1. (i) Dacă R, S inele, atunci $U(R\times S)=U(R)\times U(S)$.

(ii) Dacă A, B inele, $A\simeq B$, atunci grupurile $U(A)$ și $U(B)$ sunt izomorfe.

(iii) Dacă $m, n\in\mathbb{N}$, $m, n\geq 2$, cu $(m,n)=1$, atunci $\varphi(mn)=\varphi(m)\varphi(n)$

φ = indicatorul lui Euler

$$\varphi(n)=|\{i \mid 1\leq i\leq n, i\in\mathbb{N}, (i,n)=1\}|$$

(i) Fie $(a,b)\in R\times S$, $a\in R$, $b\in S$.

$(a,b)\in U(R\times S) \Leftrightarrow (\exists)\ (a',b')\in R\times S$ cu

$$(a,b)\times(a',b')=(a',b')\times(a,b)=(\underset{\substack{\uparrow\\ R}}{1},\underset{\substack{\uparrow\\ S}}{1})$$

$\Leftrightarrow (\exists)\ a'\in R$ și $b'\in S$ a.î.

$aa'=1$ și $bb'=1$

$a'a=1$ $\quad$ $b'b=1$

$\Updownarrow$ $\quad$ $\Updownarrow$

$a\in U(R)$ $\quad$ $b\in U(S)$

$\Downarrow$

$$U(R\times S)=U(R)\times U(S)$$

(ii) Fie $f: A \to B$ izomorfism de inele

Caut $g: U(A) \to U(B)$ izomorfism de grupuri

$g(xy) = g(x)g(y)$, $(\forall)$ $x, y \in U(A)$

g bij.

Dacă $x \in U(A) \overset{?}{\Rightarrow} f(x) \in U(B)$

$\Downarrow$

$(\exists)$ x^{-1} a.î. $xx^{-1} = x^{-1}x = 1$

$f(xx^{-1}) = f(x^{-1}x) = f(1)$

$= f(x) \cdot f(x)^{-1} = 1_B \Rightarrow f(x) \in U(B)$

$g: U(A) \to U(B)$

$(\forall)$ $x \in U(A)$, $g(x) = f(x)$

$g(xy) = f(xy) = f(x) \cdot f(y) = g(x) \cdot g(y)$

g injectivă ?

Presupunem că $g(x) = g(y) \Rightarrow f(x) = f(y) \Rightarrow x = y$

g surjectivă ?

Fie $u \in U(B)$.

$$\boxed{\begin{array}{l} f: A \to B \text{ izomorf. de inele} \Rightarrow f^{-1}: B \to A \text{ izomorf. de inele} \\ u \in U(B) \Rightarrow f^{-1}(u) \in U(A) \end{array}}$$

Atunci, $u = f(f^{-1}(u)) = g(f^{-1}(u))$

(iii) $\mathbb{Z}_m \times \mathbb{Z}_n \overset{\text{izo. inele}}{\simeq} \mathbb{Z}_{mn}$

$\Downarrow$ (ii)

$U(\mathbb{Z}_m \times \mathbb{Z}_n) \underset{\text{grupuri}}{\overset{\text{izo.}}{\simeq}} U(\mathbb{Z}_{mn})$

$\|$

$U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$

$U(\mathbb{Z}_n) = \{ \hat{i} \mid 1 \leq i < n, (i,n) = 1 \}$

$|U(\mathbb{Z}_n)| = \varphi(n)$

$|U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)| = |U(\mathbb{Z}_{mn})|$

$|U(\mathbb{Z}_m)|\,|U(\mathbb{Z}_n)| = \varphi(m)\,\varphi(n)$, $\quad |U(\mathbb{Z}_{mn})| = \varphi(mn)$

$r \in \mathbb{N}, r \geq 2$

$m_1, \dots, m_r \in \mathbb{N}, \geq 2$

$(m_i, m_j) = 1, (\forall) i \neq j$

$\Rightarrow \varphi(m_1 \cdots m_r) = \varphi(m_1) \cdots \varphi(m_r)$

Se demonstrează prin inducție după r.

$r = 2$ (iii)

$r-1 \to r$

$$\varphi(m_1 \dots m_r) = \varphi((m_1 \dots m_{r-1})\, m_r) \overset{(m_1\dots m_{r-1}, m_r)=1}{=\!=\!=} \varphi(m_1 \dots m_{r-1}) \cdot \varphi(m_r)$$

$$\overset{\text{Ip. ind.}}{=\!=} \varphi(m_1) \dots \varphi(m_{r-1})\varphi(m_r)$$

$p_1, \dots, p_r$ prime distincte
$k_1, \dots, k_r \in \mathbb{N}^*$

$$\varphi(\underbrace{p_1^{k_1}}_{m_1} \dots \underbrace{p_r^{k_r}}_{m_r}) = \varphi(p_1^{k_1}) \dots \varphi(p_r^{k_r})$$

p prim, $k \in \mathbb{N}^*$
$\varphi(p^k) = ?$

$$\varphi(p^k) = |\{ i \in \mathbb{N} \mid 1 \le i < p^k, \underbrace{(i, p^k) = 1}_{\Updownarrow\ p \nmid i} \}| =$$

$$= |\underbrace{\{1, \dots, p^k - 1\}}_{p^k - 1 \text{ elemente}} \setminus \underbrace{\{1 \cdot p, 2 \cdot p, \dots, (p^{k-1} - 1) \cdot p\}}_{p^{k-1}-1} | = p^k - p^{k-1}$$

$$(p^{k-1} - 1)\cdot p = p^k - p$$

$$\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

$$\varphi(p_1^{k_1} \dots p_r^{k_r}) = \varphi(p_1^{k_1}) \dots \varphi(p_r^{k_r}) =$$

$$= p_1^{k_1 - 1} \dots p_r^{k_r - 1} (p_1 - 1) \dots (p_r - 1)$$

$$= m\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

2. Arătați că $\dfrac{\mathbb{C}[X]}{(X^2+1)} \simeq \mathbb{C}\times\mathbb{C}$, $\dfrac{\mathbb{R}[X]}{(X^2+1)} \simeq \mathbb{C}$,

$\not\simeq$

$\mathbb{R}\times\mathbb{R}$

(1,0) nu e inv.

$(1,0)\cdot(0,1)=(0,0)$

$\dfrac{\mathbb{Z}[X]}{(X^2+1)} \simeq \mathbb{Z}[i]$.

$$\dfrac{\mathbb{C}[X]}{(X^2+1)} \simeq \mathbb{C}\times\mathbb{C}$$

În $\mathbb{C}[X]$:

Fie $I=(X-i)$ și $J=(X+i)$.

I și J sunt comaximale, adică

$I+J=\mathbb{C}[X]$.

$$-(X-i)+(X+i)=2i \xRightarrow{\cdot\frac{1}{2i}} \underbrace{-\frac{1}{2i}}_{\frac{i}{2}}(X-i)+\underbrace{\frac{1}{2i}}_{-\frac{i}{2}}(X+i)=1$$

Lema chineză $\Rightarrow$ $I\cap J = IJ = (X^2+1)$ și

$$\frac{\mathbb{C}[X]}{I\cap J} \simeq \frac{\mathbb{C}[X]}{I}\times\frac{\mathbb{C}[X]}{J}$$

$$\frac{\mathbb{C}[X]}{(X^2+1)} \simeq \underbrace{\frac{\mathbb{C}[X]}{(X-i)}}_{\simeq\ \mathbb{C}}\times\underbrace{\frac{\mathbb{C}[X]}{(X+i)}}_{\simeq\ \mathbb{C}} \Rightarrow \frac{\mathbb{C}[X]}{(X^2+1)} \simeq \mathbb{C}\times\mathbb{C}$$

$$\frac{\mathbb{R}[X]}{(X^2+1)} \simeq \mathbb{C}$$

Sol. 2:

$$\frac{\mathbb{R}[X]}{(X^2+1)} = \{\widehat{a+bX} \mid a, b \in \mathbb{R}\}$$

$$\widehat{a+bX} = \widehat{c+dX} \iff \begin{cases} a = c \\ b = d \end{cases}$$

$$\widehat{a+bX} + \widehat{c+dX} = \widehat{(a+c)+(b+d)X}$$

$$\widehat{a+bX} \cdot \widehat{c+dX} = \widehat{(a+bX)(c+dX)}$$

$$= \widehat{ac+(ad+bc)X+bdX^2}$$

$$= \widehat{ac-bd+(ad+bc)X+\cancel{bd(X^2+1)}}$$

$$\frac{A[X]}{(X-a)} \simeq A$$

$$\varphi : \frac{\mathbb{R}[X]}{(X^2+1)} \to \mathbb{C}$$

$$\varphi(\widehat{a+bX}) = a+bi$$

inj.: $\varphi(\widehat{a+bX}) = \varphi(\widehat{c+dX}) \Rightarrow$

$$\Rightarrow a+bi = c+di \Rightarrow \begin{matrix} a=c \\ b=d \end{matrix} \Rightarrow$$

$$\Rightarrow \widehat{a+bX} = \widehat{c+dX}$$

surj.: $a+bi = \varphi(\widehat{a+bX})$
$\uparrow$
$\mathbb{C}$

φ morfism de inele:

$$\varphi(\widehat{a+bX} + \widehat{c+dX}) \overset{?}{=} \varphi(\widehat{a+bX}) + \varphi(\widehat{c+dX})$$

$$\varphi(\widehat{(a+c)+(b+d)X}) \qquad\qquad a+bi + c+di$$

$$(a+c)+(b+d)i \overset{ok!}{=} (a+c)+(b+d)i$$

$$\varphi(\widehat{a+bX} \cdot \widehat{c+dX}) \overset{?}{=} \varphi(\widehat{a+bX}) \cdot \varphi(\widehat{c+dX})$$

$$\varphi(\widehat{ac-bd+(ad+bc)X}) \qquad\qquad (a+bi)\cdot(c+di)$$

$$ac-bd+(ad+bc)i \overset{ok!}{=} (ac-bd)+(ad+bc)i$$

$\Rightarrow \varphi$ izomorfism

Sol. 1:

$$\frac{R}{I} \simeq S$$
$\Uparrow$
$\exists \left[f: R \to S \text{ morf. surj. de inele cu } \operatorname{Ker} f = I \right.$

Găsim neapărat de
$f: \mathbb{R}[X] \to \mathbb{C}$ morf. surj. de inele cu $\operatorname{Ker} f = (X^2+1)$

$$\begin{tikzcd}
a \in \mathbb{R} \arrow[r] \arrow[dr] \arrow[d, mapsto, "\text{incl}"'] & \mathbb{R}[X] \arrow[d, dashed] \\
a & \mathbb{C} \ni i
\end{tikzcd}$$

$(\exists!)$ f morf. inele cu $f(a)=a$, $(\forall)\, a\in\mathbb{R}$

și $f(X)=i$

$$f(P) = f(\underbrace{a_0+a_1X+\dots+a_mX^m}_{P}) =$$

$$= a_0 + a_1 i + \dots + a_m i^m = P(i)$$

$f(P)=P(i)$ morf. de inele

$f(a+bX) = \underline{a+bi} \Rightarrow f$ surj.

$P \in \operatorname{Ker} f \overset{?}{\Leftrightarrow} P \,\vdots\, (X^2+1)$

$\downarrow$

în $\mathbb{R}[X]$

„$\Leftarrow$": $P = (X^2+1)\cdot F$, $F \in \mathbb{R}[X]$

$\Downarrow$

$$P(i) = \underbrace{(i^2+1)}_{0}\cdot F(i) = 0$$

$\Downarrow$

$P \in \operatorname{Ker} f$

„$\Rightarrow$": Fie $P \in \operatorname{Ker} f$, deci $P \in \mathbb{R}[X]$ și $\underline{P(i)=0}$

Împart P la X^2+1 în $\mathbb{R}[X]$.

$$P = (X^2+1)\cdot C + \cancel{a+b}X \qquad a, b \in \mathbb{R}$$

$\Downarrow$ eval. în i

$$\underbrace{P(i)}_{=0} = \cancel{0 + a + bi} \Rightarrow a = 0, b = 0 \Rightarrow$$

$$\Rightarrow P \in (X^2+1)$$