Ex 23.

1) $P = X^3 - X + 2 \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X]$

$c(P) = 1$ donc par Gauss : P irréd. dans $\mathbb{Z}[X]$ $\Leftrightarrow$ P irréd. dans $\mathbb{Q}[X]$

On suppose (par l'absurde) P réductible

alors $\exists\ a, b, c \in \mathbb{Z}$ tq

$$X^3 - X + 2 = (\underset{(\pm 1)}{1}X^2 + aX + b)(\underset{(\pm 1)}{X} - c)$$

On obtient : P a une racine dans $\mathbb{Z}$: c

et $-bc = 2$ ie $c \mid 2$

Ainsi $c = \{-1, +1, 2, -2\}$

on évalue P en ces valeurs et on a une absurdité.

2) $y = \overline{X} \in \mathbb{Q}[X]/(P)$. But $y^{-1} = ?$

Remarque : $\mathbb{Q}[X]/(P) = \mathbb{Q}\cdot\overline{1} + \mathbb{Q}\cdot\overline{X} + \mathbb{Q}\cdot\overline{X^2}$

Générateurs ?

Soit $T \in \mathbb{Q}[X]$ $\quad T = A \times P + R \leftarrow a + bX + cX^2$

$$\overline{T} = \overline{A} \times \underbrace{\overline{P}}_{0} + \overline{R} = a\overline{1} + b\overline{X} + c\overline{X^2}$$

Libre. Soient $a, b, c \in \mathbb{Q}$ tq $a\overline{1} + b\overline{X} + c\overline{X}^2 = \overline{0}$

Alors $a + bX + cX^2 \in \langle P \rangle$ ie $a\,bX + cX^2$ multiple de P.

ça implique $a = b = c = 0$.

On cherche a, b, c tq $\overline{X} \times (a\overline{1} + b\overline{X} + c\overline{X}^2) = \overline{1}$

ie $a\overline{X} + b\overline{X}^2 + c\underbrace{\overline{X}^3} = \overline{1}$ or $\overline{X}^3 = \overline{X - 2}$

$a\overline{X} + b\overline{X}^2 + c(\overline{X} - \overline{2}) = \overline{1}$

$-2c\overline{1} + (a + c)\overline{X} + b\overline{X}^2 = \overline{1}$

d'où

$-2c = 1$, $a + c = 0$, $b = 0$ ie $c = -\frac{1}{2}$, $a = \frac{1}{2}$

$y^{-1} = \frac{1}{2} - \frac{1}{2}y^2$

Ex 23 (2)

variante : X, X^3-X+2 premiers entre eux

Bezout : $\exists A, B \in \mathbb{Q}[X]$ tq $A\times X + B\times(X^3-X+2)=1$

$\rightsquigarrow \overline{A(X)} \times \overline{X} = \overline{1}$

$X^3-X+2 = X(X^2-1)+2$

$\frac{1}{2}(X^3-X+2) + \frac{1}{2}(1-X^2)X = 1$

3) $1+y+y^2 \in \mathbb{Q}[X]$

$(\bar{1}+\bar{X}+\bar{X}^2)(a+b\bar{X}+c\bar{X}^2) = \bar{1}$

$\Leftrightarrow a+(a+b)\bar{X}+(a+b+c)\bar{X}^2+\underset{\sim\sim\sim\sim\sim}{(c+b)\bar{X}^3+c\bar{X}^4} = \bar{1}$

$(\overline{X^3-X+2} = \bar{0} \Leftrightarrow \bar{X}^3 = \bar{X}-\bar{2})$

$\Leftrightarrow a+(c+b)\bar{X}+(a+b+c)\bar{X}^2+(c+b)(\bar{X}-2)+c\bar{X}(\bar{X}-2) = 1$

$\Leftrightarrow a-2c-2b+(a+2b-c)\bar{X}+(a+b+2c)X^2 = 1$

$\begin{cases} a-2c-2b=1 \\ a+2b-c=0 \\ a+b+2c=0 \end{cases}$ suite en exo ____ .

Ex 24

1) $P = X^5 + 121 X^4 + 1221 X^3 + 12221 X^2 + 122221 X + 222222 \in \mathbb{Q}[X]$

$c(P) = 1$ donc par Gauss, on regarde la réductibilité dans $\mathbb{Z}[X]$.

si $P = Q \times R$:

alors dans $\mathbb{Z}/_{11\mathbb{Z}}[X]$: $\underset{\overline{1}X^5}{\underset{\shortparallel}{\overline{P}}} = \overline{Q} \times \overline{R}$

Donc $Q = \alpha X^m + \underbrace{--- + a_0}_{\text{termes nuls mod } 11}$ $\qquad n + m = 5$

$R = \beta X^n + \underbrace{-- -- + b_0}_{\text{termes nul mod } 11}$

$Q(0) = a_0$ et $R(0) = b_0$ multiples de 11.

donc $P(0) = Q(0)\, R(0)$ est multiple de 11^2

Absurde car 222222 n'est pas multiple de 11^2

$\rightsquigarrow$ On a refait Eisenstein.

2) Dans $\mathbb{C}[X, Y]$

$f = X^2Y^3 + X^2Y^2 + Y^3 - 2XY^2 + Y^2 + X - 1$

$\in (\mathbb{C}[X])[Y]$ ou $\in (\mathbb{C}[Y])[X]$.

On suppose : $f = P \times Q \in \mathbb{C}[X][Y]$

$P = p_1 + p_2 Y + p_3 Y^2$ et $Q = q_1 + q_2 Y$

où $p_i, q_i \in \mathbb{C}[X]$

$f = (X^2+1)\, Y^3 + \underbrace{(X^2 - 2X + 1)}_{(X-1)^2} Y^2 + X - 1$

Ex 24 (2)

$f = P \times Q = (p_1 + p_2 Y + p_3 Y^2)(q_1 + q_2 Y)$

$= p_1 q_1 + (p_1 q_2 + p_2 q_1) Y + (p_2 q_2 + q_1 p_3) Y^2 + p_3 q_2 Y^3$

$= X-1 + 0 \cdot Y + (X-1)^2 Y^2 + (X^2+1) Y^3$

$$\begin{cases} p_1 q_1 = X-1 \\ p_1 q_2 + p_2 q_1 = 0 \\ p_2 q_2 + q_1 p_3 = (X-1)^2 \\ p_3 q_2 = X^2+1 \end{cases}$$

$\Rightarrow p_1 = 1$ et $q_1 = X-1$
ou $p_1 = X-1$ et $q_1 = 1$

Cas : $q_1 = X-1$ et $p_1 = 1$

$(L2)$: $q_2 = -(X-1) p_2$

$(L4)$: $p_3 \times (-(X-1)) \times p_2 = X^2+1$ Absurde

cas : $p_1 = X-1$ $q_1 = 1$

$(L2)$: $p_2 = -(X-1) q_2$

$(L3)$: $-(X-1) q_2^2 + p_3 = (X-1)^2$

D'où $X-1 \mid p_3$

ce implique $X-1 \mid X^2+1$ Absurde.

(2) Dans $\mathbb{F}_2[X,Y]$: $f = X^2Y^3 + X^2Y^2 + Y^3 \underbrace{- 2XY^2}_{0} + Y^2 + X - 1$

$f = (X^2+1) Y^3 + (X^2+1) Y^2 + X + 1$

(Dans $\mathbb{F}_2[X,Y]$: $(X+1)^2 = X^2 + \cancel{2X} + 1 = X^2+1$

$f = (X+1) \times ((X+1) Y^3 + (X+1) Y^2 + 1)$

f est réductible.

Ex 24 (3)

$f = Y^7 + Y^6 + 7Y^4 + XY^3 + 3X^2Y^2 - 5Y + X^2 + X + 1 \in \mathbb{Q}[X,Y]$

$= (3Y^2+1)X^2 + (Y^3+1)X + Y^7 + Y^6 + 7Y^4 - 5Y + 1$

$P = aX + b$, $Q = cX + d$ où $a,b,c,d \in \mathbb{Q}[Y]$

$PQ = acX^2 + (ad+bc)X + bd$

$f = PQ \iff \begin{cases} ac = 3Y^2+1 \leftarrow \text{irréd. dans } \mathbb{Q}[Y] \\ ad + bc = Y^3+1 \\ bd = Y^7 + Y^6 + 7Y^4 - 5Y + 1 \end{cases}$

On a : (symétrique en a et c) : $a = 1$ et $c = 3Y^2+1$

$(L2)$: $d + b\times(3Y^2+1) = Y^3+1$

Notons $\delta = \deg(d)$, $\beta = \deg(b)$. $(L3)$ dit : $\delta + \beta = 7$

$\begin{cases} \delta = 0, \beta = 7 \\ \delta = 1 \quad \beta = 6 \\ \delta = 2 \quad \beta = 5 \end{cases}$ $\quad \delta = 3, \beta = 4 \quad \delta = 4, \beta = 3 \quad \delta = 5 \quad \beta = 2$ $\quad \delta = 6 \quad \beta = 1 \quad \delta = 7, \beta = 0$

L'analyse des degrés dans (L2) montre que L2 est impossible.

f est bien irréductible.

Ex 25 $I = \langle X^2 + Y^2 + 1 \rangle$

Indication : considérer $J = \langle X^2+1, Y \rangle$

$\underset{\uparrow}{I \subseteq} J \underset{\uparrow}{\subseteq} \mathbb{C}[X,Y]$

stricts ?

$J \neq \mathbb{C}[X,Y]$: Si $1 \in J$ alors $\exists A, B \in \mathbb{C}[X,Y]$

tq $1 = A \times (X^2+1) + B \times Y$

On évalue en $X = i$ et $Y = 0$ et

on obtient $1 = 0$ [Dans $\mathbb{Z}/2\mathbb{Z}$, $X = 1$ et $Y = 0$]

$I \subsetneq J$: Si on avait $Y \in I$ alors $\exists A \in \mathbb{C}[X,Y]$ tq

$Y = A \times (X^2 + Y^2 + 1)$. Egalité impossible à cause du degré en Y.

I n'est pas max.

Ex 26

1) F. Euclidien $\Rightarrow$ principal et $\mathbb{R}(X,Y)$ non principal.
pourquoi ? $I = \langle X, Y \rangle$.
Si I est principal : $\langle X, Y \rangle = \langle P \rangle$

$$X = A \times P \leftarrow \deg_Y(X) = 0 \text{ donc } \deg_Y(P) = 0$$
$$Y = B \times P \leftarrow \deg_X(Y) = 0 \text{ donc } \deg_X(P) = 0$$

$P = c \in \mathbb{R}$. Donc $c = Q_1 \times X + Q_2 \times Y$
on fait $X = Y = 0$: $c = 0$ Absurde.

2) F (voir exo 5)

3) $\mathbb{Z}$ factoriel. $\rightsquigarrow \mathbb{Z}[X]$ factoriel.
V $\rightsquigarrow \mathbb{Z}[X][Y]$ aussi
$= \mathbb{Z}[X,Y]$

4) F (exemple $\mathbb{Z}[X]$)

5) V (voir le cours)

6) Euclidien $\Rightarrow$ principal $\Rightarrow$ factoriel

A factoriel : $\rightarrow$ un élément irréd.

$$\forall x \in A, \quad x = \underset{\text{inversible}}{u} \times q_1^{\alpha_1} \times \dots \times q_r^{\alpha_r}, \quad q_i \text{ irréd.}$$

et la décomp. est unique à l'ordre près des termes

Ex 27 $f : \underset{\text{corps}}{K} \longrightarrow A$, $f \neq 0$.

f inject $\Leftrightarrow \ker f = \{0\}$.
Soit $x \in \ker(f)$. But $x = 0$. Supposons $x \neq 0$.
Dans x est inversible.

$$f(x \cdot x^{-1}) = f(1_K) = 1_A$$
$$\| $$
$$f(x) f(x^{-1}) = 0 \times f(x^{-1}) = 0$$

Absurde