Teorema 1 (Wedderburn)**.** *Orice corp finit este comutativ.*

Teorema 2. *F este un corp finit dacă şi numai dacă există p un număr prim şi există $f \in \mathbb{Z}_p[X]$ un polinom ireductibil astfel încât*

$$F \cong \mathbb{Z}_p[X]/(f).$$

Observaţia 3. Teorema de mai sus ne spune că pentru orice corp finit F există un polinom $X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{Z}_p[X]$, ireductibil peste $\mathbb{Z}_p$ astfel încât F poate fi scris sub forma

$$F = \{\alpha_0 + \alpha_1 t + \ldots + \alpha_{n-1}t^{n-1} \mid \alpha_0 \ldots, \alpha_{n-1} \in \mathbb{Z}_p\},$$

unde t satiface egalitatea $t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 = 0$ (adică t este o rădăcină a polinomului de mai sus).

Teorema 4. *Orice două corpuri finite cu acelaşi număr de elemente sunt izomorfe.*

Ex. 1. Completaţi tablele operaţiilor pentru corpurile cu 2,4, 8, 16, 3, 9 respectiv 27 de elemente.

Soluţie. Corpurile cu 2, respectiv 3 elemente sunt $F_2 = (\mathbb{Z}_2, +, \cdot)$ şi $F_3 = (\mathbb{Z}_3, +, \cdot)$. (Tema: Scrieţi efectiv tablele operaţiilor!).

Caclulăm F_4 astfel: $4 = 2^2$, deci vom cauta un polinom de gradul al doilea ireductibil peste $\mathbb{Z}_2$. De exemplu $X^2 + X + 1$ este un astfel de polinom (calculele sunt făcute modulo 2, dar scriem simplu 0 sau 1 în loc de $\hat{0}$ sau $\hat{1}$). Atunci

$$\begin{aligned} F_4 &= \{\alpha_0 + \alpha_1 t \mid \alpha_0, \alpha_1 \in \mathbb{Z}_2, t^2 = t + 1 (= -t - 1)\} \\ &= \{0, 1, t, 1 + t\}. \end{aligned}$$

Este clar că $(F_4, +) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$. Calcuăm înmulţirea:

$0x = 0$ pentru orice $x \in F_4$

$1x = x$ pentru orice $x \in F_4$

$t^2 = 1 + t$

$t(1 + t) = t + t^2 = t + t + 1 = 1$

$(1 + t)(1 + t) = (1 + t)^2 = 1 + 2t + t^2 = 1 + t^2 = 1 + 1 + t = t.$

Deci obţinem tablele

$+$	0	1	t	$1+t$
0	0	1	t	$1+t$
1	1	0	$1+t$	t
t	t	$1+t$	0	1
$1+t$	$1+t$	t	1	0

$\cdot$	0	1	t	$1+t$
0	0	0	0	0
1	0	1	t	$1+t$
t	0	t	$1+t$	1
$1+t$	0	$1+t$	1	t

Analog pentru F_9: $9 = 3^2$ deci căutam un polinom de grad 2 peste $\mathbb{Z}_3$. De exemplu $X^2 + 1$ este un asfel de polinom. Prin urmare

$$\begin{aligned} F_9 &= \{\alpha_0 + \alpha_1 t \mid \alpha_0, \alpha_1 \in \mathbb{Z}_3, t^2 + 1 = 0\} \\ &= \{0, 1, -1, t, 1+t, -1+t, -t, 1-t, -1-t\} \end{aligned}$$

Atunci $(F_9, +) \cong (\mathbb{Z}_3 \times \mathbb{Z}_3, +)$, iar pentru înmulţire procedem astfel: înmulţim elementele din F_9 ca polinoame în nedetreminata t şi apoi luăm restul la împarţirea cu $1 + t^2$ pentru că $1 + t^2 = 0$ in F_9. (Aşa se procedează în general, aşa am procedat şi pentru F_4, unde am împărţit la $t^2 + t + 1 = 0$, doar ca nu am enunţat în mod explicit procedeul.) De exemplu

$$(1+t)(1-t) = 1 - t^2 = -(1+t^2) - 1 = -1,$$

$$(-1+t)t = -t + t^2 = (t^2+1) - 1 - t = -1 - t \text{ etc. (restul temă).}$$

Pentru $F_8 = F_{2^3}$ căutăm un polinom ireductibil de grad 3 peste $\mathbb{Z}_2$. De exxemplu $X^3 + X + 1$.

Pentru $F_{16} = F_{2^4}$ căutm un polinom ireductibil de grad 4 peste $\mathbb{Z}_2$, de exemplu $X^4 + X^2 + 1$.

Pentru $F_{27} = F_{3^3}$ a se vedea exerciţiul 3 de mai jos.

Ex. 2. (a). Arătaţi că într-un corp comutativ K ecuaţia $x^2 = a$, unde $a \in K$ este arbitrar, are cel mult 2 soluţii.

(b). În care corpuri comutative este valabilă formula uzuală de rezolvare a ecuaţiei de gradul al doilea?

Soluţie. Fie K un corp cumutativ (finit sau infinit!).

(a). Dacă nu există $b \in K$ astfel încât $b^2 = a$, atunci ecuaţia data nu are soluţii. Dacă există $b \in K$ astfel încât $b^2 = a$, atunci

$$0 = x^2 - a = x^2 - b^2 = (x-b)(x+b),$$

iar pentru că un corp nu are divizori ai lui zero $x-b=0$ sau $x+b=0$, deci ecuaţia dată are soluţiile b şi $-b$ (ele pot fi egale sau diferite, dar sunt cel mult două).

(b). Considerăm o ecuaţie de gradul al doilea

$$ax^2+bx+c=0,\ a,b,c\in K, a\neq 0.$$

Scriem ecuaţia în forme echivalente (împărţim cu a, apoi formăm pătrat perfect etc.):

$$\begin{aligned}
&a(x^2+a^{-1}bx+a^{-1}c)=0\\
&x^2+a^{-1}bx+a^{-1}c=0\\
&x^2+2(2^{-1}a^{-1}b)x+a^{-1}c=0 \text{ (aici 2 înseamnă } 1+1)\\
&x^2+2(2^{-1}a^{-1}b)x+(2^{-1}a^{-1}b)^2-(2^{-1}a^{-1}b)^2+a^{-1}c=0\\
&(x+2^{-1}a^{-1}b)^2-2^{-2}a^{-2}b^2+a^{-1}c=0\\
&(x+2^{-1}a^{-1}b)^2=2^{-2}a^{-2}b^2-a^{-1}c=0\\
&(x+2^{-1}a^{-1}b)^2=2^{-2}a^{-2}(b^2-2^2ac)\\
&(x+2^{-1}a^{-1}b)^2=(2^{-1}a^{-1})^2\Delta \text{ unde } \Delta=b^2-2^2ac.
\end{aligned}$$

Conform cu cele discutate la (a) dacă nu există $\delta\in K$ astfel încât $\delta^2=\Delta$ atunci ecuaţia nu are soluţii în K. Dacă există $\delta\in K$ astfel încât $\delta^2=\Delta$ atunci

$$x+2^{-1}a^{-1}b=\pm 2^{-1}a^{-1}\delta,$$

deci ecuaţia iniţială are soluţiile:

$$x_{1,2}=2^{-1}a^{-1}(-b\pm\delta).$$

Revenind asupra argumentului de mai sus, putem constata că am folosit numai proprietăţi valabile în general într-un corp comutativ, cu o singură excepţie şi anume când am considerat $2^{-1}=(1+1)^{-1}$. Pentru ca argumentul să fie valid, trebuie ca să existe 2^{-1} în K, deci trebuie ca $2\neq 0$ (corpul K să nu aibă caracteristica 2).

Ex. 3. (a). Demonstraţi că

$$F=\{\alpha_0+\alpha_1t+\alpha_2t^2\mid \alpha_0,\alpha_1,\alpha_2\in\mathbb{Z}_3, t^3=t-1\}$$

şi

$$G=\{\beta_0+\beta_1t+\beta_2t^2\mid \beta_0,\beta_1,\beta_2\in\mathbb{Z}_3, t^3=t^2-t-1\}$$

sunt corpuri izomorfe.

(b). Rezolvaţi în F ecuaţia $x^3-x+1=0$ (remarcăm ca toate calculele sunt făcute modulo 3, dar scriem simplu 0 sau 1 în loc de $\hat{0}$ sau $\hat{1}$ etc.).

Soluţie. (a). Polinoamele X^3-X+1 şi X^3-X^2+X+1 sunt ireductibile peste $\mathbb{Z}_3$ (verificare directă!) deci F şi G sunt ambele corpuri cu 27 elemente, ceea ce implică $F \cong G$.

(b). t este o solutie a ecuaţiei $x^3 - x + 1 = 0$, deci $(X - t)$ divide X^3-X-1. Facem împărţirea la $X-t$ (unde ţinem cont că $t^3-t+1 = 0$):

$$\begin{aligned} X^3 - X - 1 &= X^3 - tX^2 + tX^2 - t^2X + (t^2 - 1)X - t(t^2 - 1) + (t^3 - t + 1) \\ &= X^2(X - t) + tX(X - t) + (t^2 - 1)(X - t) + 0 \\ &= (X^2 + tX + t^2 - 1)(X - t). \end{aligned}$$

Rezolvăm acum excuaţia $X^2 + tX + (t^2 - 1) = 0$ (corpul are caracteristica $3 \neq 2$ deci putem aplica formula):

$$\Delta = t^2 - 4(t^2 - 1) = t^2 - t^2 + 4 = 4 = 1,$$

iar posibilele soluţii ale ecuaţiei $\delta^2 = 1$ sunt 1 şi -1. Găsim aşadar soluţiile ecuaţiei de gredul al doilea:

$$x_{1,2} = 2^{-1}(-t \pm 1) = -(-t \pm 1) = t \mp 1.$$

În final soluţiile ecuaţiei de gradul al treilea sunt $t, t - 1, t + 1$.