Elemente de teoria corpurilor

Toate corpurile considerate aici sunt comutative.

Fie F un corp şi $f, g \in F[X]$. Spunem că f divide g (şi notăm $f \mid g$) dacă există $h \in F[X]$ astfel încât $g = fh$. Mai spunem în această situaţie că f este divizor al lui g sau că g este multiplu pentru f.

Polinomul $f \in F[X]$ se numeşte *ireductibil* dacă $f \notin R$ (i.e. $\mathrm{grad}(f) \geq 1$) şi din $f = gh$ rezultă $g \in F$ sau $h \in F$ (adică f nu are divizori netriviali).

Teorema 1. *Dacă F este un corp, atunci orice polinom din $F[X]$ are o descompunere într-un produs cu toţi factorii polinoame ireductibile. Mai mult, descompunerile în polinoame ireductibile au următoarea proprietate de unicitate:*
dacă $f = p_1 \dots p_k = q_1 \dots q_l$, unde polinoamele $p_1, \dots, p_k, q_1, \dots, g_l$ sunt ireductibile, atunci $k = l$ şi după o permutare a polinoamelor q_j, $j = 1, \dots, k$, avem

$$\forall i = \overline{1, k}, \exists \alpha_i \in F: \; q_i = \alpha_i f_i.$$

Exemplul 2. Pentru $f = 15x^6 - 15 \in \mathbb{Q}[X]$ putem găsi descompunerile:

$$f = 15(X^3-1)(X^3+1) = (3X-3)(5X^2+5X+5)(X+1)(X^2-X+1),$$

respectiv

$$f = 15(X^2-1)(X^4+X^2+1) = (3X+3)(5X-5)(X^2+X+1)(X^2-X+1).$$

Fie $f = a_nX^n + \cdots + a_1X + a_0 \in F[X]$. Funcţia $\widetilde{f} : F \to F$, $f(a) = a_na^n + \cdots + a_1a + a_0$ se numeţe funcţia polinomială asociată lui f. Pentru comoditatea scrierii vom scrie $f(a)$ în loc de $\widetilde{f}(a)$.

Observaţia 3. Este posibil ca polinoame diferite să inducă aceeaşi funcţie polinomială. De ex. $f = X + \widehat{1}$ şi $g = X^3 + X^2 + X + \widetilde{1}$ din $\mathbb{Z}_2[X]$ induc aceeaşi funcţie polinomială.

Un element $a \in F$ este *rădăcină* pentru $f \in F[X]$ dacă $\widetilde{f}(a) = 0$.

Propoziţia 4. *Un element $a \in F$ este rădăcină pentru $f \in F[X]$ dacă şi numai dacă $X - a \mid f$.*

Proof. Scriem $f = (X - a)q + r$, unde $r \in F$ (teorema împărţirii cu rest). Consclzia este acum evidentă. ☐

Corolarul 5. *Un polinom din $F[X]$ de grad 2 sau 3 este ireductibil ddacă nu are rădăcini în F.*

Teorema 6. *Un polinom de grad $n \geq 0$ cu coeficienţi într-un corp comutativ F are cel mult n rădăcini în F.*

Observaţia 7. Dacă $f \in F[X]$ are gradul n şi are n răd acini, atunci el admite o descompunere

$$f = a_n(X - r_1) \dots (X - r_n),$$

unde a_n este coeficientul termenului dominant al lui f şi $r_1, \dots, r_n$ sunt rădăcinile lui f (acestea nu sunt neapărat distincte).

Temă: Demonstraţi că dacă $F[X]/(f)$ este un corp, atunci f este ireductibil.

Teorema 8. *Fie $f = a_nX^n + \dots + a_1X + a_0 \in F[X]$ un polinom ireductibil de grad n. Atunci:*

(1) $F[X]/(f)$ este un corp (unde $(f) = fF[X]$ este idealul generat de f);
(2) $\varphi : F \to F[X]/(f)$, $\varphi(a) = a + (f)$, este un morfism injectiv de corpuri;
(3) $F[X]/(f)$ este un F-spaţiu vectorial de dimensiune n faţă de înmulţirea cu scalari $\alpha(g + (f)) = \alpha g + (f)$, iar $(1 + (f), X + (f), \dots, X^{n-1} + (f))$ reprezintă o bază a acestuia.
(4) Polinomul $\varphi(f) = \varphi(a_n)Y^n + \dots + \varphi(a_1)Y + \varphi(a_0) \in (F[X]/(f))[Y]$ are răd acina $X + (f)$.

Dacă F este un subcorp al corpului E, atunci spunem că E este o *extindere* a lui F.

Fie $f \in F[X]$ un polinom de grad n. Spunem că o extindere E a lui f este *corpul de descompunere* al lui f dacă f are n rădăcini în E şi E este generat de F şi de rădăcinile lui f.

Teorema 9. *Orice polinom $f \in F[X]$ cu $\operatorname{grad}(f) \geq 1$ are un corp de descompunere. Orice două corpuri de descompunere ale lui f sunt izomorfe.*

Exemplul 10. 1) $f = x^2 + 1 \in \mathbb{Q}[X]$. Corpul să de descompunere este $\mathbb{Q}(i) = \{a + ib \mid a, b \in \mathbb{Q}\}$.
2) $f = x^2 + 1 \in \mathbb{R}[X]$. Corpul să de descompunere este $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$.
3) $f = (x^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$. Corpul să de descompunere este

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}.$$

Exemplul 11. $f = X^3 + X + 1 \in \mathbb{Z}_2[X]$ este un polinom ireductibil peste $\mathbb{Z}_2$. Dacă $E = \mathbb{Z}_2[X]/(f)$, atunci polinomul $F = Y^3 + Y + 1 \in E$ are rădăcina $e = X + (f)$.

Căutăm o descompunere $Y^3 + Y + 1 = (Y - e)q(Y)$ cu $q(Y)$ polinom de grad 2 peste E. Prin calcule se obţine

$$Y^3 + Y + 1 = [Y - (X + (f))][Y - (X^2 + X + (f))][Y - (X^2 + (f))].$$

Obs. Orice element din E este reprezentat de un polinom de grad cel mult 2.

1. Corpuri finite

Teorema 12. (Wedderburn) *Orice corp finit este comutativ.*

In continuare prezentăm câteva rezultate legate de structura corpurilor finite.

Teorema 13. *Dacă p este un număr prim şi $f \in \mathbb{Z}_p[X]$ este un polinom ireductibil de grad $n > 0$ peste $\mathbb{Z}_p$ atunci $F = \mathbb{Z}_p[X]/f\mathbb{Z}_p[X]$ este un corp cu p^n elemente.*

Proof. Aplicăm Teorema 8. □

Observaţia 14. In $\mathbb{Z}_p[X]/f\mathbb{Z}_p[X]$ fiecare element este reprezentat de un polinom de grad cel mult $n-1$. Dacă $g \in \mathbb{Z}_p[X]$, atunci $g+(f) = r+(f)$, unde r este restul împărţirii lui g la f. Calculele se realizează într-un mod similar cu calculele din inelele clase de resturi.

Exemplul 15. 1) Polinomul $f = X^3 + X^2 + \widehat{1} \in \mathbb{Z}_2[X]$ este ireductibil. Deci $\mathbb{Z}_2[X]/(X^3 + X^2 + \widehat{1})$ este un corp cu 8 elemente. In acest corp $X^3+(f) = -X^2-\widehat{1}+(f) = X^2+\widehat{1}+(f)$. Deci $X^4+(f) = X^3+X+(f) = X^2 + X + \widehat{1} + (f)$.

Exemplu de calcul: $[X^2 + (f)][X + 1 + (f)] = X^3 + X^2 + (f) = -\widehat{1} + (f) = \widehat{1} + (f)$.
$[X^2 + (f)][X^2 + 1 + (f)] = X^4 + X^2 + (f) = X^2 + X + \widehat{1} + X^2 + (f) = X + \widehat{1} + (f)$.

2) Polinoamele $x^2 + \widehat{1}$ şi $X^2 + X + \widehat{2}$ sunt ireductibile peste $\mathbb{Z}_3$. Deci $\mathbb{Z}_3/(x^2 + \widehat{1})$ şi $\mathbb{Z}_3/(x^2 + X + \widehat{2})$ sunt corpuri cu 9 elemente.

3) $\mathbb{Z}_5/(x^3 - \widehat{3})$ este un corp cu 5^3 elemente.

Propoziţia 16. *Dacă F este un corp finit, atunci există p un număr prim şi $n \in \mathbb{N}^\star$ astfel încât $|F| = p^n$*

Proof. Caracteristica lui F este un număr natural nenul (pentru că F este finite), deci este un număr prim p (pentru că F este corp). Subcorpul prim $P(F)$ al lui F (vezi Seminarul 13) este un corp cu p elemente, iar înmulţirea cu elementele lui $P(F)$ determină pe F are o structură de $P(F)$ spaţiu vectorial. Cum F este finit, rezultă că el are o bază finită. Dacă n este dimensiunea lui F ca $P(F)$-spaţiu vectorial, atunci $|F| = p^n$. □

Lema 17. *Fie $(G, \cdot)$ un grup abelian finit. Presupunem că $g \in G$ are proprietatea că $\forall x \in G$, $\operatorname{ord}(x) \leq \operatorname{ord}(g)$. Atunci $\forall x \in G$, $\operatorname{ord}(x) | \operatorname{ord}(g)$.*

Propoziţia 18. *Dacă F este un corp finit, atunci $(F^\star, \cdot)$ este un grup ciclic.*

Proof. Folosind Teorema lui Wedderburn obţinem că $(F^\star, \cdot)$ este un grup abelian finit. Fie m valoarea maximă din mulţimea ordinelor elementelor lui $F^\star$. Din Lema anterioară deducem că pentru orice $x \in F^\star$ avem $x^m = 1$. Rezultă că polinomul $X^m - 1$ are $|F^\star| = q - 1$ rădăcini. Deci $q - 1 \leq m$. Dar inegalitatea inversă rezultă din Teorema lui Lagrange. Deci $m = q - 1$. Am demonstrat că există $f \in F^\star$ astfel încât $\mathrm{ord}(f) = |F^\star|$. Rezultă cu a $F^\star$ e cilcic, generat de f. $\square$

Teorema 19. (Structura corpurilor finite) *Fie F un corp finit cu p^n elemente.*
a) Există un polinom ireductibil $f \in \mathbb{Z}_p[X]$ astfel încât $F \cong \mathbb{Z}_p[X]/(f)$;
b) F este corpul de descompunere al lui $f \in \mathbb{Z}_p[X]$;
c) Dacă F' este un corp cu $|F'| = p^n$, atunci $F \cong F'$.

Proof. a) Folosind Teorema 8, deducem că există un morfism injectiv $\mathbb{Z}_p \to F$. Pentru simplificarea scrierii, putem presupunem fără să restrângem generalitatea că $\mathbb{Z}_p$ este subcorp al lui F. Atunci orice polinom din $f \in \mathbb{Z}_p[X]$ poate fi privit ca având coeficienţi în F.

Fie a un generator pentru grupul $(F^\star, \cdot)$. Considerăm funcţia $\Phi : \mathbb{Z}_p[X] \to F$, $\Phi(f) = f(a)$. Este evident că Φ este un morfism de inele. Pentru că a este generator, rezultă că pentru orice $g \in F^\star$ există $k \in \mathbb{N}^\star$ astfel încât $g = a^k = \Phi(X^k)$. In plus $\Phi(0) = 0$ şi rezultă că Φ este surjectiv. Aplicăm prima teoremă de izomorfism şi faptul că $\mathbb{Z}_p[X]$ este cu ideale principale. Rezultă că există $f \in \mathbb{Z}_p[X]$ ireductibil, astfel încât $F \cong \mathbb{Z}_[X]/(f)$.

b) Din Teorema lui Lagrange, rezultă că pentru orice $x \in F^\star$ avem $x^{p^n-1} = 1$. Rezultă că pentru orice $x \in F$ avem $x^{p^n} - x = 0$. Cum corpul de descompunere asociat polinomului $X^{p^n} - X$ are cel puţin p^n elemente, se deduce imediat că F este acest corp de descompunere.

c) Rezultă din faptul că orice două corpuri de descompunere asociate aceluiaşi polinom sunt izomorfe $\square$

Notaţia 20. Un corp cu p^n elemente se notează de obicei cu $\mathbb{F}_{p^n}$.

Observaţia 21. Se poate demonstra că pentru orice p prim şi orice $n \in N^\star$ există un corp cu p^n elemente.

In final, prezentăm o teoremă care descrie subcorpurile unui corp finit.

Teorema 22. *a) Fie K un subcorp în $\mathbb{F}_{p^n}$. Atunci există $d \mid n$ astfel încât $K \cong \mathbb{F}_{p^d}$.*

b) Pentru orice divizor $d \mid n$ *există un singur subcorp al lui* $\mathbb{F}_{p^n}$ *care are* p^d *elemente.*