Questions après les devs

Cadre : Soit A un anneau commutatif unitaire intègre. Soit $\mathbb{K}$ un corps. $A^\times$ désigne l'ensemble des éléments inversibles de A.

I - Notion de principalité

1 - Anneaux Principaux [PER]

p.42 **Définition 1 :** Un idéal I de A est dit principal s'il est engendré par un élément $x \in A$, c'est-à-dire si $I = x.A$. On le note (x).

Exemple 2 : les idéaux de $\mathbb{Z}$ sont principaux, de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$.

p.49 **Définition 3 :** Un anneau A est dit principal s'il est intègre et si tout idéal de A est principal.

Exemple 4 : $\mathbb{Z}$ est un anneau principal

Contre-exemple 5 : $\mathbb{Z}[X]$ n'est pas principal.

p.51 **Proposition 6 :** si $A[X]$ est principal, alors A est un corps.

2 - Un exemple : les anneaux euclidiens [PER p.52-54]

Définition 7 : Un anneau A est dit euclidien si A est intègre et s'il existe une fonction $\delta : A^* \to \mathbb{N}$, appelée stathme, telle que si $a, b \in A^*$, il existe $q, r \in A$ avec $a = bq + r$ et $r = 0$ ou $\delta(r) < \delta(b)$.

Exemple 8 : $\mathbb{Z}$ muni de $\delta(n) = |n|$ est euclidien

Proposition 9 : Un anneau euclidien est principal.

Proposition 10 : Division euclidienne dans $A[X]$
Soit $P \in A[X] \setminus \{0\}$ de coefficient dominant inversible dans A. Soit $F \in A[X]$. Alors, il existe un unique couple $(Q, R) \in A[X]^2$ tel que $F = PQ + R$ avec $\deg(R) < \deg(P)$ ou $R = 0$.

Corollaire 11 : $\mathbb{K}[X]$ est euclidien muni du stathme $\delta(P) = \deg(P)$, donc $\mathbb{K}[X]$ est principal.

Proposition 12 : $A[X]$ est principal ssi A est un corps

Application 13 : $\mathbb{C}[X,Y]/(Y-X^2)$ et $\mathbb{C}[X,Y]/(XY-1)$ sont des anneaux principaux. **DEV 1** [FG Alg 1]

⚠ Sautille Prop 3-?

Proposition 14 : Si A est euclidien, alors il existe $x \in A \setminus A^\times$ tel que $\pi_x|_{A^\times \cup \{0\}}$ soit surjective, où π_x est la projection canonique de A sur $A/(x)$.

Exemple 15 :
- $A = \mathbb{Z}$, $A^\times = \{\pm 1\}$, on peut prendre $x = 2$ ou 3.
- $A = \mathbb{K}[X]$, $A^\times = \mathbb{K}^*$, on peut prendre $x = X - a$, $a \in \mathbb{K}$.

Application 16 : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal ~~non euclidien~~ **DEV 2**

II - Arithmétique dans les anneaux principaux

1 - Introduction à la notion d'idéal. [PER 42-43]

Définition 17 : un idéal I de A est dit premier si $I \neq A$ et si, pour tous $a, b \in A$, $(ab \in I \Rightarrow a \in I$ ou $b \in I)$.

Proposition 18 : I est premier ssi A/I est intègre

Exemple 19 : si $A = \mathbb{Z}$, $I = n\mathbb{Z}$ est premier ssi $n = 0$ ou n est premier.

Définition 20 : un idéal I de A est dit maximal si $I \neq A$ et si, pour tout idéal J de A tel que $I \subset J$ et $J \neq A$, on a $J = I$.

Proposition 21 : I est maximal ssi A/I est un corps.

Exemple 22 : les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$ avec p premier.

Proposition 23 : Si A est principal, alors on a l'équivalence : I est maximal $\Leftrightarrow$ I est premier

Remarque 24 : Dans un anneau quelconque, on a seulement la première implication.
ex : $I=\{0\}$ dans $\mathbb{Z}$ est premier mais non maximal.

2 - Divisibilité [Per 46-49 / S2P5]

Définition 25 : Soient $a, b \in A$. On dit que b divise a s'il existe $c \in A$ tel que $a = cb$ et on note $b|a$.

Proposition 26 : $b|a \Leftrightarrow (a) \subset (b)$

Proposition 27 : $(a)=(b) \Leftrightarrow \exists u \in A^\times, a = bu$

Définition 28 : $a, b \in A$ sont dits associés si $a|b$ et $b|a$; c'est-à-dire si $(a)=(b)$.

Exemple 29 : les associés à 1 sont les inversibles

Définition 30 : on dit que $p \in A$ est irréductible si :
1) $p \notin A^\times$
2) $p = ab \Rightarrow a \in A^\times$ ou $b \in A^\times$

Exemple 31 :
- Dans $\mathbb{Z}$, les irréductibles sont les nombres premiers
- Dans $\mathbb{K}[X]$, les polynômes de degré 1 sont irréductibles.

Proposition 32 : Si p est irréductible, alors (p) est maximal parmi les idéaux principaux propres de A.

Proposition 33 : si (p) est premier, alors p est irréductible.

Définition 34 : un élément $p \in A^*$ est premier si ($p|ab \Rightarrow p|a$ ou $p|b$)

Exemple 35 : Dans $\mathbb{Z}$, les éléments premiers sont les nombres premiers.

Proposition 36 : $p \in A$ est premier $\Leftrightarrow$ (p) premier

Proposition 37 : Dans un anneau principal,
p premier $\Longleftrightarrow$ p irréductible

Remarque 38 : Dans un anneau intègre, on a seulement la première implication.
ex : Dans $\mathbb{Z}[i\sqrt{5}]$, 2 est irréductible mais pas premier

Conséquence 39 : $\mathbb{Z}[i\sqrt{5}]$ n'est pas principal.

Résumé : Soient A principal et $p \in A^*$. les conditions suivantes sont équivalentes :
1) p irréductible
2) p premier
3) (p) premier
4) (p) maximal
5) $A/(p)$ est un corps

Application 40 : Construction de $\mathbb{C}$ qui est défini comme $\mathbb{C} \simeq \mathbb{R}[X]/(X^2+1)$ avec (X^2+1) irréductible.

Définition 41 : Soient $(a_i)_{i\in I} \in A^I$ et $d \in A$. On dit que d est un pgcd des (a_i) si d divise tous les a_i et si tout diviseur commun aux a_i est un diviseur de d. TAL Alg 227

Définition 42 : Soient $(a_i)_{i\in I} \in A^I$ et $m \in A$. On dit que m est un ppcm des (a_i) si tous les a_i divisent m et si tout multiple commun aux a_i est un multiple de m. TAL Alg 227

Remarque 43 : si d est un pgcd de a et b, l'ensemble des pgcd de a et b est $dA^\times = \{du, u \in A^\times\}$

Proposition 44 : Dans un anneau principal, tout couple admet un pgcd et un ppcm.

Conséquence 45 : le théorème de Bézout est valable dans un anneau principal.
$\hookrightarrow$ thm : Si A est principal, $a, b \in A^*$ tels que a et b admettent un pgcd d, alors $(d) = (a)+(b)$, càd : il existe $\lambda, \mu \in A$ tels que $d = \lambda a + \mu b$.

3 - Factorialité [Per 47-49]

Définition 46 : on appelle P un système de représentants des irréductibles de A, un ensemble P d'irréductibles tel que pour tout p irréductible, il existe un unique $q \in P$ vérifiant $(q) = (p)$.

Définition 47: Un anneau A est dit factoriel si:
- A est intègre
- $\forall a\in A^*$, a s'écrit $a=u\prod_{p\in P} p^{v_p(a)}$ avec $u\in A^\times$, $v_p(a)\in\mathbb{N}$ et les $v_p(a)$ sont nuls sauf un nombre fini. (E)
- Cette écriture est unique (U)

Exemple 48: $\cdot\mathbb{Z}$ avec $P=\{$nombres premiers$\}$
$\cdot\mathbb{K}[X]$ avec $P=\{$polynômes unitaires irréductibles$\}$

Contre-exemple 49: $\mathbb{Z}[i\sqrt{5}]$ non factoriel : $6=2\times3=(1+i\sqrt{5})(1-i\sqrt{5})$

Proposition 50: Soit A intègre vérifiant (E). On a équivalence entre: 1) A vérifie (U), c'est-à-dire A est factoriel
2) lemme d'Euclide: si p irréductible et $p|ab$, alors $p|a$ ou $p|b$
3) p irréductible $\Leftrightarrow$ (p) premier
4) Théorème de Gauss: si $a|bc$ et a et b premiers entre eux, alors $a|c$.

Proposition 51: un anneau principal est factoriel

Contre-exemple 52: $\mathbb{Z}[X]$ est factoriel et non principal

Proposition 53: si A est factoriel, $A[X]$ est factoriel

Proposition 54: Si A est factoriel, alors un pgcd et un ppcm existent pour tout $(a,b)\in(A^*)^2$: si $a=u\prod_{p\in P}p^{v_p(a)}$ et $b=v\prod_{p\in P}p^{v_p(b)}$ alors $\mathrm{ppcm}(a,b)=\prod_{p\in P}p^{\sup\{v_p(a),v_p(b)\}}$ et $\mathrm{pgcd}(a,b)=\prod_{p\in P}p^{\inf\{v_p(a),v_p(b)\}}$

FG Alg 1 p.44

Proposition 55: Un anneau factoriel qui vérifie le théorème de Bézout est principal.

III - Applications

1 - L'anneau $\mathbb{K}[[X]]$ [FG Alg 1 p68]

Proposition 56: Soient $a=\sum_{i=0}^{\infty}a_iX^i\in\mathbb{K}[[X]]$. Alors a est inversible ssi $a_0\neq0$.

Application 57: tout idéal non nul de $\mathbb{K}[[X]]$ est de la forme (X^p), $p\in\mathbb{N}$.
$\triangleright$ $\mathbb{K}[[X]]$ est principal

Proposition 58: X est le seul irréductible de $\mathbb{K}[[X]]$ à association près.

Proposition 59: $\mathbb{K}[[X]]$ est euclidien.

2 - L'anneau $\mathbb{Z}[i]$ [PER 56-58]

Problème: déterminer $\Sigma=\{n\in\mathbb{N}\mid n=a^2+b^2,\ a,b\in\mathbb{N}\}$

Exemple 60: $0,1,2,4,5,8\in\Sigma$ et $3,6,7,11,12\notin\Sigma$

Définition 61: $\cdot$ on appelle anneau des entiers de Gauss, l'ensemble $\mathbb{Z}[i]=\{a+ib\mid a,b\in\mathbb{Z}\}$
$\cdot$ on définit l'application $N:\mathbb{Z}[i]\to\mathbb{N}$, $z=a+ib\mapsto a^2+b^2=z\bar{z}$ est multiplicative

Conséquence 62: $\cdot\mathbb{Z}[i]^\times=\{\pm1,\pm i\}$
$\cdot\Sigma$ est multiplicative

Lemme 63: $p\in\Sigma\Leftrightarrow p$ n'est pas irréductible dans $\mathbb{Z}[i]$

Proposition 64: $\mathbb{Z}[i]$, muni du stathme N, est euclidien

Théorème 65: $\cdot p\in\Sigma$ premier $\Leftrightarrow p=2$ ou $p\equiv1[4]$
$\cdot$ si $n=\prod p^{v_p(n)}$, $n\in\Sigma\Leftrightarrow v_p(n)$ pair pour $p\equiv3[4]$

DEV 3

Proposition 66: les irréductibles de $\mathbb{Z}[i]$ sont, aux inversibles près: 1) les entiers premiers $p\in\mathbb{N}$ avec $p\equiv3[4]$.
2) les entiers de Gauss $a+ib$ dont la norme a^2+b^2 est un nombre premier.

Application 67: Résoudre $x^2+y^2=z^2$.

3 - Algèbre linéaire

OA 161

Proposition 68: Soient E un $\mathbb{K}$-ev de dimension finie et $u\in\mathcal{L}(E)$. On définit: $\varphi_u:\mathbb{K}[X]\to\mathcal{L}(E)$, $P\mapsto P(u)$. $\mathrm{Ker}(\varphi_u)\neq\{0\}$ est un idéal de $\mathbb{K}[X]$
Comme $\mathbb{K}[X]$ est principal, il existe un unique polynôme unitaire π_u qui engendre $\mathrm{Ker}(\varphi_u)$: c'est le polynôme minimal de u.

Proposition 69: u est diagonalisable ssi π_u est scindé à racines simples.

GOU 125

Proposition 70: Lemme des noyaux
Soit $f\in\mathcal{L}(E)$ et soit $P=P_1\cdots P_k\in\mathbb{K}[X]$, les polynômes P_i étant premiers entre eux deux à deux. Alors: $\mathrm{Ker}\,P(f)=\mathrm{Ker}\,P_1(f)\oplus\cdots\oplus\mathrm{Ker}\,P_k(f)$

$\mathbb{C}[X,Y]/(Y-X^2)$ et $\mathbb{C}[X,Y]/(XY-1)$ sont principaux

- Francinou - Gianella : Exercices de mathématiques pour l'agrégation. Algèbre 1 p 70

I- $\mathbb{C}[X,Y]/(Y-X^2)$ est principal

Le polynôme $Y-X^2$ est irréductible dans $\mathbb{C}[X,Y]$ (car de degré 1 et unitaire dans $(\mathbb{C}[X])[Y]$)

Donc $(Y-X^2)$ est premier (car $\mathbb{C}[X,Y]$ est factoriel)

Donc $\mathbb{C}[X,Y]/(Y-X^2)$ est intègre.

Posons $\varphi : \mathbb{C}[X,Y] \longrightarrow \mathbb{C}[T]$ est un morphisme
$P(X,Y) \longmapsto P(T,T^2)$

* φ est surjectif car $\varphi(X)=T$ et φ est un morphisme

* Montrons $\ker(\varphi) = (Y-X^2)$

on a $(Y-X^2) \subset \ker(\varphi)$

Soit $P \in \ker(\varphi)$.

On remarque que le coefficient dominant de $Y-X^2$ en tant qu'élt de $(\mathbb{C}[X])[Y]$ est inversible dans $\mathbb{C}[X]$

On peut donc effectuer la division euclidienne de P par $Y-X^2$ dans $\mathbb{C}[X][Y]$

Il existe $Q, R \in (\mathbb{C}[X])[Y]$ tq $P(X,Y) = Q(X,Y)(Y-X^2) + R(X,Y)$

tel que $\deg_Y R < 1$

d'où $\deg_Y R = 0$, $R \in \mathbb{C}[X]$

Comme $P \in \ker(\varphi)$, $\varphi(P) = P(T,T^2) = R(T) = 0$

donc $R=0$

donc $P \in (Y-X^2)$

D'après le 1^{er} théorème d'isomorphisme, on a

$$\mathrm{Im}(\varphi) \simeq \mathbb{C}[X,Y]/(Y-X^2)$$

$$\underbrace{\mathbb{C}[T]} \simeq \mathbb{C}[X,Y]/(Y-X^2) \quad \text{car } \varphi \text{ est surjectif}$$

principal (même euclidien car $\mathbb{C}$ corps)

Donc $\boxed{\mathbb{C}[X,Y]/(Y-X^2) \text{ est principal.}}$

II- $\mathbb{C}[X,Y]/(XY-1)$ est principal

Comme précedement, on a $XY-1$ est irréductible

donc $\mathbb{C}[X,Y]/(XY-1)$ est intègre

Posons ψ : $\mathbb{C}[X,Y] \longrightarrow \mathbb{C}(T)$
$P(X,Y) \longmapsto P(T, \frac{1}{T})$

(ψ n'est pas surjectif, $\frac{1}{1-T}$ ne peut pas s'écrire comme un polynôme en X et Y)

Montrons que $\ker(\psi) = (XY-1)$

* $(XY-1) \in \ker(\psi)$
* Soit $P \in \ker(\psi)$

Contrairement au cas précédent, on ne peut pas utiliser la division de P par $XY-1$ car ni X, ni Y est inversible dans $\mathbb{C}[X]$, dans $\mathbb{C}[Y]$

Pour remédier à cela, on se place dans $\mathbb{C}(X)[Y]$ où $X \in \mathbb{C}(X)^\times$

Il existe $Q, R \in \mathbb{C}(X)[Y]$ tq $P(X,Y) = (XY-1)Q(Y) + R(X)$
tel que $\deg_Y R < 1$, $R \in \mathbb{C}(X)$

Soit $A(X)$ le ppcm des dénominateurs de Q et R

$A(X)P(X,Y) = (XY-1)Q_0(Y) + R_0(X)$ où $Q_0 \in \mathbb{C}[X][Y]$ et $R_0 \in \mathbb{C}[X]$

On a donc $\psi(A(X)P(X,Y)) = A(T)P(T, \frac{1}{T}) = A(T) \times R_0(T)$

Comme $\psi(P) = 0$, on a $R_0(T) = 0$

Donc $P \in (XY-1)$

D'où $\mathbb{C}[T;\frac{1}{T}] \simeq \mathbb{C}[X;Y]/_{(XY-1)}$

Montrons $\mathbb{C}[T;\frac{1}{T}]$ est euclidien

Posons $F = \{1, T, T^2, \dots, T^k \dots\}$

$$\mathbb{C}[T;\tfrac{1}{T}] = \left\{ \frac{P}{Q} \in \mathbb{C}(T) \text{ avec } P \in \mathbb{C}[T] \text{ et } Q \in F \right\}$$
$$:= F^{-1}\mathbb{C}[T]$$

Il est clair que $F^{-1}\mathbb{C}[T]$ est un sous-anneau de $\mathbb{C}[T]$ et $\mathbb{C}[T]$ est euclidien de stathme le degré

Soit $x \in F^{-1}\mathbb{C}[T]$, posons $v(x) = \inf\{\deg(T^n x),\ T^n x \in \mathbb{C}[T]\}$

x s'écrit $\frac{P}{T^k}$ avec $P(0) \neq 0$ et $k \in \mathbb{N}$, donc $v(x) = \deg(P)$

Montrons $(F^{-1}\mathbb{C}[T], v)$ euclidien

Soit $x, y \in F^{-1}\mathbb{C}[T]$, $x = \frac{P_1}{T^{k_1}}$ et $y = \frac{P_2}{T^{k_2}}$ avec $P_1(0) \neq 0$ et $P_2(0) \neq 0$

Il existe $Q, R \in \mathbb{C}[T]$ tel que $P_1 = QP_2 + R$ avec $\deg(R) < \deg(P_2)$

$$\frac{P_1}{T^{k_1}} = \left(\frac{QT^{k_2}}{T^{k_1}}\right) \times \frac{P_2}{T^{k_2}} + \frac{R}{T^{k_1}}$$

$$x = \left(\frac{QT^{k_2}}{T^{k_1}}\right) \times y + \frac{R}{T^{k_1}}$$

$$v\left(\frac{R}{T^{k_1}}\right) \leqslant \deg(R) < \deg(P_2) = v(y)$$

donc $\left(\mathbb{C}[T;\frac{1}{T}], v\right)$ est euclidien

D'où $\boxed{\mathbb{C}[X,Y]/_{(XY-1)} \text{ est principal.}}$

- Pourquoi on a besoin des complexes?
- Pourquoi φ est un morphisme? (évaluation)
- Démontrer l'unicité de la prop 10 (intègre ⊕ degré)
- Inversibles de $\mathbb{Z}[X]$? $\Longrightarrow$ $c(P) = 1$
- Donner 4 corps à 4 éléments? $\mathbb{Z}/2\mathbb{Z} / (X^2+X+1)$
- Démontrer $a \wedge b = 1$, $a|c$, $b|c$ $\Rightarrow$ ... (valable dans un anneau factoriel.

– est-ce que l'existence d'une décomp en premiers suffit pour dire qu'un anneau est factoriel ?

– est-ce qu'il faut factoriel pour l'existence d'un pgcd ?

↳ non mais pour le couple

– condit° sur les idéaux pour avoir un ppcm

$(a)\cap(b)=(m)$

Étude de l'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$

Leçons : 122

[Per], partie II.5

Théorème

On note $\alpha = \dfrac{1+i\sqrt{19}}{2}$ et $A = \mathbb{Z}[\alpha]$.
A est un anneau principal, non-euclidien.

Démonstration :

Étape 1 : α est racine de $P = T^2 - T + 5$, car $\alpha + \overline{\alpha} = 1$ et $\alpha\overline{\alpha} = 5$.
Ainsi, $A = \left\{a + b\alpha \middle| (a,b) \in \mathbb{Z}^2\right\}$ est un sous-anneau de $\mathbb{C}$. [1]
Donc A est intègre ; et comme $\overline{\alpha} = 1 - \alpha$, A est stable par conjugaison.
Pour $z = a + b\alpha \in A$, on définit la norme :

$$N(z) = z\overline{z} = (a+b\alpha)(a+b\overline{\alpha}) = a^2 + ab(\alpha+\overline{\alpha}) + b^2\alpha\overline{\alpha} = a^2 + ab + 5b^2.$$

Alors $N(z) \in \mathbb{N}$, et $N(zz') = N(z)N(z')$.
De plus, $N(z) = 0 \Rightarrow \left(a + \dfrac{b}{2}\right)^2 + \dfrac{19}{4}b^2 = 0 \Rightarrow a = b = 0 \Rightarrow z = 0$.
Soit $z \in A^\times$, alors $N(z)N\left(z^{-1}\right) = 1$ donc $N(z) = 1$.
Alors $\left(a + \dfrac{b}{2}\right)^2 + \underbrace{\dfrac{19}{4}}_{>1} b^2 = 1$, donc $b = 0$ et $a = \pm 1$. Ainsi, $A^\times = \{\pm 1\}$.

Étape 2 : Supposons A euclidien, alors $\exists x \in A \backslash A^\times$, $\pi_{A/(x)}\big|_{A^\times \cup \{0\}}$ est surjective. [2]
En particulier, $A/(x)$ est un corps et $\# A/(x) \leqslant 3$, donc $A/(x) = K$, où $K \simeq \mathbb{F}_2$ ou $\mathbb{F}_3$.
On en déduit l'existence d'un morphisme d'anneaux surjectif $\varphi : A \to K$.
Alors $\beta = \varphi(\alpha)$ vérifie $\beta^2 - \beta + 5 = 0$.
Mais cette équation ne possède de solution ni dans $\mathbb{F}_2$, ni dans $\mathbb{F}_3$. [3]
On aboutit à une contradiction, et A n'est donc pas euclidien.

Étape 3 : On introduit une "pseudo-division euclidienne".

Lemme

Soient $a, b \in A \backslash \{0\}$.
Alors il existe $(q,r) \in A^2$, tels que :

1. $N(r) < N(b)$;
2. $a = bq + r$ ou $2a = bq + r$.

Démonstration :
Soit $x = \dfrac{a}{b} = \dfrac{a\overline{b}}{N(b)} \in \mathbb{C}$, qu'on écrit aussi $x = u + v\alpha$, où $u, v \in \mathbb{Q}$. On note $n = \lfloor v \rfloor$.

– Supposons que $v \notin \left]n + \dfrac{1}{3}, n + \dfrac{2}{3}\right[$; soient s et t les plus proches entiers de u et v.
Ainsi, $|s - u| \leqslant \dfrac{1}{2}$ et $|t - v| \leqslant \dfrac{1}{3}$.
On pose $q = s + t\alpha \in A$ et :

$$(x-q)\overline{(x-q)} = (s-u)^2 + (s-u)(t-v) + 5(t-v)^2 \leqslant \frac{1}{4} + \frac{1}{6} + \frac{5}{9} = \frac{9+6+20}{36} = \frac{35}{36} < 1.$$

On pose $r = a - bq = b(x-q)$ et on a $N(r) < N(b)$.

1. Car A est un sous-groupe de $\mathbb{C}$, contient 1 et est stable par multiplication.
2. La démonstration est dans le rappel sur les anneaux, en page ??.
3. Cela se démontre facilement en cherchant de façon exhaustive.

– Supposons désormais que $v \in \left]n+\frac{1}{3}, n+\frac{2}{3}\right[$, alors $2x = 2u + 2v\alpha$ et $2v \in \left]2n+\frac{2}{3}, 2n+1+\frac{1}{3}\right[$ et on est ramené au cas précédent : on peut écrire $2a = bq + r$, avec $N(r) < N(b)$. ■

Étape 4 : Montrons que A est principal.
On a : $A \simeq \mathbb{Z}[T]/(P)$, donc $A/(2) \underset{4}{\simeq} \mathbb{Z}[T]/(2,P) \underset{5}{\simeq} \mathbb{F}_2[T]/(P)$.

Mais $T^2 - T + 5$ est irréductible sur $\mathbb{F}_2$ car de degré 2 sans racine ; donc $A/(2)$ est un corps et (2) est maximal dans A.
Soit $I \neq (0)$ un idéal de A, et soit $a \in I \backslash \{0\}$ de norme $N(a)$ minimale.
Soit $x \in I \backslash (a)$;

→ Si $x = aq + r$ avec $N(r) < N(a)$ ou $r = 0$, alors comme $r \in I$, par minimalité de $N(a)$, on a $r = 0$.
Ainsi $x \in (a)$: contradiction.

→ Ainsi, $2x = aq + r$, et même $2x = aq$ en répétant le procédé qu'on vient à peine de faire.
Comme (2) est maximal, l'idéal (2) est premier, d'où $a \in (2)$ ou $q \in (2)$.
Si $q \in (2)$, alors $q = 2q'$ et $x = aq'$ donc $x \in (a)$. Contradiction.
Donc $a \in (2)$, c'est-à-dire : $a = 2a'$.
Comme $q \notin (2)$ et (2) est maximal, on a : $(2, q) = A$, donc $\exists \lambda, \mu \in A, 2\lambda + q\mu = 1$.
Donc $a' = 2\lambda a' + q\mu a' = \lambda a + \mu x \in I$.
Or $0 < N(a') < N(a)$. Contradiction.

Ainsi, $I = (a)$ et A est principal. ■

Références

[Per] D. PERRIN – *Cours d'algèbre*, Ellipses, 1996.

4. Notons $\pi_P : \mathbb{Z}[T] \to \mathbb{Z}[T]/(P)$ et $\pi_{\overline{2}} : \mathbb{Z}[T]/(P) \to \left(\mathbb{Z}[T]/(P)\right)/(\overline{2})$ les projections canoniques.
Ker $\pi_{\overline{2}} \circ \pi_P = \left\{f \in \mathbb{Z}[T] \middle| \exists u \in \mathbb{Z}[T], \overline{f} = \overline{2u}\right\} = \{f \in \mathbb{Z}[T] | \exists u, v \in \mathbb{Z}[T], f = 2u + Pv\} = (2, P)$.
Ainsi $\pi_{\overline{2}} \circ \pi_P$ induit un isomorphisme $\mathbb{Z}[T]/(2,P) \simeq \left(\mathbb{Z}[T]/(P)\right)/(\overline{2}) \simeq A/(2)$.

5. Notons $\pi_2 : \mathbb{Z}[T] \to \mathbb{Z}[T]/(2)$ et $\pi_{\overline{P}} : \mathbb{Z}[T]/(2) \to \left(\mathbb{Z}[T]/(2)\right)/(\overline{P})$ les projections canoniques.
Ker $\pi_{\overline{P}} \circ \pi_2 = \left\{f \in \mathbb{Z}[T] \middle| \exists u \in \mathbb{Z}[T], \overline{f} = \overline{Pu}\right\} = \{f \in \mathbb{Z}[T] | \exists u, v \in \mathbb{Z}[T], f = Pu + 2v\} = (2, P)$.
Ainsi $\pi_{\overline{P}} \circ \pi_2$ induit un isomorphisme $\mathbb{Z}[T]/(2,P) \simeq \left(\mathbb{Z}[T]/(2)\right)/(\overline{P}) \simeq \mathbb{F}_2[T]/(P)$.

Théorème des 2 carrés

- Perrin

[Problème. Déterminer l'ensemble des entiers qui s'écrivent comme somme de deux carrés.]

Posons $\Sigma = \{ n \in \mathbb{N} \ , \ n = a^2 + b^2 \ ; a, b \in \mathbb{N} \}$

Si $n \in \Sigma$, $n = a^2 + b^2$ dans $\mathbb{C}$ on a $n = (a+ib)(a-ib)$

Cette relation a aussi lieu dans $\mathbb{Z}[i]$

Posons $N : \begin{array}{ccc} \mathbb{Z}[i] & \longrightarrow & \mathbb{N} \\ z & \longmapsto & z\bar{z} \end{array}$ est multiplicative

Ceci permet de montrer que * $\mathbb{Z}[i]^{\times} = \{ \pm 1 ; \pm i \}$
* Σ est multiplicative
(ce qui permet de restreindre l'étude aux élts premiers appartenant à Σ)

1°/ Montrons $(\mathbb{Z}[i], N)$ est euclidien

Soient $z_1, z_2 \in \mathbb{Z}[i]$, $z_1 = a + ib$ et $z_2 = c + id$ avec $a, b, c, d \in \mathbb{N}$

$$\frac{z_1}{z_2} = P + iQ \quad \text{avec } P, Q \in \mathbb{Q}$$

il existe $x, y \in \mathbb{Z}$ et $\alpha, \beta \in \mathbb{Q}$ tq $|\alpha| \leqslant \frac{1}{2}$ et $|\beta| \leqslant \frac{1}{2}$

tel que $\frac{z_1}{z_2} = (x + iy) + (\alpha + i\beta)$

$$z_1 = z_2 \underbrace{(x+iy)}_{:= q} + \underbrace{(\alpha + i\beta) z_2}_{:= r}$$

Comme z_1, z_2 , $x + iy \in \mathbb{Z}[i]$, alors $r \in \mathbb{Z}[i]$

donc $N(r) = N(z_2) \times N(\alpha + i\beta) \leqslant \left(\frac{1}{4} + \frac{1}{4}\right) N(z_2) < N(z_2)$

Donc $\underline{(\mathbb{Z}[i], N) \text{ est euclidien.}}$ ■

2°/ Soit p premier, $p \in \Sigma \Leftrightarrow p = 2$ ou $p \equiv 1[4]$

$\Rightarrow$ * $p = 1+1 = 2 \in \Sigma$

* Soit p un nombre premier impair, alors $p \equiv 1[4]$ ou $p \equiv 3[4]$

Comme $p \in \Sigma$, $p = a^2 + b^2$.

Si a est pair, $a^2 \equiv 0[4]$

Si a est impair, $a^2 \equiv 1[4]$

Donc en combinant les différentes possibilités, on a

$p \equiv \cancel{0}, 1, \cancel{2}[4]$

Donc $p \equiv 1[4]$

$\Leftarrow$ On commence par introduire un lemme.

Lemme : Soit p un nombre premier.

$p \in \Sigma \Leftrightarrow p$ est réductible dans $\mathbb{Z}[i]$

On a $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$

donc $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2+1)$

On a (p) non premier $\Leftrightarrow X^2+1$ réductible dans $\mathbb{F}_p[X]$

$\Leftrightarrow X^2+1$ a une racine dans $\mathbb{F}_p$

Comme $\mathbb{Z}[i]$ est principal, on a (p) non premier

$\Leftrightarrow p$ non irréductible

Donc d'après le lemme, $p \in \Sigma \Leftrightarrow (-1)$ est un carré dans $\mathbb{F}_p$

Il faut donc montrer, $p = 2$ ou $p \equiv 1[4] \Rightarrow (-1)$ est un carré dans $\mathbb{F}_p$

* si $p=2$, $\mathbb{F}_2=\{0;1\}$ et $-1=1$
donc -1 est un carré dans $\mathbb{F}_2$

* si $p\equiv 1[4]$, le cardinal de l'ens. des carrés de $(\mathbb{F}_p)^\times$ est $\frac{p-1}{2}$ qui est pair.

Or un groupe de cardinal pair a forcément un élt d'ordre 2.

Donc il existe x tel que $x^2=1$ et $x\neq 1$

Donc $x=-1$ et -1 est donc un carré de $\mathbb{F}_p$. ■

3°/ Soit $n\geqslant 2$, $n=\prod_{p\in\mathcal{P}} p^{v_p(n)}$, $n\in\Sigma \Leftrightarrow v_p(n)$ pair pour $p\equiv 3[4]$

$(\Leftarrow)$ $$n=\underbrace{\left(\prod_{p\equiv 3[4]} p^{v_p(n)/2}\right)^2}_{\substack{\text{possible car } v_p(n) \\ \text{est pair pour } p\equiv 3[4] \\ \in\Sigma \text{ car carré parfait}}} \times \underbrace{\prod_{p\equiv 1[4]} p^{v_p(n)}}_{\substack{\in\Sigma \\ \text{d'après 2}}} \in \Sigma$$ car stable par multiplication

$(\Rightarrow)$ On suppose, $n\in\Sigma$ et $p\equiv 3[4]$

On va montrer que $v_p(n)$ est pair par récurrence sur $v_p(n)$

* $v_p(n)=0$ OK
* $v_p(n)>0$, donc $p\mid n$, $p\mid a^2+b^2=(a+ib)(a-ib)$

Comme $p\equiv 3[4]$, d'après le lemme p est irréductible dans $\mathbb{Z}[i]$

donc, d'après le lemme d'Euclide, $p\mid a+ib$ par exemple

Comme $p\in\mathbb{N}$, $p\mid a$ et $p\mid b$, donc $p^2\mid n$

On a donc $a=a'p$ et $b=b'p$, donc $\frac{n}{p^2}=a'^2+b'^2\in\Sigma$

Or $v_p\left(\frac{n}{p^2}\right)=v_p(n)-2$,

Donc $v_p\left(\frac{n}{p^2}\right)<v_p(n)$, par hypothèse de récurrence

$v_p\left(\frac{n}{p^2}\right)$ est pair.

Donc $v_p(n) = v_p(\frac{n}{p^2}) + 2$ est pair.

On a montré par récurrence que $v_p(n)$ est pair. ■

En résumé, les entiers n qui s'écrivent comme somme de deux carrés sont les nombres qui sont produit de nombres premiers tel que $p = 2$ ou $p \equiv 1[4]$ ou $p \equiv 3[4]$ avec $v_p(n)$ pair

- p premier de $\mathbb{Z}$, l'est-il de $\mathbb{Z}[i]$?
- $\mathbb{Z}[i\sqrt{5}]$ décomp unique en $a+i\sqrt{5}$?

$\mathbb{Z}[i\sqrt{5}]^*$?

2 est il irréductible ? $1+i\sqrt{5}$?

- $\mathbb{Z}[i\sqrt{5}]$ principal ? Non car pas factoriel car pas unicité ?

Connaître les isomorphismes entre les équivalents

→ Mettre la divisibilité avant