SEMINAR 7

Având în vedere ultima parte a seminarului 6, o vorbă despre acele radicale se cuvine. Pentru a înţelege de ce trebuie luate în considerare, trebuie să ne întoarcem la greci. Până la pitagoreici, treaba se făcea în cadrul mulţimii $\mathbb{Q}_+$. Problema ridicată de pitagoreici a fost cea a comensurabilităţii diagonalei unui pătrat cu lungimea laturei egală cu 1; adică, putem găsi un instrument (o riglă) care să ne permită măsurarea diagonalei? (nu uitaţi: gradarea riglei poate fi făcută doar în termeni de raţionale). Aceştia descoperă că, notând cu d lungimea diagonalei, $d^2 = 1^2 + 1^2$; dar o astfel de cantitate, pe care o notăm $\sqrt{2}$, nu poate sta în $\mathbb{Q}_+$! (De ce?) Iată de ce e crucială "teorema lui Pitagora": a dat la iveală continuumul numeric (bineînţeles că nu toate numerele sunt nişte radicali, esenţial vorbind, însă radicalii au dat la iveală o cu totul altă natură a numerelor, natură ce a fost numită "iraţională"). Astfel, deoarece, pe cealaltă parte, o dreaptă geometrică e considerată prin definiţie (sau, mai bine zis, prin intuiţie comună) un continuum 1-dimensional, terenul era pregătit pentru bijecţia lui Descartes.

Acum, revenind la situaţia noastră, dacă vrem să pregătim terenul pentru legătura dintre obiecte geometrice şi ideale ("numerele ideale"), trebuie să luăm în considerare radicalele idealelor. Cum le definim? Pentru un număr pozitiv x, avem $\sqrt{x}^2 = x$. Atunci, pentru un ideal I al unui inel A, punem $\sqrt{I} = \{a \in A; a^n \in I \text{ pentru un } n \in \mathbb{N}\}$. Consideraţi morfismul canonic $\pi : A \longrightarrow \frac{A}{I}$: avem $\pi^{-1}(\mathcal{N}il(\frac{A}{I})) = \sqrt{I}$ (în particular, radicalul unui ideal e un ideal, aşa cum radicalul unui număr e tot un număr).

Mai ţin să fac o precizare. La momentul respectiv, incursiunea pitagoreicilor a generat o întreagă criză (întreţinută de implicaţiile filozofice). Dacă voi nu reuşiţi să resimţiţi această criză, vă invit să citiţi despre *ipoteza continuumului.* (Exerciţiu)

Cum spuneam, mai exersăm cu teorema fundamentală de izomorfism. Repet, în tot acest timp trebuie să înţelegeţi că aceste izomorfisme exprimă, la nivel de obiecte, încercarea de a rezolva ecuaţii. Dacă avem o ecuaţie căreia nu-i găsim soluţii într-un anume sistem de numere, atunci trebuie să le căutăm în sisteme mai largi decât cel iniţial - sigur sunt pe undeva acele soluţii (ideea lui Gauss). Dar cum le găsim? Avem o ecuaţie $f(x) = a_0 + a_1 x + \ldots + a_n x^n = 0$ într-un sistem numeric k ale cărei soluţii nu se află toate în k. Atunci ne uităm la extinderea $k[X] \big/ \langle f(X) \rangle$ pentru că "împărţind" prin idealul generat de f, acest $f(X)$ devinde 0, *i.e.* acel X (nedeterminată - nu ştim cine e, în general) devine soluţie a ecuaţiei (tehnica lui Kronecker). Astfel, devine important să devoalăm identitatea obiectului misterios $k[X] \big/ \langle f \rangle$. Cum facem asta? Răspuns: teorema fundamentală de izomorfism.

1. $\mathbb{R}[X] \big/ \langle X^2 + 1 \rangle \simeq \mathbb{C}$

Soluţie. Inelul $\mathbb{R}[X] \big/ \langle X^2 + 1 \rangle$ se obţine "împărţind" pe $\mathbb{R}[X]$ la $\langle X^2 + 1 \rangle$, adică impunem lui $\mathbb{R}[X]$ relaţia $X^2 + 1 = 0$, *i.e.* $X = i$, aşa că $\mathbb{R}[X] \big/ \langle X^2 + 1 \rangle \simeq \mathbb{R}[i] \simeq \mathbb{C}$. Riguros, considerăm din nou morfismul de evaluare $\varphi : \mathbb{R}[X] \longrightarrow \mathbb{C}$, $\varphi(f) = f(i)$. În primul rând, φ e surjectiv: pentru orice $z = a + bi \in \mathbb{C}$, avem $f = a + bX \in \mathbb{R}[X]$ astfel încât $\varphi(f) = z$; deci $Im(\varphi) = \mathbb{C}$. Trebuie să arătăm că $\langle X^2 + 1 \rangle = Ker(\varphi)$. Din nou, teorema lui Bezout arată acest lucru. Dacă $f \in \langle X^2 + 1 \rangle$, înseamnă că $f = (X^2 + 1)g$, pentru un $g \in \mathbb{R}[X]$, şi deci $\varphi(f) = g(i)(i^2 + 1) = g(i) \cdot 0 = 0$, *i.e.* $f \in Ker(\varphi)$, aşa că $\langle X^2 + 1 \rangle \subseteq Ker(\varphi)$. Reciproc, dacă $f \in Ker(\varphi)$, înseamnă că $0 = \varphi(f) = f(i)$, adică i e rădăcină a lui f, şi deci teorema lui Bezout spune că $X - i$ divide f; însă f e un polinom cu coeficienţi reali, aşa că odată cu o rădăcină z a sa, şi $\overline{z}$ e rădăcină a sa, deci şi $-i$ e rădăcină a lui f, de unde $X - (-i)$ divide f (încă o dată cu teorema lui Bezout). Astfel, $X - i$ şi $X + i$ divid f, deci şi $X^2 + 1 = (X - i)(X + i)$ divide f, *i.e.* există $g \in \mathbb{R}[X]$ astfel încât $f = (X^2 + 1)g$, adică $f \in \langle X^2 + 1 \rangle$. Astfel avem şi $Ker(\varphi) \subseteq \langle X^2 + 1 \rangle$.

Subexerciţiu. Soluţia de mai sus e corectă, numai că trebuie lămurit ceva într-un anume punct. Ce? (la incluziunea $Ker(\varphi) \subseteq \langle X^2 + 1 \rangle$, desigur)
În altă ordine de idei, soluţia e tâmpă. Dacă $f \in Ker(\varphi)$, aplicăm pur şi simplu teorema împărţirii cu rest pentru f şi $X^2 + 1$: există $q, r \in \mathbb{R}[X]$, cu $0 \leq deg(r) < 2$, astfel încât $f = q(X^2 + 1) + r$. Cum $f \in Ker(\varphi)$, $f(i) = 0$, adică $q(i)(i^2 + 1) + r(i) = 0$, sau, scriind $r = a + bX$ ($deg(r) < 2$), $a + bi = 0$, *i.e.* $a = b = 0$. Astfel, $r = 0$ şi

deci $f = q(X^2+1) \in \langle X^2+1 \rangle$.

Astfel, deşi ecuaţia X^2+1 nu are soluţii în $\mathbb{R}$, îi găsim soluţiile în extinderea $\mathbb{R}[X] \big/ \langle X^2+1 \rangle$, iar cu teorema fundamentală de izomorfism, vedem că asta este o deghizare a lui $\mathbb{C}$.
Apropo de teorema împărţirii cu rest; faptul că ea are loc în inelele de polinoame $k[X]$ ne arată încă o clasă de inele care moştenesc trăsături ale lui $\mathbb{Z}$ (le zicem inele euclidiene); zic "o altă clasă" pentru că am mai discutat alte astfel de inele: $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{d}]$, $\mathbb{Z}[\omega]$. Poate e de neaşteptat la prima vedere, însă toate acestea sunt mult mai simple decât $\mathbb{Z}$. Toate eforturile de a înţelege aceste inele sunt menite, în cele din urmă, înţelegerii lui $\mathbb{Z}$.

2. $\mathbb{Z}[X] \big/ \langle X^2-d \rangle \simeq \mathbb{Z}[\sqrt{d}]$, unde $d \in \mathbb{Z} \setminus \{0\}$ e liber de pătrate.

Soluţie. E aceeaşi situaţie. Consideraţi $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[\sqrt{d}]$, $\varphi(f) = f(\sqrt{d})$, etc.

Înainte de a vedea următorul exerciţiu, ne trebuie o scurtă pregătire. Ştim cum rezolvăm o ecuaţie de forma $ax = b$ în $\mathbb{C}$, însă cum rezolvăm o congruenţă $ax \equiv b (\mathrm{mod}\ m)$, cu $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ fixaţi? Cu alte cuvinte, cum rezolvăm ecuaţia $ax = b$ în $\frac{\mathbb{Z}}{m\mathbb{Z}}$? E clar că pentru a avea soluţii, o condiţie necesară e ca $d \mid b$, unde $d = (a, m)$. Atunci ne uităm la congruenţa mai simplă $\frac{a}{d}x = \frac{b}{d}(\mathrm{mod}\ \frac{m}{d})$, încercăm să-i găsim soluţiile acesteia din urmă, cu care apoi să generăm toate soluţiile congruenţei iniţiale. Rezultatul e următorul: congruenţa $ax \equiv b(\mathrm{mod}\ m)$ are d soluţii (când $d \mid b$), anume $t, t+\frac{m}{d}, t+2\frac{m}{d}, \ldots, t+(d-1)\frac{m}{d}$, unde t e unica soluţie a congruenţei $\frac{a}{d}x \equiv \frac{b}{d}(\mathrm{mod}\ \frac{m}{d})$ (poate revizuiţi exerciţiul pe care l-am făcut mai demult legat de $Hom_{\mathbb{Z}}(\mathbb{Z}_M, \mathbb{Z}_N)$). În particular, vedem că în mediile finite, o ecuaţie poate avea mai multe (sau mai puţine) soluţii decât îi este gradul (de exemplu, $X^4 - 1 = 0$ are 8 soluţii în $\frac{\mathbb{Z}}{16\mathbb{Z}}$, iar $X^4 - 2 = 0$ nu are soluţii în $\frac{\mathbb{Z}}{16\mathbb{Z}}$); ce vă spuneam, lucrurile nu-s aşa lejere în sistemele finite (având în vedere teorema fundamentale a algebrei).

Ridicăm puţin ştacheta, considerând de data asta un sistem de congruenţe

$$\begin{cases} a_1x \equiv b_1(mod\, m_1) \\ a_2x \equiv b_2(mod\, m_2) \\ \dots\dots \\ a_rx \equiv b_r(mod\, m_r) \end{cases}$$

şi presupunem că modulele $m_1, \dots, m_r$ sunt mutual coprime, *i.e.* $(m_i, m_j) = 1$ oricare ar fi $1 \leq i, j \leq r$ (ca să nu avem repetiţii). La fel, pentru a avea soluţii, trebuie ca $(a_i, m_i) \mid b_i$ oricare ar fi $1 \leq i \leq r$. În acest caz, nu avem decât să le luăm pe fiecare în parte, le găsim soluţiile, şi apoi vedem care dintre ele se potrivesc pentru toate. Astfel, sistemul e redus la un sistem de forma

$$\begin{cases} x \equiv c_1(mod\, n_1) \\ x \equiv c_2(mod\, n_2) \\ \dots\dots \\ x \equiv c_r(mod\, n_r) \end{cases}$$

(aici $n_i = \frac{m_i}{(a_i,m_i)}$, iar coeficientul lui x e 1 pentru că coeficientul său după reducţie are clasa inversabilă modulo n_i, şi, deci, putem înmulţi cu inversul său, conform discuţiei de mai sus pentru $ax \equiv b(mod\, m)$). Înglobăm modulele într-unul singur: fie $n = n_1n_2 \dots n_r = n_1N_1 = n_2N_2 = \dots = n_rN_r$. Deoarece $(n_i, N_i) = 1$, există un u_i astfel încât $u_iN_i \equiv 1(mod\, n_i)$ (am văzut cum se arată asta într-un seminar trecut), iar acest u_i e unic modulo n_i, oricare ar fi $1 \leq i \leq r$. Atunci luăm combinaţia $x = u_1N_1c_1 + \dots + u_rN_rc_r$ şi vedem imediat că $x \equiv u_iN_ic_i \equiv c_i(mod\, n_i)$ oricare ar fi $1 \leq i \leq r$; deci x e soluţie a sistemului. Mai mult, dacă y e o altă soluţie a sistemului, atunci $y \equiv c_i \equiv x\,(mod\, n_i)$, oricare ar fi i, de unde $y \equiv x\,(mod\, n)$ (căci n_i-urile sunt coprime). Aşadar:

Lema chineză a resturilor. Dacă $n_1, \dots, n_r$ sunt mutual coprime, atunci sistemul $x \equiv c_i\,(mod\, n_i)$, $1 \leq i \leq r$, are soluţie unică modulo n.

Acum să încercăm să exprimăm mai algebric acest rezultat; să zicem că $r = 2$. În primul rând suntem în inelul $\mathbb{Z}$. Apoi, a lucra modulo n_i înseamnă a lucra în $\frac{\mathbb{Z}}{I_i}$, unde $I_i = n_i\mathbb{Z}$, $i = 1, 2$. A cere ca $x \equiv c_1\,(mod\, n_1)$, $x \equiv c_2\,(mod\, n_2)$ e tot una cu a avea {clasa lui x modulo I_1 e tot una cu clasa lui c_1 modulo I_1} şi {clasa lui x modulo I_2 e tot una cu clasa lui c_2 modulo I_2}. Cu alte cuvinte, a rezolva sistemul e tot una cu a găsi un element $x \in \mathbb{Z}$ astfel încât $\pi_1(x) = \pi_1(c_1)$ şi $\pi_2(x) = \pi_2(c_2)$, unde $\pi_i : \mathbb{Z} \longrightarrow \frac{\mathbb{Z}}{I_i}$ e morfismul canonic, $i = 1, 2$. Astfel, considerând morfismul $\varphi : \mathbb{Z} \longrightarrow \frac{\mathbb{Z}}{I_1} \times \frac{\mathbb{Z}}{I_2}$, $\varphi(x) = (\pi_1(x), (\pi_2(x))$,

partea din lema chineză a resturilor care ne spune că oricum am lua c_1 şi c_2, sistemul are o soluţie x, se traduce prin aceea că morfismul φ e surjectiv, iar partea care ne spune că soluţia e unică modulo $n = n_1 n_2$ ne spune că morfismul φ e injectiv modulo $n\mathbb{Z}$. Cu alte cuvinte, exprimarea algebrică a lemei chineze a resturilor e următoarea: dacă $(n_1, n_2) = 1$, atunci $\frac{\mathbb{Z}}{n_1 n_2 \mathbb{Z}} \simeq \frac{\mathbb{Z}}{n_1 \mathbb{Z}} \times \frac{\mathbb{Z}}{n_2 \mathbb{Z}}$. Observaţi că $(n_1, n_2) = 1$ se traduce prin $I_1 + I_2 = \mathbb{Z}$, *i.e.* I_1 şi I_2 sunt comaximale.
În general, situaţia e următoarea:

3. (Lema chineză a resturilor în variantă abstractă)

Fie A un inel comutativ şi $I_1, \ldots I_r$ ideale ale lui A. Avem morfismul natural $\varphi : A \longrightarrow \prod_{i=1}^{r} \frac{A}{I_i}$, $\varphi(x) = (\pi_1(x), \ldots, \pi_r(x))$, unde $\pi_i : A \longrightarrow \frac{A}{I_i}$, $1 \leq i \leq r$, sunt morfismele canonice.
(a) Dacă $I_1, \ldots, I_r$ sunt mutual comaximale, atunci $\prod I_i = \bigcap I_i$.
(b) φ e surjectivă dacă şi numai dacă $I_1, \ldots, I_r$ sunt mutual comaximale.
(c) φ e injectivă dacă şi numai dacă $\bigcap I_i = 0$.

Soluţie. (a) Procedăm inductiv asupra lui r. Cazul $r = 2$ e lejer (în general, pentru orice două ideale I, J avem că $IJ \subseteq I \cap J$; dacă sunt comaximale, obţineţi şi incluziunea inversă folosind faptul că există $a \in I$ şi $b \in J$ astfel încât $1 = a + b$). Presupunem $r > 2$ şi că rezultatul e adevărat pentru $I_1, \ldots, I_{r-1}$. Fie şi $I = \prod_{i=1}^{r-1} I_i$. Deoarece pentru $1 \leq i \leq r-1$, avem $I_i + I_r = A$ (conform ipotezei), există $a_i \in I_i$ şi $x_i \in I_r$ astfel încât $a_i + x_i = 1$, de unde $a_1 \ldots a_{r-1} - 1 = (1 - x_1)(1 - x_2) \ldots (1 - x_{r-1}) - 1 = 1-$ (ceva din I_r) $-1 \in I_r$. Astfel, $I_r + I = A$ şi deci $\prod_{i=1}^{r} I_i = II_r = I \cap I_r = \bigcap_{i=1}^{r} I_i$ (a doua egalitate reiese din cazul inductiv $r = 2$, iar a treia egalitate reiese din ipoteza inductivă asupra lui I).
(b) "$\Rightarrow$": Presupunem că φ e surjectivă. Trebuie să arătăm că oricare ar fi $1 \leq i, j \leq r$, $I_i + I_j = A$. Pentru simplitatea scrierii, arătăm că I_1 şi I_2 sunt comaximale. Deoarece φ e surjectivă, există $x \in A$ astfel încât $\varphi(x) = (1, 0, \ldots, 0)$ (omitem scrierea simbolurilor de luare a clasei, deci 1 înseamnă clasa lui 1 modulo I_1, 0 - clasa lui 0 modulo I_2, etc). Conform definirii lui φ, asta înseamnă că $x \equiv 1 (mod\, I_1)$ şi $x \equiv 0\, (mod\, I_2)$, aşa că $1 = (1 - x) + x \in I_1 + I_2$.
"$\Leftarrow$": Presupunem că idealele sunt mutual comaximale. Ca să arătăm că φ e surjectivă e suficient să verificăm că elementele $(1, 0, \ldots, 0)$,

$(0, 1, \ldots, 0)$, ..., $(0, \ldots, 0, 1)$ stau în $Im(\varphi)$ (”vectorii” din baza canonică). De exemplu, arătăm că există $x \in A$ astfel încât $\varphi(x) = (1, 0, \ldots, 0)$. Deoarece $I_1 + I_i = A$, oricare ar fi $i > 1$, avem $a_i + b_i = 1$ pentru nişte $a_i \in I_1$, $b_i \in I_i$. Atunci luăm $x = b_2 b_3 \ldots b_r$. Avem că $x = \prod(1 - a_i) \equiv 1 \,(mod\, I_1)$ şi $x \equiv 0 \,(mod\, I_i)$, oricare ar fi $i > 1$, adică $\varphi(x) = (1, 0, \ldots, 0)$.
(c) Rezultă direct din definiţii că $\bigcap I_i = Ker(\varphi)$, de unde echivalenţa cerută.

4. $\mathbb{R}[X] \Big/ \langle X^2 - 1 \rangle \simeq \mathbb{R} \times \mathbb{R}$.

Soluţie. Deoarece $X^2 - 1 = (X + 1)(X - 1)$, ne gândim să aplicăm exerciţiul 3. Fie $I = \langle X + 1 \rangle$ şi $J = \langle X - 1 \rangle$. Observăm că $1 = \frac{1}{2}(X + 1) - \frac{1}{2}(X - 1) \in I + J$, *i.e.* I şi J sunt comaximale. Astfel, $\varphi : \mathbb{R}[X] \longrightarrow \frac{\mathbb{R}[X]}{I} \times \frac{\mathbb{R}[X]}{J}$ e surjectivă (ex. 3, (b)). Dar $\frac{\mathbb{R}[X]}{I} \times \frac{\mathbb{R}[X]}{J} = \frac{\mathbb{R}[X]}{\langle X-(-1)\rangle} \times \frac{\mathbb{R}[X]}{\langle X-1\rangle} \simeq \mathbb{R} \times \mathbb{R}$ (cf. seminar 6, ex. 1). Nucleul lui φ este IJ (cf. ex. 3, (c) şi (a)), aşa că $\frac{\mathbb{R}[X]}{IJ} \simeq \mathbb{R} \times \mathbb{R}$ (teorema fundamentală de izomorfism). Aşadar, suntem gata dacă arătăm că $IJ = \langle X^2 - 1 \rangle$. Evident, $\langle X^2 - 1 \rangle \subseteq IJ$. Fie $f \in IJ$. Asta înseamnă că $f = \sum_{i=1}^{n} g_i h_i$, cu $g_i \in \langle X + 1 \rangle$, $h_i \in \langle X - 1 \rangle$. Atunci scriem $g_i = G_i(X + 1)$, $G_i \in \mathbb{R}[X]$, oricare ar fi i, $h_i = H_i(X - 1)$, $H_i \in \mathbb{R}[X]$, oricare ar fi i, şi obţinem că $f = \sum_i G_i(X + 1)H_i(X - 1) = (\sum G_i H_i)(X^2 - 1) \in \langle X^2 - 1 \rangle$.

5. $\mathbb{C}[X] \Big/ \langle X^2 + 1 \rangle \simeq \mathbb{C} \times \mathbb{C}$.

Soluţie. E de aşteptat acest izomorfism, având în vedere ex. 1: $\frac{\mathbb{C}[X]}{\langle X^2+1\rangle} = \frac{(\mathbb{R}\times\mathbb{R})[X]}{\langle X^2+1\rangle} \simeq \frac{\mathbb{R}[X]\times\mathbb{R}[X]}{\langle X^2+1\rangle\times\langle X^2+1\rangle} \simeq \frac{\mathbb{R}[X]}{\langle X^2+1\rangle} \times \frac{\mathbb{R}[X]}{\langle X^2+1\rangle} \simeq \mathbb{C} \times \mathbb{C}$.
Riguros, (de ce nu e corectă argumentarea anterioară?) definim un morfism $\varphi : \mathbb{C}[X] \longrightarrow \mathbb{C} \times \mathbb{C}$ în felul următor: pentru un $f \in \mathbb{C}[X]$, scriem $f = a_0 + a_1 X + \ldots + a_n X^n = \alpha_0 + \beta_0 i + (\alpha_1 + \beta_1 i)X + \ldots + (\alpha_n + \beta_n i)X^n = (\alpha_0 + \alpha_1 X + \ldots + \alpha_n X^n) + (\beta_0 + \beta_1 X + \ldots + \beta_n X^n)i = u + vi$, unde $u, v \in \mathbb{R}[X]$ şi punem $\varphi(f) = (u(i), v(i))$. Pur şi simplu am mimat definirea morfismului de la ex. 1. Avem $\varphi(X^2 + 1) = (i^2 + 1, 0(i)) = (0, 0)$, deci $\langle X^2 + 1 \rangle \subseteq Ker(\varphi)$. Invers, dacă $f \in Ker(\varphi)$, înseamnă că, scriind $f = u + iv$, $u(i) = 0 = v(i)$. Cum $u, v \in \mathbb{R}[X]$, rezultă că $(X^2 + 1) \mid u$, $(X^2 + 1) \mid v$ (ca la ex. 1) şi deci $X^2 + 1$ divide $u + iv = f$, adică $f \in \langle X^2 + 1 \rangle$. Aşadar, $Ker(\varphi) = \langle X^2 + 1 \rangle$ şi e imediat că $Im(\varphi) = \mathbb{C} \times \mathbb{C}$, aşa că teorema fundamentală de izomorfism

oferă concluzia.

Numai că nu e aşa: soluţia e eronată. Aceasta pentru că acel φ nu e morfism de inele! (operaţia multiplicativă de pe $\mathbb{C} \times \mathbb{C}$ e trivială, pe când înmulţirea cantităţilor complexe are substanţă).
Însă, vă e clar cum să trataţi acest exerciţiu: pentru a da o soluţie corectă, procedaţi exact precum pentru ex. 4.

Următorul seminar va începe cu o discuţie asupra construcţiei corpului de fracţii al unui domeniu de integritate.