CURS 13: ELEMENTE PRIME ŞI IREDUCTIBILE. CORPURI FINITE

SAI

1. Elemente prime şi ireductibile

Peste tot, R este un domeniu de integritate (inel comutativ fără divizori ai lui zero nenuli).

Definiţia 1. *(i) $p \in R$ se numeşte prim dacă $p \neq 0$, $p \notin U(R)$ şi $\forall\ a, b \in R$ astfel încât $p \mid ab$ rezultă $p \mid a$ sau $p \mid b$.*

(ii) $q \in R$ se numeşte ireductibil dacă $q \neq 0$, $q \notin U(R)$ şi $\forall\ a, b \in R$ astfel încât $q = ab$ rezultă $a \in U(R)$ sau $b \in U(R)$ (echivalent: $q \sim a$ sau $q \sim b$).

Observaţia 2. Orice element prim p este ireductibil.

Într-adevăr, dacă $p = ab$ atunci $p \mid ab$, deci $p \mid a$ sau $p \mid b$. Dacă $p \mid a$, scriem $a = pa'$ cu $a' \in R$, şi obţinem $p = pa'b$, adică $a'b = 1$. Rezultă $b \in U(R)$. Analog, dacă $p \mid b$ atunci $a \in U(R)$.

Există domenii de integritate R ce conţin elemente ireductibile ce nu sunt prime, deci reciproc nu este adevărat.

Propoziţia 3. *Dacă în R există c.m.m.d.c. pentru orice două elemente atunci orice element ireductibil din R este prim.*

Demonstraţie: Fie $q \in R$ un element ireductibil şi $a, b \in R$ a.î. $q \mid ab$. Atunci $(ab, q) = q \neq 1$ şi, deci, nu putem avea simultan $(a, q) = 1$ şi $(b, q) = 1$. Dacă $(a, q) = d \neq 1$, scriem $a = da'$, $q = dq'$ cu $(a', q') = 1$. Cum q este ireductibil iar $d \neq 1$ implică $d \notin U(R)$ (c.m.m.d.c. este unic până la o asociere în divizibilitate), deducem $q' \in U(R)$ şi $d \sim q$. Deci $q \sim d \mid a$, adică $q \mid a$. Analog, dacă $(q, b) \neq 1$ atunci $q \mid b$. □

Reamintim că în $\mathbb{Z}$ şi $K[X]$ există c.m.m.d.c.-ul oricăror două elemente, deci în $\mathbb{Z}$ şi $K[X]$ noţiunile de element prim şi ireductibil coincid.

Exemplul 4. *(i) Elementele prime şi ireductibile în $\mathbb{Z}$ coincid cu numerele prime.*

(ii) Elementele prime şi ireductibile în $K[X]$, K corp comutativ, coincid cu polinoamele ireductibile. Mai mult, în $K[X]$

- polinoamele de grad 1 sunt ireductibile,

- un polinom ireductibil de grad ≥ 2 nu are rădăcini în K,

- un polinom de grad 2 *sau* 3 *este ireductibil dacă şi numai dacă nu are rădăcini în* K*;*

(iii) $1+i$ *şi* 3 *sunt elemente prime în* $\mathbb{Z}[i]$*, dar* $5=(1+2i)(1-2i)$ *nu este ireductibil (şi, deci, nici prim).*

Este imdediat că $U(\mathbb{Z})=\{\pm 1\}$ iar $U(K[X])=K^\times:=K\backslash\{0\}$.

Theorem 5. *Fie* $R\in\{\mathbb{Z},K[X]\}$*. Atunci orice element din* R *nenul şi neinversabil se scrie în mod unic ca un produs de elemente prime* $\equiv$ *ireductibile.*

Demonstraţie: Fie $\varphi:R^\times\to\mathbb{N}$ funcţia modul dacă $R=\mathbb{Z}$, respectiv funcţia grad dacă $R=K[X]$.

Presupunem prin absurd că

$$X:=\{\varphi(a)\mid a\notin U(R)\cup\{0\},a \text{ nu se scrie ca un produs de ireductibile}\}$$

este nevidă. Cum $\mathbb{N}$ este bine ordonată, $\exists\ x\in X$ un prim element, adică un $a\notin U(R)\cup\{0\}$ ce nu se scrie ca un produs de ireductibile a.î $x=\varphi(a)$ este mai mic decât orice alt element din X.

Clar, a nu este ireductibil, deci există $b,c\notin U(R[X])\cup\{0\}$ a.î $a=bc$. Din definiţia lui φ, $\varphi(b),\varphi(c)<\varphi(a)=x$, deci b,c se scriu ca produs de ireductibile şi, deci, $a=bc$ se scrie ca un produs de ireductibile, contradicţie!

Fie $a=p_1^{\alpha_1}\cdots p_n^{\alpha_n}=q_1^{\beta_1}\cdots q_m^{\beta_m}$ două descompuneri ale lui $a\notin U(R)\cup\{0\}$ în produs de elemente ireductibile $\equiv$ prime distincte.

Prin inducţie după $M=\alpha_1+\cdots+\alpha_n\in\mathbb{N}$ arătăm că $n=m$ şi, eventual după o renumerotare, $p_i\sim q_i$ şi $\alpha_i=\beta_i\ \forall\ i$.

Dacă $M=1$ atunci $a=p_1=q_1^{\beta_1}\cdots q_m^{\beta_m}$ cu $p_1,q_1,\cdots,q_m$ ireductibile. Clar $m=1$, $\beta_1=1$ şi $p_1=q_1$.

Dacă $M>1$, din $p_n\mid a$ şi p_n prim rezultă că $p_n\mid q_t$; putem presupune $p_n\mid q_m$. Cum p_n,q_m sunt ireductibile, este imdediat că $p_n\sim q_m$, deci

$$p_1^{\alpha_1}\cdots p_{n-1}^{\alpha_{n-1}}p_n^{\alpha_n-1}=q_1^{\beta_1}\cdots q_{m-1}^{\beta_{m-1}}q_m^{\beta_m-1}.$$

Din ipoteza de inducţie rezultă concluzia dorită. □

2. Corpuri finite

Un corp K se numeşte finit dacă mulţimea elementelor sale este finită.

Theorem 6. *Fie* K *un corp comutativ şi* $K^\times$ *grupul multiplicativ al elementelor sale nenule. Atunci:*

(i) Orice subgrup finit $G\leq K^\times$ *este ciclic.*

(ii) Dacă K *este corp finit atunci* $K^\times$ *este grup ciclic finit, deci izomorf cu* $\mathbb{Z}_{q-1}$*, unde* $q=\mid K\mid$.

Demonstraţie: Fie $n =| G |$ şi $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ descompunerea sa în produs de prime distincte. Pentru orice i, polinomul $X^{\frac{n}{p_i}} - 1 \in K[X]$ are cel mult $\frac{n}{p_i} < n =| G |$ rădăcini în K, deci există $x_i \in G$ a.î. $x_i^{\frac{n}{p_i}} \neq 1$. Atunci $y_i := x_i^{\frac{n}{p_i^{\alpha_i}}} \in G$ are ordinul $p_i^{\alpha_i}$: $y_i^{p_i^{\alpha_i}} = x_i^n = 1$ (Lagrange) şi, deci, $ord(y_i) \mid p_i^{\alpha_i}$. Cum p_i este prim obţinem $ord(y_i) = p_i^{\beta_i}$ cu $\beta_i \leq \alpha_i$. Dacă $\beta_i < \alpha_i$ atunci $1 = y_i^{p_i^{\beta_i}} = x_i^{\frac{n}{p_i^{\alpha_i - \beta_i}}}$ şi, deci, $1 = 1^{p_i^{\alpha_i - \beta_i - 1}} = x_i^{\frac{n}{p_i}}$, o contradicţie ($\alpha_i - \beta_i - 1 \geq 0$, chiar ≥ 1).

Deci $ord(y_i) = p_i^{\alpha_i}$, $\forall i$. Cum K este comutativ, G este grup abelian. În plus, $(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$, $\forall\ i \neq j$, de unde rezultă că $y := y_1 \cdots y_t \in G$ are ordinul $ord(y) = ord(y_1) \cdots ord(y_t) = p_1^{\alpha} \cdots p_t^{\alpha_t} = n =| G |$. Prin urmare, G este ciclic generat de y. □

Un rezultat celebru în teoria corpurilor afirmă că orice corp finit este comutativ; pentru demonstraţie se poate consulta [2].

Teorema lui Wedderburn. Orice corp finit este comutativ.

Din cele două teoreme prezentate mai sus obţinem:

Theorem 7. *Dacă K este corp finit atunci $K^\times$ este ciclic. În particular, există $x \in K$ astfel încât $K = \{\widetilde{f}(x) \mid f \in P[X]\}$, unde $P \cong \mathbb{Z}_p$ este subcorpul prim al lui K.*

Demonstraţie: K este corp finit comutativ, deci $K^\times$ este grup ciclic. Dacă x generează pe $K^\times$, atunci orice $a \in K^\times$ este de forma x^t pentru un $0 \leq t \leq | K^\times | -1$. Deci $a = \widetilde{X^t}(x)$; incluziunea inversă este imediată. □

Observaţia 8. *$\mathbb{Z}_p^\times$ este grup ciclic, izomorf cu $\mathbb{Z}_{p-1}$. Însă nu se cunoaşte un algoritm care să furnizeze generatorul lui $\mathbb{Z}_{p-1}$, pentru orice p prim.*

Fie K un corp finit (deci şi comutativ) şi $P \cong \mathbb{Z}_p$ subcorpul său prim (p este număr prim). Atunci K admite o structură de $P \cong \mathbb{Z}_p$-spaţiu vectorial; cum este finit, este de dimensiune finită, să zicem n. Rezultă că $K \cong P^n$ ca P-spacţii vectoriale, deci

Theorem 9. *Dacă K este corp finit de caracteristică p (p prim) atunci $| K |= p^n$, pentru un anumit $n \in \mathbb{N}^*$.*

Vom demonstra că pentru orice p prim şi $n \in \mathbb{N}^*$ există un corp cu p^n elemente. Peste tot de acum înainte corpurile considerate sunt comutative.

Propoziţia 10. *(*Kronecker*) Fie $f \in K[X]$ de grad $n \geq 1$. Există un corp F astfel încât $K \subseteq F$ şi f are toate rădăcinile în F.*

Demonstraţie: Inducţie după $n \geq 1$.

Dacă $n = 1$, $f = aX + b \in K[X]$ cu $a \neq 0$. Atunci $x = -a^{-1}b$ este unica rădăcină a lui f şi $x \in K$; iau $F = K$.

Dacă $n > 1$, sunt două posibilităţi:

(1) f este ireductibil. Iau inelul factor $L := \frac{K[X]}{(f)}$ şi arăt că este un corp. Într-adevăr, dacă $\hat{0} \neq \hat{g} \in L$ atunci f nu divide g şi cum f este ireductibil≡prim rezultă că $(f, g) = 1$. Există $u, v \in K[X]$ a.î. $uf + vg = 1$, deci $\hat{v}\hat{g} = \hat{1}$, adică $\hat{g}$ este inversabil în L cu inversul $\hat{v}$. Dacă $x = \hat{X} \in L$ atunci $\widetilde{f}(x) = \hat{f} = \hat{0}$, deci x este rădăcină a lui f în L. Mai mult, cum orice morfism de corpuri este injectiv, K se poate identifica cu un subgrup al lui L via compunerea de morfisme $K \xrightarrow{i} K[X] \xrightarrow{p} L = \frac{K[X]}{(f)}$. Pe scurt, există $K \subseteq L$ şi $x \in L$ rădăcină a lui f în L. Scriem $f = (X - x)g$ cu $g \in L[X]$ de grad $n - 1$. Aplic ipoteza de inducţie şi găsesc $L \subseteq F$ în care g are toate rădăcinile, deci şi f.

(2) f este reductibil, $f = f_1 f_2$ cu $f_1, f_2 \in K[X]$ de grad $< n$. Aplic ipoteza de inducţie pentru f_1 şi găsesc $K \subseteq F_1$ a.î. f_1 are toate rădăcinile în F_1. Privesc $f_2 \in K[X] \subseteq F_1[X]$ şi aplic din nou ipoteza de inducţie: există $F_1 \subseteq F$ în care f_2 are toate rădăcinile. Rezultă că f are toate rădăcinile în F. □

Definiţia 11. *Dacă $f = \sum_{i=0}^{n} a_i X^i \in K[X]$, derivata lui f este polinomul $f' = \sum_{i=1}^{n} i a_i X^{i-1} \in K[X]$.*

Lemma 12. *Fie $f \in K[X]$ de grad ≥ 1 şi $K \subseteq F$ corp în care f are toate rădăcinile. Atunci f nu are rădăcini multiple dacă şi numai dacă $(f, f') = 1$ în $K[X]$.*

Demonstraţie: Dacă f are o rădăcină multiplă α putem să scriem $f = (X - \alpha)^2 g$ cu $g \in F[X]$. Cum $f' = 2(X - \alpha)g + (X - \alpha)^2 g'$ rezultă că $X - \alpha \mid (f, f') \neq 1$ în $K[X]$, deci şi în $F[X]$ (algoritmul lui Euclid este acelaşi, din cauza unicităţii scrierii în teorema împărţirii cu rest). Deci $(f, f') = 1$ implică f nu are rădăcini multiple.

Reciproc, dacă $X - \alpha \mid f, f'$ atunci $f = (X - \alpha)g$ şi $f' = (X - \alpha)h$ cu $g, h \in F[X]$. Rezultă $g + (X - \alpha)g' = (X - \alpha)h$, deci $X - \alpha \mid g$ şi, deci, $(X - \alpha)^2 \mid f$. Prin urmare, dacă f nu are rădăcini multiple atunci $(f, f') = 1$. □

Theorem 13. *(*Galois*) Pentru orice p prim şi $n \in \mathbb{N}^*$ există un corp cu p^n elemente.*

Demonstraţie: Fie $q = p^n$ şi $f = X^q - X \in \mathbb{Z}_p[X]$. Există $F \supseteq \mathbb{Z}_p$ corp în care f are toate rădăcinile. Clar, F este de caracteristică p (conţine pe $\mathbb{Z}_p$, corp prim, ca subcorp). Fie $\mathbb{F}_q$ mulţimea rădăcinilor lui f în F. Cum f este de grad q, $\mid \mathbb{F}_q \mid \leq q$. Dar $f' = qX^{q-1} - 1 = -1$, fiindcă $q = p^n$ şi p este caracteristica lui $\mathbb{Z}_p$, deci $(f, f') = 1$. Astfel, f nu are rădăcini multiple şi $\mid \mathbb{F}_q \mid = q$.

Că $\mathbb{F}_q$ este corp rezultă din $\varphi : F \ni x \mapsto x^p \in F$ este morfism de corpuri, deci şi $\varphi^n : F \ni x \mapsto x^{p^n} = x^q \in F$. Mai exact, dacă $a, b \in \mathbb{F}_q \subseteq F$ atunci $(a-b)^q = a^q - b^q = a - b$, $(ab)^q = a^q b^q = ab$ şi $(c^{-1})^q = c^{-q} = c^{-1}$, pentru orice $a, b, c \in \mathbb{F}_q$ cu $c \neq 0$. Prin urmare, $\mathbb{F}_q$ este subcorp al lui F, deci un corp cu p^n elemente. □

Unicitatea corpurilor finite de cardinal $q = p^n$ a fost demonstrată 60 de ani (1893) mai târziu de către E. H. Moore.

Theorem 14. *Orice două corpuri finite cu p^n elemente sunt izomorfe.*

Demonstraţie (schiţă): Fie K un corp cu $q = p^n$ elemente. Cum $K^\times$ are $q - 1$ elemente din Lagrange obţinem $x^{q-1} = 1$, $\forall\ x \in K^\times$, deci $x^q = x$, $\forall\ x \in K$. Deci K este un corp ce conţine toate rădăcinile polinomului $f = X^q - X \in P[X]$, $P \cong \mathbb{Z}_p$ fiind subcorpul prim al lui K. De aici (unicitatea corpului de descompunere=cea mai mică extensie în care un polinom are toate rădăcinile) rezultă $K \cong \mathbb{F}_q$, ca şi corpuri. □

Exemplul 15. *(1) $f = X^2 + X + 1 \in \mathbb{Z}_2[X]$ este ireductibil (nu are rădăcini). Atunci $\mathbb{F}_4 = \frac{\mathbb{Z}_2[X]}{(f)} = \{a + b\zeta \mid a, b \in \mathbb{Z}_2\}$ cu $\zeta^2 = -\zeta - 1 = \zeta + 1$; $\zeta := \hat{X} \in \mathbb{F}_4$.*

(2) $f_1 = X^2 + 1$, $f_2 = X^2 + X - 1$ şi $f_3 = X^2 - X - 1$ sunt polinoame ireductibile în $\mathbb{Z}_3[X]$ şi ele produc (via un izomorfism) pe $\mathbb{F}_9$: $\mathbb{F}_9 \cong \frac{\mathbb{Z}_3[X]}{(f_i)}$. $\forall\ i = 1, 2, 3$.

(3) $g_1 = X^3 - X + 1$, $g_2 = X^3 + X^2 - X + 1$, $g_3 = X^3 - X^2 - X - 1$ sunt polinoame ireductibile în $\mathbb{Z}_3[X]$ şi ele produc (via un izomorfism) pe $\mathbb{F}_{27}$: $\mathbb{F}_{27} \cong \frac{\mathbb{Z}_3[X]}{(g_i)}$. $\forall\ i = 1, 2, 3$.

Bibliografie

[1] T. Dumitrescu, *Algebra*, Ed. Universităţii din Bucureşti, 2006.
[2] I. D. Ion, N. Radu, *Algebra*, Ed. Universităţii din Bucureşti, 1981.
[3] C. Năstăsescu, C. Niţă, C. Vraciu, *Bazele algebrei*, Ed. Academiei, Bucureşti, 1986.