решење јединствено?