SEMINAR 6

Aţi văzut la curs definiţia noţiunii de ideal maximal al unui inel. De ce le acordăm atenţie specială acestora? Pe de o parte, amintiţi-vă ce am discutat la început despre rezolvarea ecuaţiilor peste $\mathbb{Z}$. Acolo am văzut că problema era de a lămuri dacă teorema fundamentală a aritmeticii persistă în acele inele de numere, cum ar fi $\mathbb{Z}[\omega]$, şi că punctul culminant a fost schimbarea conceptuală adusă de către Kummer, cu ale sale ”numere ideale”. Vă spuneam că la acest nivel (al idealelor) teorema fundamentală se menţine mereu: orice ideal $I \subset \mathbb{Z}[\omega]$ se scrie, în mod unic, sub forma $I = P_1^{\alpha_1} \dots P_r^{\alpha_r}$. Aceste P_i-uri sunt ideale maximale ale lui $\mathbb{Z}[\omega]$: $\mathbb{Z}[\omega] \big/ P_i$ e un $\mathbb{F}_q$! (toată munca efectuată în $\mathbb{Z}[\omega]$ pentru a înţelege ecuaţia $x^n + y^n = z^n$ se contorizează în mediile finite; e un lucru fantastic cum ideea aceasta de a înţelege inele precum $\mathbb{Z}[\omega]$ pentru a rezolva ecuaţii peste $\mathbb{Z}$ se îmbină cu ideea, ce are acelaşi scop, de a studia reducţii modulo p ale ecuaţiilor). Pe de altă parte, fie d o dreaptă dintr-un plan euclidian. Am discutat despre acel punct de cotitură în care Descartes pune în bijecţie punctele de pe d cu numerele reale: $d \simeq \mathbb{R}$. Atunci, în cadrul acestui izomorfism, dacă $P \in d$ e un punct, acesta e localizat printr-o coordonată $a \in \mathbb{R}$. Ca să continuăm linia de idei, amintiţi-vă discuţia despre punctul de vedere funcţional al lui Riemann şi, în acelaşi timp, ţineţi cont că, făcând algebră, vrem ca discuţia să funcţioneze pentru cât mai multe corpuri k în locul lui $\mathbb{R}$. Atunci funcţiile care ne mai rămân la dispoziţie pentru a descrie acel punct sunt cele polinomiale (aspectele astea le-am mai discutat); mai precis, fiind într-o singură dimensiune (suntem pe o dreaptă), trebuie să căutăm în $\mathbb{R}[X]$. Zerourile căror polinoame oferă a? Primul care apare e cel evident, $X - a$. De fapt, toate care au ca rădăcină pe a sunt de forma $f(X - a)$, $f \in \mathbb{R}[X]$ (Teorema lui Bezout), deci idealul $\langle X - a\rangle \subset \mathbb{R}[X]$ e contrapartea algebrică a obiectului geometric $P \in d$. Dar $\langle X - a\rangle$ e ideal maximal în $\mathbb{R}[X]$: $\frac{\mathbb{R}[X]}{\langle X-a\rangle} \simeq \mathbb{R}$ (deci e corp). Asta reiese din următorul exerciţiu:

1. Fie A un inel comutativ şi $a \in A$. Atunci $\frac{A[X]}{\langle X-a\rangle} \simeq A$.

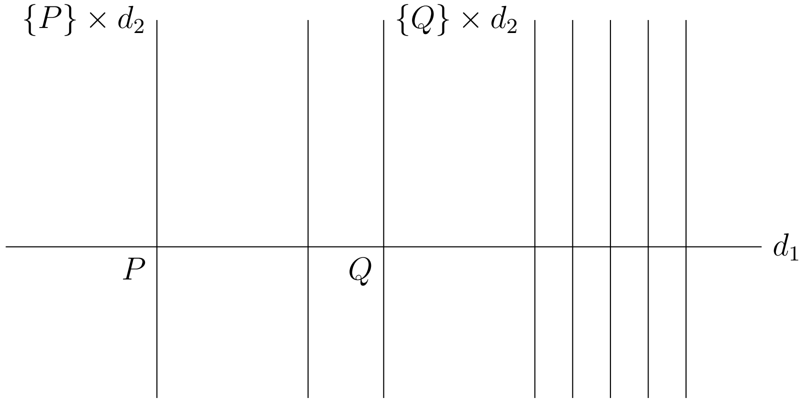
Soluţie. Vă spuneam că principala fabricare de izomorfisme e conţinută în teorema fundalentală de izomorfism. Avem morfismul de evaluare în a, $\varphi : A[X] \longrightarrow A$, $\varphi(f) = f(a)$ (e cea mai naturală cale de a ajunge din $A[X]$ în A). Având în vedere izomorfismul dorit şi teorema amintită, vrem ca $Im(\varphi) = A$ şi $Ker(\varphi) = \langle X - a \rangle$. Că φ e surjectivă, e clar: orice element din A poate fi privit ca polinom constant. A doua egalitate e un alt fel de a exprima teorema lui Bezout.

De fapt, mai general, $\frac{A[X_1,\ldots,X_n]}{\langle X_1-a_1,\ldots,X_n-a_n\rangle} \simeq A$ (încă avem o teoremă de împărţire cu rest şi în $A[X_1, \ldots, X_n]$, dar ceva mai slăbită; însă intuitiv, când împărţim $A[X_1, \ldots, X_n]$ la idealul $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$, X_i-urile devin a_i şi, deci, $A[X_1, \ldots, X_n]$ devine $A[a_1, \ldots, a_n] = A$). Încă o observaţie legată de acest exerciţiu: trebuie să înţelegem că una e un polinom, şi alta e funcţia asociată acestuia. De exemplu, fie $f = X^2 - X \in \mathbb{F}_2[X]$. Acesta e un polinom nenul, însă funcţia asociată lui, anume $\mathbb{F}_2 \longrightarrow \mathbb{F}_2$, $x \mapsto f(x)$, e identic nulă (în sinea lui, un polinom e doar o expresie formală $a_0 + a_1X + a_2X^2 + a_3X^3$ ce înglobează în ea toate situaţiile concrete în care punem ceva în loc de X - un număr, o matrice,...., un t să-i zicem, atâta timp cât a_it^i are sens; de unde şi denumirea de nedeterminată pentru X).

Revenind la discuţie, deducem următorul lucru: noţiunea de ideal maximal e întruchiparea algebrică (abstractă) a ideilor de număr şi punct! (deci e o noţiune fundamentală).

Înainte de a trece la nişte exerciţii, trebuie să vă mai fac o precizare (precum altele asemenea, şi asta e pentru peste câţiva ani): există o desăvârşire sublimă a punctului de vedere cartezian numită Nullstellensatz (Hilbert): în bijecţia lui Descartes, păstrăm aspectul geometric, însă înlocuim pe cel analitic (exprimat prin $\mathbb{R}$) cu cel algebric (exprimat prin inele de polinoame).

2. Fie $A_1, \ldots, A_n$ inele comutative şi fie $A = A_1 \times \ldots \times A_n$, produsul lor direct. Să se determine idealele maximale ale inelului A.
Soluţie. Mai întâi, până a trece la rezolvarea propriu-zisă, o discuţie neriguroasă (şi chiar eronată). Să ne închipuim că în loc de inelele $A_1, \ldots, A_n$ avem nişte drepte şi să zicem că $n = 2$; deci $A = \mathbb{R} \times \mathbb{R}$ e planul euclidian şi trebuie să îi descriem punctele. Ce înseamnă acel "$\times$", geometric vorbind? Primul $\mathbb{R}$ e o dreaptă d_1, iar al doilea, o dreaptă d_2 şi formăm $d_1 \times d_2$ pur şi simplu punând d_2 perpendicular peste fiecare punct P de pe d_1; deci măturăm continuu toate punctele folosind toate copiile lui d_2 de forma $\{P\} \times d_2$, $P \in d_1$:



Să revenim la exerciţiul nostru. Ştim că un ideal I al lui A e de forma $I_1 \times \ldots \times I_n$, cu I_i ideal al lui A_i oricare ar fi $1 \leq i \leq n$ (era unul din exerciţiile pentru prezentare). Din discuţia anterioară, ne uităm la cele de forma $M = A_1 \times \ldots \times A_{i-1} \times M_i \times A_{i+1} \times \ldots \times A_n$, cu M_i ideal maximal al lui A_i. Sunt aceste M-uri ideale maximale ale lui A? În general avem:

($*$) dacă I_i e ideal în A_i, $1 \leq i \leq n$, atunci avem un izomorfism canonic (natural) $\frac{A_1 \times \ldots \times A_n}{I_1 \times \ldots \times I_n} \simeq \frac{A_1}{I_1} \times \ldots \times \frac{A_n}{I_n}$
(într-adevăr, e teorema fundamentală de izomorfism aplicată morfismului $A_1 \times \ldots \times A_n \longrightarrow \frac{A_1}{I_1} \times \ldots \times \frac{A_n}{I_n}$, $(a_1, \ldots, a_n) \mapsto (a_1 + I_1, \ldots, a_n + I_n)$, unde $a_i + I_i$ notează clasa lui a_i modulo I_i).

La noi, $\frac{A}{M} \simeq 0 \times \ldots \times 0 \times \frac{A_i}{M_i} \times 0 \times \ldots 0 \simeq \frac{A_i}{M_i}$, deci $\frac{A}{M}$ e corp (M_i e maximal în A_i), *i.e.* M e maximal în A.
De fapt, acestea sunt toate maximalele lui A. Într-adevăr, fie $M \subset A$ un ideal maximal oarecare. Atunci, fiind ideal, M e de forma $I_1 \times \ldots \times I_n$, cu I_i ideal în A_i oricare ar fi i. Dacă ar fi doi indici $i \neq j$ pentru care $\frac{A_i}{I_i} \neq 0$ şi $\frac{A_j}{I_j} \neq 0$, atunci luăm un $x_i \in \frac{A_i}{I_i} \setminus \{0\}$ şi un $x_j \in \frac{A_j}{I_j} \setminus \{0\}$ şi găsim $a, b \in \frac{A}{M} \setminus \{0\}$ astfel încât $ab = 0$: în inelul $\prod\limits_{r=1}^{n} \frac{A_r}{I_r}$ avem elementele nenule $\alpha = (0, \ldots, 0, x_i, 0, \ldots, 0)$ şi $\beta = (0, \ldots, 0, x_j, 0, \ldots, 0)$ cu $\alpha\beta = 0$ (căci $i \neq j$) şi îi transferăm în $\frac{A}{M}$ via ($*$), obţinând astfel a şi b. Aceasta e o contradicţie căci într-un corp nu avem divizori ai lui zero (M e maximal în A). Astfel, există cel mult un indice i pentru care $I_i \neq A_i$ şi deci $M = A_1 \times \ldots \times A_{i-1} \times I_i \times A_{i+1} \times \ldots \times A_n$. Mai mult, I_i e maximal în A_i (rezultă ca mai sus, din ($*$)).

3. Fie A un inel comutativ şi $a \in A$. Idealul $\langle X, a \rangle$ e maximal în $A[X]$ dacă şi numai dacă idealul $\langle a \rangle$ e maximal în A.

Soluţie. Ca să lămurim, $\langle X, a\rangle$ e idealul din $A[X]$ generat de polinoamele X şi a (a văzut ca polinom constant), iar $\langle a\rangle$ e idealul din A generat de constanta a. Ca să evităm confuzia, ar trebui să notăm $\langle X, a\rangle$ cu $A[X]\cdot X + A[X]\cdot a$ şi $\langle a\rangle$ cu Aa, dar sper că e clar.
Pentru ca $\langle X, a\rangle$ să fie maximal în $A[X]$, trebuie arătat că $\frac{A[X]}{\langle X,a\rangle}$ e corp; ditto pentru $\langle a\rangle$. Deci, trebuie să depistăm inelele $\frac{A[X]}{\langle X,a\rangle}$ şi $\frac{A}{\langle a\rangle}$. De fapt, acestea sunt izomorfe. Dacă din $A[X]$ eliminăm $\langle X, a\rangle$, X-ul dispare (idealul $\langle X, a\rangle = \langle X - 0, a\rangle$, deci prima relaţie e $X = 0$) şi rămânem cu $\frac{A}{\langle a\rangle}$. Riguros, observăm morfismul $\varphi : A[X] \longrightarrow \frac{A}{\langle a\rangle}$, $\varphi(f) = \widehat{f(0)}$, şi aplicăm teorema fundamentală: $\frac{A[X]}{Ker(\varphi)} \simeq Im(\varphi)$. Evident, φ e surjectiv, adică $Im(\varphi) = \frac{A}{\langle a\rangle}$. Avem şi $Ker(\varphi) = \langle X, a\rangle$. Într-adevăr, dacă $f \in \langle X, a\rangle$, înseamnă că există $g, h \in A[X]$ astfel încât $f = Xg + ah$, de unde $f(0) = 0g(0) + ah(0) = a\cdot h(0) \in \langle a\rangle$, *i.e.* $\widehat{f(0)} = 0$, *i.e.* $f \in Ker(\varphi)$; deci $\langle X, a\rangle \subseteq Ker(\varphi)$. Invers, dacă $f \in Ker(\varphi)$, scriem $f = a_0 + a_1X + \ldots + a_nX^n$, $a_i \in A$. Deoarece $\varphi(f) = 0$, înseamnă că $\widehat{f(0)} = 0$, adică $a_0 = f(0) \in \langle a\rangle$, *i.e.* $a_0 = \alpha a$ pentru un $\alpha \in A$; deci $f = \alpha a + (a_1 + a_2X + \ldots + a_nX^{n-1})X \in \langle X, a\rangle$. Astfel avem şi $Ker(\varphi) \subseteq \langle X, a\rangle$.
Aşadar, $\frac{A[X]}{\langle X,a\rangle} \simeq \frac{A}{\langle a\rangle}$, de unde echivalenţa.

Am văzut că punctele se corespund cu idealele maximale: ceea ce e minimal în imaginea geometrică, devine maximal în viziune algebrică, şi invers - spunem că legătura e contravariantă (fenomenul acesta e, în esenţă, un manifest al celor două doctrine dominante în geometrie: extrinsec şi intrinsec). Atunci, având în vedere inversiunea asta, faptul că printr-un orice punct trece mereu un obiect geometric (o curba, de exemplu) şi că, în general, obiectele geometrice ar trebui să se corespundă cu ideale, ne aşteptăm atunci ca orice ideal să fie conţinut într-unul maximal. Aşa şi este:

4. Dacă A e un inel şi I un ideal al său, $I \neq A$, atunci există un ideal maximal M al lui A astfel încât $M \supseteq I$.
Soluţie. (vezi teoria mulţimilor) Nu avem decât să considerăm toate idealele ce conţin I şi să le reunim într-unul singur. Considerăm mulţimea $\mathcal{P}_I = \{J \mid J \text{ e ideal al lui } A, J \neq A \text{ şi } J \supseteq I\}$ împreună cu relaţia de incluziune. Perechea $(\mathcal{P}_I, \subseteq)$ e inductiv ordonată. Într-adevăr, dacă $\{I_\lambda\}_{\lambda\in\Lambda}$ e o parte nevidă şi total ordonată a sa, atunci $J = \bigcup_{\lambda\in\Lambda} I_\lambda$ e majorant pentru familia $\{I_\lambda\}$ (e clar că $J \supseteq I_\lambda$ oricare ar fi λ, dar trebuie să verificaţi şi că $J \in \mathcal{P}_I$). Atunci lema lui Zorn ne spune că

$\mathcal{P}_I$ admite un element maximal, M să-i zicem (observaţi că totul are sens: $\mathcal{P}_I \neq \emptyset$). Evident (din construcţie) că M e un ideal maximal al lui A ce conţine I (din nou, revizuiţi materia din semestrul I de la teoria mulţimilor pentru lema lui Zorn; nu trebuie să vă fie teamă de ea - e doar o variantă îmbunătăţită a inducţiei clasice, tocmai pentru că oferă pasul de inducţie în prezenţa unui infinit mai mare decât cel cu care se ocupă inducţia uzuală, anume $\mathbb{N}$).

Există inele ce conţin doar un singur ideal maximal, aşa cum e cazul corpurilor. Pentru un exemplu netrivial: $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$, cu p prim şi n natural (singurul maximal al său e $\frac{p\mathbb{Z}}{p^n\mathbb{Z}}$). Un inel comutativ ce are un singur ideal maximal M se numeşte inel local, caz în care $K = \frac{A}{M}$ se numeşte corpul rezidual al lui A (Care e corpul rezidual din exemplul anterior?).

5. (i) Fie A un inel comutativ şi $M \neq A$ un ideal astfel încât orice $x \in A \setminus M$ e unitate (element inversabil). Atunci A e inel local, de ideal maximal M.
(ii) Fie A un inel comutativ şi M un ideal maximal al său astfel încât orice element de forma $1 + x$, $x \in M$, e unitate în A. Atunci A e inel local.
Soluţie. (i) Fie $I \neq A$ un ideal oarecare. Deoarece $1 \notin I$ (căci $I \neq A$), trebuie ca I să conţină doar elemente neinversabile şi, deci, trebuie ca $I \subseteq M$ (conform ipotezei). Astfel, M e singurul maximal.
(ii) Folosim (i). În acest scop, arătăm că orice element din $A \setminus M$ e unitate. Fie $x \in A \setminus M$. Deoarece idealul $Ax + M$ conţine strict pe M, iar M e maximal, trebuie să avem $Ax + M = A$. Astfel, există $y \in A$ şi $a \in M$ astfel încât $yx + a = 1$, sau $yx = 1 - a$ şi, deci, yx e unitate (conform ipotezei), de unde reiese că x e unitate (suntem în cadrul comutativ).

Dacă ne situăm în cadrul unei topologii rigide, nu mai putem apela la exprimări de forma "fie V o vecinătate suficient de mică în jurul punctului p". Cum substituim acest principiu de localizare (preponderent în cadrul analizei matematice)? Răspuns: inele locale.

La un moment dat am discutat despre nilradicalul unui inel. Similar acestuia, se defineşte radicalul Jacobson al unui inel A ca fiind intersecţia tuturor idealelor maximale din A: $\mathcal{J}(A) = \bigcap\limits_{M \subset A} M$, unde intersecţia se face după toate maximalele. Acesta se poate descrie cu ajutorul elementelor astfel:

6. Fie A un inel comutativ. Atunci $x \in \mathcal{J}(A)$ dacă şi numai dacă $1 - xy$ e unitate în A oricare ar fi $y \in A$.
Soluţie. *Necesitatea.* Fie $x \in \mathcal{J}(A)$. Presupunem, prin absurd, că ar exista un $y \in A$ astfel încât $1 - xy$ nu e unitate. Atunci există un ideal maximal M al lui A ce conţine $1 - xy$ (cf. ex. 4 - $\langle 1 - xy \rangle \neq A$). Dar $x \in M$ (pentru că $\mathcal{J}(A) \subseteq M$, prin definiţie), aşa că $xy \in M$, de unde contradicţia $1 \in M$.
Suficienţa. Presupunem că $1 - xy$ e inversabil oricare ar fi $y \in A$. Să zicem că am avea $x \notin \mathcal{J}(A)$. Asta înseamnă că există un maximal $M \subset A$ astfel încât $M \not\ni x$. Atunci $Ax + M = A$ (din nou, $Ax + M \supsetneq M$ şi M e maximal) şi, deci, $yx + a = 1$, pentru nişte $y \in A, a \in M$; atunci $1 - xy \in M$, aşa că $1 - xy$ nu are cum să fie inversabil - contradicţie.

Discuţia a fost axată pe ideale maximale. Mai exersăm cu teorema fundamentală de izomorfism la începutul seminarului următor (cu situaţii mai concrete).