$(C, D, U) = (7, 8, 7)$.

Problema 1. *Considerem l'equació* $C : X^2 - 3(U+1)XY + 3Y^2 + (D+1)X - 2Y - 1 = 0$ *(escrivim* C : $f(X,Y) = 0$ *amb* $f \in \mathbb{R}[X,Y]$*). Intenta fer un canvi de variables on s'escrigui l'equació com* $a(X')^2 + b(Y')^2 = 1$ *per certes constants* a *i* b *i variables* X', Y'*. Intenteu donar una paremetrització de la corba. Estudieu si* $L := \mathbb{R}(X)[Y]/(f(X,Y))$ *és un cos, i en cas de ser-ho, decidiu si existeix* t *on* $L = \mathbb{R}(t)$*. Podem fer el mateix enunciat i preguntes amb* $\mathbb{Q}$ *enlloc de* $\mathbb{R}$*?*

Solució. Projectivitzem C a $\mathbb{P}^2(K)$, $K = \mathbb{Q}, \mathbb{R}$ ($\mathrm{car}(K) \neq 2$). Considerem la corba $f(X,Y,Z) := aX^2 + bY^2 + cZ^2 + dXY + eYZ + fXZ$, on $(a,b,c,d,e,f) := (1, 3, -1, -24, -2, 9) \in \mathbb{R}^6$. Tenim que $a \neq 0_{\mathbb{R}}$. Aleshores, fent el canvi de variable $X \to \mathscr{X} := X + \frac{d}{2a}Y + \frac{f}{2a}Z$ obtenim

$$f(\mathscr{X}, Y, Z) = a\mathscr{X}^2 + \big(b - \tfrac{d^2}{4a}\big)Y^2 + \big(c - \tfrac{f^2}{4a}\big)Z^2 + \big(e - \tfrac{fd}{2a}\big)YZ$$

Com $e - \frac{fd}{2a} = 106 \neq 0_K$ i $b - \frac{d^2}{4a} = -141 \neq 0_K$, fent el canvi de variable $Y \to \mathscr{Y} := Y + \frac{(e - \frac{fd}{2a})}{2(b - \frac{d^2}{4a})}Z$ obtenim

$$\begin{aligned} f(\mathscr{X}, \mathscr{Y}, Z) &= a\mathscr{X}^2 + \big(b - \tfrac{d^2}{4a}\big)\mathscr{Y}^2 + \Big(\big(c - \tfrac{f^2}{4a}\big) - \tfrac{(e - \frac{fd}{2a})^2}{4(b - \frac{d^2}{4a})}\Big)Z^2 \\ &= \mathscr{X}^2 - 141\mathscr{Y}^2 - \tfrac{749}{564}Z^2 \end{aligned}$$

Imposant $Z = 1$, resulta l'equació $a'\mathscr{X}^2 - b'\mathscr{Y}^2 = 1$, on $(a', b') := (\frac{564}{749}, \frac{79524}{749})$.
Una parametrització real de $f(\mathscr{X}, \mathscr{Y}) = a'\mathscr{X}^2 + b'\mathscr{Y}^2 - 1 = 0$ és $\varphi(t) := (\frac{\cosh t}{\sqrt{a'}}, \frac{\sinh t}{\sqrt{b'}})$ $(= (\mathscr{X}, \mathscr{Y}))$. Aleshores,

$$\begin{aligned} \{(X,Y) \in \mathbb{R}^2 : f(X,Y) = 0\} &= \Big\{\Big(\tfrac{\cosh t}{\sqrt{a'}} - \tfrac{d}{2a}\Big(\tfrac{\sinh t}{\sqrt{b'}} - \tfrac{(e - \frac{fd}{2a})}{2(b - \frac{d^2}{4a})}\Big) - \tfrac{f}{2a}, \tfrac{\sinh t}{\sqrt{b'}} - \tfrac{(e - \frac{fd}{2a})}{2(b - \frac{d^2}{4a})}\Big) : t \in \mathbb{R}\Big\} \\ &= \Big\{\Big(\sqrt{\tfrac{749}{564}}\cosh t - \tfrac{\sqrt{2247}}{141}\sinh t + \tfrac{212}{47}, \sqrt{\tfrac{749}{79524}}\sinh t + \tfrac{53}{141}\Big) : t \in \mathbb{R}\Big\} \end{aligned}$$

dona la parametrització real de $f(X,Y)$. Ara, per donar una parametrització racional, necessitem un punt racional de $f(X,Y)$. Podem comprovar que $(0,1) \in \{(X,Y) \in \mathbb{Q}^2 : f(X,Y) = 0\}$. Amb els canvis de variable anteriors, obtenim que $(-\frac{15}{2}, \frac{88}{141}) \in \{(\mathscr{X}, \mathscr{Y}) \in \mathbb{Q}^2 : f(\mathscr{X}, \mathscr{Y}) = 0\}$. Considerem la recta ℓ que passa per $(-\frac{15}{2}, \frac{88}{141})$ i té pendent m. Tenim que

$$\ell \cap \{(\mathscr{X}, \mathscr{Y}) \in \mathbb{Q}^2 : f(\mathscr{X}, \mathscr{Y}) = 0\} - \{(-\tfrac{15}{2}, \tfrac{88}{141})\} = \{(-\tfrac{2115m^2 + 352m + 15}{2(141m^2 - 1)}, -\tfrac{12408m^2 + 2115m + 88}{141(141m^2 - 1)}) : m \in \mathbb{Q}\}$$

que ens dona una parametrització racional de $f(\mathscr{X}, \mathscr{Y})$. Desfent els canvis de variable, donat $m \in \mathbb{Q}$, $(\frac{-397056m^2 - 66928m - 2820}{188(141m^2 - 1)}, \frac{-4935m^2 - 2115m - 141}{144(144m^2 - 1)})$ dona una parametrització racional de $f(X,Y)$.
$L := K(\mathscr{X})[\mathscr{Y}]/(f(\mathscr{X}, \mathscr{Y}))$ és cos si i només si $f(\mathscr{X}, \mathscr{Y}) \in K(\mathscr{X})[\mathscr{Y}]$ és irreductible sobre $K(\mathscr{X})$.

1. Si $K = \mathbb{R}$, $f(\mathscr{X}, \mathscr{Y}) = -141\mathscr{Y}^2 + (\mathscr{X} - \sqrt{(a')^{-1}})(\mathscr{X} + \sqrt{(a')^{-1}})$, d'on deduïm per Eisenstein que $f(\mathscr{X}, \mathscr{Y})$ és irreductible sobre $\mathbb{R}(\mathscr{X})$.

2. Si $K = \mathbb{Q}$, $f(\mathscr{X}, \mathscr{Y}) = -141\mathscr{Y}^2 + (\mathscr{X}^2 - a')$, d'on deduïm per Eisenstein que $f(\mathscr{X}, \mathscr{Y})$ és irreductible sobre $\mathbb{Q}(\mathscr{X})$.

Per tant, L és un cos.
Ara, fixem-nos que $f(\mathscr{X}, \mathscr{Y})$ té solució a K. Sabem que si K és un cos amb $\mathrm{car}(K) \neq 2$, considerem l'extensió de cossos $K \subset K(x) \subset K(x,y)$ on x és transcendent sobre K i $ax^2 + by^2 = c$ amb $(a,b,c) \in K^3$ té una solució en K, aleshores existeix $u \in K(x,y)$ transcendent sobre K tal que $K(u) = K(x,y)$[1]. En el nostre cas,

1. Si $K = \mathbb{R}$, existeix $u \in K(\cosh t, \sinh t)$ tal que $K(u) = K(\cosh t, \sinh t) \cong L$.

2. Si $K = \mathbb{Q}$, existeix $u \in K(-\frac{2115m^2 + 352m + 15}{2(141m^2 - 1)}, -\frac{12408m^2 + 2115m + 88}{141(141m^2 - 1)})$ tal que $K(u) = K(-\frac{2115m^2 + 352m + 15}{2(141m^2 - 1)}, -\frac{12408m^2 + 2115m + 88}{141(141m^2 - 1)}) \cong L$.

Per tant, en ambdós casos existeix u on $L = K(u)$ $\square$

[1] Teorema 1.21., peu de pàgina.

Problema 2. *Doneu un criteri per existir l'arrel quadrada de $-(U+3)$ en un cos finit $\mathbb{F}_p$.*

Solució. Donar un criteri per a que $-(U+3) := -10$ sigui un quadrat a $\mathbb{F}_p$ és equivalent a decidir per quins p tenim $\left(\frac{-10}{p}\right) = 1$ (per $p = 5$, tenim que $-10 = 0$, un quadrat). El problema es redueix a trobar una expressió per $\left(\frac{5}{p}\right)$, ja que, per multiplicitat del símbol de Legendre, $\left(\frac{-10}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{10}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{5}{p}\right)$ i sabem que $\left(\frac{-1}{p}\right) = (-1)^{\alpha(p)}$ i $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$, on

$$\alpha(p) = \begin{cases} 0 & \text{si } p \equiv 1 \pmod 4 \\ 1 & \text{si } p \equiv -1 \pmod 4 \end{cases}, \ \omega(p) = \begin{cases} 0 & \text{si } p \equiv \pm 1 \pmod 8 \\ 1 & \text{si } p \equiv -\pm 5 \pmod 4 \end{cases}$$

Per la llei de reciprocitat quadràtica, tenim que $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)(-1)^{\frac{p-1}{2}\frac{5-1}{2}} = \left(\frac{p}{5}\right)$. Aleshores, $\left(\frac{1}{5}\right) = 1$, $\left(\frac{2}{5}\right) = (-1)^{\omega(5)} = -1$, $\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right)(-1)^{\frac{3-1}{2}\frac{5-1}{2}} = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\omega(3)} = -1$ i $\left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$. Si definim

$$\beta(p) = \begin{cases} 0 & \text{si } p \equiv \pm 1 \pmod 5 \\ 1 & \text{si } p \equiv \pm 2 \pmod 5 \end{cases},$$

$\left(\frac{5}{p}\right) = (-1)^{\beta(p)}$. Tot plegat tenim que $\left(\frac{-10}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\alpha(p)}(-1)^{\omega(p)}(-1)^{\beta(p)} = (-1)^{\alpha(p)+\omega(p)+\beta(p)}$. Aleshores, -10 és un quadrat a $\mathbb{F}_p$ si i només si $\alpha(p)+\omega(p)+\beta(p) \equiv 0 \pmod 2$. □

Problema 3. *Trobeu una successió de nombres racionals que convergeixin a $(U+1)(C+1)$ a $\mathbb{Q}_p$ però no convergeixi als nombres reals.*

Solució. $(U+1)(C+1) := 2^6$. Considerem $\{x_n := 2^6 + n!\}_{n\in\mathbb{N}}$. Tenim que $|x_n - 2^6|_p = |n!|_p = p^{-v_p(n!)} = p^{-\sum_{i=1}^{\lfloor \log_p n\rfloor} \lfloor \frac{n}{p^i}\rfloor} \to 0$, d'on $\{x_n\}_{n\in\mathbb{N}}$ convergeix a 2^6 a $\mathbb{Q}_p$. Però, $\{x_n\}_{n\in\mathbb{N}}$ clarament no convergeix a $\mathbb{R}$. □

Problema 4. *Trieu el primer més petit p complint $p > (C+D+10U)$ i calculeu els enters a que són un quadrat en $\mathbb{Q}_p$.*

Solució. Tenim que $89 = \min\{p : p \text{ primer} \wedge p > (C+D+10U) = 85\}$. Sigui $p := 89 > 2$. Pel problema 35 sabem que tot element $\mathbb{Q}_p^*$ s'escriu com $p^n u$ amb $n \in \mathbb{Z}$ i $u \in \mathbb{Z}_p^*$ de manera única. Pel problema 37, si $p > 2$, $p^n u \in (\mathbb{Q}_p^*)^2$ si i només si $n \equiv 0 \pmod 2$ i (la imatge de) u és un quadrat a $\mathbb{F}_p$, és a dir, si $\pi : \mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/(p) =: \mathbb{F}_p$ és la projecció, $\left(\frac{\pi(u)}{p}\right) = 1$. Aleshores,

$$\begin{aligned}(\mathbb{Q}_p^*)^2 &= \{p^{2n}u \in \mathbb{Q}_p^* : n \in \mathbb{Z} \wedge u \in \pi^{-1}(\{\alpha \in \mathbb{F}_p : \left(\tfrac{\alpha}{p}\right) = 1\})\} \\ &= \{p^{2n}\big(\textstyle\sum_{i\geq 0} a_i p^i\big) \in \mathbb{Q}_p^* : n \in \mathbb{Z} \wedge \sum_{i\geq 0} a_i p^i \neq 0 \wedge \left(\tfrac{\pi(a_0)}{p}\right) = 1\}\end{aligned}$$

on $\{\alpha \in \mathbb{F}_p : \left(\frac{\alpha}{p}\right) = 1\} = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{16}, \overline{17}, \overline{18}, \overline{20}, \overline{21}, \overline{22}, \overline{25}, \overline{32}, \overline{34}, \overline{36}, \overline{39}, \overline{40}, \overline{42}, \overline{44}, \overline{45}, \overline{47}, \overline{49}, \overline{50}, \overline{53}, \overline{55}, \overline{57}, \overline{64}, \overline{67}, \overline{68}, \overline{69}, \overline{71}, \overline{72}, \overline{73}, \overline{78}, \overline{79}, \overline{80}, \overline{81}, \overline{84}, \overline{85}, \overline{87}, \overline{88}\}$. $0 \in \mathbb{Q}_p$ també és un quadrat. □

Problema 5. *Trobeu totes les extensions quadràtiques de $\mathbb{Q}_p$ amb el primer p que useu en l'exercici anterior.*

Solució. Sigui $u \in \{u \in \mathbb{Q}_p^* : \left(\frac{\pi(u)}{p}\right) = -1\}$, on $\pi : \mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/(p)$ és la projecció. Veiem que totes les extensions quadràtiques de $\mathbb{Q}_p$ són $\mathbb{Q}_p(\sqrt{u}), \mathbb{Q}_p(\sqrt{p}), \mathbb{Q}_p(\sqrt{up})$. Considerem $p^{2n}(\sum_{i\geq 0} a_i p^i) \in \mathbb{Q}_p^*$ i $X^2 - p^{2n}(\sum_{i\geq 0} a_i p^i) \in \mathbb{Q}_p[X]$. Sense pèrdua de la generalitat, podem suposar que o bé $a_0 \neq 0$ o bé $a_1 \neq 0$. Suposem que $a_0 \neq 0$.

1. Si $\left(\frac{\pi(a_0)}{p}\right) = 1$, aleshores $p^{2n}(\sum_{i\geq 0} a_i p^i) \in (\mathbb{Q}_p^*)^2$, d'on $x \in \mathbb{Q}_p$ solució de $X^2 - p^{2n}(\sum_{i\geq 0} a_i p^i)$.
2. Si $\left(\frac{\pi(a_0)}{p}\right) = -1$, aleshores $\left(\frac{\pi(a_0 u)}{p}\right) = \left(\frac{\pi(a_0)}{p}\right)\left(\frac{\pi(u)}{p}\right) = (-1)(-1) = 1$, d'on $p^{2n}(\sum_{i\geq 0} a_i u p^i) \in (\mathbb{Q}_p^*)^2$ i $\sqrt{u}x \in \mathbb{Q}_p$ solució $uX^2 - p^{2n}(\sum_{i\geq 0} a_i u p^i) \in \mathbb{Q}_p[X]$ (i, per tant, $x \in \mathbb{Q}_p(\sqrt{u})$ solució de $X^2 - p^{2n}(\sum_{i\geq 0} a_i p^i)$).

Suposem que $a_0 = 0$. Aleshores, $a_1 \neq 0$.

1. Si $\left(\frac{\pi(a_1)}{p}\right) = 1$, aleshores $p^{2n}(\sum_{i\geq 0} a_{i+1} p^i) \in (\mathbb{Q}_p^*)^2$, d'on $\frac{x}{\sqrt{p}} \in \mathbb{Q}_p$ solució de $\frac{1}{p}X^2 - p^{2n}(\sum_{i\geq 0} a_{i+1} p^i) \in \mathbb{Q}_p[X]$ (i, per tant, $x \in \mathbb{Q}_p(\sqrt{p})$ solució de $X^2 - p\big(p^{2n}(\sum_{i\geq 0} a_{i+1} p^i)\big) = X^2 - (p^{2n}(\sum_{i\geq 0} a_i p^i))$

2. Si $\left(\frac{\pi(a_1)}{p}\right) \neq 1$, aleshores $\left(\frac{\pi(a_1 u)}{p}\right) = \left(\frac{\pi(a_1)}{p}\right)\left(\frac{\pi(u)}{p}\right) = (-1)(-1) = 1$, d'on $p^{2n}(\sum_{i\geq 0} a_{i+1}up^i) \in (\mathbb{Q}_p^*)^2$ i $\frac{x\sqrt{u}}{\sqrt{p}} \in \mathbb{Q}_p$ solució de $\frac{u}{p}X^2 - p^{2n}(\sum_{i\geq 0} a_{i+1}up^i) \in \mathbb{Q}_p[X]$ (i, per tant, $x \in \mathbb{Q}_p(\sqrt{up})$ solució de $X^2 - p\big(p^{2n}(\sum_{i\geq 0} a_{i+1}up^i)\big) = X^2 - (p^{2n}(\sum_{i\geq 0} a_i up^i))$

Veiem que aquestes extensions quadràtiques i $\mathbb{Q}_p$ són totes diferents. Suposem que $\mathbb{Q}_p = \mathbb{Q}_p(\sqrt{p})$. Aleshores, $\sqrt{p} \in \mathbb{Q}_p$, d'on $v_p(\sqrt{p}) = \frac{v_p(\sqrt{p})+v_p(\sqrt{p})}{2} = \frac{v_p(\sqrt{p}\sqrt{p})}{2} = \frac{v_p(p)}{2} = \frac{1}{2} \notin \mathbb{Z}$, contradicció. Aleshores, $\mathbb{Q}_p \neq \mathbb{Q}_p(\sqrt{p})$. Com $u \notin (\mathbb{Q}_p^*)^2$, clarament $\mathbb{Q}_p \neq \mathbb{Q}_p(\sqrt{u})$. Per arguments similars, $\mathbb{Q}_p \neq \mathbb{Q}_p(\sqrt{up})$.
Suposem que $\mathbb{Q}_p(\sqrt{u}) = \mathbb{Q}_p(\sqrt{p})$. Aleshores, $\sqrt{u} \in \mathbb{Q}_p(\sqrt{p})$, d'on $\exists a \exists b(a, b \in \mathbb{Q}_p \wedge \sqrt{u} = a + b\sqrt{p})$. Obtenim $u = (a^2 + pb^2) + 2ab\sqrt{p} \in \mathbb{Q}_p$. Com $\sqrt{p} \notin \mathbb{Q}_p$, o bé $a = 0$ o bé $b = 0$.

1. Si $a = 0$, $u = pb^2$. Obtenim $-1 = \left(\frac{\pi(u)}{p}\right) = \frac{\pi(pb^2)}{p} = 0$, contradicció.

2. Si $b = 0$, $u = a^2 \in (\mathbb{Q}_p^*)^2$, contradicció.

Per tant, $\mathbb{Q}_p(\sqrt{u}) \neq \mathbb{Q}_p(\sqrt{p})$. Suposem que $\mathbb{Q}_p(\sqrt{u}) = \mathbb{Q}_p(\sqrt{up})$. Aleshores, $\sqrt{p} = \frac{\sqrt{up}}{\sqrt{u}} \in \mathbb{Q}_p(\sqrt{u})$, contradicció. Aleshores, $\mathbb{Q}_p(\sqrt{u}) \neq \mathbb{Q}_p(\sqrt{up})$. Suposem que $\mathbb{Q}_p(\sqrt{p}) = \mathbb{Q}_p(\sqrt{up})$. Aleshores, $\sqrt{u} = \frac{\sqrt{up}}{\sqrt{p}} \in \mathbb{Q}_p(\sqrt{p})$, contradicció. Aleshores, $\mathbb{Q}_p(\sqrt{p}) \neq \mathbb{Q}_p(\sqrt{up})$. Per tant, les extensions quadràtiques $\mathbb{Q}_p(\sqrt{u}), \mathbb{Q}_p(\sqrt{p}), \mathbb{Q}_p(\sqrt{up})$ i $\mathbb{Q}_p$ són totes diferents. Especialitzant-nos amb $p := 89$, tenim que totes les extensions quadràtiques són $\mathbb{Q}_{89}(\sqrt{3}), \mathbb{Q}_{89}(\sqrt{89}), \mathbb{Q}_{89}(\sqrt{267})$, on $\pi(3) \in \{u \in \mathbb{Q}_p^* : \left(\frac{\pi(u)}{p}\right) = -1\}$. □

Problema 6. *Considera l'equació $Y^2 - pX^2 = -1$ amb p un primer congruent amb 1 mòdul 4. Demostreu que l'equació té infinites solucions a $\mathbb{Z}$.*

Demostració. Sigui $p \equiv 1 \pmod 4$ i $(u, v) \in \{(X, Y) \in \mathbb{Z}^2 : Y^2 - pX^2 = 1\} - \{(0, 1), (0, -1)\}$ tal que $|u|$ és mínima. Volem veure que $u \equiv 0 \pmod 2$ i $v \equiv 1 \pmod 2$. En efecte,

1. Suposem $u \equiv 0 \pmod 2$ i $v \equiv 0 \pmod 2$. Aleshores, $1 \equiv v^2 - pu^2 \equiv 0 \pmod 2$, contradicció.

2. Suposem $u \equiv 1 \pmod 2$ i $v \equiv 1 \pmod 2$. Aleshores, $1 \equiv v^2 - pu^2 \equiv 1 - 1 \equiv 0 \pmod 2$, contradicció.

3. Suposem $u \equiv 1 \pmod 2$ i $v \equiv 0 \pmod 2$. Aleshores, $u^2 \equiv 1 \pmod 4$ i $v^2 \equiv 0 \pmod 4$, d'on $1 \equiv v^2 - pu^2 \equiv v^2 - u^2 \equiv -1 \pmod 4$, contradicció.

Aleshores, la única possibilitat és que $u \equiv 0 \pmod 2$ i $v \equiv 1 \pmod 2$.
Com $(u, v) \in \{(X, Y) \in \mathbb{Z}^2 : Y^2 - pX^2 = 1\}$, $v^2 - pu^2 = 1$ podem escriure $pu^2 = v^2 - 1 = (v - 1)(v + 1)$. Tenim que $u \equiv 0 \pmod 2 \wedge v \equiv 1 \pmod 2 \iff \exists \ell(\ell \in \mathbb{Z} \wedge u = 2\ell) \wedge \exists k(k \in \mathbb{Z} \wedge v = 2k + 1)$. Aleshores, $4p\ell^2 = pu^2 = (v-1)(v+1) = 4k(k+1)$, d'on deduïm $p\ell^2 = k(k+1)$. Tenim que $k(k+1) \in (p) \in \operatorname{Spec}(\mathbb{Z})$. Per tant, o bé $k \in (p)$ o bé $k + 1 \in (p)$. Suposem que $k \in (p)$. Com $\mathbb{Z}$ és un domini de factorització única, ℓ admet una descomposició en elements primers $\ell = \prod_{i=1}^n p_i^{e_i}$. Com $\gcd(k, k + 1) = 1$, existeix $\mathscr{I} \subset \{1, \ldots, n\}$ tal que $k = p\big(\prod_{i\in\mathscr{I}} p_i^{e_i}\big)^2$ i $k + 1 = \big(\prod_{i\notin\mathscr{I}} p_i^{e_i}\big)^2$. Aleshores, $\big(\prod_{i\notin\mathscr{I}} p_i^{e_i}\big)^2 - p\big(\prod_{i\in\mathscr{I}} p_i^{e_i}\big)^2 = (k + 1) - k = 1$, d'on

$$\Big(\big(\prod_{i\in\mathscr{I}} p_i^{e_i}\big)^2, \big(\prod_{i\notin\mathscr{I}} p_i^{e_i}\big)^2\Big) \in \{(X, Y) \in \mathbb{Z}^2 : Y^2 - pX^2 = 1\}$$

Però, $|\prod_{i\in\mathscr{I}} p_i^{e_i}| \leq |\prod_{i=1}^n p_i^{e_i}| = |\ell| = |\frac{u}{2}| < |u|$, contradient la minimalitat d'u. Aleshores, $k + 1 \in (p)$. Similarment, com $\gcd(k, k+1) = 1$, existeix $\mathscr{I}' \subset \{1, \ldots, n\}$ tal que $k+1 = p\big(\prod_{i\in\mathscr{I}'} p_i^{e_i}\big)^2$ i $k = \big(\prod_{i\notin\mathscr{I}'} p_i^{e_i}\big)^2$. Aleshores, $\big(\prod_{i\notin\mathscr{I}'} p_i^{e_i}\big)^2 - p\big(\prod_{i\in\mathscr{I}'} p_i^{e_i}\big)^2 = k - (k + 1) = -1$. Per tant,

$$\Big(\big(\prod_{i\in\mathscr{I}'} p_i^{e_i}\big)^2, \big(\prod_{i\notin\mathscr{I}'} p_i^{e_i}\big)^2\Big) \in \{(X, Y) \in \mathbb{Z}^2 : Y^2 - pX^2 = -1\}$$

Sigui $(r_1, s_1) \in \{(X, Y) \in \mathbb{Z}^2 : Y^2 - pX^2 = -1\}$ amb $|r_1|$ mínim i $(r_1, s_1) \in \mathbb{N}^2$. Veiem que $(r_n, s_n) \in \mathbb{Z}^2$ definit per $r_n + \sqrt{p}s_n := (r_1 + \sqrt{p}s_1)^{2n+1} \in \mathbb{Z}[\sqrt{p}]$ és solució de $Y^2 - pX^2 = -1$. En efecte, si $\sigma \in \operatorname{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q})$ és la conjugació, $s_n^2 - pr_n^2 = (s_n - \sqrt{p}r_n)(s_n + \sqrt{p}r_n) = \sigma(s_n + \sqrt{p}r_n)(s_n + \sqrt{p}r_n) = \sigma\big((s_1 + \sqrt{p}r_1)^{2n+1}\big)(s_1 + \sqrt{p}r_1)^{2n+1} = \sigma(s_1 + \sqrt{p}r_1)^{2n+1}(s_1 + \sqrt{p}r_1)^{2n+1} = (\sigma(s_1 + \sqrt{p}r_1)(s_1 + \sqrt{p}r_1))^{2n+1} = ((s_1 - \sqrt{p}r_1)(s_1 + \sqrt{p}r_1))^{2n+1} = (-1)^{2n+1} = -1$. Aleshores, $Y^2 - pX^2 = -1$ té infinites solucions. □

Problema 7. *Proveu un isomorfisme d'anells: $\mathbb{Z}_p \cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}, \mathbb{Z}[\frac{1}{p}]/\mathbb{Z})$.*

Seguirem un argument similar a [Lam99]. Donat R anell (commutatiu amb unitat), direm que un R-mòdul J és injectiu si el functor $\mathrm{Hom}_R(-,J) : \mathrm{Mod}_R \to \mathrm{Mod}_R$ és exacte. Equivalentment, J és injectiu si i només si per tot ideal $I \subset R$ i $f \in \mathrm{Hom}_R(I,J)$ existeix $g \in \mathrm{Hom}_R(R,J)$ tal que $g|_I = f$. Donats $M \subset N$ R-mòduls, direm que $M \subset N$ és una extensió essencial de M si tot R-submòdul no trivial interseca M no trivialment o, equivalentment, $\forall n(n \in N - \{0_N\} \Rightarrow \exists r(r \in R \wedge ar \in M - \{0\}))$. Donem la següent caracterització sense demostració: donats $M \subset I$ R-mòduls, I és l'injectiu més petit que conté M si i només si I és injectiu i $M \subset I$ és una extensió sobre M. Si I R-mòdul satisfà qualsevol de les propietats anteriors, direm que I és l'envolvent injectiu de M sobre R. L'envolvent injectiu de M sobre R és únic llevat isomorfisme. Volem demostrar el següent: *Sigui* $(R,\mathfrak{m})$ *anell noetherià local,* E *envolvent injectiu de* $R/\mathfrak{m}$ *sobre* R*. Aleshores,* $\mathrm{Hom}_R(E,E) \cong \varprojlim_{n\in\mathbb{N}} R/\mathfrak{m}^n$.
Amb el darrer isomorfisme, serà suficient veure que $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ és l'envolvent injectiu de $\mathbb{Z}/(p)$ sobre $\mathbb{Z}$. Recordem que un grup abelià (o $\mathbb{Z}$-mòdul) G és divisible si $\forall x \forall n((x \in G \wedge n \in \mathbb{N}) \Rightarrow \exists y(y \in G \wedge ny = x))$.

Proposició 1. *Tot* $\mathbb{Z}$*-mòdul* J *divisible és injectiu.*

Demostració. Siguin $A \subset B$ $\mathbb{Z}$-mòduls i $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(A,J)$. Volem estendre φ a un element de $\mathrm{Hom}_{\mathbb{Z}}(B,J)$.
Sigui $\mathscr{S} := \{(A',\varphi') \in \mathrm{Obj}(\mathrm{Mod}_{\mathbb{Z}}) \times \mathrm{Hom}_{\mathbb{Z}}(A',J) : A \subset A' \subset B \wedge \varphi'|_A = \varphi\}$ conjunt parcialment ordenat per l'ordre $\leq$ definit per $(A',\varphi') \leq (A'',\varphi'') :\iff A' \subset A'' \wedge \varphi''|_{A'} = \varphi'$. $\mathscr{S} \neq \emptyset$, ja que $(A,\varphi) \in \mathscr{S}$. Considerem una cadena $\{(A_i,\varphi_i) : i \in \mathscr{I}\}$ de $\mathscr{S}$. Tenim que $(\bigcup_{i\in\mathscr{I}} A_i, \varphi) \in \mathscr{S}$ és una cota superior de $\{(A_i,\varphi_i) : i \in \mathscr{I}\}$, on $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(\bigcup_{i\in\mathscr{I}} A_i, J)$ ve definida per $\varphi(x) := \varphi_i(x)$ si $x \in A_i$. Aleshores, pel lema de Zorn, $\mathscr{S}$ té un element maximal $(A',\varphi') \in \mathscr{S}$.
Volem veure que $A' = B$. Suposem que $A' \subsetneq B$. Sigui $x \in B - A'$. Suposem que $\forall n(n \in \mathbb{Z} \Rightarrow nx \notin A')$. Definim $\varphi'' \in \mathrm{Hom}_{\mathbb{Z}}(A' + \mathbb{Z}x, J)$ per $\varphi''(a+nx) := \varphi(a)$. Tenim que $(A',\varphi') \leq (A'+\mathbb{Z}x, \varphi'') \in \mathscr{S}$, contradicció amb la maximalitat de (A',φ'). Suposem que $\exists n(n \in \mathbb{Z} \wedge nx \in A')$ A més, imposem que n sigui mínima. Per divisibilitat de J, $\forall x(x \in A' \Rightarrow \exists y(y \in J \wedge ny = \varphi(nx)))$. Considerem $\varphi'' \in \mathrm{Hom}_{\mathbb{Z}}(A' \oplus \mathbb{Z}, J)$ definit per $\varphi''(a,m) := \varphi(a) + mny$. Considerem $\varphi_0 \in \mathrm{Hom}_{\mathbb{Z}}(A' \oplus \mathbb{Z}, B)$ definit per $\varphi_0(a,m) := a + mnx$. Si $(a,m) \in \ker\varphi_0$, $\varphi''(a,m) = \varphi(a) + mny = \varphi(a) + m\varphi(nx) = \varphi(a+mnx) = \varphi(0) = 0$. Per tant, $\ker\varphi_0 \subset \ker\varphi''$, d'on tenim la factorització

$$\begin{tikzcd} A' \oplus \mathbb{Z} \arrow[rr, "\varphi''"] \arrow[dr, "\varphi_0"'] & & J \\ & A' + x(n) \arrow[ur, dotted, "\overline{\varphi}_0"'] & \end{tikzcd}$$

$\overline{\varphi}_0 \in \mathrm{Hom}_{\mathbb{Z}}(A' + x(n), J)$ definida per $\overline{\varphi}_0(a + mnx) := \varphi(a) + mnz$. Obtenim $(A',\varphi') \leq (A' + x(n), \overline{\varphi}_0) \in \mathscr{S}$, contradicció amb la maximalitat de (A',φ'). Per tant, $A' = B$. $\square$

El recíproc també és cert. És fàcil veure que $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ és p-divisible i, per tant, divisible. Com $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ és un $\mathbb{Z}$-mòdul, deduïm que $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ és injectiu. A més, $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ és essencial sobre $\mathbb{Z}/(p)$ ($\cong \mathbb{Z}_{(p)}/(p)\mathbb{Z}_{(p)}$) ja que $p(\sum_{j=0}^{i} a_j p^{-j} + \mathbb{Z}) = \sum_{j=0}^{i-1} a_{j-1} p^{-j} + (p^i) \in \mathbb{Z}/(p)$. Per tant,

$$\begin{aligned} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[\tfrac{1}{p}]/\mathbb{Z}, \mathbb{Z}[\tfrac{1}{p}]/\mathbb{Z}) &= \mathrm{Hom}_{\mathbb{Z}_{(p)}}(\mathbb{Z}[\tfrac{1}{p}]/\mathbb{Z}, \mathbb{Z}[\tfrac{1}{p}]/\mathbb{Z}) && \text{(Hom-sets coincideixen)} \\ &\cong \varprojlim_{i\in\mathbb{N}} \mathbb{Z}_{(p)}/\big((p)\mathbb{Z}_{(p)}\big)^i && ((\mathbb{Z}_{(p)}, \mathbb{Z}_{(p)}/(p)\mathbb{Z}_{(p)}) \text{ anell noetherià local}) \\ &\cong \varprojlim_{i\in\mathbb{N}} \mathbb{Z}/(p^i) \cong \mathbb{Z}_p && (\mathbb{Z}_{(p)}/\big((p)\mathbb{Z}_{(p)}\big)^i \cong \mathbb{Z}/(p^i)) \end{aligned}$$

d'on resulta el problema. Ara, ens centrem en demostrar l'isomorfisme $\mathrm{Hom}_R(E,E) \cong \varprojlim_{n\in\mathbb{N}} R/\mathfrak{m}^n$. Veiem uns resultat sobre mòduls injectius.

Lema 1. *Sigui* $R \to S$ *un morfisme d'anells. Si* E *és un* R*-mòdul injectiu, aleshores* $\mathrm{Hom}_R(S,E)$ *és un* S*-mòdul injectiu.*

Demostració. Donat un S-mòdul M, tenim la correspondència $\mathrm{Hom}_R(M_R, E) \leftrightarrow \mathrm{Hom}_S(M, \mathrm{Hom}_R(S,E))$ donada per $\alpha \mapsto (n \mapsto (s \mapsto \alpha(sn)))$ amb inversa $\beta \mapsto (n \mapsto \beta(n)(1_S))$. Com E és R-mòdul injectiu, $\mathrm{Hom}_R(-,E)$ és exacte. Per la correspondència, $\mathrm{Hom}_R(-,E) = \mathrm{Hom}_S(-, \mathrm{Hom}_R(S,E))$, d'on deduïm que $\mathrm{Hom}_S(-, \mathrm{Hom}_R(S,E))$ és exacte i, per tant, $\mathrm{Hom}_R(S,E)$ és S-mòdul injectiu. $\square$

Lema 2. *Sigui $f : (R, \mathfrak{m}_R) \to (S, \mathfrak{m}_S)$ un epimorfisme d'anells locals, E envolvent injectiu de $R/\mathfrak{m}_R$ sobre R. Aleshores $\mathrm{Ann}_E(\ker f)$ és l'envolvent injectiu de $S/\mathfrak{m}_S$ sobre S.*

Demostració. Veure [Sta24], 47.7.1. □

Lema 3. *Sigui I R-mòdul injectiu, $E \subset I$ R-submòdul. Són equivalents:*

1. *E injectiu.*
2. *Per tot $E \subset E' \subset I$ amb $E \subset E'$ extensió essencial, $E = E'$.*

Demostració. Suposem E injectiu. Sigui $E' \subset I$ amb $E \subset E'$ extensió essencial. Per injectivitat d'E, $id_E \in \mathrm{Hom}_R(E, E)$ es pot estendre a $\alpha \in \mathrm{Hom}_R(E', E)$. Com $\alpha|_E = id_E$, $\ker \alpha = \{0\}$. Com $E \subset E'$ extensió essencial i $\ker \alpha = \{0\}$, $\ker \alpha = \{0\}$. Aleshores, $E' \cong E'/\ker \alpha \cong \mathrm{im}\, \alpha \subset E$, d'on deduïm que $E = E'$.
Suposem que per tot $E \subset E' \subset I$ amb $E \subset E'$ extensió essencial, $E = E'$. Siguin $M \subset N$ R-mòduls i $\varphi \in \mathrm{Hom}_R(M, E)$. Sigui $\mathscr{S} := \{(M', \varphi') \in \mathrm{Obj}(\mathrm{Mod}_R) \times \mathrm{Hom}_{\mathbb{Z}}(M', J) : M \subset M' \subset N \wedge \varphi'|_M = \varphi\}$ conjunt parcialment ordenat per l'ordre $\le$ definit per $(M', \varphi') \le (M'', \varphi'') :\iff M' \subset M'' \wedge \varphi''|_{M'} = \varphi'|$. $\mathscr{S} \neq \emptyset$, ja que $(M, \varphi) \in \mathscr{S}$. Considerem una cadena $\{(M_i, \varphi_i) : i \in \mathscr{I}\}$ de $\mathscr{S}$. Tenim que $(\bigcup_{i \in \mathscr{I}} M_i, \varphi) \in \mathscr{S}$ és una cota superior de $\{(M_i, \varphi_i) : i \in \mathscr{I}\}$, on $\varphi \in \mathrm{Hom}_R(\bigcup_{i \in \mathscr{I}} A_i, J)$ ve definida per $\varphi(x) := \varphi_i(x)$ si $x \in M_i$. Aleshores, pel lema de Zorn, $\mathscr{S}$ té un element maximal $(M', \varphi') \in \mathscr{S}$.
Sigui $\iota : E \hookrightarrow I$ la inclusió. Com I és un R-mòdul injectiu, podem estendre $\iota \circ \varphi' \in \mathrm{Hom}_R(M', I)$ a $\psi \in \mathrm{Hom}_R(N, I)$. Suposem que $\psi(N) \subset E$. Aleshores, $\psi : N \to \psi(N) \hookrightarrow E$ i $\psi|_M = (\iota \circ \varphi')|_M = \varphi'|_M = \phi$, d'on deduïm que E és injectiu ($\psi \in \mathrm{Hom}_R(N, E)$ esten $\varphi \in \mathrm{Hom}_R(M, E)$). Suposem que $\psi(N) \not\subset E$. Tenim $E \subsetneq E + \psi(N) \subset I$, d'on $E \subset E + \psi(N)$ no és essencial. Aleshores, existeix $K \subset E + \psi(N)$ no trivial tal que $K \cap E = \{0\}$. Com $M' \subset \psi^{-1}(E) \subsetneq \psi^{-1}(E + K)$, $\pi \circ \psi|_{\psi^{-1}(E+K)} : \psi^{-1}(E + K) \to E + K \twoheadrightarrow E$ és tal que $(\pi \circ \psi|_{\psi^{-1}(E+K)})|_{M'} = \varphi'$ i $\psi^{-1}(E + K) \subset N$, tenim que $(M', \varphi') \le (\psi^{-1}(E + K), \pi \circ \psi|_{\psi^{-1}(E+K)}) \in \mathscr{S}$, contradicció amb la maximalitat de (M', φ'). □

Lema 4. *Sigui R anell noetherià, I R-mòdul injectiu.*

1. *Sigui $f \in R$. Aleshores, $\bigcup_{n>0} \mathrm{Ann}_I(f^n)$ R-submòdul injectiu de I.*

   Demostració. Sigui $E' \subset I$ amb $\bigcup_{n>0} \mathrm{Ann}_I(f^n) \subset E'$ extensió essencial. Suposem que $\bigcup_{n>0} \mathrm{Ann}_I(f^n) \subsetneq E'$. Aleshores, $\exists x (x \in E' - \bigcup_{n>0} \mathrm{Ann}_I(f^n))$. Considerem l'ideal $\bigcup_{n>0} \mathrm{Ann}_R(f^n x) \subset R$. Com R és noetherià, $\exists g_1 \dots \exists g_t (g_1, \dots, g_t \in R \wedge \bigcup_{n>0} \mathrm{Ann}_I(f^n x) = (g_1, \dots, g_t))$. Com $g_1, \dots, g_t \in \bigcup_{n>0} \mathrm{Ann}_I(f^n x)$, $\exists n_1 \dots \exists n_t (n_1, \dots, n_t > 0 \wedge \forall i (g_i f^{n_i} x = 0))$. Definim $x' := f^{\max\{n_i\}} x \in E' - \bigcup_{n>0} \mathrm{Ann}_I(f^n)$. Sigui $r \in \bigcup_{n>0} \mathrm{Ann}_I(f^n x)$. Com $\bigcup_{n>0} \mathrm{Ann}_I(f^n x) = (g_1, \dots, g_t)$, $\exists a_1 \dots \exists a_t (a_1, \dots, a_t \in R \wedge r = \sum_{i=1}^t a_i g_i)$, d'on $rx' = \sum_{i=1}^t a_i (g_i f^{\max\{n_i\}} x) = \sum_{i=1}^t a_i 0 = 0$. Per tant, $r \in \mathrm{Ann}_R(x')$ i $\bigcup_{n>0} \mathrm{Ann}_I(f^n x) \subset \mathrm{Ann}_R(x')$. Com $\mathrm{Ann}_R(x') = \mathrm{Ann}_R(f^{\max\{n_i\}} x) \subset \bigcup_{n>0} \mathrm{Ann}_R(f^n x)$, deduïm que

   $$\mathrm{Ann}_R(x') = \bigcup_{n>0} \mathrm{Ann}_R(f^n x)$$

   Sigui $r \in \bigcup_{n>0} \mathrm{Ann}_R(f^n x)$. Com $\bigcup_{n>0} \mathrm{Ann}_R(f^n x) = (g_1, \dots, g_t)$, $\exists a_1 \dots \exists a_t (a_1, \dots, a_t \in R \wedge r = \sum_{i=1}^t a_i g_i)$, d'on $r(f^n x') = \sum_{i=1}^t a_i g_i f^n f^{\max\{n_i\}} x = 0$ i $r \in \bigcap_{n>0} \mathrm{Ann}_R(f^n x') \subset \bigcup_{n>0} \mathrm{Ann}_R(f^n x')$. Per tant, $\bigcup_{n>0} \mathrm{Ann}_R(f^n x) \subset \bigcup_{n>0} \mathrm{Ann}_R(f^n x')$. Com $\bigcup_{n>0} \mathrm{Ann}_R(f^n x') = \bigcup_{n>0} \mathrm{Ann}_R(f^{n+\max\{n_i\}} x) \subset \bigcup_{n>0} \mathrm{Ann}_R(f^n x)$, deduïm que

   $$\bigcup_{n>0} \mathrm{Ann}_R(f^n x) = \bigcup_{n>0} \mathrm{Ann}_R(f^n x')$$

   Per transitivitat de $=$,

   $$\mathrm{Ann}_R(x') = \bigcup_{n>0} \mathrm{Ann}_R(f^n x')$$

   Sigui $r \in Rx' \cap \bigcup_{n>0} \mathrm{Ann}_R(f^n)$. Aleshores, $\exists n (n > 0 \wedge r f^n = 0)$ i $\exists r' (r' \in R \wedge r' x' = r)$, d'on $r' f^n x' = r f^n = 0$ i $r' \in \bigcup_{n>0} \mathrm{Ann}_R(f^n x')$. Com $\mathrm{Ann}_R(x') = \bigcup_{n>0} \mathrm{Ann}_R(f^n x')$, $r' \in \mathrm{Ann}_R(x')$, d'on $r = r' x' = 0$. Per tant, $Rx' \cap \bigcup_{n>0} \mathrm{Ann}_R(f^n) = \{0\}$, d'on deduïm que $\bigcup_{n>0} \mathrm{Ann}_R(f^n) \subset E'$ no és una extensió essencial, contradicció. Per tant, $\bigcup_{n>0} \mathrm{Ann}_R(f^n) = E'$ i, pel lema anterior, $\bigcup_{n>0} \mathrm{Ann}_R(f^n)$ és R-submòdul injectiu de I. □

2. *Sigui $J \subset R$ ideal. Aleshores, $\bigcup_{n>0} \operatorname{Ann}_I(J^n)$ R-submòdul injectiu de I.*

Demostració. Com R és noetherià, $\exists f_1 \dots \exists f_t (f_1, \dots f_t \in R \wedge J = (f_1, \dots, f_t))$. Aleshores, com

$$\bigcup_{n>0} \operatorname{Ann}_I(J^n) = \bigcup_{n>0} \operatorname{Ann}_{\bigcup_{n>0} \operatorname{Ann}_{\cdots (\bigcup_{n>0} \operatorname{Ann}_{(\bigcup_{n>0} \operatorname{Ann}_I(f_1^n))}(f_2^n))\cdots}(f_{t-1}^n)}(f_t^n)$$

ens reduïm al cas anterior i procedim per inducció. $\square$

Lema 5. *Sigui $(R, \mathfrak{m})$ un anell noetherià local, E envolvent injectiu de $R/\mathfrak{m}$ sobre R, E_n envolvent injectiu de $R/\mathfrak{m}$ sobre $R/\mathfrak{m}^n$. Aleshores, $E \cong \bigcup_{n>0} E_n$ i $E_n \cong \operatorname{Ann}_E(\mathfrak{m}^n)$.*

Demostració. Com E és l'envolvent injectiu de $R/\mathfrak{m}$ sobre R, $\pi : R \twoheadrightarrow R/\mathfrak{m}^n$ és un epimorfisme d'anells locals amb $\ker \pi = \mathfrak{m}^n$ i el cos residual de $R/\mathfrak{m}^n$ és $R/\mathfrak{m} \cong (R/\mathfrak{m}^n)/(\mathfrak{m}/\mathfrak{m}^n)$, tenim que $\operatorname{Ann}_E(\mathfrak{m}^n)$ és l'envolvent injectiu de $R/\mathfrak{m}$ sobre $R/\mathfrak{m}^n$. Per tant, $E_n \cong \operatorname{Ann}_E(\mathfrak{m}^n)$.
Ara, com R és noetherià i E és un R-mòdul injectiu, $\bigcup_{n>0} \operatorname{Ann}_E(\mathfrak{m}^n)$ és un R-submòdul injectiu d'E. Fixem-nos que $R/\mathfrak{m} \subset \bigcup_{n>0} \operatorname{Ann}_E(\mathfrak{m}^n)$. Com E és l'envolvent injectiu de $R/\mathfrak{m}$, E és l'injectiu més petit que conté $R/\mathfrak{m}$, d'on resulta $E \subset \bigcup_{n>0} \operatorname{Ann}_E(\mathfrak{m}^n)$ i, per tant, $E \cong \bigcup_{n>0} \operatorname{Ann}_E(\mathfrak{m}^n)$. $\square$

Fixem-nos que $\varinjlim_{n\in\mathbb{N}} \operatorname{Ann}_E(\mathfrak{m}^n) \cong \bigcup_{n>0} \operatorname{Ann}_E(\mathfrak{m}^n)$ via la propietat universal del límit directe. Aleshores, obtenim $E \cong \varinjlim_{n\in\mathbb{N}} \operatorname{Ann}_E(\mathfrak{m}^n)$.

Teorema 1. *Sigui $(R, \mathfrak{m})$ anell noetherià local, E envolvent injectiu de $R/\mathfrak{m}$ sobre R. Aleshores,* $\operatorname{Hom}_R(E, E) \cong \varprojlim_{n\in\mathbb{N}} R/\mathfrak{m}^n$.

Demostració. Fixem-nos que $\operatorname{Hom}_R(R/\mathfrak{m}^n, E) \cong \operatorname{Ann}_E(\mathfrak{m}^n)$ via $\varphi \mapsto \varphi(1_R + \mathfrak{m}^n)$. Tenim la successió exacta curta

$$0 \longrightarrow \mathfrak{m}^{n-1}/\mathfrak{m}^n \longrightarrow R/\mathfrak{m}^n \longrightarrow R/\mathfrak{m}^{n-1} \longrightarrow 0$$

Com E és l'envolvent injectiu de $R/\mathfrak{m}$ sobre R, en particular E és injectiu, és a dir, el functor contravariant $\operatorname{Hom}_R(-, E)$ és exacte, d'on tenim la successió exacta curta

$$0 \longrightarrow \operatorname{Hom}_R(R/\mathfrak{m}^{n-1}, E) \longrightarrow \operatorname{Hom}_R(R/\mathfrak{m}^n, E) \longrightarrow \operatorname{Hom}_R(\mathfrak{m}^{n-1}/\mathfrak{m}^n, E) \longrightarrow 0$$

Per exactitud, obtenim els isomorfismes

$$\begin{aligned}
\operatorname{Hom}_R(\mathfrak{m}^{n-1}/\mathfrak{m}^n, E) &\cong \operatorname{Hom}_R(R/\mathfrak{m}^n, E)/\ker(\operatorname{Hom}_R(R/\mathfrak{m}^n, E) \to \operatorname{Hom}_R(\mathfrak{m}^{n-1}/\mathfrak{m}^n, E)) \\
&= \operatorname{Hom}_R(R/\mathfrak{m}^n, E)/\operatorname{im}(\operatorname{Hom}_R(R/\mathfrak{m}^{n-1}, E) \to \operatorname{Hom}_R(R/\mathfrak{m}^n, E)) \\
&\cong \operatorname{Hom}_R(R/\mathfrak{m}^n, E)/\operatorname{Hom}_R(R/\mathfrak{m}^{n-1}, E) \\
&\cong \operatorname{Ann}_E(\mathfrak{m}^n)/\operatorname{Ann}_E(\mathfrak{m}^{n-1})
\end{aligned}$$

d'on deduïm

$$\begin{aligned}
\mathfrak{m}^{n-1}/\mathfrak{m}^n &\cong \operatorname{Hom}_R(\operatorname{Hom}_R(\mathfrak{m}^{n-1}/\mathfrak{m}^n, E), E) && (x \mapsto ev_x,\ ev_x(f) := f(x)) \\
&\cong \operatorname{Hom}_R(\operatorname{Ann}_E(\mathfrak{m}^n)/\operatorname{Ann}_E(\mathfrak{m}^{n-1}), E) && (\operatorname{Hom}_R(\mathfrak{m}^{n-1}/\mathfrak{m}^n, E) \cong \operatorname{Ann}_E(\mathfrak{m}^n)/\operatorname{Ann}_E(\mathfrak{m}^{n-1}))
\end{aligned}$$

En particular, $\mathfrak{m}^{n-1}/\mathfrak{m}^n$ i $\operatorname{Hom}_R(\operatorname{Ann}_E(\mathfrak{m}^n)/\operatorname{Ann}_E(\mathfrak{m}^{n-1}), E)$ tenen la mateixa dimensió com $R/\mathfrak{p}$-espai vectorial. Definim $\varphi_n \in \operatorname{Hom}_R(R/\mathfrak{m}^n, \operatorname{Hom}_R(\operatorname{Ann}_E(\mathfrak{m}^n), E))$ per $\varphi_n(r + \mathfrak{m}^n)(x) := rx$. Si $r + \mathfrak{m}^n \in \ker \varphi_n$, per tot $x \in \operatorname{Ann}_E(\mathfrak{m}^n)$ tenim $\varphi_n(r + \mathfrak{m}^n)(x) = rx = 0$, d'on $r \operatorname{Ann}_E(\mathfrak{m}^n) = 0$ i $r \in \mathfrak{m}^n$. Per tant, $\ker \varphi_n = \{0\}$ i φ_n és monomorfisme. Clarament φ_0 és isomorfisme. Suposem que φ_{n-1} és isomorfisme. Considerem els següent diagrama commutatiu:

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{m}^{n-1}/\mathfrak{m}^n \arrow[r] \arrow[d, "\varphi_n|_{\mathfrak{m}^{n-1}/\mathfrak{m}^{n-1}}"] & R/\mathfrak{m}^n \arrow[r] \arrow[d, "\varphi_n"] & R/\mathfrak{m}^{n-1} \arrow[r] \arrow[d, "\varphi_{n-1}"] & 0 \\
0 \arrow[r] & \operatorname{Hom}_R\left(\frac{\operatorname{Ann}_E(\mathfrak{m}^n)}{\operatorname{Ann}_E(\mathfrak{m}^{n-1})}, E\right) \arrow[r] & \operatorname{Hom}_R(\operatorname{Ann}_E(\mathfrak{m}^n), E) \arrow[r] & \operatorname{Hom}_R(\operatorname{Ann}_E(\mathfrak{m}^{n-1}), E) \arrow[r] & 0
\end{tikzcd}$$

Com les files són exactes, $\varphi_n|_{\mathfrak{m}^{n-1}/\mathfrak{m}^{n-1}}$ és isomorfisme (ja que $\varphi_n|_{\mathfrak{m}^{n-1}/\mathfrak{m}^{n-1}}$ és monomorfisme i el domini i la imatge tenen la mateixa $R/\mathfrak{m}$-dimensió) i φ_{n-1} és isomorfisme, pel lema dels cinc, φ_n és isomorfisme. Aleshores,

$$\begin{aligned}\operatorname{Hom}_R(E,E) &\cong \operatorname{Hom}_R(\varinjlim \operatorname{Ann}_E(\mathfrak{m}^n), E)\\ &\cong \varprojlim \operatorname{Hom}_R(\operatorname{Ann}_E(\mathfrak{m}^n), E)\\ &\cong \varprojlim R/\mathfrak{m}^n\end{aligned}$$

com volíem veure. $\square$

Referències

[Lam99] T. Y. Lam. “Free Modules, Projective, and Injective Modules”. A: *Lectures on Modules and Rings*. New York, NY: Springer New York, 1999, pàg. 1 - 120. ISBN: 978-1-4612-0525-8. DOI: `10.1007/978-1-4612-0525-8_1`. URL: `https://doi.org/10.1007/978-1-4612-0525-8_1`.

[Sta24] The Stacks project authors. *The Stacks project*. `https://stacks.math.columbia.edu`. 2024.