SEMINAR 12

Problema 1. Arătaţi că inelul $\mathbb{Z}_{1001}$ este izomorf cu un produs direct de corpuri.

Soluţie: Se aplică Corolarul 2 din Cursul 12 pentru inelul $A = \mathbb{Z}$, şi elementele $7, 11, 13 \in \mathbb{Z}\backslash\{\pm 1\}$, care sunt prime şi deci coprime.
$1001 = 7 \cdot 11 \cdot 13$ şi deci $\mathbb{Z}_{1001} \simeq \mathbb{Z}_7 \times \mathbb{Z}_{11} \times \mathbb{Z}_{13}$. 7, 11, 13 fiind numere prime rezultă că $\mathbb{Z}_7, \mathbb{Z}_{11}, \mathbb{Z}_{13}$ sunt corpuri.

Problema 2. Arătaţi că:
(i) $\widehat{77}$ este element nilpotent în inelul $\mathbb{Z}_{847}$,
(ii) inelul $\mathbb{Z}_{847}$ nu este izomorf cu un produs direct de corpuri.

Soluţie:
(i) $847 = 7 \cdot 11^2$. Problema 5 din Seminar 10 spune că $\hat{x} \in \mathbb{Z}_n$ este nilpotent dacă şi numai dacă x se divide cu toţi factorii primi ai lui n. $77 = 7 \cdot 11$ se divide cu 7 şi 11, factorii primi ai numărului 847. Deci $\widehat{77}$ este nilpotent.
$\widehat{77}^2 = \widehat{77^2} = \widehat{7^2 \cdot 11^2} = \widehat{7 \cdot 7 \cdot 11^2} = \widehat{7} \cdot \widehat{7 \cdot 11^2} = \widehat{7} \cdot \widehat{0} = \widehat{0}$. Deci ordinul de nilpotenţă este 2.
(ii) Aplicând acelaşi Corolar 2 din Curs 12, $\mathbb{Z}_{847} \simeq \mathbb{Z}_7 \times \mathbb{Z}_{121}$, dar $\mathbb{Z}_{121}$ nu este corp ($\widehat{11}$ este nilpotent, $\widehat{11}^2 = \widehat{0}$).

Problema 3. Rezolvaţi sistemul de congruenţe în $\mathbb{Z}$:
$x \equiv 3 (\mathrm{mod}\, 5)$, $x \equiv 7 (\mathrm{mod}\, 11)$, $x \equiv 8 (\mathrm{mod}\, 13)$

Soluţie: Sistemul de nilpotenţe se rezolvă conform algoritmului din Curs 12.
$a = a_1 \cdot a_2 \cdot a_3 = 5 \cdot 11 \cdot 13 = 715$. $b_1 = \frac{a}{a_1} = \frac{715}{5} = 143$, $b_2 = \frac{a}{a_2} = \frac{715}{11} = 65$, $b_3 = \frac{a}{a_3} = \frac{715}{13} = 55$.
$b_1 \equiv_5 3$; c_1 inversul lui $3 (\mathrm{mod}\, 5)$ este 2.
$b_2 \equiv_{11} 10$; c_2 inversul lui $10 (\mathrm{mod}\, 11)$ este 10.
$b_3 \equiv_{13} 3$, c_3 inversul lui $3 (\mathrm{mod}\, 13)$ este 9.
$x = 143 \cdot 2 \cdot 3 + 65 \cdot 10 \cdot 7 + 55 \cdot 9 \cdot\ 8 = 9368 \equiv_{715} 73$.
Deci soluţia este $x = 73 + 715k, k \in \mathbb{Z}$.
Se verifică imediat că $73 \equiv 3 (\mathrm{mod}\, 5)$, $73 \equiv 7 (\mathrm{mod}\, 11)$ şi $73 \equiv 8 (\mathrm{mod}\, 13)$.

Problema 4. Arătaţi că numerele
(i) numerele $2 + i, 2 - i$ sunt comaximale în $\mathbb{Z}[i]$,
(ii) inelul factor $\mathbb{Z}[i]/ < 5 >$ este izomorf cu $\mathbb{Z}_5 \times \mathbb{Z}_5$. (folosiţi **problema 8** din seminarul 11).

Soluţie:
(i) Arătăm că idealele generate de cele elemente sunt comaximale.
$(2 + i) \cdot (-1) + (2 - i)(1 + i) = -2 - i + (2 + 1 + 2i - i = -2 - i + 3 + i = 1$. Deci cele două ideale generate de $(2 + i)$ şi $(2 - i)$ sunt comaximale.
(ii) Aplicăm Corolar 1 din Cursul 12 pentru inelul $\mathbb{Z}[i]$ şi elementele $(2 + i)$, $(2 - i)$ şi obţinem $\mathbb{Z}[i]/(2 + i)(2 - i)\mathbb{Z}[i] \simeq \mathbb{Z}[i]/(2 + i)\mathbb{Z}[i] \times \mathbb{Z}[i]/(2 - i)\mathbb{Z}[i]$.
$(2 + i)(2 - i) = 5$ şi izomorfismul de mai sus se scrie

$$\mathbb{Z}[i]/ < 5 > \simeq \mathbb{Z}[i]/ < (2 + i) > \times \mathbb{Z}[i]/ < (2 - i) >$$

Pentru a termina trebuie să demonstrăm că cele dpuă inele factor din membrul drept sunt fiecare izomorfe cu $\mathbb{Z}_5$. În Problema 8 din Seminar 11 am arătat că $\mathbb{Z}[i]/ < (2-i) > \simeq \mathbb{Z}_5$.

Similar vom demonstra că $\mathbb{Z}[i]/ < (2+i) > \simeq \mathbb{Z}_5$.

Considerăm $\alpha : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_5, \alpha(a+bi) = \widehat{a-2b}$.

• Arătăm că α este morfism.

$\alpha((a+bi)+(c+di)) = \alpha((a+c)+(b+d)i) = \widehat{(a+c)-2(b+d)} = \widehat{(a-2b)+(c-2d)} = \widehat{a-2b} + \widehat{c-2d} = \alpha(a+bi)+\alpha(c+di)$.

$\alpha((a+bi)\cdot(c+di)) = \alpha((ac-bd)+(ad+bc)i) = \widehat{(ac-bd)-2(ad+bc)} = \widehat{(ac+4bd)-2(ad+bc)}$ (în $\mathbb{Z}_5, -1 \equiv_5 4$) $= \widehat{(a-2b)(c-2d)} = (\widehat{a-2b})\cdot(\widehat{c-2d}) = \alpha(a+bi)\cdot\alpha(c+di)$.

$\alpha(0) = \widehat{0}, \alpha(1) = \widehat{1}$.

• α este surjectiv pentru că $(\forall)\widehat{a} \in \mathbb{Z}_5$, $(\exists)a+0i \in \mathbb{Z}[i]$ a.î. $\alpha(a+0i) = \widehat{a}$.

• $\mathrm{Ker}(\alpha) =< (2+i) >$.

" $\subseteq$ " Fie $a+bi \in \mathbb{Z}[i] \Leftrightarrow \widehat{a-2b} = \widehat{0} \in \mathbb{Z}_5 \Leftrightarrow a-2b = 5k, k \in \mathbb{Z} \Leftrightarrow a = 2b+5k$.

Deci un element arbitrar din $\mathrm{Ker}(f)$ este de forma $(2b+5k)+bi, b, k \in \mathbb{Z}$. Pentru a arăta incluziunea trebuie să vedem că $(5k+2b)+bi \in < 2+i >$, adică trebuie să găsim $m, n \in \mathbb{Z}$ a.î. $(5k+2b)+bi = (m+ni)(2+i) \Leftrightarrow (5k+2b)+bi = (2m+n)+(-m+2n)i$.

Sistemul $\begin{cases} 2m-n &= 5k+2b \\ m+2n &= b \end{cases}$. Înmulţim cu 2 prima ecuaţie şi adunăm cele două ecuaţii. Obţinem $m = 2k+b$. Introducând în a doua ecuaţie obţinem $n = -k$.

Deci $(5k+2b)+bi = ((2k+b)-ki)(2+i) \in < 2+i >$.

" $\supseteq$ " Este suficient să verificăm că $2+i \in \mathrm{Ker}(\alpha)$. $\alpha(2+i) = \widehat{2-2\cdot 1} = \widehat{2-2} = \widehat{0}$.

Din teorema fundamentală de izomorfism pentru inele rezultă că $\mathbb{Z}[i]/ < 2-i > \simeq \mathbb{Z}_5$.

Deci $\mathbb{Z}[i]/ < 5 > \simeq \mathbb{Z}_5 \times \mathbb{Z}_5$.

Problema 5. Aplicaţi Lema Chineză a Resturilor pentru idealele $I =< 2, 1+\sqrt{-5} >$, $J =< 3, 1+\sqrt{-5} >$ în inelul $\mathbb{Z}[\sqrt{-5}]$ pentru a deduce că inelul factor $\mathbb{Z}[\sqrt{-5}]/ < 1+\sqrt{-5} >$ este izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Soluţie: Pentru a aplica LCR trebuie să demonstăm că $I+J = \mathbb{Z}[\sqrt{-5}]$. Avem $2\cdot(-1)+3\cdot 1 = 1$. Deci I şi J sunt comaximale.

Din LCR rezultă că $\mathbb{Z}[\sqrt{-5}]/(I \cap J) \simeq \mathbb{Z}[\sqrt{-5}]/I \times \mathbb{Z}[\sqrt{-5}]/J$.

Trebuie să arătăm că: $I \cap J =< 1+\sqrt{-5} >$, $\mathbb{Z}[\sqrt{-5}]/I \simeq \mathbb{Z}_2$ şi $\mathbb{Z}[\sqrt{-5}]/J \simeq \mathbb{Z}_3$.

• $I \cap J =< 1+\sqrt{-5} >$.

" $\supseteq$ " $1+\sqrt{-5} \in I, 1+\sqrt{-5} \in J \Rightarrow < 1+\sqrt{-5} > \subseteq I \cap J$.

" $\subseteq$ " Fie $u \in I \cap J$. $u = 2p + (1+\sqrt{-5})q; p, q \in \mathbb{Z}[\sqrt{-5}]$ şi $u = 3s + (1+\sqrt{-5})t; s, t \in \mathbb{Z}[\sqrt{-5}]$. Deci $u = 2(a+b\sqrt{-5}) + (1+\sqrt{-5})(c+d\sqrt{-5}); a, b, c, d \in \mathbb{Z}$ şi
$u = 3(x+y\sqrt{-5}) + (1+\sqrt{-5})(z+w\sqrt{-5}); x, y, z, w \in \mathbb{Z}$.

Făcând calculele şi adunând termenii asemenea va rezulta sistemul
$\begin{cases} 2a+c-5d &= 3x+z-5w \\ 2b+c+d &= 3y+z+w \end{cases}$.

Scădem ecuaţia a doua din prima şi obţinem $2(a-b)-6d = 3(x-y)-6w \Leftrightarrow 2(a-b) = 3[(x-y)+2(d-w)]$, toate numerele fiind în $\mathbb{Z}$. De aici $(a-b) = 3k, k \in \mathbb{Z}$, deci $a = 3k+b$.

Am obţinut $u = 2(3k+b+b\sqrt{-5}) + (1+\sqrt{-5})q = 6k + 2b(1+\sqrt{-5}) + (1+\sqrt{-5})q = (1+\sqrt{-5})(1-\sqrt{-5})k + 2b(1+\sqrt{-5}) + (1+\sqrt{-5})q = (1+\sqrt{-5})[(1-\sqrt{-5})k + 2b + q]$. Paranteza dreaptă reprezintă un element din $\mathbb{Z}[\sqrt{-5}]$.

Deci am arătat că $u \in < 1+\sqrt{-5} >$.

• $\mathbb{Z}[\sqrt{-5}]/I \simeq \mathbb{Z}_2$.

Considerăm morfismul $\beta : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}_2, \beta(a+b\sqrt{-5}) = \widehat{a+b}$. Trebuie arătat că β este morfism surjectiv de inele şi $\text{Ker}(\beta) = I$.

$\beta((a+b\sqrt{-5})+(c+d\sqrt{-5})) = \beta((a+c)+(b+d)\sqrt{-5}) = (a+c)\widehat{+}(b+d) = (a+b)\widehat{+}(c+d) = \widehat{a+b} + \widehat{c+d} = \beta(a+b\sqrt{-5}) + \beta(c+d\sqrt{-5})$

$\beta((a+b\sqrt{-5})\cdot(c+d\sqrt{-5})) = \beta((ac-5bd)+(ad+bc)\sqrt{-5}) = (ac-5bd)\widehat{+}(ad+bc) = (-5 \equiv_2 1) = (ac+bd)\widehat{+}(ad+bc) = a(c+d)\widehat{+}b(c+d) = (a+b)\widehat{(c+d)} = \widehat{(a+b)}\cdot\widehat{(c+d)} = \beta(a+b\sqrt{-5})\cdot\beta(c+d\sqrt{-5})$.

$\beta(0) = \hat{0}, \beta(1) = \hat{1}$ ceea ce implică şi faptul că β este surjectiv.

$\text{Ker}(\beta) = I$.

" $\supseteq$ " $\beta(2) = \hat{2} = \hat{0}, \beta(1+\sqrt{-5}) = \widehat{1+1} = \hat{2} = \hat{0}$.

" $\subseteq$ " Fie $a+b\sqrt{-5} \in \text{Ker}(\beta) \Leftrightarrow \widehat{a+b} = \hat{0} \Leftrightarrow a+b = 2k \Leftrightarrow a = -b+2k$. Deci un element arbitrar din $\text{Ker}(\beta)$ este de forma $-b+2k+b\sqrt{-5} = -2b+2k+b+b\sqrt{-5} = 2(-b+k)+(1+\sqrt{-5})b \in I$.

Din teorema fundamentală de izomorfism pentru inele obţinem $\mathbb{Z}[\sqrt{-5}]/I \simeq \mathbb{Z}_2$.

• $\mathbb{Z}[\sqrt{-5}]/J \simeq \mathbb{Z}_3$.

Considerăm morfismul $\gamma : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}_3, \gamma(a+b\sqrt{-5}) = \widehat{a+2b}$.

Se demonstrează ca şi mai sus că γ este morfism surjectiv de inele şi $\text{Ker}(\gamma) = J$.

$\gamma((a+b\sqrt{-5})\cdot(c+d\sqrt{-5})) = \gamma((ac-5bd)+(ad+bc)\sqrt{-5}) = (ac-5bd)\widehat{+}2(ad+bc) = (-5 \equiv_3 1 \equiv_3 4) = (ac+4bd)\widehat{+}2(ad+bc) = a(c+2d)\widehat{+}2b(c+2d) = (a+2b)\widehat{(c+2d)} = \widehat{(a+2b)}\cdot\widehat{(c+2d)} = \gamma(a+b\sqrt{-5})\cdot\gamma(c+d\sqrt{-5})$.

Problema 6. Găsiţi un idempotent netrivial în inelul $\mathbb{Z}[\sqrt{-5}]/ < 1+\sqrt{-5} >$.

Soluţie: În problema precedentă am arătat că $\mathbb{Z}[\sqrt{-5}]/ < 1+\sqrt{-5} > \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$. Un idemponent netrivial în $\mathbb{Z}_2 \times \mathbb{Z}_3$ este $(\hat{1}, \overline{0})$. Elementul corespunzător perechii $(\hat{1}, \overline{0})$ în $\mathbb{Z}[\sqrt{-5}]/ < 1+\sqrt{-5} >$ este 3.

Să vedem că este idempotent.

$3^2 = 9 = 3+6$. Dar $6 \equiv_{1+\sqrt{-5}} 0 (6 = (1+\sqrt{-5})(1-\sqrt{-5}))$. Deci $3^2 \equiv_{1+\sqrt{-5}} 3$, adică clasa lui 3 este idempotent.

Problema 7. Aplicaţi Lema Chineză a Resturilor pentru idealele $I =< X >, J =< X-1 >$ în inelul $\mathbb{Z}[X]$ pentru a deduce că inelul factor $\mathbb{Z}[X]/ < X^2 - X >$ este izomorf cu $\mathbb{Z} \times \mathbb{Z}$.

Soluţie: I şi J sunt comaximale pentru că $X \cdot 1 + (X-1)\cdot(-1) = X - X + 1 = 1$.

Folosind Corolar 1 din Curs 12 obţinem

$$\mathbb{Z}[X]/X(X-1)\mathbb{Z}[X] \simeq \mathbb{Z}[X]/X\mathbb{Z}[X] \times \mathbb{Z}[X]/(X-1)\mathbb{Z}[X]$$

. Trebuie să arătăm izomorfismele $\mathbb{Z}[X]/X\mathbb{Z}[X] \simeq \mathbb{Z}$ şi $\mathbb{Z}[X]/(X-1)\mathbb{Z}[X] \simeq \mathbb{Z}$.

• $\mathbb{Z}[X]/ < X > \simeq \mathbb{Z}$.

Considerăm aplicaţia $\delta : \mathbb{Z}[X] \longrightarrow \mathbb{Z}$, $\delta(f(X)) = f(0)$, unde $f(X) \in \mathbb{Z}[X]$.

Dacă $f(X) = \sum_{i=0}^{n} a_i X^i$, atunci $\delta(f(X)) = a_0$. δ este morfism de inele.

$\delta(f(X)+g(X)) = \delta(\sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{p} b_i X^i) = \delta(\sum_{i=0}^{\max\{n,p\}}(a_i+b_i)X^i) = a_0 + b_0$

$= \delta(f(X)) + \delta(g(X))$

$\delta(f(X)\cdot g(X)) = \delta(\sum_{i=0}^{n+p}(\sum_{h+k=i} a_h b_k)X^i) = a_0 b_0 = \delta(f(X))\delta(g(X))$.

Pentru orice polinom constant c, $\delta(c) = c$. Acest lucru arată că δ este surjectiv. Pentru $\forall c \in \mathbb{Z}, \exists c \in \mathbb{Z}[X]$ a.î. $\delta(c) = c$.

$\delta(X) = 0 \Rightarrow < X > \subset \text{Ker}(\delta)$.

Fie $f(X) \in \text{Ker}(\delta)$, deci $\delta(f(X)) = 0 \Leftrightarrow f(0) = 0 \Leftrightarrow X \mid f(X) \Leftrightarrow f(X) = X \cdot g(X)$, cu $g(X) \in \mathbb{Z}[X] \Leftrightarrow f(X) \in < X >$. Deci $\text{Ker}(\delta) \subset < X >$.

Din teorema fundamentală de izomorfism obţinem $\mathbb{Z}[X]/ < X > \simeq \mathbb{Z}$.

• $\mathbb{Z}[X]/ < X - 1 > \simeq \mathbb{Z}$.

Se consideră aplicaţia $\tau : \mathbb{Z}[X] \longrightarrow \mathbb{Z}, \tau(f(X)) = f(1)$.

• Fie $c \in \mathbb{Z}$, în acest caz $\tau(c) = c$. Deci τ este surjectiv.

• $\tau(f(X) \cdot g(X)) = \tau(\sum_{k=0}^{n+p}(\sum_{i+j=k} a_i b_j)X^k) = \sum_{k=0}^{n+p}(\sum_{i+j=k} a_i b_j) = (a_0 + a_1 + \ldots + a_n)(b_0 + b_1 + \ldots + b_p) = f(1)g(1) = \tau(f(X))\tau(g(X))$.

• $\text{Ker}(\tau) = < X - 1 >$.

" $\subset$ " Fie $f(X) \in \text{Ker}(\tau) \Leftrightarrow \tau(f(X)) = 0 \Leftrightarrow f(1) = 0 \Rightarrow (X - 1) \mid f(X)$ (teorema Bezout) $\Leftrightarrow f(X) = (X - 1)g(X) \Leftrightarrow f(X) \in < X - 1 >$

" $\supset$ " $\tau(X - 1) = 1 - 1 = 0 \Rightarrow (X - 1) \in \text{Ker}(\tau) \Leftrightarrow < X - 1 > \subset \text{Ker}(\tau)$.

Din teorema fundamentală de izomorfism rezultă că $\mathbb{Z}[X]/ < X - 1 > \simeq \mathbb{Z}$.

Problema 8. Arătaţi că inelul factor $\mathbb{Z}[X]/ < X^2 - 1 >$ nu este izomorf cu $\mathbb{Z} \times \mathbb{Z}$.

Soluţie: În inelul factor $\overline{X^2} = \overline{1}$, deci în acest inel factor polinoamele au cel mult grad 1. Voi lucra cu clase modulo $< X^2 - 1 >$, fără a mai folosi notaţia bar.

$\mathbb{Z} \times \mathbb{Z}$ are patru idempotenţi $(0, 0), (1, 0), (0, 1), (1, 1)$.

Fie $a + bX \in \mathbb{Z}[X]/ < X^2 - 1 >$.

Este idempotent dacă verifică relaţia $(a + bX)^2 = a + bX \Leftrightarrow a^2 + 2abX + b^2 = a + bX \Leftrightarrow \begin{cases} a^2 + b^2 = a \\ 2ab = b \end{cases}$. A doua ecuaţie este $b(2a - 1) = 0$, cu $a, b \in \mathbb{Z}$. Deci $a \neq \frac{1}{2}$, de unde singura posibilitate este $b = 0$.

Prima ecuaţie devine $a^2 - a = 0$, adică $a \in \{0, 1\}$. Deci idempotenţii din $\mathbb{Z}[X]/ < X^2 - 1 >$ sunt 0 şi 1. Deci $\mathbb{Z}[X]/ < X^2 - 1 >$ are numai doi idempotenţi faţă de $\mathbb{Z} \times \mathbb{Z}$ care are patru.

Deci inelele nu pot fi izomorfe.

Avem $\mathbb{Z}[X]/ < X^2 - 1 > \simeq A = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x - y \text{ par}\}$ izomorfism care se demonstrează folosind aplicaţia $\tau : \mathbb{Z}[X] \longrightarrow A$, $\tau(f(X)) = (f(1), f(-1))$. Se demonstrează similar ca în **problema 7** că τ este morfism de inele, este surjectiv şi $\text{Ker}(\tau) = < X^2 - 1 >$.