

Éléments de corrections TD 1

Ex 6.

q1) La DE (division euclidienne) dans l'anneau $A = \mathbb{R}[x]$ permet de voir que ce dernier est un anneau euclidien en prenant pour stathme le degré des polynômes. En effet si $(S, T) \in (\mathbb{R}[x])^2 \setminus \{(0)\}$ alors $\exists (Q, R) \in (\mathbb{R}[x])^2$ tq

$$S = TQ + R \text{ et } R = 0 \text{ ou } \deg R < \deg T.$$

$$\begin{aligned} \text{Donc } \deg : \mathbb{R}[x] \setminus \{0\} &\rightarrow \mathbb{N} \text{ et } \\ P &\longmapsto \deg P \end{aligned}$$

stathme euclidien (la condition $\deg(T) \leq \deg(S)$ si $(S, T) \in (\mathbb{R}[x] \setminus \{0\})^2$ est facilement vérifiée).

De plus ne y a dans \mathbb{R} pas annulation du couple (Q, R) : si $S = TQ + R' = TQ + R$ on a $T(Q' - Q) = R - R'$, si $Q' - Q \neq 0$ on a $\deg T(Q' - Q) \geq \deg T$ et $\deg(R - R') < \deg T$. (par convention $\deg 0 = -\infty$). Donc $Q' - Q = 0$ et $R - R' = 0$, c'est à dire $Q = Q'$ et $R = R'$.

$$\begin{array}{r} x^3 - 2x^2 - 2x - 3 \\ - x^3 + 2x^2 + 3x \\ \hline x - 3 \end{array} \quad \left| \begin{array}{r} x^2 - 2x - 3 \\ \hline x \end{array} \right.$$

$$\text{donc } P_1 = xP_2 + (x-3)$$

$$Q_1 = x, R_2 = x-3$$

Exemple

$$\begin{array}{r} x^2 - 2x - 3 \\ -x^2 + 3x \\ \hline x - 3 \\ -x + 3 \\ \hline 0 \end{array} \quad \left| \begin{array}{c} x-3 \\ x+1 \end{array} \right.$$

done

$$P_2 = (x+1) R_2 + R_3 \quad \text{avec } Q_2 = x+1, R_3 = 0$$

Cela signifie que $R_2 = x-3 \Rightarrow \text{pgcd}(P_1, P_2)$.

q3) On a $P_2(x) = (x-3)(x+1)$ et

$$\begin{array}{r} x^3 - 2x^2 - 2x - 3 \\ -x^3 + 3x^2 \\ \hline x^2 - 2x - 3 \\ -x^2 + 3x \\ \hline x - 3 \\ -x + 3 \\ \hline 0 \end{array} \quad \left| \begin{array}{c} x-3 \\ x^2 + x + 1 \end{array} \right.$$

$$\text{donc } P_1 = (x-3)(x^2 + x + 1).$$

On sait que $x^2 + x + 1$ est irreductible

dans $\mathbb{R}[x]$ (de racines complexes j et \bar{j}).

Par conséquent on retrouve $\text{pgcd}(P_1, P_2) = x-3$

Ex 5.

Pour $P_1 = 3x^5 + 4x^2 + 1$ et

$P_2 = x^2 + 2x + 3$ on obtient

$$\begin{array}{r}
 P_0 = 3x^5 + 4x^2 + 1 \\
 - 3x^5 - 6x^4 - 9x^3 \\
 \hline
 -6x^4 - 9x^3 + 4x^2 + 1 \\
 + 6x^4 + 12x^3 + 18x^2 \\
 \hline
 3x^3 + 22x^2 + 1 \\
 - 3x^3 - 6x^2 - 9x \\
 \hline
 16x^2 - 32x - 48 \\
 - 16x^2 - 32x - 48 \\
 \hline
 0
 \end{array}
 \quad \left| \begin{array}{l} x^2 + 2x + 3 = R_1 \\ 3x^3 - 6x^2 + 3x + 16 = Q_1 \end{array} \right.$$

donc $P_1 = Q_1 R_1 + R_2$

Si $\text{car } K = 41$ alors $R_2 = -6 = 35$ donc

$\text{pgcd}(P_1, P_2) = 1$ et l'algorithme d'Euclide se termine juste par

$$P_2 = Q_2 \cdot R_2 + R_3 \quad \text{avec } R_3 = 0, Q_2 = \frac{P_2}{35}.$$

Si $\text{car } K \neq 41$ on peut effectuer la DE
implémentaire

$$P_2 = Q_2 R_2 + R_3 \quad \text{avec } Q_2 = -\frac{x}{41} - \frac{35}{1681}$$

$$\text{et } R_3 = \frac{3398}{1681} = \frac{2 \times 1699}{1681}$$

Si $\text{car } K = 2$ ou $\text{car } K = 1699$ alors $R_3 = 0$

et $\text{pgcd}(P_1, P_2) = R_2$

Si $\text{car } K \neq 2$ et $\text{car } K \neq 1699$ on a de

encore $\text{pgcd}(P_1, P_2) = 1$ et une dernière

étape dans l'algorithme d'Euclide $R_2 = R_3 \cdot \frac{P_2}{R_3} + R_4$
avec $R_4 = 0$.

$$\text{Si } P_1 = 3x^5 + 2x^4 - x^2 + 1 \text{ et}$$

$$P_2 = x^3 + x + 2 \text{ sur a}$$

$$P_1 = Q_1 P_2 + R_1 \text{ avec } Q_1 = 3x^2 + 2x - 3$$

$$\text{et } R_1 = -9x^2 - x + 7$$

$$\text{Si } \text{car} K = 3 \text{ alors } Q_1 = 2x, R_1 = 2x + 1$$

$$\text{et } P_2 = Q_2 R_2 + R_3 \text{ avec } Q_2 = 2x^2 + 2x + 1$$

$$R_3 = 1$$

$$\text{done pgcd}(P_1, P_2) = 1$$

$$\text{Si } \text{car} K \neq 3 \text{ sur a } P_2 = Q_2 R_2 + R_3$$

$$\text{avec } Q_2 = -\frac{x}{9} + \frac{1}{81} \quad R_3 = \frac{145x}{81} + \frac{155}{81}$$

$$(145 = 5 \times 29)$$

$$\text{Si } \text{car} K = 5 \text{ alors } R_3 = 0 \text{ et}$$

$$\text{pgcd}(P_1, P_2) = R_2 = x^2 + 4x + 2$$

$$\text{Si } \text{car} K = 29 \text{ alors } R_3 = \frac{10}{81} \text{ et}$$

$$\text{pgcd}(P_1, P_2) = 1$$

$$\text{Si } \text{car} K \neq 5 \text{ et } \text{car} K \neq 29 \text{ alors}$$

$$R_2 = Q_3 R_3 + R_4 \text{ avec } Q_3 = -\frac{729}{145}x + \frac{4050}{841}$$

$$\text{et } R_4 = -\frac{1863}{841} \quad (1863 = 3^4 \times 23)$$

$$\text{Si } \text{car} K = 23 \text{ alors } R_4 = 0 \text{ et } \text{pgcd}(P_1, P_2) = R_3$$

$$\text{Si } \text{car} K \neq 23 \text{ alors } \text{pgcd}(P_1, P_2) = 1.$$

$$\left(\text{et il y a encore une étape } R_3 = R_4 \cdot \frac{Q_4}{R_4} + R_5 \right)$$

avec $R_5 = 0$

Si on pose $P_1 = x^4 + x^3 + x - 2$ et
 $P_2 = x^2 - 2x + 4$ on a

$$P_1 = Q_1 P_2 + R_2 \quad \text{avec} \quad Q_1 = x^2 + x - 2$$

$$R_2 = -7x + 6$$

Si $\operatorname{car} k = 7$ on a $\operatorname{pgcd}(P_1, P_2) = 1$

Si $\operatorname{car} k \neq 7$ on a

$$P_2 = Q_2 R_2 + R_3 \quad \text{avec} \quad Q_2 = -\frac{x}{7} + \frac{8}{49}$$

$$R_3 = \frac{148}{49}$$

$$\text{et } 148 = 2^2 \times 37.$$

Si $\operatorname{car} k = 2$ ou $\operatorname{car} k = 37$ alors $R_3 = 0$

donc $\operatorname{pgcd}(P_1, P_2) = R_2$

Si non $\operatorname{pgcd}(P_1, P_2) = 1$ on va vite jeter

à reporter à l'étape $R_2 = Q_3 R_3 + R_4$

avec $R_4 = 0$ et $Q_3 = \frac{R_2}{R_3}$.

Ex 9.

Si a une racine multiple de p alors

$$P(x) = (x-a)^\alpha Q(x) \quad \text{avec} \quad \alpha \geq 2 \quad \text{et} \quad Q(a) \neq 0.$$

$$\begin{aligned} \text{Donc} \quad P'(x) &= \alpha(x-a)^{\alpha-1} Q(x) + (x-a)^\alpha Q'(x) \\ &= (x-a)^{\alpha-1} (\alpha Q(x) + (x-a) Q'(x)) \end{aligned}$$

avec $\alpha-1 \geq 1$. On a alors $(x-a) \mid \operatorname{pgcd}(P, P')$

Donc P et P' ne sont pas premiers entre eux.

D'autre part $\operatorname{pgcd}(P, P') = D$ et $\deg D \geq 1$

alors il existe $t, q \in \mathbb{C}$ tq $(x-a) \mid D$ ce qui

signifie que $(x-a) \mid p$ et $(x-a) \mid p'$!

Ecrivons $p(x) = (x-a)^\alpha q(x)$ avec $\alpha \geq 1$
et $q(a) \neq 0$.

On a $p'(x) = (x-a)^{\alpha-1} (\alpha q(x) + (x-a) q'(x))$

Comme $Q(a) \neq 0$, l'évaluation de

$$\alpha Q(x) + (x-a) Q'(x) \text{ en } a \text{ est non nulle}$$

donc, vu que $x \mid p'$, on trouve que
 $\alpha-1 \geq 1$. Cela signifie $\alpha \geq 2$ et a
racine multiple de p .

D'où $\text{pgcd}(p, p') = 1 \Leftrightarrow p$ n'a que des
racines simples.

Si $\deg p < 1$ alors $p' = 0$ et $p' \mid p$ signifie
 $p = p' = 0$.

Si $\deg p = 1$ alors p' est une constante et
on a bien $p' \mid p$.

Si $\deg p > 1$ alors not $m = \deg p$.

On écrit $p = p' \cdot Q$ avec $Q \in \mathbb{C}[x]$, $\deg Q = 1$
(vu que $\deg p' = \deg p - 1$).

Ecrivons $Q = \alpha x + \beta$, $\alpha \neq 0$.

Par conséquent

$p = p' \cdot (\alpha x + \beta)$ et une
racine de p , distincte de $-\frac{\beta}{\alpha}$, admet
la même multiplicité dans p' et dans p
ce qui n'est pas possible. Ainsi la seule
racine de p est $-\frac{\beta}{\alpha} = a$.

Et ce cas convient car si $P = \lambda(x-a)^n$
est un polynôme avec une seule racine,
alors $P' = \lambda n(x-a)^{n-1}$ qui divise bien P .

Si on regarde les mêmes questions sur $\mathbb{R}[x]$
on aura toujours certaines implications.

Par exemple si P a une racine multiple
alors $\text{pgcd}(P, P') \neq 1$ sûrement.

Donc si $\text{pgcd}(P, P') = 1$ alors P n'a que
des racines complexes simples, donc en particulier
que des racines réelles simples.

En outre si P n'a que des racines réelles
simples mais il a des racines complexes multiples
on ne peut pas conclure à ce que $\text{pgcd}(P, P') = 1$
(car le pgcd verra le même qu'il soit
calculé dans $\mathbb{C}[x]$ ou dans $\mathbb{R}[x]$).

Par exemple pour $P = (x^2 + x + 1)^2 X$ on a
bien 0 racine simple mais $P' = (x^2 + x + 1)(3x^2 + 3x + 1)$
donc $\text{pgcd}(P, P') = x^2 + x + 1 \neq 1$.

Sur $P' | P$ on trouve les mêmes polynômes.

Si on se place sur $K = \mathbb{F}_p$ d'autres anomalies
apparaissent

Si P a une racine multiple, disons 0,
alors $P = x^n Q$ avec $Q(0) \neq 0$, $n \geq 2$

$$\text{et } P' = nx^{n-1}Q + x^nQ'$$

Si $p \mid m$ alors $P' = x^nQ'$ et donc
 $\text{pgcd}(P', P) \neq 1$. Si $p \nmid m$ alors
 $\text{pgcd}(P', P) \neq 1$ comme ci-dessus.

Donc $\text{pgcd}(P, P') = 1$ implique encore que P
n'a que des racines simples dans \mathbb{F}_p .

Mais si par exemple $P = (x^2+1)^2$ dans $\mathbb{F}_3[x]$
on a $P' = 2(x^2+1)(2x)$ et $\text{pgcd}(P, P') = x^2+1$
donc que P n'a pas de racine dans \mathbb{F}_3 .

On voit par contre que les racines peuvent
avoir la même multiplicité dans P et dans P'
comme le montre l'exemple

$$P(x) = x^n(x+1), \quad P'(x) = x^n \quad | P(x)$$

Ainsi $P = x^n$ et sa dérivée nulle donc
 P' ne divise pas P dans ce cas.

Ex. 12.

Notons $a = bq + r$ la DE de a par b

$$\text{On a } x^a - 1 = x^r(x^{bq} - 1) + x^r - 1$$

Puisque $x^{bq} - 1 \mid x^r(x^{bq} - 1)$ et $r < b$
le reste de la DE de $x^a - 1$ par $x^{bq} - 1$ est
 $x^r - 1$.

On peut supposer que $a \geq b$. En effectuant
l'algorithme d'Euclide de a par b on
obtient $n_0 \geq a \geq n_1 = q \geq n_2 \geq \dots \geq n_m = d$
tel que, pour $2 \leq j \leq m$, $n_j \mid n_{j-1}$ et le reste
de la DE de n_{j-2} par n_{j-1} est $n_{j-1} \mid n_{j-1}$.

C'est le pgcd de a et b .

On déduit que le reste de la DE de
 $x^{n_{j-2}} - 1$ par $x^{n_{j-1}} - 1$ est $x^{n_j} - 1$; de plus
 $x^{n_{m-1}} \mid x^{n_m} - 1$. D'après l'algorithme
d'Euclide (par exemple dans $\mathbb{Q}[X]$), mais

tous les polynômes concernés sont dans $\mathbb{Z}[X]$)
 $\text{pgcd}(x^a - 1, x^b - 1) = x^d - 1$.

On peut aussi dire que pour une relation
de Bézout $am + bn = d$ on ne peut pas
avoir $m, n > 0$ (sauf si $a=0$ ou $b=0$).

On peut donc, quitte à échanger a et b ,

écrire dans le , m, n, d, alors

$$(x^{am-1}) - x^d(x^{bm-1}) = x^d - 1$$

puisque $x^{a-1} \mid x^{am-1}$ et $x^{b-1} \mid x^{bm-1}$

cette égalité et une relation de Bezout

$$\text{On a deduit que } \operatorname{pgcd}(x^{a-1}, x^{b-1}) \mid x^d - 1$$

Mais comme $x^d - 1 \mid \operatorname{pgcd}(x^{a-1}, x^{b-1})$

$$\text{on a bien } x^d - 1 = \operatorname{pgcd}(x^{a-1}, x^{b-1}).$$

Finalement on peut aussi regarder les racines complexes des polynômes : les racines communes de x^{a-1} et x^{b-1} sont les w ∈ C tq $w^a = w^b = 1$.

Si $d = am + bn$ alors $w^d = 1$ donc les racines communes de x^{a-1} et x^{b-1} sont les racines de $x^d - 1$. Donc $\operatorname{pgcd}_{\mathbb{C}}(x^{a-1}, x^{b-1}) = x^d - 1$

Or ce pgcd est le même sur K on a donc

s'il y avait un plus grand sur K, il serait

réalisable sur C aussi, donc c'est finalement le pgcd sur K aussi.

Ex 7.

On a $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ sur \mathbb{C} et
 \mathbb{R} et irreductible sur \mathbb{Q}
(car $\sqrt{2}$ n'est pas rationnel)

$x^2 + 2 = (x - i\sqrt{2})(x + i\sqrt{2})$ sur \mathbb{C} et
irreductible sur \mathbb{R} (donc sur \mathbb{Q}) car
pas de racine réelle.

$x^2 + x + 1 = (x - j)(x - \bar{j})$ sur \mathbb{C} et
irreductible sur \mathbb{R} (donc sur \mathbb{Q}) car
pas de racine réelle

$$x^4 - 4 = (x^2 - 2)(x^2 + 2) = (x - \sqrt{2})(x + \sqrt{2})(x - i\sqrt{2})(x + i\sqrt{2})$$

sur \mathbb{C}
 $x^4 - 4 = (x - \sqrt{2})(x + \sqrt{2})(x^2 + 2)$ sur \mathbb{R}
d'après ci-dessus

$x^4 - 4 = (x^2 - 2)(x^2 + 2)$ sur \mathbb{Q} d'après
ci-dessus

$x^4 + 4 = (x - (1+i))(x - (1-i))(x + (1+i))(x + 1-i)$
sur \mathbb{C} car les racines 4-ièmes de -4 sont
 $\pm 1 \pm i$

$$\begin{aligned} x^4 + 4 &= x^4 + 4x^2 + 4 - 4x^2 = (x^2 + 2)^2 - 4x^2 = \\ &= (x^2 + 2x + 2)(x^2 - 2x + 2) \text{ sur } \mathbb{R} \text{ et} \\ &\quad \text{sur } \mathbb{Q} \text{ car on deux} \end{aligned}$$

polynômes sont irréductibles sur \mathbb{Q} (dans $\mathbb{Q}[x]$)
 car qu'ils n'ont pas de racine réelle
 $(x^2 - 2x + 2 = (x - (1+i))(x - (1-i)))$

$$\text{et } x^2 + 2x + 2 = (x + (1+i))(x + 1-i)$$

$$x^4 - x^2 + 1 = \frac{x^6 + 1}{x^2 + 1} = (x - i\sqrt{3}) (x - \bar{i}\sqrt{3})(x + i\sqrt{3})(x + \bar{i}\sqrt{3})$$

sur \mathbb{C}

$$\text{où } i\sqrt{3} = -\frac{\sqrt{3}}{2} - \frac{1}{2}i, \bar{i}\sqrt{3} = -\frac{\sqrt{3}}{2} + \frac{1}{2}i$$

$$-i\sqrt{3} = \frac{\sqrt{3}}{2} + \frac{1}{2}i, -\bar{i}\sqrt{3} = \frac{\sqrt{3}}{2} - \frac{1}{2}i$$

sont les racines 6-èmes de -1, sauf $\pm i$

qui sont les racines 2-èmes de -1.

$$\begin{aligned} x^4 - x^2 + 1 &= (x^2 + \sqrt{3}x + 1)(x^2 - \sqrt{3}x + 1) \\ &= (x^2 + 1)^2 - 3x^2 \quad \text{sur } \mathbb{R} \end{aligned}$$

et $x^4 - x^2 + 1$ est irréductible sur \mathbb{Q}
 car pas de racine sur \mathbb{Q} et pas de
 décomposition en produit de 2 facteurs de
 degré 2 sur \mathbb{Q} (car elle serait valable sur
 \mathbb{R} , et elle sur \mathbb{R} n'est pas sur \mathbb{Q}).

On peut montrer aussi le fait qu'il
 s'agit de Φ_{12} le 12ème polynôme
 cyclotomique qui est irréductible dans $\mathbb{Z}[x]$
 donc dans $\mathbb{Q}[x]$.

Ex 16

On a $P(x)$ réductible $\Leftrightarrow P(x) = P_1(x)P_2(x)$

avec $\deg P_1 < \deg P$, $\deg P_2 < \deg P$ (\Leftarrow)

$P(x+a) = P_1(x+a)P_2(x+a)$ avec

$\deg P_1 = \deg P_1(x+a) < \deg P(x+a) = \deg P$

$\deg P_2 = \deg P_2(x+a) < \deg P(x+a) = \deg P$

$\Rightarrow P(x+a)$ réductible.

On a $\exists P(x)=x$ un exemple de polynôme irreductible tel que $P(x^2)=x^2$ ne l'int pas.

Ex 17

1) red : $\mathbb{Z}[x] \rightarrow \mathbb{Z}/p\mathbb{Z}[x]$ est bien

$$a_0 + \dots + a_n x^n \mapsto \bar{a}_0 + \dots + \bar{a}_n x^n$$

un morphisme d'anneaux car

$$\text{red}(P+Q) = \text{red}(P) + \text{red}(Q)$$

$$\text{red}(PQ) = \text{red}(P) \text{ red}(Q)$$

$$\text{red}(\lambda) = \bar{\lambda}$$

2) Si P est réductible dans $\mathbb{Z}[x]$ alors

$$P = ST \text{ avec } S, T \in \mathbb{Z}[x] \text{ et } S, T$$

non constants car P est premier (de

contenu égal à 1 donc $\text{rged}(\text{coeff de } f) = 1$).

On a pour s_α, t_β les coefficients dominants de S et respectivement T la relation $s_\alpha t_\beta = r_{\alpha+\beta}$

avec $r_{\alpha+\beta}$ le coefficient dominant de P .

Comme $r \neq r_{\alpha+\beta}$ on a également $r \neq s_\alpha$ et

$r \neq t_\beta$ donc $\text{red}(P) = \text{red}(S)\text{red}(T)$ et

$\deg \text{red}(f) = \deg P$, $\deg S = \deg \text{red}(S)$
et $\deg T = \deg \text{red}(T)$.

Donc $\deg \text{red}(S) < \deg \text{red}(P)$ et

$\deg \text{red}(T) < \deg \text{red}(P)$ ce qui

signifie que $\text{red}(P)$ est irréductible.

Par conséquent $\text{red}(P)$ irréductible dans $\mathbb{F}_p[x]$
implique P irréductible dans $\mathbb{K}[x]$ (et alors
d'après un résultat du cours on a aussi P irréductible
dans $\mathbb{Q}[x]$.)

Ce critère s'appelle critère d'irréductibilité
par réduction mod P .

On note $\text{red}(f) = \overline{f}$ en général.

3) Le réciproque est faux : par exemple le polynôme $x^4 + 1$ est irréductible dans $\mathbb{Z}[x]$ (et dans $\mathbb{Q}[x]$) mais est réductible dans tous les $\mathbb{F}_p[x]$ avec p premier.

En effet $x^4 + 1 = (x^2 - \sqrt{-1}x + 1)(x^2 + \sqrt{-1}x + 1)$
 n'a pas de racine réelle et sa décomposition en irréductibles de $\mathbb{R}[x]$ n'est pas valable dans $\mathbb{Q}[x]$. Comme il est unitaire (donc premier) cela revient au même que l'irréductibilité dans $\mathbb{Z}[x]$.

Ensuite si $p=2$, $x^4 + 1 = (x^2 + 1)^2 = (x+1)^4$ dans $\mathbb{F}_2[x]$.

$$\text{Si } p \neq 2 \text{ on peut écrire } x^4 + 1 = x^4 - (-1)$$

$$x^4 + 1 = (x^2 - 1)^2 - (-2x^2) = (x^2 + 1)^2 - (2x^2)$$

Si -1 est un carré dans \mathbb{F}_p , on n'a 2, on -2 sont des carrés dans \mathbb{F}_p la décomposition est immédiate.

On $(-1)(-2) \cdot 2 = 4$ est toujours un carré dans \mathbb{F}_p

(A) On sait que le produit de 2 non carrés est un carré et que le produit d'un carré avec un non carré est un non carré, donc si les 3 sont des non carrés on aboutit à une contradiction.

$$\text{En effet si } \epsilon: \mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times \text{ et} \\ x \longmapsto x^2$$

la morphisme de groupes multiplicatif de passage au carré, alors (pour $p \geq 2$) on a
 l'ensemble $\{\pm 1\}$ et donc l'ensemble des carrés
 Zurc est un sous-groupe d'indice 2
 de \mathbb{F}_p^\times , isomorphe à $\mathbb{F}_p^\times / \{\pm 1\}$.

En choisissant un non-carré n on a
 donc $\mathbb{F}_p^\times = \text{Zurc} \sqcup n \cdot \text{Zurc}$ et
 l'affirmation (\Leftarrow): $n \cdot k^2 \cdot n \cdot l^2 = (n \cdot k \cdot l)^2$, $n \cdot k \cdot l \notin \text{Zurc}$
 C'est ainsi que l'on aboutit au symbole de
 Legendre $\left(\frac{a}{p}\right) \in \begin{cases} 0 & \text{si } p \mid a \\ 1 & \text{si } a \equiv k^2 \pmod{p}, k \in \mathbb{Z} \\ -1 & \text{si } a \text{ n'est pas un carré} \\ & \text{modulo } p \end{cases}$

$$\text{qui est multiplicatif } \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Avec ce symbole on peut donc écrire

$$\left(\frac{-1}{p}\right)\left(\frac{-2}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{4}{p}\right) = 1 + (-1)^3 = \left(\frac{-1}{p}\right)\left(\frac{-2}{p}\right)\left(\frac{2}{p}\right)$$

$$\text{avec l'hypothèse } \left(\frac{-1}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right) = -1.$$

Si le contenu de P n'est plus 1 on ne peut plus conclure car par exemple $3x+3$ est réductible

dans $\mathbb{K}[x]$ et $\overline{3x+3} = x+1$ est irréductible
dans $\mathbb{F}_2[x]$.

On peut montrer par contre que P est irréductible
dans $\mathbb{Q}[x]$ en écrivant $P = c(P) \tilde{P}$ avec \tilde{P}
primitif dans $\mathbb{K}[x]$. Alors $\tilde{P} = \overline{c(P)} \tilde{\tilde{P}}$ et $\overline{c(P)} \neq 0$
dans \mathbb{F}_p car $r \nmid c(P)$. Donc $r \nmid \tilde{P}$ et ainsi dans $\mathbb{F}_p[x]$, $\tilde{\tilde{P}}$ aussi.

$$4) \text{ On a } \overline{x^4 + 10x^3 + 7} = x^4 + 1 \text{ dans } \mathbb{F}_2[x] \\ = (x+1)^4$$

donc on ne peut pas utiliser $p=2$.

Regardons $\overline{x^4 + 10x^3 + 7} = x^4 + x^3 + 1 \in \mathbb{F}_3[x]$

On 1 est racine de ce polynôme et on ne
peut pas utiliser $p=3$ non plus.

Soit $\overline{x^4 + 10x^3 + 7} = x^4 + 2 \in \mathbb{F}_5[x]$.

Ce polynôme n'a pas de racine dans \mathbb{F}_5 car
 $(\pm 1)^4 + 2 = 3 \approx (\pm 2)^4 + 2$ car $(\pm 2)^2 = -1$.

Si $(x^2 + \alpha x + p)(x^2 + \beta x + \gamma) = x^4 + 2$

$$\text{on a } \begin{cases} \alpha + \beta = 0 \\ \beta + \gamma + \alpha\beta = 0 \\ \alpha\gamma + \beta\gamma = 0 \\ \beta\gamma = 2 \end{cases} \Rightarrow \begin{cases} \gamma = -\alpha \\ \alpha^2 = \beta + \gamma \\ \alpha(\gamma - \beta) = 0 \\ \beta\gamma = 2 \end{cases}$$

$$\Rightarrow \begin{cases} \alpha = \beta = 0, \beta = -\gamma, \beta^2 = -2 \\ \text{impossible car } 0^2 = 0, (\pm 1)^2 = 1, (\pm 2)^2 = -1 \end{cases}$$

$$\begin{cases} \alpha \neq 0 \neq \beta, \gamma = \beta, \beta^2 = 2 \text{ impossible} \end{cases}$$

Donc x^4+2 est irréductible dans $\mathbb{F}_5[x]$

et par conséquent x^4+10x^3+7 est irréductible sur $\mathbb{Z}[x]$ (donc sur \mathbb{Q} , d'après le cours)

Regardons $\overline{x^4 \pm x^3 + 2x + 1} = x^4 + x^3 + 1 \in \mathbb{F}_2[x]$.

Le polynôme n'a pas de racines dans \mathbb{F}_2 .

De plus le seul polynôme irréductible de degré 2 de $\mathbb{F}_2[x]$ est x^2+x+1
(les autres ont tous de racines dans \mathbb{F}_2)

Donc la seule possibilité pour décomposer x^4+x^3+1 en produit de 2 polynômes de degré 2 irréductibles serait

$$x^4+x^3+1 = (x^2+x+1)^2 = x^4+x^2+1.$$

Ceci étant faux, on a bien x^4+x^3+1 irréductible dans $\mathbb{F}_2[x]$ donc

$x^4 \pm x^3 + 2x + 1$ irréductible sur \mathbb{Z} .

D'après le cours, il est aussi irréductible sur \mathbb{Q} .

Ex 19.

a) Le critère de réduction ne montre

rien d'autre que $\bar{P} = x^2+1 = (x+1)^2 \in \mathbb{F}_2[x]$

$$\bar{P} = -x^7 \in \mathbb{F}_3[x] \quad \bar{P} = 2x^7 \in \mathbb{F}_5[x]$$

et le degré est trop élevé pour avoir des réductions dans $\mathbb{F}_p[x]$ avec p premier > 5 .

On peut quand même appliquer ici le critère d'Eisenstein, car pour $p=5$ on

a) $5/45$, $25/45$, $5/15$ et $5/2$.

Donc $2x^7 + 15x^2 - 45$ est irreductible sur \mathbb{Q} . Comme son coefficient est 1, il est aussi irreductible sur \mathbb{Z} .

b) Nous avons déjà regardé le polynôme à l'exercice 17 q4) et l'avons trouvé irreductible sur \mathbb{Q} , et \mathbb{Z} , par réduction modulo 2.

c) On a $P(x) = \frac{2}{9}x^5 + \frac{5}{3}x^4 + x^3 + \frac{1}{3} =$
 $= \underbrace{2x^5 + 15x^4 + 9x^3 + 3}_9$ irreductible sur \mathbb{Q}

(sur \mathbb{Z} la question ne se pose pas car $P(x) \notin \mathbb{Z}[x]$)

si, et seulement si, $Q(x) = 2x^5 + 15x^4 + 9x^3 + 3$ est irreductible sur \mathbb{Q} . C'est le cas d'après le critère d'Eisenstein pour $p=3$.

d) x^n-p est irreductible sur \mathbb{Q} d'après le critère d'Eisenstein pour p le premier égal à son coefficient constant.

e) Il s'agit de $\phi_p = \frac{x^n-1}{x-1}$ le p -ième

polynôme cyclotomique. On regarde $\phi_p(x+1) =$

$$= \frac{(x+1)^n - 1}{x} = \frac{\sum_{k=1}^n \binom{n}{k} x^k}{x} = \sum_{k=1}^n \binom{n}{k} x^{k-1}$$

On $\binom{n}{k}$ pour $1 \leq k \leq n-1$ car

$$\binom{n}{k} \geq \frac{n!}{k!(n-k)!} \text{ et le facteur premier } p$$

de $p!$ ne se simplifie pas au dénominateur.

On peut donc appliquer le critère d'irréductibilité avec p à ce polynôme unitaire de coefficient constant égal à p :

$$\phi_p(x+1) = x^{n-1} + p x^{n-2} + \binom{n}{2} x^{n-3} + \dots + \binom{n}{2} x + p$$

Comme $\phi_p(x+1)$ est irréductible sur \mathbb{Q} , $\phi_p(x)$
l'est aussi (voir par exemple l'exercice 16)

$$2) \text{ On a } P = 6(x^5 + 5x^2 + 2x - 2) = \\ = 6(x+1)(x^4 - x^3 + x^2 + 4x - 2)$$

Écrivons ($\text{car } x^4 - x^3 + x^2 + 4x - 2$ n'a pas de racine $\pm 1, \pm 2$)
donc pas de racine dans \mathbb{K}) $x^4 - x^3 + x^2 + 4x - 2 = (x^2 + ax + b)(x^2 + cx + d)$

avec $a, b, c, d \in \mathbb{K}$.

Alors $b+d=-2$ donc $b=-1, d=2$ ou $b=1, d=-2$

(qu'il faut échanger b et d). Si $b=-1, d=2$, on a

$$a+c=-1, 2-1+ac=+1, 2a-c=4 \quad (\Rightarrow ac=0, a=1, c=-2)$$

alors $a=c=1$. Si $b=1, d=-2$ on a $a+c=-1, -2+ac=1, -2a+c=4$

$$(\Rightarrow -a-1=4, ac=2, c=-1-a \text{ alors car } a \in \mathbb{K}).$$

Donc $x^4 - x^3 + x^2 + 4x - 2$ est irréductible sur \mathbb{K} , et la
décomposition recherchée est $2 \cdot 3 \cdot (x+1)(x^4 - x^3 + x^2 + 4x - 2)$.

Ex 20)

q1) D'après le critère d'Eisenstein appliqué
sur \mathbb{F}_3 on a f irréductible sur \mathbb{Q}
(et sur \mathbb{Z} car multiple)

q2) Un polynôme de degré 3 a toujours une
racine réelle donc f est réductible sur \mathbb{R} .

q3) $\bar{P} = x^3 \in \mathbb{F}_3[x]$ donc \bar{P} est réductible
sur \mathbb{F}_3 .

q4) $\bar{P} = x^3 + x + 1 \in \mathbb{F}_2[x]$ sans racine dans \mathbb{F}_2 .
Donc \bar{P} est irréductible sur \mathbb{F}_2 (et par le
critère de réduction on obtient de nouveau que P
est irréductible sur \mathbb{Q}).

Ex 21

q1) On a $2x+2 = 2(x+1)$ donc
 $\frac{2(x)}{(2x+2)}$ n'est pas unitaire ($\bar{2} \cdot \bar{x+1} = \bar{0}$
mais que $\bar{2} = \bar{0}$ ou $\bar{x+1} = \bar{0}$) et ne peut pas

être un corps.

q2) On a $2x+2$ irréductible sur \mathbb{Q} donc
l'idéal $(2x+2)$ est premier et même maximal
dans $\mathbb{Q}[x]$ ce qui équivaut à $\mathbb{Q}[x]/(2x+2)$
n'étant pas un corps.

q3) Un polynôme de degré 4 et toujours réductible sur \mathbb{Q} donc $(x^4 + x^3 + 2x^2 + 7)$ n'est pas un idéal premier, ce qui signifie que $\mathbb{Q}[x]/(x^4 + x^3 + 2x^2 + 7)$ n'est pas intègre, donc ce n'est pas un corps.

q4) On a $P = x^7 - 12x^4 + 9x^2 - 3$ irréductible sur \mathbb{Q} (et en tant que polynôme unitaire sur \mathbb{K} aussi) par le critère d'Eisenstein avec $p=3$.
 On $\mathbb{K}[x]$ est un anneau factoriel, donc l'idéal $(P) = (x^7 - 12x^4 + 9x^2 - 3)$ est premier et le quotient est un anneau intègre. Mais cet idéal n'est pas maximal car nous trouvons dans l'idéal $(P, 3)$. En effet si $\beta \in (P)$ alors $\beta = P \cdot Q$ avec $Q \in \mathbb{K}[x]$ donc $\deg \beta = 0 = \deg P \cdot Q \geq \deg P = 7$ absurdité.
 Donc $3 \notin (P)$ et $\bar{3}$ n'est pas inversible dans $\mathbb{K}[x]/(P)$: si $\bar{3} \cdot \bar{Q} = \bar{1}$ alors

$$\begin{aligned} P &\mid 3Q - 1 \quad \text{donc } 1 = PR + 3Q \\ &= x^7 \cdot R + 3T \quad \text{dans } \mathbb{K}[x] \quad \text{d'où} \\ &\bar{1} = x^7 \bar{R} \quad \text{dans } \mathbb{F}_3[x] \end{aligned}$$

ce qui signifie que x^7 est inversible dans $\mathbb{F}_3[x]$, alors que les seuls inversibles de $\mathbb{F}_3[x]$ sont les constantes.

$$\text{En fait } \mathbb{K}[x]/(P) \cong \mathbb{F}_3[x]/(\bar{P}) = \mathbb{F}_3[x]/(x^7)$$

qui n'est pas un corps non plus, donc $(3, P)$ n'est pas maximal non plus.

Prouvons la non-isomorphisme : on a un morphisme φ obtenu par composition du morphisme de réduction et la projection canonique

$$\varphi: \mathbb{K}[x] \xrightarrow{\text{red}} \mathbb{F}_3[x] \xrightarrow{\pi} \mathbb{F}_3[x]/(\bar{P})$$

$$Q \longmapsto \bar{Q} \longmapsto [\bar{Q}] \in \text{classe modulo } \bar{P}$$

Alors $3 \in \ker \varphi$ et $p \in \ker \varphi$ donc $(3, p) \subset \ker \varphi$.

Si $Q \in \ker \varphi$ alors $\pi(\bar{Q}) = [0]$ donc $\bar{Q} \in (\bar{P})$ donc

$$\bar{P} \mid \bar{Q} \text{ dans } \mathbb{F}_3[x] \text{ donc } \bar{Q} = \bar{P} \cdot \bar{R} \Leftrightarrow Q = P \cdot R + 3T$$

avec $T \in \mathbb{K}[x]$. On cela signifie exactement que $Q \in (3, p)$

D'où $(3, p) = \ker \varphi$. Or φ est injective car red et π l'ont.

D'après le premier théorème d'isomorphisme on a bien

$$\mathbb{K}[x]/(3, p) \cong \mathbb{F}_3[x]/(\bar{P}) \quad \text{et cela est valable pour}$$

tout nombre premier p , et polynôme P en général sous la

$$\text{forme } \mathbb{K}[x]/(p, q) \cong \mathbb{F}_p[x]/(\bar{P}).$$

Au passage nous avons vérifié que $(3, p) \neq \mathbb{K}[x]$ (car $1 \notin (3, p)$)

Nous pouvons faire de même avec l'idéal $(2, p)$ car $2 \notin (p)$ pour les mêmes raisons de degré et $(2, p) \neq \mathbb{K}[x]$ car $1 \notin (2, p)$. En effet si $1 = PR + 2Q$ on a

$$\bar{1} = \bar{P}\bar{R} \in \mathbb{F}_2[x] \quad \text{donc } \bar{P} \in \mathbb{F}_2[x]^{\times} \text{ car } \deg \bar{P} = 0$$

Or $\bar{P} = x^7 + x^2 + 1$ est de degré 7 dans $\mathbb{F}_2[x]$ d'où une contradiction.

Pour décider si $(2, p)$ est maximal ou pas il faudrait regarder l'irréductibilité de $\bar{P} \in \mathbb{F}_2[x]$...

5) On a que $P = x^7 - 12x^4 + 9x^2 - 3$ est un 3-Eisenstein
 donc P est irréductible sur \mathbb{Q} , donc (P) est un idéal
 premier non nul de $\mathbb{Q}[x]$, donc (P) est maximal
 (car $\mathbb{Q}[x]$ est principal). Donc $\mathbb{Q}(x)/(P)$ est un corps.

6) On a que $P = x^4 + 5x^3 + 2x + 1$ admet pour réduction
 $\tilde{P} = x^4 + x^3 + 1 \in \mathbb{F}_2[x]$ et ce polynôme a été
 montré irréductible sur \mathbb{F}_2 à l'exercice 17, q4.
 Donc P est irréductible dans $\mathbb{Q}[x]$ et $\mathbb{Q}(x)/(P)$ est un
 corps comme à la question 5.

Ex 22. On a p^2 polynômes de degré 2, certains sur \mathbb{F}_p
 qui sont de la forme $x^2 + ax + b$ avec $a, b \in \mathbb{F}_p$.
 Ils font éliminer ceux qui sont produits de $x-\alpha$ avec $x-\beta$
 avec $\alpha, \beta \in \mathbb{F}_p$. C'est à dire $(x-\alpha)^2, \alpha \in \mathbb{F}_p$ (p de car. fini)
 et les $(x-\alpha)(x-\beta), \alpha \neq \beta$ ($\binom{p^2}{2}$ de ceux-là).
 Donc $I(2, p) = \#\{ \text{pol. irréductibles de degré 2 de } \mathbb{F}_p[x] \}$
 $= p^2 - (p + \binom{p^2}{2}) = p^2 - (\binom{p^1}{p} + \binom{p^2}{p}) = p^2 - \binom{p^2}{p+1} =$
 $= p^2 - \frac{\binom{p(p+1)}{2}}{2} = \frac{2p^2 - p^2 - p}{2} = \frac{p^2 - p}{2}.$

Pour calculer $I(3, p) = \#\{ \text{pol. irréductibles de degré 3 de } \mathbb{F}_p[x] \}$

on procède de même :

$$\begin{aligned} I(3, p) &= p^3 - \#\{ (x-\alpha)(x-\beta)(x-\gamma) \mid \alpha \neq \beta \neq \gamma \neq \alpha \} \\ &\quad - \#\{ (x-\alpha)^2(x-\beta) \mid \alpha \neq \beta \} \\ &\quad - \#\{ (x-\alpha)^3 \mid \alpha \in \mathbb{F}_p \} \\ &\quad - \#\{ (x-\alpha)\mathbb{Q} \mid \mathbb{Q} \text{ un idéal unitaire de degré 2} \} \\ &= p^3 - \left(\binom{p^3}{p} + 2 \binom{p^2}{p} + \binom{p^1}{p} + p \cdot \frac{p^2-p}{2} \right) = p^3 - \frac{p^3 - p^2}{2} - \left(\binom{p^2}{p} + \binom{p^3}{p} \right) \\ &\quad - \left(\binom{p^1}{p} + \binom{p^2}{p} \right) = \frac{p^3 + p^2}{2} - \left(\binom{p^3}{p+1} + \binom{p^2}{p+1} \right) = \frac{p^3 + p^2}{2} - \binom{p^3}{p+2} \end{aligned}$$

$$\begin{aligned}
 &= \frac{r^3 + r^2}{2} - \frac{(r+2)(r+1)r}{6} = r \frac{(r+1)}{2} \left(r - \frac{r+2}{3} \right) = \frac{r(r+1)(2r-2)}{6} \\
 &= \frac{r(r+1)(r-1)}{3} = \frac{r^3 - r^2}{3}.
 \end{aligned}$$

Ex 2).

q1) Par propriété universelle de l'anneau des polynômes à plusieurs variables on a bien un morphisme ϕ de $\mathbb{C}[x,y]$ dans $\mathbb{C}[T]$ qui vient du morphisme $\iota: \mathbb{C} \hookrightarrow \mathbb{C}[T]$ et du choix de deux éléments T^2 et T^3 dans $\mathbb{C}[T]$, tel que $\phi(p) = p(T^2, T^3)$.

q2) On applique le rappel avec $A = \mathbb{C}[y]$ et $p_0 = x^3 - y^2 \in A[x]$ et on obtient $(Q, R) \in A[x]$ tels que $p = p_0 Q + R \quad \deg R < 3$.

Donc $Q \in \mathbb{C}[x,y]$ et $R = R_2(y)x^2 + R_1(y)x + R_0(y)$
d'où la forme cherchée (avant d'évacuer pour Q):

on ne peut pas avoir $Q \in \mathbb{C}[y]$ pour $\deg p > 3$ tant que polynôme de $\mathbb{C}[y][x]$. Par exemple si $p = x^4$

$$\text{soit } x^4 = (x^3 - y^2)x + x y^2 \text{ et } Q = x. \text{ Si } Q \in \mathbb{C}[y]$$

alors $\deg p \leq 3$ — tant que polynôme de $A[x]$.)

$$\text{Si } p(T^2, T^3) = 0 \text{ alors } R = R_2(T^3)T^4 + R_1(T^3)T^2 + R_0(T^3) = 0$$

$$\text{Si } \deg R_2 = n_2 \text{ ou } \deg R_2(T^3)T^4 = 4 + 3n_2 \leq 1 []$$

$$\deg R_1(T^3)T^2 = 2 + 3n_1 \geq 2 []$$

$$\deg R_0(T^3) = 3n_0 \geq 0 []$$

Donc $\deg R = \max(4 + 3n_2, 2 + 3n_1, 3n_0)$ car le coefficient dominant de R est celui de $R_2(T^3)T^4$ ou de $R_1(T^3)T^2$ ou de $R_0(T^3)$, vu que leurs coefficients dominants ne peuvent pas

s'ajouter pour donner le coefficient dominant de F ,

en vertu de la non-congruence modulo 3 de leur indice.

De proche en proche on obtient ainsi que $R_2 = R_1 = R_0 \approx$

Dann ist $f \in \text{ker}(\phi)$ also $f = g(x^2 - y^2)$ mit $g \in \mathbb{C}[x, y]$

donc $\ker \phi \subset (x^3 - y^2)$. L'autre inclusion est évidente.

93) On a $\mathbb{Z}\phi \subset \mathbb{C}[T^2, T^3] = \{ \text{polynômes en } T^2, T^3 \}$. Montrons que $\mathbb{Z}\phi = \{ T^2Q + c \mid Q \in \mathbb{C}(T), c \in \mathbb{C} \}$. En effet si $p \in \mathbb{C}[x, y]$ on a d'après l'écriture ci-dessus que $p(T^2, T^3) = R_2(T^2)T^4 + R_1(T)T^2 + R_0(T^3) = T^2Q + c$ avec $Q \in \mathbb{C}[T]$ et $c \in \mathbb{C}$. Inversement si $q(T) = q_m T^m + \dots + q_1 T + q_0$ et $c \in \mathbb{C}$ et on cherche $p \in \mathbb{C}[x, y]$ tq $p(T^2, T) = q_m T^{m+2} + \dots + q_1 T^3 + q_0 T^2 + c$ le suffit de prendre $p(x, y) = c + q_0 x + q_1 x^2 + \dots + q_m x^{\frac{m+2}{2}} + y(q_1 + q_2 x + \dots + q_{\frac{m-2}{2}} x^{\frac{m-2}{2}})$ pour $p(x, y) = c + q_0 x + \dots + q_{\frac{m-2}{2}} x^{\frac{m+1}{2}} + y(q_1 + q_2 x + \dots + q_{\frac{m-2}{2}} x^{\frac{m-1}{2}})$ min ce point.

$$\text{Mantener en } T^2 = \left(T^2 Q_1 + c_1\right) \left(T^2 Q_2 + c_2\right) = Q_1 Q_2 T^4 + (c_2 Q_1 + c_1 Q_2) T^2 + c_1 c_2$$

$$\text{avec } c_1 c_2 = 0, \quad d' \text{ est } c_1 c_2 t^2 + c_2 c_1 t c_1 = 1$$

Si $c_1 = 0$ alors $\det(\Omega_2 + c_2) = 1$ donc Ω_2 inversible et $\Omega_2 \neq 0$

$\text{can deg}(\alpha_2 T^2 + c_2) = 0$. Hence $p_2 = c_2$ at nonresonable -

Par symétrie on obtient la conservation de $\epsilon_2 = 0$.

Donc T^2 est mesurable, car T^2 n'est pas mesurable ($\mathbb{C}[T^2, T^3]/(T^2) \neq 0$)

$$\text{Since } T^3 = P_1(T^2, T^3) P_2(T^2, T^3) = (T^2 Q_1 + c_1)(T^2 Q_2 + c_1) =$$

$$= Q_1 Q_2 T^4 + (C_2 Q_1 + C_1 Q_2) T^2 + C_1 C_2 \text{ along } C_1 C_2 = 0$$

Since $\deg(P - T^2 + C) \leq 1$, since $P = 0$ it would mean

avec la même conclusion. On peut ainsi dire que toute décomposition

de T^2 ou T^3 dans $\text{Im } \phi$ est aussi une div. dans $\mathbb{C}[T]$, et comme $\mathbb{C}[T]$ est factoriel les diviseurs

de T^2 ou T^3 dans $\text{Im } \phi$ sont aussi une div. dans $\mathbb{C}[T]$, et comme $\mathbb{C}[T]$ est factoriel les diviseurs

de T^2 ou T^3 dans $\text{Im } \phi$ sont aussi une div. dans $\mathbb{C}[T]$, et comme $\mathbb{C}[T]$ est factoriel les diviseurs

94) On a d'abord que $B = \mathbb{C}[x, y] / (x^3 - y^2)$ est

integers can $\mathbb{C}[x, y]$ it factors at $y^2 - x^3$ at
irreducible come polynomials do $\mathbb{C}[x, y] = \mathbb{C}[x] \mathbb{C}[y]$

En effet, m contient 1 et donc il suffit de voir

qu'il est irréductible dans $\mathbb{C}(x)[y]$, avec $\mathbb{C}(x) = \text{Frac } \mathbb{C}[x]$.

Comme il est de degré 2, il suffit de voir qu'il n'a pas de racine dans $\mathbb{C}(x)$. Si par l'absurde

$$\exists s, r \in \mathbb{C}(x) \text{ tq } \left(\frac{s}{r}\right)^2 = x^3 \text{ ou } s^2 = r^2 x^3$$

La parité du degré montre que cela est impossible.

On remarque ensuite que x n'est pas premier car

$$\mathcal{B} /_{(x)} \simeq \mathbb{C}[x,y] /_{(x^3-y^2, x)} = \mathbb{C}[x,y] /_{(x,y^2)} \simeq$$

$$\simeq \mathbb{C}[x,y] /_{(x)} /_{(y^2)} \simeq \mathbb{C}[y] /_{(y^2)} \text{ qui n'est pas unitaire}$$

On a x est un irréductible de $\mathcal{B} \simeq \mathbb{C}[t^2, t^3]$ vu que

x correspond à t^2 dans $\mathbb{Z}\oplus$.

On a trouvé dans \mathcal{B} un élément irréductible non premier donc \mathcal{B} n'est pas factoriel.

Plus simplement, on peut aussi dire que $T^6 = (T^2)^3 = (T^3)^2$

sont deux décompositions en facteurs irréductibles distincts.

$$Ex 24. F_1 = \frac{x}{(x-2)(x+2)} = \frac{\alpha}{x-2} + \frac{\beta}{x+2} \text{ avec } \alpha = \frac{2}{4} = \frac{1}{2}$$

$$\beta = \frac{-2}{-4} = \frac{1}{2}$$

$$F_2 = \frac{x^3 - 3x^2 + x - 4}{x-1} = x^2 - 2x - 1 + \frac{-5}{x-1}.$$

$$\begin{array}{r} 2x^3 + x^2 - x + 1 \\ -2x^3 + 4x^2 - 2x \\ \hline 5x^2 - 3x + 1 \end{array}$$

$$\begin{array}{r} 5x^2 - 3x + 1 \\ -5x^2 + 10x - 5 \\ \hline 7x - 4 \\ -7x + 7 \\ \hline 3 \end{array}$$

$$F_3 = 2x+5 + \frac{7x-4}{(x-1)^2} =$$

$$= 2x+5 + \frac{7}{x-1} + \frac{3}{(x-1)^2}$$

$$\frac{x+1}{x^2+1} = \frac{x+1}{(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)} = \frac{\alpha x + \beta}{x^2-\sqrt{2}x+1} + \frac{\alpha x + \delta}{x^2+\sqrt{2}x+1}$$

$$\text{Ex}(0) \Rightarrow \beta + \delta = 1$$

$$xx, \lim_{x \rightarrow \infty} \approx \alpha + \delta = 0$$

$$\begin{aligned} \text{Donc } & (x^2+\sqrt{2}x+1)(\alpha x + \beta) + (x^2-\sqrt{2}x+1)(-\alpha x + \beta - \delta) \\ &= x^2(1 + \sqrt{2}\alpha) + x(2\sqrt{2}\beta - \sqrt{2}) + 1 = x+1 \\ \text{c'est } & \alpha = -\frac{1}{2\sqrt{2}}, \beta = \frac{1}{2\sqrt{2}}, \beta - \delta = \frac{1+\sqrt{2}}{2\sqrt{2}}, \delta = \frac{\sqrt{2}-1}{2\sqrt{2}}. \end{aligned}$$

Ex 25.

$$\begin{aligned} \text{Soit } S \cap R = 1 \text{ et } S^2 = R^2(x^2+1)^3 \\ \text{avec décomposition en éléments irréductibles sur } \mathbb{C}[x] \mid S \text{ et } (x+i) \mid S \\ \text{donc } x^2+1 \mid S \text{ donc } S = (x^2+1)A \text{ donc} \end{aligned}$$

$$(x^2+1)^2 A^2 = (x^2+1)^3 R^2 \text{ d'où } A^2 = (x^2+1)R^2$$

$$\text{Donc de même } x^2+1 \mid A \text{ et } A = (x^2+1)B$$

$$\text{D'où } (x^2+1)^2 B^2 = (x^2+1)R^2 \text{ d'où } (x^2+1)B^2 = R^2$$

d'où $x^2+1 \mid R$ ce qui contredit $S \cap R = 1$.

$$\text{Donc } \nexists S, R \in \mathbb{C}[x] \text{ tq } \left(\frac{S}{R}\right)^2 = (x^2+1)^3 \text{ ce qui signifie } \nexists F \in \mathbb{C}(x) \text{ tq } F^2 = (x^2+1)^3.$$

Ex 2.

$$1) \text{ On a } i-3 = i(1+3i) \in (1+3i) \text{ donc } i \in \mathbb{Z} \text{ dans } \mathbb{Z}(i)/(1+3i) = A.$$

$$2) \text{ On a } \phi: \mathbb{Z} \xrightarrow{i} \mathbb{Z}(i) \xrightarrow{\pi} \mathbb{Z}(i)/(1+3i) = A \text{ morphisme d'anneaux}$$

$\gamma \mapsto \gamma \mapsto \bar{\gamma}$

par composition de l'inclusion
et de la projection canonique.

$$\text{On m'a donné } \overline{a+bi} \in A \text{ on a } \overline{a+bi} = \bar{a} + \bar{b}i = \phi(a+bi)$$

$$= \bar{a} + \bar{b}\bar{i} \text{ car d'après la question 1) } \bar{b} = \bar{b}. \text{ Donc } \phi \text{ est injectif.}$$

$$3) \text{ Regardons } \text{Ker } \phi = \{z \in \mathbb{Z} \mid z \in (1+3i)\} = \{z \in \mathbb{Z} \mid z = (1+3i)(a+bi)\}$$

On $y = (1+3i)(a+bi) = a-3b + i(b+3a)$ et si $3a+b=0$ alors $b=-3a$
 si $y = a+9a = 10a$ si $y \in \mathbb{Z}$ donc $\text{Ker } \phi = \mathbb{Z}$ et
 d'après le premier théorème d'isomorphisme $A \cong \mathbb{Z}/\mathbb{Z}$.

4) On a donc $\text{car } A = \text{car } \mathbb{Z}/\mathbb{Z} = 10$.

EEx. q1) On peut étudier les inversibles de $\mathbb{Z}[j]$ en étudiant

le module complexe : si $\gamma = (a+bj)(a'+b'j)$ alors

$$\begin{aligned} 1 &= |(a+bj)|^2 |(a'+b'j)|^2 = (a+bj)(a+b\bar{j})(a'+b'j)(a'+b'\bar{j}) = \\ &= (a^2 + b^2 - ab)(a'^2 + b'^2 - a'b') \quad \text{avec } a^2 - ab + b^2 \in \{1, -1\} \end{aligned}$$

$$\text{Comme } a^2 - ab + b^2 = a^2 - ab + \frac{b^2}{4} + \frac{3}{4}b^2 = (a - \frac{b}{2})^2 + \frac{3}{4}b^2 \geq 0$$

$$\text{on doit avoir } a^2 - ab + b^2 = 1 \iff (2a-b)^2 + 3b^2 = 4$$

$$\iff (b=0, a=\pm 1) \text{ ou } (b=\pm 1, a=0) \text{ ou } (b=-1, a=1) \text{ ou } (b=1, a=1)$$

Réiproquement $\pm 1, \pm j$ et $\pm(1+j) \in \mathbb{Z}[j]^\times$ donc on a

$$\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm(1+j)\} \quad \text{En effet } j \cdot j^2 = 1 \text{ et}$$

$$1+j+j^2=0 \quad \text{donc } 1+j=-j^2 \text{ et ces relations nous donnent}$$

les inverses des 6 éléments considérés. Vu que $2 \notin \{\pm 1, \pm j, \pm(1+j)\}$

on voit que 2 n'est pas inversible dans $\mathbb{Z}[j]$.

$$\text{D'autre part si } \gamma = 2 \cdot (a+bj) \text{ on devrait avoir } 1 = 4(a^2 - ab + b^2)$$

ce qui est impossible dans \mathbb{Z} .

2) $\mathbb{Z}[j]$ est un sous-anneau de \mathbb{C} qui est intègre, $\mathbb{Z}[j]$ est intègre aussi.

3) On effectue la division euclidienne de P par le polynôme

unitaire $x^2 + x + 1$ dans $\mathbb{Z}[x]$ et on obtient

$$P = (x^2 + x + 1)Q + R \quad \text{avec } \deg R < 2$$

4) D'après la propriété universelle de l'anneau des polynômes

on a que $\rho: \mathbb{Z}[x] \longrightarrow \mathbb{Z}[j]$ est un morphisme d'anneaux,

$P \mapsto P(j)$ il est injectif car si

$a+bj \in \mathbb{Z}[j]$ alors $a+bj = \rho(a+bx)$. En fait si on considère

la morphine d'anémie $f: \mathbb{Z}[x] \rightarrow \mathbb{C}$ ou a que
 $p \mapsto f(p)$

$\chi[j] = \sup p$ et c'est un sous-anneau de C tel que
 qui l'image de ce morphisme. En effet $p(j) = a + b j$, $a, b \in \mathbb{K}$
 car que $j^2 = -1 - j$ (on applique la q3 avec $R(x) = a + bx$)

5) On a $\text{Ker } p = \{ f_j \mid p(f_j) = 0 \}$. Comme $p(f_j) = R(f_j)$ d'après la question 3, et que $R(f_j) = a + b f_j$, on doit avoir $a + b f_j = 0$ ($\Leftrightarrow a - \frac{1}{2}b + \frac{R(f_j)}{2} = 0$) ($\Leftrightarrow b=0, a=0 \Leftrightarrow R=0$).

Per conseguente $\{k \in \mathbb{N} \mid P \vdash (x^2 + x + 1)\} = \{x^2 + x + 1\}$.

D'après le premier théorème d'isomorphisme $\mathbb{Z}[x]/(x^2 + x + 1) \cong \mathbb{Z}[j]$.

6) Le polynôme x^2+x+1 est irréductible dans $\mathbb{Z}[x]$ (car sans racine dans \mathbb{Z}) donc (x^2+x+1) est premier dans l'anneau factoriel $\mathbb{Z}[x]$. On $\mathbb{Z}[x]/(x^2+x+1) \cong \mathbb{Z}[j]$ n'est pas un corps car que $2 \neq 0$ j est un diviseur de 0. Donc (x^2+x+1) n'est pas un idéal maximal de $\mathbb{Z}[x]$, fait qui a été prouvé aussi dans le cours dans un cadre plus général.

Ex 4. Les multimitables de $\mathbb{K}[x]$ sont les constants multimitables de \mathbb{K} .

($\pm p$, avec p premier) ou les polynômes irréductibles de $\mathbb{K}[x]$ de degré ≥ 1 , c'est-à-dire les polynômes irréductibles de $\mathbb{Q}[x]$ qui sont premiers. En effet si $p \in \mathbb{K}(x) \setminus \mathbb{K}$ n'est pas premier, p s'écrit

ceci est une décomposition de P avec $e(P)$ et P_1 non-nuls dans $\mathbb{Z}(x)$. Et si $P \in \mathbb{Z}(x) \setminus \mathbb{Z}$ est premier, si $P = P_1 P_2$ avec

$\deg p_i \geq 1$, $p_i \in \mathbb{Q}[x]$ on sait que $p = \tilde{p}_1 \cdot \tilde{p}_2$ avec $\deg \tilde{p}_i = \deg p_i$ et $\tilde{p}_i \in \mathbb{Z}[x]$. Non, $(2, x) \subset (\varphi)$ donnerait $\deg p = 0$, $p = \pm 2$ (vu que $\mathbb{I} \neq \mathbb{Z}[x]$) or $1 = 2\mathbb{Q} + x\mathbb{Q}_2$ donne en réduction modulo 2 une absurdité $\bar{1} = x\bar{\mathbb{Q}}_2$ dans $\mathbb{F}_2[x]$) et $x = 2\mathbb{Q}$ ut absurdum en réduction modulo 2 : $x = \bar{0}$.

Donc $\mathbb{K}(x)$ n'est pas principal. On a $\mathbb{K}(x)/(x) \cong \mathbb{K}$ intègre et $\mathbb{K}(x)/(x^2) \cong \mathbb{K}$ intègre donc (x) et (x^2) sont premiers. Ils ne sont pas maximaux car les quotients ne sont pas des corps.