Seminar 3 – Aritmetică și polinoame

1 Aritmetica în $\mathbb{Z}$ și $\Bbbk[X]$

În teoria numerelor, se lucrează cu proprietăți aritmetice ale inelelor de forma $\mathbb{Z}[i\sqrt{d}]$, pentru $d \geqslant 0$ un număr natural. De asemenea, în unele situații, se apelează la corpul de fracții al inelelor de această formă, anume $\mathbb{Q}[i\sqrt{d}]$.

Ne vom concentra asupra proprietăților aritmetice elementare, extinse din contextul numerelor întregi, aplicabile în situații generale (în inele integre), precum *divizibilitate, elemente prime, elemente ireductibile, cmmdc, cmmmc* ș.a.

Dacă nu se precizează altfel, vom lucra într-un inel A, comutativ, unitar și integru.

Definiţie 1.1: Fie A un inel integru și $a, b \in A$ două elemente arbitrare. Spunem că a *divide* pe b, scris $a \mid b$ dacă există $c \in A$ cu $b = ac$. În acest caz, a se numește *divizor*, iar b, *multiplu*.

Să observăm că *divizibilitatea este o relație de preordine* (reflexivă și tranzitivă). De asemenea, ea are sens în cazuri mai generale, precum în inele de matrice sau chiar în inele de funcții.

O situație specială, care în $\mathbb{Z}$ este trivială, dar nu și în inele mai generale, este următoarea:

Definiţie 1.2: Elementele a, b se numesc *asociate în divizibilitate*, scris $a \sim b$ sau $a \sim_d b$ dacă $a \mid b$ și $b \mid a$.

Cum spuneam, în inelul numerelor întregi, asocierea în divizibilitate înseamnă $a = \pm b$, însă mai general, dacă a și b sînt asociate în divizibilitate, atunci există o unitate $u \in \mathcal{U}(A)$, astfel încît $a = ub$. (justificați!)

Următoarele noțiuni pe care le generalizăm din cazul numerelor întregi sînt acelea de numere (elemente, în general) prime, respectiv ireductibile.

Definiţie 1.3: Elementul $a \in A$ se numește:

(1) *ireductibil*, dacă oricînd $a = bc$, cu $b, c \in A$ rezultă $b \in \mathcal{U}(A)$ sau $c \in \mathcal{U}(A)$;

(2) *prim*, dacă oricînd $a \mid bc$, pentru $b, c \in A$, rezultă că $a \mid b$ sau $a \mid c$.

Din nou, să observăm că în cazul mulțimii numerelor întregi, cele două noțiuni coincid. Însă, în inele integre arbitrare, nu este cazul:

Propoziţie 1.1: *Orice element prim este ireductibil. Reciproc, este fals: 2 este ireductibil în $\mathbb{Z}[i\sqrt{5}]$, dar nu este prim.*

Definițiile pentru cmmdc și cmmmc sînt date mai jos.

Definiţie 1.4: Fie $a, b \in A$. Elementul $d \in A$ se numește *cel mai mare divizor comun* al elementelor a și b dacă $d \mid a, d \mid b$ și oricînd există un alt element $D \in A$, cu $D \mid a$ și $D \mid b$, rezultă că $D \mid d$.

Definiţie 1.5: Fie $a, b \in A$. Elementul $m \in A$ se numește *cel mai mic multiplu comun* al elementelor a și b dacă $a \mid m$ și $b \mid m$ și oricînd există un alt element $M \in A$ cu $a \mid M$ și $b \mid M$, rezultă că $m \mid M$.

Atît noțiunea de cel mai mare divizor comun, cît și aceea de cel mai mic multiplu comun se pot generaliza pentru mai multe elemente, inductiv: $\mathrm{cmmdc}(a, b, c) = \mathrm{cmmdc}(a, \mathrm{cmmdc}(b, c))$ ș.a.m.d.

Observaţie 1.1: Într-un inel arbitrar, nu orice două elemente au cmmdc sau cmmmc! Totuși, dacă unul dintre ele există mereu, atunci există și celălalt, legătura dintre ele fiind dată de formula binecunoscută: $cmmdc(a,b)\cdot cmmmdc(a,b)=a\cdot b$.

Dacă într-un inel, există cmmdc și cmmmc pentru oricare două elemente, inelul se numește *domeniu gcd* (sau inel cu cmmdc). Dacă aceasta este situația, atunci în asemenea inele, un element este prim dacă și numai dacă este ireductibil.

Pentru a calcula cmmmdc sau cmmmc al două elemente, se poate folosi descompunerea în factori primi, dar nu în general! Există inele în care descompunerea în factori primi (sau elemente ireductibile) nu este unică. Mai mult, două descompuneri diferite ale aceluiași element nu sînt suficient de "legate" încît să poată fi folosite oricare pentru calcul. De aceea, metoda cea mai generală pentru calculul cmmdc este *algoritmul lui Euclid*, fie prin scăderi repetate, fie prin împărțiri repetate. Folosind algoritmul lui Euclid, se demonstrează imediat următorul rezultat:

Propoziţie 1.2: $cmmdc(a,b)=d\iff\exists\alpha,\beta\in A$ *a.î.* $d=\alpha a+\beta b$.

Cîteva proprietăți simple ale cmmdc sînt conținute în rezultatul următor.

Propoziţie 1.3: *Fie* $a,b\in A$ *și* $d=cmmdc(a,b)$.

(1) $\exists a',b'\in A$ *cu* $a=da',b=db'$ *și* $cmmdc(a',b')=1$*;*

(2) $cmmdc(ac,bc)=c\cdot cmmdc(a,b),\forall c\in A$*;*

(3) Dacă $cmmdc(a,b)=1$ *și* $cmmdc(a,c)=1$*, atunci* $cmmdc(a,bc)=1$*;*

(4) Dacă $a\mid bc$ *și* $cmmdc(a,b)=1$*, atunci* $a\mid c$*;*

(5) Dacă $a\mid c,b\mid c$ *și* $cmmdc(a,b)=1$*, atunci* $ab\mid c$.

Cazul inelului $\Bbbk[X]$ este foarte asemănător cazului inelului numerelor întregi, deoarece ambele inele sînt integre, comutative și se bucură de aceleași proprietăți, anume:

(1) Există cmmdc și cmmmc pentru orice două elemente;

(2) Elementele prime și elementele ireductibile coincid;

(3) Are loc teorema împărțirii cu rest și algoritmul lui Euclid;

(4) Descompunerea în factori primi este unică;

(5) Unitățile sînt ±1, deci asocierea în divizibilitate înseamnă cel mult o diferență de semn.

De asemenea, mai trebuie adăugate două rezultate.

Teoremă 1.1 (Teorema fundamentală a algebrei)**:** *Orice polinom din* $\mathbb{R}[X]$ *de grad* n *are exact* n *rădăcini complexe.*

Așadar, căutînd polinoame ireductibile peste $\mathbb{C}$, sîntem conduși la concluzia că acestea trebuie să aibă gradul cel mult 1.

Criterii de ireductibilitate vor fi studiate ulterior, însă unul dintre acestea se poate dovedi de folos:

Teoremă 1.2 (Eisenstein)**:** *Fie* $h\in\mathbb{Z}[X]$ *un polinom neconstant și* p *un număr prim. Dacă* p *divide toți coeficienții lui* h*, cu excepția coeficientului dominant, iar* p^2 *nu divide termenul liber al lui* h*, atunci* h *este ireductibil peste* $\mathbb{Q}$.

Deoarece cazurile inelelor $\mathbb{Z}$ și $\Bbbk[X]$ sînt similare, vom trece la a discuta cîteva proprietăți particulare pentru polinoame. Mai precis, vom studia elementele idempotente, nilpotente și inversabile din inele de polinoame mai generale, de forma $A[X]$, unde A este un inel comutativ arbitrar.

Să pornim cu un rezultat mai general:

Propoziție 1.4: *Dacă elementul $a \in A$ este nilpotent, atunci elementul $1 + a$ este inversabil.*

O teoremă dificilă privitoare la zero-divizorii din inele de polinoame este următoarea:

Teoremă 1.3 (McCoy)**:** *Fie $p \in A[X]$ un polinom, cu A un inel comutativ arbitrar. Polinomul $p = \sum_{i=0}^{n} a_i X^i$ este zero divizor dacă și numai dacă există $b \neq 0$ un element din A, cu $bp = 0$.*

Dem.: O implicație este clară, deoarece dacă există $b \in R$ ca în enunț, atunci pentru $q = b \in R[X]$, un polinom de grad zero, rezultă că $p \in \mathcal{ZD}(R[X])$.

Pentru implicația reciprocă, presupunem că p este divizor al lui zero și fie $q = \sum_{i=0}^{m} b_i X^i$ astfel încît $pq = 0$. Alegem q de grad minim cu această proprietate. Arătăm inductiv că $a_i q = 0$, pentru toți $0 \leqslant i \leqslant n$.

Pasul de verificare: $pq = \sum_{k=0}^{n+m} \Big(\sum_{i+j=k} a_i b_j \Big) X^k = 0$. Coeficientul lui X^{n+m} din această scriere este $a_n b_m = 0$. Dar atunci gradul polinomului $a_n q$ este strict mai mic decît gradul lui q (deoarece monomul de grad m este anulat de a_n), o contradicție cu alegerea lui q. Așadar, nu se poate decît $a_n q = 0$, adică $a_n b_i = 0$, $\forall 0 \leqslant i \leqslant m$.

Pasul de inducție: Fie un $0 \leqslant t < n$ astfel încît $a_r q = 0$, $\forall t \leqslant r \leqslant n$. Din scrierea de mai sus a produsului pq, coeficientul lui X^{m+t} este zero într-un membru și $\sum_{i+j=m+t} a_i b_j$ în celălalt. Deci $\sum a_i b_j = 0$. Dacă $i \geqslant t$, atunci $a_i b_j = 0$, din ipoteza de inducție. Deci toți termenii de felul acesta sînt nuli.

Dacă $i < t$, atunci $j > m$, ceea ce este imposibil. Atunci $a_t b_m = 0$ și deci $a_t qp = 0$, iar $a_t q$ are gradul mai mic decît q și-l anulează pe p. Ca în cazul de verificare, rezultă $a_t q = 0$.

Așadar, $a_i q = 0$, pentru toți $0 \leqslant i \leqslant n$. În particular, $a_i b_m = 0$, deci $b_m p = 0$. □

Privitor la polinoame nilpotente, un rezultat important este:

Propoziție 1.5: *Un polinom $p = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ este nilpotent dacă și numai dacă toți coeficienții săi sînt nilpotenți.*

Dem.: Implicația " $\Leftarrow$ " este clară, deoarece putem ridica p la cmmmc al indicilor de nilpotență pentru coeficienții săi și atunci obținem p nilpotent.

Pentru implicația directă, fie p nilpotent. Scădem din p toți termenii care au coeficienți nilpotenți și obținem un nou polinom, tot nilpotent. Dacă este zero, am terminat. Dacă nu, are un cel mai mare termen aX^h pentru care coeficientul a nu este nilpotent. Dar atunci, pentru orice $\alpha \in \mathbb{N}$, f^α are termenul dominant $a^\alpha x^{\alpha h}$, care este nenul, contradicție. □

Polinoamele idempotente, însă, sînt foarte ușor de caracterizat, datorită aditivității gradului la înmulțire:

Propoziție 1.6: *Un polinom p este idempotent dacă și numai dacă termenul liber este idempotent și toți ceilalți coeficienți sînt nuli.*

În fine, polinoamele inversabile sînt caracterizate astfel:

Teoremă 1.4: *Fie A un inel comutativ. Polinomul $p = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ este inversabil dacă și numai dacă a_0 este inversabil și toți ceilalți coeficienți a_i sînt zero-divizori, pentru toți $i = 1, \ldots, n$.*

Dem.: " $\Leftarrow$ " : Dacă are coeficienții ca în enunț, atunci, conform propoziției de mai sus, va fi o sumă între un element inversabil și nu polinom nilpotent. Să presupunem că $a_0b = 1$ și $p - a_0$ îl notăm cu g, cu $g^N = 0$. Este suficient să arătăm că $b(a_0 + g) = 1 + bg = 1 - h$ este inversabil, unde cu h am notat $-bg$, avînd proprietatea $h^N = 0$. Dar, cum am văzut mai sus, $(1-h)(1+h+h^2+\cdots+h^{N-1}) = 1 - h^N = 1$, ceea ce trebuia demonstrat.

Pentru implicația cealaltă, din $pq = 1$ rezultă $p(0)q(0) = 1$, deci obținem că termenul liber trebuie să fie inversabil. Pentru nilpotența celorlalți coeficienți, obținem din aproape în aproape, astfel: dacă $p = \sum_{i=0}^{n} a_i X^i$ și $q = \sum_{j=0}^{m} b_j X^j$, făcînd produsul, obținem succesiv:

$$\begin{gathered} a_0b_1 + a_1b_0 = 0 \\ a_0b_2 + a_1b_1 + a_2b_0 = 0 \\ \cdots\cdots\cdots \\ a_{n-1}b_m + a_nb_{m-1} = 0 \\ a_nb_m = 0. \end{gathered}$$

Înmulțim penultima relație cu a_n și obținem $a_n^2 b_{m-1} = 0$. Dacă înmulțim antepenultima ecuație cu a_n^2, obținem $a_n^3 b_{m-2} = 0$ ș.a.m.d., pînă la $a_n^{m+1} b_0 = 0 \Rightarrow a_n$ este nilpotent. Similar procedăm pentru a obține nilpotența și pentru ceilalți coeficienți. □

2 Polinoame simetrice

Polinoamele simetrice sînt instrumente utile în studiul polinoamelor de mai multe variabile. Astfel, ele joacă rolul aproximativ al unei baze dintr-un spațiu vectorial, în sensul că orice polinom simetric de mai multe variabile poate fi exprimat în funcție de unele așa-numite elementare.

Definiția este următoarea:

Definiţie 2.1: Un polinom $p \in \mathbb{k}[X_1, X_2, \ldots, X_n]$ se numește *simetric* dacă pentru orice permutare $\sigma \in S_n$ avem:

$$p(X_1, X_2, \ldots, X_n) = p(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}).$$

Practic, înseamnă că putem schimba variabilele între ele, dar polinomul nu se schimbă.

Cîteva exemple:

- $X_1^3 + X_2^3 + 5$;
- $4X_1^2X_2^2 + X_1^3X_2 + X_1X_2^3 + (X_1 + X_2)^3$;
- $X_1X_2X_3 - X_1X_2 - X_1X_3 - X_2X_3$.

Vom introduce un algoritm care ne va permite să exprimăm orice polinom simetric în funcție de niște polinoame simetrice fundamentale. Însă pentru aceasta, mai avem nevoie să definim o relație de ordine totală pe mulțimea polinoamelor în mai multe nedeterminate. Pentru polinoamele într-o singură nedeterminată, e clar că le putem ordona după grad. Atunci cînd avem mai multe nedeterminate, este necesar să utilizăm o altă relație.

Pe mulțimea monoamelor din $R[X_1, \ldots, X_n]$, definim o relație de ordine totală, numită *ordinea lexicografică* prin:

$X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n} > X_1^{j_1}X_2^{j_2}\cdots X_n^{j_n} \Leftrightarrow$ prima componentă nenulă a vectorului $(i_1-j_1, \ldots, i_n-j_n)$ este pozitivă.

Polinoamele simetrice fundamentale sunt (le puteți asemăna cu relațiile lui Viète):

$$\begin{gathered} s_1 = X_1 + X_2 + \cdots + X_n; \\ s_2 = X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n; \\ \cdots\cdots\cdots \\ s_n = X_1 \cdots X_n. \end{gathered}$$

Termenul principal al polinomului f, notat $T(f)$ sau $LT(f)$ este termenul corespunzător celui mai mare monom al său, în ordinea lexicografică.

Algoritmul de exprimare a unui polinom simetric în funcție de cele fundamentale:

INPUT: $f \in R[X_1, \ldots, X_n]$ simetric;
OUTPUT: $g \in R[Y_1, \ldots, Y_n]$ a.î. $f = g(s_1, \ldots, s_n)$.

- $g = 0,\ h = f$;
- while $(h \neq 0)$ do
  - begin
    - $aX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n} = LT(h)$;
    - $h := h - as_1^{i_1-i_2}s_2^{i_2-i_3}\cdots s_{n-1}^{i_{n-1}-i_n}s_n^{i_n}$;
    - $g := g + aY_1^{i_1-i_2}Y_2^{i_2-i_3}\cdots Y_{n-1}^{i_{n-1}-i_n}Y_n^{i_n}$;
  - end

Teoremă 2.1 (Formulele lui Newton)**:** *Fie polinoamele:*

$$p_k = X_1^k + X_2^k + \cdots + X_n^k, k \geqslant 1$$

și fie $s_1, s_2, \ldots, s_n \in A[X_1, \ldots, X_n]$ *polinoamele simetrice fundamentale. Au loc egalitățile:*

(1) $p_k - s_1p_{k-1} + s_2p_{k-2} - \cdots + (-1)^n s_n p_{k-n} = 0, \forall k \geqslant n$;

(2) $p_k - s_1p_{k-1} + \cdots + (-1)^{k-1}s_{k-1}p_1 + (-1)^k k s_k = 0, \forall 1 \leqslant k \leqslant n-1$.

3 Criterii de ireductibilitate a polinoamelor

Criteriul reducerii

Fie $f \in \mathbb{Z}[X]$ un polinom şi $p \in \mathbb{N}$ un număr prim. Notăm cu f_p polinomul obţinut prin reducerea tuturor coeficienţilor lui f modulo n.

Dacă f este reductibil peste $\mathbb{Z}$, atunci f_p este reductibil peste $\mathbb{Z}_p$. Echivalent, dacă f_p este ireductibil peste $\mathbb{Z}_p$, atunci f este ireductibil peste $\mathbb{Z}$.

Schimbarea de variabilă

Fie f un polinom în $\mathbb{Z}[X]$. Introducem variabila $Y = X + a,\ a \in \mathbb{Z}$. Obţinem, astfel, un polinom $g(Y) = f(X + a)$.

Dacă g este reductibil peste $\mathbb{Z}$, atunci şi f este reductibil peste $\mathbb{Z}$. Echivalent, dacă f este ireductibil peste $\mathbb{Z}$, atunci g este ireductibil peste $\mathbb{Z}$.

Rădăcini raţionale

Fie $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbb{Z}[X]$.

Dacă f are o rădăcină raţională $\dfrac{\alpha}{\beta} \in \mathbb{Q}$ (cu $(\alpha, \beta) = 1$), atunci $\beta \mid a_n$ şi $\alpha \mid a_0$.

În particular, dacă f are o rădăcină întreagă $\gamma \in \mathbb{Z}$, atunci $\gamma \mid a_0$.

Rădăcini conjugate

Fie $f \in \mathbb{Z}[X]$ un polinom.

Dacă $\alpha = a + b\sqrt{c}$ este o rădăcină reală a lui f, atunci şi $\overline{\alpha} = a - b\sqrt{c}$ este o rădăcină reală a lui f.

În plus, dacă $\beta = a + bi$ este o rădăcină complexă a lui f, atunci şi $\overline{\beta} = a - bi$ este o rădăcină complexă a lui f.

Definiţie 3.1: Fie $f = \sum_{i=0}^{n} a_i X^i$ un polinom din $\Bbbk[X]$. Se numește *conținutul* lui f, notat $c(f)$, cel mai mare divizor comun al coeficienților săi.

Dacă $c(f) = 1$, atunci polinomul f se numește *primitiv*.

Propoziţie 3.1: *Conținutul este multiplicativ, ca funcție, i.e.* $c(fg) = c(f)c(g), \forall f, g \in \Bbbk[X]$.

Criteriul lui Eisenstein

Fie A un inel factorial şi K corpul său de fracţii. Considerăm un polinom $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in A[X]$, cu $n \geqslant 1$ şi $a_n \neq 0$. Fie $p \in A$ un element prim.

Dacă p divide toţi coeficienţii a_i, $0 \leqslant i < n$, dar $p \nmid a_n$ şi $p^2 \nmid a_0$, atunci f este ireductibil peste K. Aşadar, dacă f este primitiv, atunci este ireductibil peste A.

4 Exerciții

1. Arătaţi că următoarele polinoame sînt ireductibile:

(a) $f = X^3 + 27X^2 + 5X + 97$ peste $\mathbb{Z}$;

(b) $f = X^4 + 4X^3 + 6X^2 + 4X + 4$ peste $\mathbb{Z}$;

(c) $f(X, Y) = X^2 + Y^2 + 1 \in \mathbb{C}[X, Y]$ peste $\mathbb{C}$;

(d) $f(X, Y) = X^3 + Y^3 + 1 \in \mathbb{C}[X, Y]$ peste $\mathbb{C}$;

(e) $f(X, Y) = X^2 - Y \in \mathbb{C}[X, Y]$ peste $\mathbb{C}$;

(f) $f(X, Y, Z) = X^2 - Y^2Z \in \mathbb{C}[X, Y, Z]$ peste $\mathbb{C}$;

(g) $f = \sqrt{3}X^5 + 25X^4 + (5 + 5\sqrt{3})X - 15 \in \mathbb{Z}[\sqrt{3}][X]$ peste $\mathbb{Z}$;

(h) $f = X^p + p - 1 \in \mathbb{Z}[X]$, peste $\mathbb{Z}$ (cu p număr prim);

(i) $f = X^4 + 3X^3 + 3X^2 - 5 \in \mathbb{Z}[X]$ peste $\mathbb{Z}$.

2. Arătați, folosind polinoame, că $\sqrt[5]{2} \notin \mathbb{Q}$.

3. Fie inelul $A = \{f \in \mathbb{Z}[X] \mid f = a_0 + a_2X^2 + a_3X^3 + \cdots + a_nX^n, a_i \in \mathbb{Z}, n \in \mathbb{N} - \{1\}\}$. Arătați că:

(a) $A = \mathbb{Z}[X^2, X^3]$;

(b) $cmmdc(X^2, X^3) = 1$, dar $cmmmc(X^2, X^3)$ nu există (în A);

4. Arătați că orice ideal al lui $\mathbb{Z}$ sau $\Bbbk[X]$ este principal, adică generat de un singur element.

5. Arătați că inelele $\mathbb{Z}[X]$ și $\mathbb{Z}[X, Y]$ nu sînt izomorfe.

6. Arătați că polinomul $X^p - X + \widehat{1}$ este ireductibil în $\mathbb{Z}_p[X]$.

7. (a) Exprimați polinomul $f = X^3 + Y^3 + Z^3$ în funcție de polinoamele simetrice fundamentale.
   (b) Calculați suma cuburilor rădăcinilor ecuației $x^3 - 5x^2 + 7x + 11 = 0$.