(122)

114

NOM : Pellet-Mary Prénom : Alice Jury :

(Algèbre) ↔ Entourez l'épreuve → Analyse

Sujet choisi : 122 Anneaux principaux. Exemples et applications.

Autre sujet : Rej : Perrin, Goblot, Beck-Malick-Peyré, Ireland-Ros (pour ZL)
D. Serre

peut se rendre un peu + synthétique en faisant un préliminaire A/ & B/ idéaux

Dans toute la suite, A est un anneau commutatif unitaire et intègre.

I) Définitions et propriétés :

1) Arithmétique dans les anneaux :

Déf 1 : Soient $a,b \in A$, on dit que a divise b (et on écrit $a|b$) si il existe $c \in A$ t.q. $b = ac$.

Déf 2 : Soit $a \in A$, on dit que a est inversible s'il existe $b \in A$ t.q. $ab = 1$. On note $A^\times = \{a \in A,\ a \text{ inversible}\}$.

Prop 3 : Si $a|b$ et $b|a$ alors $\exists u \in A^\times$ t.q. $a = bu$.

Déf 4 : On dit que d est un pgcd de $a,b \in A$ si $d|a$, $d|b$ et $\forall c \in A$ t.q. $c|a$ et $c|b$, on a $c|d$. On dit que m est un ppcm de $a,b \in A$ si $a|m$, $b|m$ et $\forall c \in A$ tel que $a|c$ et $b|c$, alors $m|c$.

Déf 5 : On dit que a et $b \in A$ sont premiers entre eux si 1 est un pgcd de (a,b).

Déf 6 : Soit $a \in A^\times$. On dit que a est premier si $\forall b,c \in A$ t.q. $a|bc$, on a $a|b$ ou $a|c$. On dit que a est irréductible si $a = bc \Rightarrow b \in A^\times$ ou $c \in A^\times$.

Prop 7 : Si $a \in A^\times$ est premier, alors a est irréductible.

Prop 8 : $a \in A^\times$ est premier si $A/(a)$ est intègre.

2) Anneaux factoriels :

Déf 9 : On dit qu'un anneau A est factoriel si :
$\forall a \in A \setminus \{0\}$, $a = u p_1 \dots p_r$ avec $u \in A^\times$ et $p_1, \dots, p_r$ irréductibles, et cette décomposition est unique à permutation près des facteurs et à multiplication près par des inversibles.

Ex 10 : $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[X]$ (K corps) sont factoriels.

Prop 11 : Si A est factoriel et $a \in A^\times$, a irréductible alors a premier.

Contre-ex 12 : $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

Ex 13 : Dans $\mathbb{Z}$ les irréductibles sont les nombres premiers.
Dans $K[X]$ les irréductibles sont les polynômes de degré 1.

Lemme 14 : (Gauss) Si A factoriel, $a,b,c \in A$, $a|bc$ et a et b sont premiers entre eux, alors $a|c$.

3) Anneaux principaux :

Déf 15 : Un idéal I de A est principal s'il est engendré par un élément $a \in A$. On note $I = (a)$.

Déf 16 : Un anneau A est principal si tous ses idéaux sont principaux.

Ex 17 : $\mathbb{Z}$, $K[X]$ (K corps), $\mathbb{Z}[i]$, $\mathbb{Z}[j]$ (avec $j = e^{2i\pi/3}$), $K[[X]]$ sont principaux.

Prop 18 : Un anneau principal est factoriel.

Ex 19 : $\mathbb{Z}[X]$ est factoriel non principal (l'idéal $(2,X)$ n'est pas principal).

Prop 20 : Soit A principal et $a,b \in A$. Alors il existe $d \in A$ tel que $(a,b) = (d)$ et d est un pgcd de a et b. De plus, il existe $u,v \in A$ t.q. $au + bv = d$ (Thm de Bezout).

Ex 21 : $A = \mathbb{Z}$, $a = 6$, $b = 10$, on a $d = 2 = 2 \times 6 - 1 \times 10$.

Prop 21 : (Théorème chinois) Soit A principal et $a_1, \dots, a_n \in A$ premiers entre eux deux à deux. Alors $A/(a_1 \dots a_n)$ est isomorphe à $A/(a_1) \times \dots \times A/(a_n)$.

Ex 22 : Le système $\begin{cases} x \equiv 1 [5] \\ x \equiv 2 [5] \end{cases}$ a une unique solution dans $\mathbb{Z}/5\mathbb{Z}$. C'est $x \equiv 7 [15]$.

Prop 23 : Soit $p \in A$ principal. Alors p est irréductible si $A/(p)$ est un corps.

4) Anneaux euclidiens :

Déf 24 : A est euclidien s'il existe un stathme $v : A \setminus \{0\} \to \mathbb{N}$ tel que pour tout $a,b \in A$, $b \neq 0$, il existe $q,r \in A$ avec $a = bq + r$ et $(r = 0$ ou $v(r) < v(b))$.

Ex 25 : $\mathbb{Z}$ est euclidien pour $v = |\cdot|$; $K[X]$ est euclidien pour $v =$ degré, $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$ sont euclidiens pour $v = |\cdot|^2$ (module complexe).

Prop 26 : Un anneau euclidien est principal.

Remarque 27 : En général, pour montrer que A est principal on montre qu'il est euclidien.

Contre-ex 28 : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais non euclidien.

Remarque 28 : Dans un anneau euclidien on a un algorithme pour calculer le pgcd et les coefficients de Bezout (algo d'Euclide étendu, cf annexe).

II) Exemple d'anneaux principaux et applications

1) K[X] et polynômes minimaux :

Dans toute la suite, K désigne un corps.

Prop 29 : K[X] muni du stathme v = degré des polynômes, est un anneau euclidien.

⚠ A principal ⇏ A[X] principal. On a même :

Prop 30 : A[X] principal ⇒ A est un corps.

Ex 31 : Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 sans racine réelle.
- Dans $\mathbb{F}_p[X]$ il y a des irréductibles de tout degré.

Prop 32 : Les inversibles de K[X] sont les $P \in K[X] \setminus \{0\}$ de degré 0.

Application 33 : Existence de polynômes minimaux

* Soit L/K une extension de corps, $\alpha \in L$ algébrique sur K, alors il existe un polynôme annulateur de α minimal π, i.e. $\pi(\alpha)=0$ et $\forall P \in K[X]$ t.q. $P(\alpha)=0$, $\pi \mid P$. $\pi \in K[X]$
* Soit E un K-ev de dimension finie et f un endomorphisme de E. Alors il existe $\pi \in K[X]$ t.q. $\pi(f)=0$ et $\forall P \in K[X]$ t.q. $P(f)=0$, $\pi \mid P$.

2) $\mathbb{Z}[j]$ et étude des cubes :

Dans cette partie, $j = e^{2i\pi/3}$.

Déf 34 : L'anneau $\mathbb{Z}[j] = \{a+bj,\ a,b \in \mathbb{Z}\}$ est appelé anneau des entiers d'Eisenstein. (C'est bien un anneau car $j^2 = -1-j$).

Prop 35 : $\mathbb{Z}[j]$ est euclidien pour le stathme $v(y) = |y| = y\bar{y}$ (module complexe).

Prop 36 : Les inversibles de $\mathbb{Z}[j]$ sont $\{1, -1, j, -j, j^2, -j^2\}$.

Prop 37 : Les irréductibles de $\mathbb{Z}[j]$ sont (aux inversibles près)
- $1-j$
- $q \in \mathbb{Z}$ t.q. q est un nombre premier et $q \equiv 2\ [3]$
- $\pi \in \mathbb{Z}[j]$ t.q. $N(\pi) = p \in \mathbb{Z}$ avec p un entier premier, et $p \equiv 1\ [3]$.

Déf / Prop 38 : Soit $\pi \in \mathbb{Z}[j]$ premier. On définit, pour $a \in \mathbb{Z}[j]$, le symbole de résiduosité cubique $(a/\pi)_3$ par :
- $(a/\pi)_3 = 0$ si $\pi \mid a$
- $(a/\pi)_3 = a^{(N(\pi)-1)/3}\ [\pi]$ sinon (dans ce cas, $(a/\pi)_3 = 1, j$ ou j^2).

Prop 39 : $(a/\pi)_3 = 1$ ssi $x^3 = a\ [\pi]$ admet une solution, et $a \neq 0\ [\pi]$.

Remarque 40 : $(\cdot/\cdot)_3$ est l'analogue du symbole de Legendre, mais pour étudier les cubes.

3) $\mathbb{Z}[i]$ et le théorème des 2 carrés :

Déf 41 : L'anneau $\mathbb{Z}[i] = \{a+ib,\ a,b \in \mathbb{Z}\}$ ($i \in \mathbb{C}$ t.q. $i^2=-1$) est l'anneau des entiers de Gauss.

Prop 42 : $\mathbb{Z}[i]$ est euclidien pour le stathme $v(y) = |y| = y\bar{y}$ (module complexe).

Prop 43 : Les inversibles de $\mathbb{Z}[i]$ sont les y tels que $|y| = 1$, i.e. ce sont $\{1, -1, i, -i\}$.

Déf 44 : On note $\Sigma = \{n \in \mathbb{N} \mid n = a^2+b^2,\ a,b \in \mathbb{N}\}$

Lemme 45 : Σ est stable par multiplication.

Lemme 46 : Soit $p \in \mathbb{N}$ un nombre premier, alors $p \in \Sigma$ ssi $p=2$ ou $p \equiv 1\ [4]$.

Théorème 47 (des 2 carrés) Soit $n \in \mathbb{N}$. On décompose n en facteurs premiers :
$n = \prod_{i=1}^{r} p_i^{\alpha_i}$ p_i 2 à 2 distincts.
Alors $n \in \Sigma \iff \alpha_i$ pair $\forall i$ t.q. $p_i \equiv 3\ [4]$

Prop 48 : Les irréductibles de $\mathbb{Z}[i]$ sont (aux inversibles près) :
- $p \in \mathbb{N}$, p premier et $p \equiv 3\ [4]$
- $a+ib$ $(a,b \in \mathbb{Z})$ t.q. $a^2+b^2 \in \mathbb{N}$ est premier

III) Trois propriétés des anneaux principaux et leurs applications :

Dans toute la suite, A est supposé principal.

1) Applications du théorème de Bezout :

Rappel 49 (Bezout) : Soient $a, b \in A$ et $d = \mathrm{pgcd}(a,b)$, alors $\exists u, v \in A$ t.q. $au+bv=d$.

* **Appl 50** : Résolution de l'équation diophantienne (E) $ax+by=c$, $a,b,c \in \mathbb{Z}$

Prop 51 : On note $d = \mathrm{pgcd}(a,b)$ et $u_0, v_0 \in A$ t.q. $au_0+bv_0=d$. On a alors :
- si $d \nmid c$, (E) n'a pas de solution
- si $c = \gamma \times d$, (E) admet des solutions. Et l'ensemble des solutions est $\{(\gamma u_0 + k\frac{b}{d}, \gamma v_0 - k\frac{a}{d}),\ k \in \mathbb{Z}\}$.

Ex 52 : L'ensemble des solutions de $6x+10y=4$ est $\{(4+5k, -2-3k),\ k \in \mathbb{Z}\}$

* **Appl 51** : Calcul de l'inverse dans $\mathbb{Z}/n\mathbb{Z}$.

Prop 52 : Soient $m, n \in \mathbb{Z}$, $n \geq 2$. Alors m est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi $\mathrm{pgcd}(m,n)=1$.
Dans ce cas, le théo de Bezout nous

▷ On comprend pas trop l'intérêt de la loi de réciprocité cubique.
Trouver une autre appli ? (équa° diophantiennes : $x^3+y^3=z^3$)

donné $u,v \in \mathbb{Z}$ t.q. $mu+nv=1$ et alors $m^{-1}=u$ dans $\mathbb{Z}/n\mathbb{Z}$.

Appl 53 : cryptosystème RSA (cf annexe 2).
On a $n=pq$ (p,q premiers), e inversible modulo $\varphi(n)$, d'inverse d. Le chiffré d'un message $m \in (\mathbb{Z}/n\mathbb{Z})^*$ est $m^e = c \in \mathbb{Z}$ pour déchiffrer on calcule $c^d = m$ [n].

***Appl 54** : Lemme des noyaux.

Prop 55 : Soit E un K-ev de dim finie, $g \in \mathcal{L}(E)$ et $P = P_1 \cdots P_r \in K[X]$ avec les P_i premiers entre eux 2 à 2 et $P(g)=0$. Alors
$E = \ker(P_1(g)) \oplus \cdots \oplus \ker(P_r(g))$.

Corollaire 56 : g est diagonalisable ssi π_g (son polynôme minimal) est scindé à racines simples.

2) Théorème chinois :

Rappel 57 : si $a,b \in A$ sont premiers entre eux, on a un isomorphisme $A/(ab) \simeq A/(a) \times A/(b)$

Remarque 58 : Le théorème de Bezout permet d'expliciter la bijection.

***Application 59** : factorisation de $n \in \mathbb{N}$.

Prop 60 : Soit $n = p_1 \cdots p_r$, p_i impairs 2 à 2 distincts et x choisi de façon uniforme dans $S = \{y \in \mathbb{Z}/n\mathbb{Z},\ y^2 = 1\}$. Alors, avec probabilité $\geq \frac{1}{2}$, $\gcd(x-1, n)$ est un facteur non trivial de n.

Ex 61 : $n=15$, $S = \{1,4,11,14\}$, et $\gcd(4-1,15)=3$, $\gcd(11-1,15)=5$.

***Appl 62** : Attaque du cryptosystème RSA

Prop 63 : Si $n=pq$ (p,q premiers distincts), et $m = \mathrm{ppcm}(p-1, q-1)$, alors $a^m \equiv 1$ [n] ($a \in (\mathbb{Z}/n\mathbb{Z})^\times$)

Conséquence 64 : Connaissant n, e et d, on peut calculer p et q en temps polynomial.

***Application 65** : Algorithme de Berlekamp.
L'algorithme de Berlekamp permet de factoriser des polynômes à coefficients dans un corps fini $\mathbb{F}_q$. sans facteurs carrés

Dvpt 2

Remarque 66 : Il existe une variante probabiliste qui a une complexité polynomiale.

3) A-modules :

Théorème 67 : Soit M un A-module libre de type fini et N un sous-A-module de M. Alors N est libre de type fini, de rang inférieur au rang de M.

⚠ C'est faux si A n'est pas principal.

Contre-ex 68 : $B = \mathbb{Z}[X]$, $M = B$, $N = (2,X)$.
M est un B-module libre de type fini, mais N n'est pas libre (en tant que B-module).
$B = K[X_i,\ i \in \mathbb{N}]$, $M = B$, $N = \langle X_i,\ i \in \mathbb{N}\rangle$
M est un B-module libre de type fini, mais N n'est pas de type fini.

Remarque 69 : Si B est tel que $\forall M$, B-module libre, N ss-module de $M \Rightarrow N$ libre, alors B est principal.

***Appl 70** : réseaux euclidiens.

Déf 71 : Un réseau de $\mathbb{R}^n$ est un sous-groupe additif R de $\mathbb{R}^n$, discret, et qui engendre $\mathbb{R}^n$ comme $\mathbb{R}$-ev.

Prop 72 : Une partie $R \subset \mathbb{R}^n$ est un réseau de $\mathbb{R}^n$ ssi il existe une base $(e_1,\dots,e_n)$ de $\mathbb{R}^n$ tel que $R = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$ ($\mathbb{Z}$-module libre de base $(e_1,\dots,e_n)$).

Remarque 73 : Etant donné $R = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$, trouver $v \in R$ de taille minimale est un problème supposé difficile. Il est à la base de plusieurs protocoles de cryptographie.

Théorème 74 (base adaptée) Soit M un A-module libre de type fini de rang n, et N un sous-module de M. Alors il existe $(e_1,\dots,e_n)$ une base de M et $d_1 | \cdots | d_s \in A \setminus \{0\}$ ($s \leq n$) t.q. $(d_1 e_1, \dots, d_s e_s)$ soit une base de N.
Les d_i sont uniques à inversibles près.

Théorème 75 (facteurs invariants) : Soit M un A-module de type fini, alors $\exists r, s \geq 0$ et $d_1 | d_2 | \cdots | d_s$ ($d_i \in A$) tels que
$$M \overset{A\text{-mod}}{\simeq} A^r \oplus \left(\bigoplus_{i=1}^{s} A/\langle d_i \rangle\right)$$

Application 76 : Si G est un groupe abélien de type fini $\exists r, s \geq 0$ et $d_1, \dots, d_s \in \mathbb{Z}$, $d_1 | \cdots | d_s$ t.q.
$$G \simeq \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$$

Corollaire 77 : Soit $M \in \mathcal{M}_n(A)$, il existe $P, Q \in GL_n(A)$ et $d_1 | d_2 | \cdots | d_n \in A$ t.q.
$M = P\,\mathrm{diag}(d_1,\dots,d_n)\,Q$.
Les d_i sont uniques à inversibles près, et appelés **facteurs invariants** de M.

Déf 78 : Soit $B \in \mathcal{M}_n(K)$. Les facteurs invariants de $XI_n - B \in \mathcal{M}_n(K[X])$ sont appelés invariants de similitude de B.

Thm 79 : Deux matrices $A, B \in \mathcal{M}_n(K)$ sont semblables ssi elles ont les mêmes invariants de similitude.

Corollaire 80 : A et A^T sont semblables.

Appl 81 : $A \in \mathcal{M}_n(\mathbb{C})$ est semblable à une matrice diagonale par blocs dont les blocs diagonaux sont des blocs de Jordan (cf Annexe 3).

mettre en forme matricielle (cor 75)

Annexe 1 : Algorithme d'Euclide étendu.

Entrée : $a, b \in A$ euclidien, $b \neq 0$

Sortie : d, u, v t.q. $au + bv = d$ et $d = pgcd(a,b)$

Algorithme :
- $u_0 = 1$, $u_1 = 0$
- $v_0 = 0$, $v_1 = 1$
- $r_0 = a$, $r_1 = b$, $i := 1$
- Tant que $r_i \neq 0$ faire
  - $r_{i-1} = q_i r_i + r_{i+1}$ $(v(r_{i+1}) < v(r_i))$
  - $u_{i+1} \leftarrow u_{i-1} - q_i u_i$
  - $v_{i+1} \leftarrow v_{i-1} - q_i v_i$
- Renvoyer $(r_{i-1}, u_{i-1}, v_{i-1})$

Annexe 2 : cryptosystème RSA

- Alice choisit 2 nombres premiers distincts p et q.
- $n = pq$, $\varphi(n) = (p-1)(q-1)$.
- L'espace des messages est $(\mathbb{Z}/n\mathbb{Z})^*$ de card $\varphi(n)$.
- Alice choisit $e \in \mathbb{Z}/\varphi(n)\mathbb{Z}$ inversible, et $d = e^{-1}[\varphi(n)]$.
- La clé publique est (n, e). La clé secrète est d.
- Pour chiffrer le message $m \in (\mathbb{Z}/n\mathbb{Z})^*$, Bob calcule $c = m^e[n]$ et envoie c à Alice.
- Pour déchiffrer le message, Alice calcule $c^d = m^{ed} = m^{k\varphi(n)+1} = m\,[n]$.

Annexe 3 : Blocs de Jordan

Les blocs de Jordan sont de la forme

$$J(a,n) = \begin{pmatrix} a & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & a \end{pmatrix} \in \mathcal{M}_n(\mathbb{C}).$$

I Défense de plan

Idée : imiter ce qu'on fait dans $\mathbb{Z}$

factoriel $\leq$ principal $\leq$ euclidien

Bezout ← rend effectif
Thm Chinois ←

II Exercices

1 $x^2+y^2=z^2$, $x,y,z \in \mathbb{N}$ Résoudre

On regarde dans $\mathbb{Z}[i]$ $(N(\cdot)=|\cdot|^2)$.

Rq : On peut se ramener au cas $x \wedge y \wedge z = 1$; en effet, si $=d$ alors $\left(\frac{x}{d}\right)^2+\left(\frac{y}{d}\right)^2=\left(\frac{z}{d}\right)^2$

$\text{pgcd}_{\mathbb{Z}}(x,y,z) = \text{pgcd}_{\mathbb{Z}}(\text{pgcd}_{\mathbb{Z}}(x,y),z)$ car $x,y,z \in \mathbb{N}$

On suppose $x \wedge y \wedge z = 1$

Soit $w \in \mathbb{Z}[i]$, $z \in \mathbb{N}$, $z^2 = w\bar{w}$ $(w = x+iy)$

$\delta = \text{pgcd}_{\mathbb{Z}[i]}(z,w)$

$\bar{\delta} = \text{pgcd}_{\mathbb{Z}[i]}(z,\bar{w})$

$\frac{z}{\delta} \times \frac{z}{\bar{\delta}} = \frac{w}{\delta} \times \frac{\bar{w}}{\bar{\delta}}$. $\frac{z}{\delta} \wedge \frac{w}{\delta} = 1$ donc $\frac{z}{\delta} \mid \frac{\bar{w}}{\bar{\delta}}$ et est = (à inv près)

pareil : $\frac{z}{\bar{\delta}} = \frac{w}{\delta} \times$ inversible

... n'aboutit pas :c

Si $a \mid x+iy$ et $a \mid x-iy$. $a = \text{pgcd}(w,\bar{w})$

$a \mid w \Rightarrow \bar{a} \mid \bar{w}$

$a \mid \bar{w} \Rightarrow \bar{a} \mid w$

Donc $\text{ppcm}(a,\bar{a}) \mid w$ et $\text{ppcm}(a,\bar{a}) \mid \bar{w}$

Donc $a = \text{ppcm}(a,\bar{a})$. Donc $\exists u \in \mathbb{Z}[i]^\times$, $\bar{a} = ua$.

$\bar{a} = a \to a \in \mathbb{Z}$

$\bar{a} = -a \to a \in i\mathbb{Z}$

$\bar{a} = ia \to a \in (1-i)\mathbb{Z}$

$\Rightarrow \bar{a} \mid a$ + prendre la norme pr déterminer que c'est un inv.

... n'aboutit pas :c

$\left.\begin{matrix} a \mid w \\ a \mid \bar{w} \end{matrix}\right\} \Rightarrow a \mid w-\bar{w} = 2x$.

et $2y$

On peut prendre a irréductible ($\leftarrow$ x, y, β tels entre eux)

$a \mid 2x \Rightarrow a \mid 2$ ou $a \mid x$

Si $a \mid 2$, $N(a) \mid 4$ de $N(a) = 1 \rightarrow$ a inversible, impossible
$N(a) = 2 \rightarrow a = 1+i$ ou $1-i$
$N(a) = 4 \rightarrow$

Si β pair alors x et y impairs (car tels entre eux et si x pair aussi alors y aussi). β pair $\rightarrow \beta^2 \equiv 0 \ [4]$
x, y impairs de $\equiv 1, 3 \ [4] \Rightarrow x^2, y^2 \equiv 1 \ [4]$
donc $x^2 + y^2 \equiv 2 \ [4]$ impossible.

$a \mid w$, $\bar{a} \mid \bar{w}$ donc $N(a) \mid w\bar{w} = \beta^2$ de $N(a) \neq 2, 4$

Donc $a \mid x$ et $a \mid y$. $N(a) \mid \underbrace{N(x)}_{x^2}$ $N(a) \mid \underbrace{N(y)}_{y^2} \Rightarrow N(a) = 1$

(x, y, β tels entre eux $\Rightarrow$ x, y premiers entre eux (sinon $d \mid x, y$ et donc $\mid \beta$ car $x^2 + y^2 = \beta^2$) $\Rightarrow x^2, y^2$ premiers entre eux)

$\rightarrow$ Poussa pour montrer que $w \wedge \bar{w} = 1$!!
$w\bar{w} = \beta^2$ $\beta = \pi q_i^{\alpha_i}$, q_i irréductible de $\mathbb{Z}[i]$

$= \left(\pi q_i^{\alpha_i}\right)^2$ $\forall i$, ($q_i \mid w$ et $q_i \nmid \bar{w}$) ou ($q_i \mid \bar{w}$ et $q_i \nmid w$)

Donc $w = \left(\pi q_i^{\alpha_i/2}\right)^2$ selon i $\quad w = (c+id)^2 = c^2 - d^2 + 2icd$

$x = c^2 - d^2$
$y = 2cd$
$\Big) \quad x^2 + y^2 = (c^2-d^2)^2 + (2cd)^2 = c^4 + d^4 - 2c^2d^2 + 4c^2d^2$
$= (c^2+d^2)^2 = \beta^2$

$\beta = c^2 + d^2$

---

2 Décomposer $(3+j)$ en irréductibles de $\mathbb{Z}[j]$

(Rq : irréductibles de $\mathbb{Z}[j]$ caract. ds prop 37)

$N(3+j) = (3+j)(3+j^2) = 3^2 + 3j^2 + 3j + 1 = 7$ premier, $\equiv 1 \ [3]$
$\Rightarrow 3+j$ irréd. (point 3, prop 37)

3 A ppal.

Pq $\exists\, v : A \to \mathbb{N}$ tq (i) $v(a) = 0 \Leftrightarrow a = 0$

(ii) $v(ab) \geq v(a) \quad \forall a, b \in A,\ b \neq 0$

(iii) $\forall a, b \in A,\ b \neq 0$:

$v(a) \geq v(b) \Rightarrow$. soit $b \mid a$

. soit $\exists q, d \in A$,

$0 < \underbrace{v(ad - bq)}_{r} < v(b)$

$(ad = bq + r)$

($a, b \in A$. $b \neq 0$. On a $\delta = \text{pgcd}(a,b)$ et $u, v \in A$ tq $au + bv = \delta$

Si $b \nmid a$, $u \neq 0$. $au = -bv + \delta$

On prend $v(a)$ = nbre de facteurs irréductibles comptés avec multiplicité

1 ok 2 ok

3. $\delta = \text{pgcd}(a,b)$. $\exists u, v$, $au + bv = \delta$ $0 < v(\delta)$ car $\delta \neq 0$

$v(\delta) < v(b)$ $\quad \delta \mid b \Rightarrow v(\delta) \leq v(b)$

Si $v(\delta) = v(b)$ $\quad \delta = bu \Rightarrow b \mid a$ absurde.

---

4 Bf existe des anneaux non ppx tq il y ait tjs une relation de Bézout entre ses élts.

Exemple : $A =$ fonc° holomorphes.

Pq A n'est pas ppal

(Idée 1 : essayer de trouver un idéal non-ppal

$I_a = \{ f,\ f(a) = 0 \}$. $a \in \mathbb{C}$ $\quad$ Si $f \in I_a$, $f(z) = (z - a)\, g(z)$. ($g \in CA$)

$I_a = \langle (z \mapsto z - a) \rangle$

essayer d'en faire l'union ? (pour un nombre gd de a)

Idée 2 : Pq A n'est pas factoriel (et de non ppal)

Soit $f \in A$ irréductible.

. Soit $f \neq 0$ sr $\mathbb{C}$ $\Rightarrow$ f inversible donc pas irréd.

. Soit $\exists\, a \in \mathbb{C}$, $f(a) = 0$ et alors $f(z) = (z - a)\, g(z)$, $g \in A$

Donc f irréductible $\Rightarrow$ f a exactement un zéro.

Donc une fonc° holomorphe ayant une infté de 0 (exple : $\sin w$) n'admet pas de décomp (sinon nbre fini de 0) donc A pas factoriel

5 Trouver les nbres premiers qui s'écrivent $p = a^2 + 2b^2$

$a^2+2b^2 = (a+i\sqrt{2}b)(a-i\sqrt{2}b)$.

→ On se place dr $A = \mathbb{Z}[i\sqrt{2}]$. $N(\cdot) = |\cdot|^2$

• Sq A est euclidien de ppal (on cherche un stathme) =

$x = a+i\sqrt{2}b \quad y = c+i\sqrt{2}d$.

$$\frac{x}{y} = \frac{a+i\sqrt{2}b}{c+i\sqrt{2}d} = \frac{(a+i\sqrt{2}b)(c-i\sqrt{2}d)}{|c^2+2d^2|} = \frac{ac+2bd}{|c^2+2d^2|} + i\sqrt{2}\,\frac{bc-ad}{|c^2+2d^2|}$$

Soient $q_1 = \left[\frac{ac+2bd}{|c^2+2d^2|}\right]$, $q_2 = \left[\frac{bc-ad}{c^2+2d^2}\right]$ $\quad q = q_1 + i\sqrt{2}q_2$

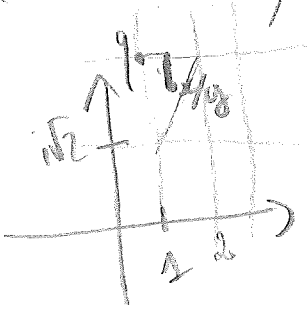
entier le + proche

$x = qy + r$

$r = x - qy = \left(\frac{x}{y} - q\right)y$. $\quad N(r) \leq \frac{1}{4} + \left(\frac{\sqrt{2}}{2}\right)^2 = \frac{1}{4} + \frac{1}{2} = \frac{1}{2}\,N(y)$

$\times N(y)$ $\quad \times N(y)$

• On refait la même chose que de la fin du dvt d.



$$\left|\frac{x}{y} - q\right| \leq \left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{2}}{2}\right)^2 = \frac{1}{4} + \frac{1}{2} = \frac{3}{4} < 1$$

$$\mathrm{Re}\left(\frac{x}{y} - q\right) \leq \frac{1}{2}$$

$$\mathrm{Im}\left(\frac{x}{y} - q\right) \leq \frac{\sqrt{2}}{2}.$$

6 $f : \mathbb{Z}^n \to \mathbb{Z}^n$ $\mathbb{Z}$-linéaire. Déterminer $\mathrm{card}\left(\mathbb{Z}^n/\mathrm{Im}f\right)$

$\exists\, B_1, B_2$ base de $\mathbb{Z}^n$ tq $\mathrm{Mat}_{(B_1,B_2)}(f) = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$ la diagonale (diviseurs élémentaires)

$\mathrm{Im}f \simeq d_1\mathbb{Z} e_1 \times \dots \times d_n\mathbb{Z} e_n \to \mathbb{Z}^n/\mathrm{Im}f \simeq \mathbb{Z}/|d_1|\mathbb{Z} \times \dots \times \mathbb{Z}/|d_n|\mathbb{Z}$ (cor 25)

de card $\prod|d_i| = |\det f|$

7| $\mathbb{C}[X,Y]/(y^2-x^3)$ et $\mathbb{C}[X,Y]/(x^4+y^2-1)$ ppx ? (5)

non

oui

(Dq : "pour savoir où chercher" ds $\mathbb{C}[X,Y]/P(X,Y)$, regarder la courbe formée par $P(X,Y)$ et si elle est lisse alors l'anneau quotient est ppae et sinon non)

(122*)

Ouvert 1/2

Développement 28

$\mathbb{Z}[i]$ et théorèmes des deux carrés

Référence : Perrin, cours d'algèbre.

Recasage : 122 = anneaux principaux
126 - équations diophantiennes
(121 - nombres premiers)

On note $\Sigma = \{ n \in \mathbb{N} \text{ t.q. } \exists a,b \in \mathbb{N},\ n = a^2+b^2 \}$
et $\mathcal{P} = \{ p \in \mathbb{N},\ p \text{ premier} \}$ et $\mathcal{P}_3 = \{ p \in \mathcal{P},\ p \equiv 3 [4] \}$

Théorème : Soit $n \geq 2$, $n = \prod_{p \in \mathcal{P}} p^{\alpha_p}$ ($\alpha_p = 0$ pour presque tous p)
Alors $n \in \Sigma$ ssi $\alpha_p \equiv 0 [2]$ pour tout $p \in \mathcal{P}_3$.

Preuve : La preuve utilise plusieurs lemmes.
Un point fondamental de la preuve est que, dans $\mathbb{Z}[i]$,
si $n, a, b \in \mathbb{N}$, alors $n = a^2+b^2$,
$\Leftrightarrow$ $n = (a+ib)(a-ib)$ dans $\mathbb{Z}[i]$. (d'où l'utilisation de $\mathbb{Z}[i]$).
Ça permet de montrer les deux premiers lemmes :

Lemme 1 : Σ est stable par multiplication.

Preuve : $n, m \in \Sigma$, d'après la remarque,
$n = y\bar{y}$, $m = y'\bar{y'}$ pour $y, y' \in \mathbb{Z}[i]$ ($N(z)$ = norme de $z \in \mathbb{C}$ = $|z|^2$)
donc $nm = y\bar{y}y'\bar{y'} \in \Sigma$
(on peut écrire explicitement une formule
$(a^2+b^2)(c^2+d^2) = N((a+ib)(c+id)) = N(ac-bd+i(ad+bc))$
$= (ac-bd)^2 + (ad+bc)^2$
$a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$
mais c'est bien plus rapide avec $\mathbb{Z}[i]$).
Ça montre l'intérêt de $\mathbb{Z}[i]$.

Lemme 2 : Soit $p \in \mathbb{N}$ premier, alors $p \in \Sigma \Leftrightarrow p$ pas premier dans $\mathbb{Z}[i]$.

carach par la norme, cf. plan

<u>Preuve</u> : $\Rightarrow$: si $p \in \Sigma$, $p = y\bar{y}$ avec $y, \bar{y}$ non inversible (sinon $p = N(y\bar{y}) = 1$), donc p n'est pas irréductible.

$\Leftarrow$: si p pas irréductible, $p = yy'$ avec y, y' non inversibles, ie $N(y) \neq 1$ et $N(y') \neq 1$.

Mais alors $p^2 = N(p) = \underbrace{N(y)}_{\in \mathbb{N}} \underbrace{N(y')}_{\in \mathbb{N}}$ donc $N(y) = p$

et $p = y\bar{y} \in \Sigma$

<u>Lemme 3</u> Soit p premier, alors $p \in \Sigma$ ssi $p \notin \mathcal{P}_3$ (ie $p = 2$ ou $p \equiv 1 [4]$).

<u>Preuve</u> : p premier, donc on a 3 possibilités :

- $p = 2 = 1^2 + 1^2 \in \Sigma$
- $p \equiv 3 [4]$. si $a \in \mathbb{N}$, on a $a^2 \equiv 0$ ou $1 [4]$

car

a	0	1	2	3
a^2	0	1	0	1

D'où $a^2 + b^2 \equiv 0, 1$ ou $2 [4]$

en particulier, si $p \equiv 3 [4]$, $p \notin \Sigma$

- si $p \equiv 1 [4]$, on va montrer que p n'est pas irréductible dans $\mathbb{Z}[i]$ et utiliser le Lemme 2.

Comme $\mathbb{Z}[i]$ est euclidien, on a p irréductible $\Leftrightarrow \mathbb{Z}[i]/(p)$ corps

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

si $p \equiv 1 [4]$, on a $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} [p] = 1$

Donc -1 est un carré dans $\mathbb{F}_p$ et X^2+1 n'est pas irréductible. Donc $\mathbb{F}_p[X]/(X^2+1)$ n'est pas un corps et $\mathbb{Z}[i]/(p)$ non plus, i.e. p n'est pas irréductible et $p \in \Sigma$ (Lemme 2).

on peut raisonner par équivalence pour faire $p \equiv 3$ et $p \equiv 1$ en même temps ici (du coup pas besoin de pl d'avant, mais) quand on met 2 à part car $\left(\frac{1}{2}\right)$ n'existe pas

$p \in \Sigma \Leftrightarrow p$ irr ds $\mathbb{Z}[i] \Leftrightarrow \mathbb{Z}[i]/(p)$ corps (car $\mathbb{Z}[i]$ ppal) $\Leftrightarrow \mathbb{Z}[X]/(X^2+1, p)$ corps (car $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$) $\Leftrightarrow \mathbb{F}_p[X]/(X^2+1)$ corps $\Leftrightarrow (X^2+1)$ irr ds $\mathbb{F}_p \Leftrightarrow -1$ pas un carré ds $\mathbb{F}_p \Leftrightarrow \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \equiv -1 [p] \Leftrightarrow \frac{p-1}{2}$ impair $\Leftrightarrow p \equiv 3 [4]$

Développement 3 — # Algorithme de Berlekamp

Références : Demazure (dans $\mathbb{F}_p$)
ou Beck-Malick-Peyré (dans $\mathbb{F}_q$)

Recasage : 123 - corps finis
141 - polynômes irréductibles
151 - dimension d'un ev
122 - anneaux principaux

Données : . $q = p^s$ avec p un nombre premier.
. $P \in \mathbb{F}_q[X]$ de degré n, sans facteur carré

Objectif : Déterminer si P est irréductible, et trouver un facteur non trivial de P s'il n'est pas irréductible

Idée générale : Pour trouver un facteur non trivial, on va en général on essaye de trouver un polynôme $S \in \mathbb{F}_q[X]$ tel que $D = \text{pgcd}(P, S) \neq 1, P$, comme ça D est un facteur non trivial de P.

On note $P = P_1 \cdots P_r$ avec les P_i irréductibles et 2 à 2 distincts (P est sans facteur carré).

Idée récurrente de l'algo : Le théorème chinois nous dit

$$A := \mathbb{F}_q[X]/(P) \cong \mathbb{F}_q[X]/(P_1) \times \cdots \times \mathbb{F}_q[X]/(P_r)$$

(A : celui on le connaît ; $P_1, \ldots, P_r$: ceux on les connaît pas, mais ce sont des corps finis.)

Dans tout l'algo, on va jongler entre A et les $\mathbb{F}_q[X]/(P_i)$ grâce au théorème chinois.

On voit A (et les $\mathbb{F}_q[X]/(P_i)$) comme l'ensemble des polynômes de degré $< n$ (ou $< n_i$).
Donc A et les $\mathbb{F}_q[X]/(P_i)$ contiennent naturellement $\mathbb{F}_q$ (l'ensemble des polynômes de degré 0).

Pour construire S, on va vouloir construire $R \in \mathbb{F}_q[X]$ tel que
$$\forall i,\ R \equiv a_i\ [P_i] \text{ avec } a_i \in \mathbb{F}_q$$
et $R \bmod P \notin \mathbb{F}_q$.

Si on a un tel R, alors il existe i, j tels que $a_i \neq a_j$. En effet, si $a_i = a_1\ \forall i$, alors $R \equiv a_1\ [P]$ d'après le théorème chinois, or on a supposé $R \bmod P \notin \mathbb{F}_q$.
Soient donc $i \neq j$ t.q. $a_i \neq a_j$.
Alors $S = R - a_i$ convient.
En effet, $S \equiv 0\ [P_i]$
$S \equiv a_j - a_i \not\equiv 0\ [P_j]$
Donc si $D = \text{pgcd}(S, P)$, $P_i \mid D$, $P_j \nmid D$ et D est bien un facteur non trivial de P.

Comment construire R ?

On va utiliser le fait que les $\mathbb{F}_q[X]/(P_i)$ sont des corps finis. Soit $B \in \mathbb{F}_q[X]/(P_i) = \mathbb{F}_{q^{n_i}}$. Alors comme $\mathbb{F}_{q^{n_i}}$ est un corps, $B \in \mathbb{F}_q$ ssi $B^q = B$ ($X^q - X$ a au plus q racines dans un corps, et les q éléments de $\mathbb{F}_q$ sont racines).
On a donc, si $R \in \mathbb{F}_q[X]$,
$$R \bmod P_i \in \mathbb{F}_q\ \forall i \iff R^q = R\ [P_i]\ \forall i$$
$$\iff R^q = R\ [P]$$
(d'après le thm chinois)

$R^q = R\ [P_i]$ n'est pas exploitable car on ne connaît pas P_i, mais on connaît P.

Comment trouver $R \in \mathbb{F}_q[X]$ tel que $R^q = R \ [P]$?

Ce qui nous sauve, c'est que

$$\varphi : A \longrightarrow A, \quad R \longmapsto R^q - R$$

est $\mathbb{F}_q$-linéaire (A est un $\mathbb{F}_q$-ev).

En effet, on a $(R_1 + \lambda R_2)^q = R_1^q + \lambda^q R_2^q$

$= R_1^q + \lambda R_2^q$ ($\lambda \in \mathbb{F}_q$)

Donc $R \longmapsto R^q$ est linéaire, et φ aussi.

On peut donc calculer une base de φ, avec un pivot de Gauss par exemple.

Avec ce qu'on vient de voir et le lemme chinois, on voit qu'on a une bijection (isomorphisme même)

$$\ker(\varphi) \longrightarrow \mathbb{F}_q \times \cdots \times \mathbb{F}_q$$
$$\bar{R} \longmapsto (R \bmod P_1, \ldots, R \bmod P_r)$$

Donc $\ker(\varphi) \cong \mathbb{F}_q^r$ et $\dim(\ker(\varphi)) = r$

On en déduit que P est irréductible ssi $\dim(\ker(\varphi)) = 1$.

Et si $\dim(\ker(\varphi)) > 1$, alors il existe

$\bar{R} \in \ker(\varphi) \setminus \mathbb{F}_q$ (car $\mathbb{F}_q$ est de dim 1 dans A).

On a donc bien R relevé de $\bar{R}$ tel que

$R \bmod P \notin \mathbb{F}_q$

et $R \bmod P_i \in \mathbb{F}_q$ $\forall i$

Donc on peut trouver un facteur non trivial de P

Remarque : Une fois qu'on a R, pour calculer S, comme on ne connaît pas a, on teste $R - a$ pour tout $a \in \mathbb{F}_q$ $\Rightarrow$ complexité $O(q)$, c'est pas super. Si q est grand, la variante probabiliste est bien plus rapide.