SEMINAR 10

Referitor la ultima parte a seminarului 9, pentru a vedea limpede că nu orice inel e noetherian, avem:

1. Inelul $k[X_1, \ldots, X_n, \ldots]$ nu este noetherian, k fiind un corp comutativ.

Soluţie. Aţi văzut construcţia inelelor de polinoame într-o infinitate de nedeterminate (aici infinitatea e numărabilă). Trebuie găsit un ideal care să nu fie finit generat. Avem idealul $I = \langle X_1, \ldots, X_n, \ldots \rangle$. Dacă ar exista nişte polinoame $f_1, \ldots, f_r \in k[X_1, \ldots, X_n, \ldots]$ aşa încât $I = \langle f_1, \ldots, f_r \rangle$, atunci am avea, de fapt, $I = \langle X_{i_1}, \ldots X_{i_s} \rangle$. Într-adevăr, $X_{i_1}, \ldots X_{i_s}$ sunt nedeterminatele care apar în expresiile f_i-urilor, şi sunt în număr finit, căci un polinom din $k[X_1, X_2, \ldots]$ se exprimă cu un număr finit de nedeterminate, conform construcţiei inelului. Dar atunci, alegând un $j \notin \{i_1, \ldots, i_s\}$, cum $X_j \in I = \langle X_1, X_2, \ldots, X_j, \ldots \rangle$, ar exista $\alpha_1, \ldots, \alpha_s \in k[X_1, X_2, \ldots]$ aşa încât $X_j = \alpha_1 X_{i_1} + \ldots + \alpha_s X_{i_s}$, o contradicţie (lămuriţi-vă că e o contradicţie).

Trecem la polinoame simetrice. Dar, mai întâi, să facem un scurt ocol. Deja aţi văzut trei tipuri de geometrii: euclidiană, afină (fără metrică), şi proiectivă (ce rămâne folosind doar rigla negradată; deci fără cercuri, fără unghiuri, fără metrică, fără relaţia "a fi între" şi fără paralelism). De precizat că "fără metrică" trebuie citit "fără metrică, în general": geometria proiectivă cuprinde pe cea euclidiană căci se poate construi o metrică pe un spaţiu proiectiv. Acum, vă gândiţi că, pe lângă acestea, mai există şi alte tipuri de geometrii (dintre acestea, geometria hiperbolică are apariţii realmente spectaculoase de-a lungul matematicii, apariţii dificil de explicat), iar subiectul e complex pentru că aici nu e doar matematica implicată: au un cuvânt de spus şi fizica, şi logica, şi filozofia. În 1872, Klein aruncă o nouă lumină asupra naturii geometriei (programul de la Erlangen). Observaţia iniţială e că o geometrie e determinată de proprietăţile configuraţiilor (figurilor) din cadrul ei. Însă ce înseamnă că "o proprietate are loc" în cutare geometrie? Păi geometria respectivă e făcută pe un anume model (spaţiu), iar de la Descartes încoace am văzut că orice spaţiu e susceptibil de a

suporta coordonate (studiul său analitic), şi deci putem spune că o proprietate a acelei geometrii este o trăsătură a figurilor, formate pe spaţiul model, care persistă (e invariată) după efectuarea oricărei schimbări de coordonate. Puteţi să vă gândiţi la definirea aceasta din punctul de vedere al fizicii. Acolo spunem că un fenomen ("proprietatea") e specific disciplinei cutare ("geometria" - cum ar fi mecanicii, sau electromagnetismului) dacă, odată observat într-un sistem de referinţă $\mathcal{R}_0$ ("coordonatele"), el poate fi observat în orice sistem de referinţă $\mathcal{R}$ care este într-o anumită mişcare (cerinţa asupra mişcării depinde de domeniul cunoaşterii în care ne aflăm) faţă de $\mathcal{R}_0$ ("invarianţa").

Dar ce înseamnă "schimbarea de coordonate"? Asta e întrebarea importantă. De fapt, răspunsul e important: nu există, şi nici nu trebuie să existe, un răspuns universal valabil. În primul rând, o schimbare de coordonate trimite cu gândul la reconfigurare, şi deci trebuie să fie o bijecţie de la spaţiul model în el însuşi. Apoi, dintre acestea, trebuie luate în considerare cele ce respectă esenţialul conceperii geometriei respective. De exemplu, aţi văzut că bijecţiile specifice geometriei euclidiene sunt acelea care păstrează distanţele, numite mişcări rigide, sau izometrii. Asemănător, aţi văzut definirea unei afinităţi şi a unei proiectivităţi. Dar toate aceste clase de transformări formează grupuri: $O(n)$ (pentru euclidiană), $AGL(n, \mathbb{R})$ (pentru afină) şi $PGL(n, \mathbb{R})$ (pentru proiectivă). Astfel, deoarece aceste grupuri acţionează în mod canonic pe spaţiile în cauză, putem spune că o proprietate a spaţiului aparţine geometriei cutare dacă e invariată de acţiunea grupului respectiv. Spre exemplu, deoarece coliniaritatea e păstrată de orice proiectivitate, ea este o proprietate care aparţine geometriei proiective; la fel şi biraportul a patru puncte. Paralelismul nu e modificat dacă aplicăm un element din $AGL(n, \mathbb{R})$, aşa că paralelismul e o noţiune specifică geometriei afine.

Programul lui Klein a constat în drumul invers: dat un grup, să se construiască geometria corespunzătoare aşa încât grupul dat să devină grupul de transformări specifice acelei geometrii. Sigur că oricine putea pune această problemă, însă Klein, împreună cu Lie, au înţeles de ce e important să faci asta...

Tot acest episod a generat o întreagă disciplină, numită *Teoria Invarianţilor*. Ne amintim că analogul algebric al dreptei reale este $\mathbb{R}[X]$; zerourile polinomului 0 sunt toate elementele din $\mathbb{R}$, iar acesta e singurul cu această proprietate, aşa cum am văzut, şi deci faţada algebrică a

dreptei $\mathbb{R}$ este inelul $\frac{\mathbb{R}[X]}{\langle 0\rangle} = \mathbb{R}[X]$, Mai general, dat un corp comutativ k, obiectul algebric asociat spaţiului afin k^n este $k[X_1, \ldots, X_n]$, $n \in \mathbb{N}^*$. Astfel, ca să algebrizăm situaţia geometrică descrisă mai sus, înlocuim acel spaţiu model cu k-algebra $k[X_1, \ldots, X_n]$. Problema principală a teoriei invarianţilor e următoarea: dat un grup G care acţionează pe $k[X_1, \ldots, X_n]$, să se determine invarianţii acestei acţiuni, *i.e.* mulţimea

$$(k[X_1, \ldots, X_n])^G \stackrel{def}{=} \{f \in k[X_1, \ldots, X_n]; gf = g, \forall g \in G\}$$

unde gf notează acţiunea lui g pe f, acţiunea lui G pe $k[X_1, \ldots, X_n]$ fiind o funcţie $G \times k[X_1, \ldots, X_n] \longrightarrow k[X_1, \ldots, X_n]$ cu proprietatea că $e \cdot f = f$ şi $(g_1 g_2)f = g_1(g_2 f)$ pentru orice $g_1, g_2 \in G$ şi orice $f \in k[X_1, \ldots, X_n]$. Observaţi că $(k[X_1, \ldots, X_n])^G$ este o k-subalgebră a lui $k[X_1, \ldots, X_n]$. Astfel, devinde importantă întrebarea următoare: este $(k[X_1, \ldots, X_n])^G$ finit generata ca şi k-algebră, *i.e.* de forma $k[t_1, \ldots, t_r]$ pentru nişte $t_1, \ldots, t_r \in (k[X_1, \ldots, X_n])^G$? Întrebarea e importantă pentru că, dacă ar fi adevărat, înseamnă că am putea găsi toţi invarianţii pornind doar de la un număr finit de invarianţi (cel puţin teoretic).

Iată un exemplu important. Observăm că grupul permutărilor de grad n, S_n, acţionează pe $k[X_1, \ldots, X_n]$ astfel (v-am mai făcut obsevaţia asta): dat $\sigma \in S_n$ şi $f \in k[X_1, \ldots, X_n]$, rezultatul acţiunii lui σ pe $f = f(X_1, \ldots, X_n)$ este polinomul $f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) \stackrel{not}{=} \sigma \cdot f$. Prin definiţie, polinoamele simetrice fundamentale $s_1, \ldots, s_n$ se află în $(k[X_1, \ldots, X_n])^{S_n}$. Aşa cum aţi văzut, are loc:

Teorema fundamentală a polinoamelor simetrice

Orice polinom $f \in k[X_1, \ldots, X_n]$ este de forma $g(s_1, \ldots, s_n)$ pentru un unic $g \in k[Y_1, \ldots, Y_n]$.

Cu alte cuvinte, algebra invarianţilor $(k[X_1, \ldots, X_n])^{S_n}$ e o algebră de polinoame, şi deci avem răspuns afirmativ la problema anterioară în cazul $G = S_n$ - iată de unde importanţa acestei teoreme. În particular, $(k[X_1, \ldots, X_n])^{S_n}$ e inel noetherian (ca să vedeţi asta, încercaţi să arătaţi că un inel factor al unui inel noetherian e noetherian, apoi folosiţi proprietatea de universalitate a algebrelor de polinoame şi teorema bazei a lui Hilbert).

O ultimă precizare : din păcate, problema teoriei invarianţilor nu are mereu răspuns pozitiv. De exemplu, $G = \frac{\mathbb{Z}}{2\mathbb{Z}}$ acţionează pe $k[X, Y]$ prin

decretările $gX = -X$, $gY = -Y$, $g \in G$ (presupunem $char(k) \neq 2$), iar $(k[X,Y])^G$ nu e algebră de polinoame. Problema e că orice algebră polinomială e inel factorial (moşteneşte de la $\mathbb{Z}$ trăsătura de a avea teoremă de descompunere în factori primi, aşa cum discutam la început), însă $(k[X,Y])^G = k[X^2, XY, Y^2]$, iar acesta nu e factorial: $(XY)^2 = XY \cdot XY = X^2 \cdot Y^2$ (nu avem unicitatea descompunerii) - vă veţi lămuri mai bine la "Aritmetica Inelelor".

Nu o să insistăm asupra scrierii unui polinom simetric în funcţie de cele fundamentale; e doar o reţetă. Cu atât mai mult cu cât nu sunteţi străini de aşa ceva: doar aţi văzut la geometrie cum se aduce o formă pătratică la forma canonică folosind metoda Gauss!

2. Fie A un inel (comutativ şi unitar, ca de obicei). În $A[X_1, X_2, X_3]$ să se scrie următoarele polinoame simetrice ca polinoame în s_1, s_2, s_3:
(a) $f = (X_1 - X_2)^2(X_1 - X_3)^2(X_2 - X_3)^2$
(b) $f = (X_1^2 + X_2^2)(X_1^2 + X_3^2)(X_2^2 + X_3^2)$

Soluţie. Puteţi alege să urmaţi demonstraţia teoremei fundamentale a polinoamelor simetrice, sau să calculaţi direct (adunând şi scăzând).
(a) Avem de-a face cu un polinom simetric, omogen, de grad 6, şi deci, având în vedere ordinea lexicografică, termenii principali care pot apărea, la fiecare pas, sunt de forma $X_1^{k_1}X_2^{k_2}X_3^{k_3}$ cu $k_1 \geq k_2 \geq k_3$ şi $k_1 + k_2 + k_3 = 6$. Astfel, $(k_1, k_2, k_3) \in \{(4,2,0), (4,1,1), (3,3,0), (3,2,1), (2,2,2)\}$ (gradul fiecărei nedeterminate în parte nu depăşeşte 4). Astfel, urmând paşii algoritmului din demonstraţia teoremei, obţinem

$$f = s_1^{4-2}s_2^{2-0}s_3^0 + bs_1^3s_2 + cs_2^2 + ds_1s_2s_3 + es_3^2$$

Apoi, ca să determinaţi constantele b, c, d, e folosiţi că $f = (X_1 - X_2)^2(X_1 - X_3)^2(X_2 - X_3)^2$, daţi valori pentru X_1, X_2, X_3, suficient de multe (şi adecvate) cât să vă ofere b, c, d, e - aceste constante sunt "universale" !(puteti să alegeţi X_1, X_2, X_3 să fie rădăcinile de ordinul 3 ale unităţii sau să fie rădăcinile lui $X^3 - X$).

3. Fie $A = k[X,Y]^{S_2} \subset k[X,Y]$ subinelul polinoamelor simetrice, k fiind un corp comutativ de caracteristică diferită de 2. Arătaţi că inelul factor $A \Big/ \langle X^2 + Y^2 \rangle$ este izomorf cu $k[X]$.

Soluţie. Considerăm aplicaţia $\varphi : k[X,Y] \longrightarrow A$ care asociază unui polinom $f(X,Y)$ polinomul simetric $f(X+Y, XY)$. Este clar că φ e morfism de inele. Cum orice polinom simetric se scrie ca polinom de polinoame simetrice fundamentale (în cazul nostru, în funcţie de

$s_1 = X + Y$ şi $s_2 = XY$), avem că φ e surjectiv. Mai mult, datorită unicităţii scrierii, avem şi injectivitate. Aşadar, $k[X,Y] \overset{\varphi}{\simeq} A$. Acum, polinomul simetric X^2+Y^2 se scrie în funcţie de polinoamele simetrice fundamentale astfel: $X^2 + Y^2 = (X+Y)^2 - 2XY = s_1^2 - 2s_2$, deci polinomul simetric $X^2 + Y^2$ provine din polinomul $X^2 - 2Y$ (avem $\varphi(X^2 - 2Y) = (X+Y)^2 - 2XY = X^2 + Y^2$). Prin urmare,

$$\frac{A}{\langle X^2 + Y^2 \rangle} \simeq \frac{k[X,Y]}{\langle X^2 - 2Y \rangle} \simeq k[X]$$

(cf. ex. 1, seminar 6, privind în $(k[X])[Y]$).

4. Fie k un corp comutativ, $char(k) \neq 2$. Dacă $P \in k[X_1, \ldots, X_n]$ satisface identitatea $P = (-1)^{\epsilon(\sigma)}\sigma P$, oricare ar fi $\sigma \in S_n$, atunci polinomul P se divide prin $\prod_{1 \leq i,j \leq n} (X_i - X_j)$.

Soluţie. E suficient să arătăm că pentru orice $i < j$, $(X_i - X_j) \mid P$. Asta înseamnă să arătăm că $P(X_1, \ldots, X_i, \ldots, X_j, \ldots, X_n)$ devine nul dacă înlocuim pe X_i cu X_j, *i.e.* $P(X_1, \ldots, X_j, \ldots, X_j, \ldots, X_n) = 0$ (Bezout). Dar $P = (-1)^{\epsilon(\sigma)}\sigma P$, pentru orice $\sigma \in S_n$, e o identitate polinomială, aşa că are loc indiferent ce punem în locul X_i-urilor (atât timp cât are sens), şi deci $P(X_1, \ldots, X_j, \ldots, X_j, \ldots, X_n) = (-1)^{\epsilon(\sigma)} P(X_{\sigma(1)}, \ldots, X_{\sigma(j)}, \ldots, X_{\sigma(j)}, \ldots, X_{\sigma(n)})$ oricare ar fi $\sigma \in S_n$. Alegând σ să fie transpoziţia $(i\ j)$, obţinem $P(X_1, \ldots, X_j, \ldots, X_j, \ldots, X_n) = -P(X_1, \ldots, X_j, \ldots, X_j, \ldots, X_n)$ (gândiţi-vă că acţiunea unei permutări doar schimbă poziţia, neavând treabă cu ce e efectiv pe poziţie), adică $2P(X_1, \ldots, X_j, \ldots, X_j, \ldots, X_n) = 0$, iar $char(k) \neq 2$.

Să analizăm mai atent polinomul ce apare în exerciţiul anterior, în variantă numerică. Dat un polinom într-o singură nedeterminată, de forma $f(X) = (X - \alpha_1) \ldots (X - \alpha_n)$ (să zicem că suntem peste $\mathbb{C}$), se consideră produsul $\delta = \delta(\alpha_1, \ldots, \alpha_n) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$. Observăm că pentru orice $\sigma \in S_n$, $\sigma\delta(\alpha_1, \ldots, \alpha_n) = \pm\delta(\alpha_1, \ldots, \alpha_n)$, aşa că $(\delta(\alpha_1, \ldots, \alpha_n))^2$ e polinom simetric în α_i-uri. Cantitatea $D_f = \prod_{i<j} (\alpha_i - \alpha_j)^2$ se numeşte discriminantul lui f. Într-adevăr, când $deg(f) = 2$, D_f e ceea ce ştiţi:

5. (cazul pătratic) Pentru $f(X) = X^2 + bX + c$, $D_f = b^2 - 4c$.

Soluţie. Scriem D_f în funcţie de polinoamele simetrice fundamentale (în rădăcinile lui f), Dacă α_1, α_2 notează rădăcinile lui f, atunci, prin

definiţie, $D_f = (\alpha_1 - \alpha_2)^2$; deci $D_f(\alpha_1, \alpha_2) = s_1(\alpha_1, \alpha_2)^2 - 4s_2(\alpha_1, \alpha_2) = b^2 - 4c$, ţinând cont de relaţiile Viète.

6. (cazul cubic) Pentru $f = X^3 + aX^2 + bX + c$ avem că $D_f = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$.

Soluţie. Mai întâi pentru polinoame de forma $f = X^3 + aX + b$. Am văzut în ex. 2, (a) că $D_f = s_1(\alpha_1, \alpha_2, \alpha_3)^2 s_2(\alpha_1, \alpha_2, \alpha_3)^2 - 4s_1(\alpha_1, \alpha_2, \alpha_3)^3 s_3(\alpha_1, \alpha_2, \alpha_3) - 4s_2(\alpha_1, \alpha_2, \alpha_3)^3 + 18s_1(\alpha_1, \alpha_2, \alpha_3)s_2(\alpha_1, \alpha_2, \alpha_3)s_3(\alpha_1, \alpha_2, \alpha_3) - 27s_3(\alpha_1, \alpha_2, \alpha_3)^2 = -4a^3 - 27b^2$ (conform relaţiilor Viète). Apoi, în cazul general, $f = X^3 + aX^2 + bX + c$, discriminantul are aceeaşi formulă, pentru că ne putem reduce la cazul anterior. Într-adevăr, scriem $f = X^3 - s_1X^2 + s_2X - s_3$ (din nou, $s_i = s_i(\alpha_1, \alpha_2, \alpha_3)$) şi facem translaţia $Y = X - \frac{1}{3}s_1$; deci $X = Y + \frac{1}{3}s_1 = Y + \frac{1}{3}(\alpha_1 + \alpha_2 + \alpha_3)$, aşa că $f(X)$ devine $f^*(Y) = Y^3 + \overline{a}Y + \overline{b} = (Y - \beta_1)(Y - \beta_2)(Y - \beta_3)$, unde $\overline{a} = s_2(\beta_1, \beta_2, \beta_3)$ şi $\overline{b} = -s_3(\beta_1, \beta_2, \beta_3)$, având $s_1(\beta_1, \beta_2, \beta_3) = 0$: $\beta_i = \alpha_i - \frac{1}{3}s_1$, $i = 1, 2, 3$ şi deci $\beta_i - \beta_j = \alpha_i - \alpha_j$, aşa că $D_{f(X)} = D_{f^*(Y)}$.

În final, vă propun să vedem demonstraţia marii teoreme a lui Fermat - dar nu în inelul $\mathbb{Z}$, ci în $\mathbb{C}[X]$! Dat $f \in \mathbb{C}[X]$, se consideră $n_0(f)$ ca fiind numărul de rădăcini distincte ale lui f. Deci, $n_0(f)$ numără rădăcinile lui f cu multiplicitatea 1 pentru fiecare, aşa că se poate ca $n_0(f)$ să fie mic în comparaţie cu $deg(f)$ (în orice caz, sigur nu-l depăşeşte). Are loc următorul rezultat:

Teoremă (Mason - Stothers). Fie $a(X), b(X), c(X) \in \mathbb{C}[X]$ polinoame relativ prime, cu proprietatea că $a(X) + b(X) = c(X)$. Atunci $max\{deg(a), deg(b), deg(c)\} \leq n_0(abc) - 1$.

7. (Marea Teoremă lui Fermat în $\mathbb{C}[X]$). Fie $a(X), b(X), c(X) \in \mathbb{C}[X]$ polinoame relativ prime aşa încât măcar unul dintre ele are gradul ≥ 1 şi $a(X)^n + b(X)^n = c(X)^n$. Atunci $n \leq 2$.

Soluţie. Folosim teorema Mason - Stothers pentru polinoamele $a(X)^n, b(X)^n$ şi $c(X)^n$, în trei rânduri. Avem:

$$\begin{aligned} n \cdot deg(a(X)) &= deg(a(X)^n) \leq max\{deg(a(X)^n), deg(b(X)^n), deg(c(X)^n)\} \\ &\leq n_0((a(X)b(X)c(X))^n) - 1 = n_0(a(X)b(X)c(X)) - 1 \leq \\ &\leq deg(a(X)b(X)c(X)) - 1 = deg(a) + deg(b) + deg(c) - 1. \end{aligned}$$

La fel obţinem şi pentru b şi c în locul lui a. Adunând cele trei inegalităţi rezultate, ajungem la

$$n(deg(a) + deg(b) + deg(c)) \leq 3(deg(a) + deg(b) + deg(c)) - 3,$$

iar asta e imposibil dacă $n \geq 3$.

Aţi mai văzut şi că teorema împărţirii cu rest are loc în $k[X]$. O să vedeţi şi că teorema fundamentală de descompunere unică în factori primi are loc în $k[X]$. Toate acestea confirmă analogia fructuoasă dintre $\mathbb{Z}$ şi $k[X]$ asupra căreia v-am atras atenţia (sper). Însă exerciţiul anterior vă convinge de ceea ce vă spuneam: $\mathbb{Z}$ e acela mai complicat. (Teorema Mason - Stothers e usor de demonstrat - vezi Lang, *Algebra*)