122

Anneaux principaux. Exemples et applications

Dans toute cette leçon A est un anneau unitaire commutatif et intègre.

I Premières propriétés

1) Anneaux principaux

Déf 1 : Un idéal I est dit principal si $\exists a \in A$, $I = (a) = aA$.
A, intègre, est dit principal si tous ses idéaux le sont.

Ex 2 : $\mathbb{Z}$, les corps, $\mathbb{C}[X,Y]/(XY-1)$, $\mathbb{C}[X,Y]/(Y-X^2)$ sont principaux. Dev

Prop 3 : Dans un anneau principal, toute suite croissante d'idéaux est stationnaire.

Déf 4 : Un idéal propre I de A est dit :
premier ssi A/I intègre ssi $\forall a,b \in A$ $ab \in I \Rightarrow a \in I$ ou $b \in I$.
maximal ssi A/I est un corps ssi I maximal pour $\subset$.

Rmq 5 : Un idéal maximal est premier

Ex 6 : Les idéaux premiers de $\mathbb{Z}$ sont les $p\mathbb{Z}$ avec $p \in \mathcal{P}$

C-Ex 7 : Dans $k[X,Y]$ (X) est premier non maximal.

Déf 8 Soit $q \in A$ q est irréductible si $q \notin A^*$, et $q = ab \Rightarrow a \in A^*$ ou $b \in A^*$

Prop 9 Si (q) est premier alors q est irréductible.

C-Ex 10 Dans $\mathbb{Z}[i\sqrt{5}]$ 2 est irréductible et (2) non-premier.
car $(1+i\sqrt{5})(1-i\sqrt{5}) = 6 \in (2)$

Prop 11 : Quand A est principal, $p \in A \setminus \{0\}$ il y a équivalence entre
(i) p irréductible
(ii) (p) est un idéal premier de A
(iii) (p) est un idéal maximal de A

Rmq 12 : En fait on a p irréductible ssi (p) maximal pour l'inclusion parmi les idéaux principaux propres de A, sans supposer A principal.

Ex 13 : Dans $\mathbb{Z}$, $p\mathbb{Z}$ est maximal et p est irréductible

App 14 : X^2+1 est irréductible dans $\mathbb{R}[X]$ principal, on définit donc un corps $\mathbb{C} := \mathbb{R}[X]/(X^2+1)$

Rem 15 : Dans $\mathbb{Z}/6\mathbb{Z}$ et $End_k(k^n)$ tous les idéaux sont engendrés par un seul élément. Cependant ce ne sont pas des anneaux principaux par défaut d'intégrité et de commutativité.

2) Anneaux euclidiens

Déf 16 : A est dit euclidien si il existe une fonction (appelée stathme) $v : A - \{0\} \to \mathbb{N}$; $\forall a \forall b \in A \setminus \{0\}$ $\exists q, r \in A$ avec $a = bq + r$ et $v(r) < v(b)$ ou $r = 0$. On dit que A est muni d'une division euclidienne.

Ex 17 : $\mathbb{N}$ et $\mathbb{Z}$ sont euclidiens pour le stathme $|\ |$
$\mathbb{Z}[i]$ est euclidien pour $v : a+ib \mapsto a^2+b^2$

Prop 18 : Un anneau euclidien est principal.

Prop 19 : Si A est euclidien il existe $x \in A \setminus A^*$ tel que la restriction de la projection sur $A/(x)$ à $A^* \cup \{0\}$ soit surjective.

C-Ex 20 : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal non-euclidien.

Prop 21 : $k[X]$ est principal ssi k est un corps.

C-Ex 22 : $\mathbb{Z}[X]$, $k[X,Y]$ ne sont pas principaux.

Ex 23 : $\mathbb{R}[X]$, $\mathbb{C}[X]$, et $\mathbb{F}_p[X]$ sont des corps pour tout p premier.

II Arithmétique dans les anneaux principaux

1) Divisibilité A est supposé principal

Déf 24 (i) Soient $a, b \in A$ on dit que "a divise b" $(a|b)$ si $(b) \subset (a)$
(ii) d est un pgcd de a et b $(d = a \wedge b)$ si $(a,b) = (d)$
(iii) m est un ppcm de a et b $(m = a \vee b)$ si $(a) \cap (b) = (m)$

Rem 25 : Ces éléments dont l'existence est assuré par la principalité de A sont respectivement le plus grand commun diviseur et le plus petit multiple commun à a et b

Prop 26 : Si $d = a \wedge b$ ssi il existe $a', b', u, v \in A$: $d = au + bv$ $a = da'$ et $b = db'$. De plus on a $m = a \vee b = a'b'd$ et $ab = md$.

Déf 27 : On dit que a et b sont premiers entre eux dans A ssi $a \wedge b = 1$, ou encore $\exists u, v$ $au + bv = 1$

Cor 28 : (Lemme de Gauss) si $a \wedge b = 1$ et $a | bc$ alors $a | c$

App 29 : L'ensemble $\mathcal{P}$ des nombres premiers est infini

Ex 30 : $(X^2+X+1) \wedge (X+2)$ sont premiers entre eux car $1 \times (X^2+2X+1) - X(X+2) = 1$

Rem 31 : L'algorithme d'Euclide étendu permet le calcul des u, v, d tel que $d = au + bv$ et $d = a \wedge b$.

App 32 : Soit $a \wedge n = 1$ $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ et si $au + nv = 1$ $\bar{u}$ est l'inverse de $\bar{a}$.

Thm 33 : (Théorème chinois) Soit $x; y \in A$ $x \wedge y = 1$ alors
$$\varphi : A/(xy) \to A/(x) \times A/(y) \qquad \pi_{xy}(a) \mapsto (\pi_x(a) ; \pi_y(a))$$
est un isomorphisme d'anneaux

où π_* la projection canonique de A sur $A/(*)$

App 34 : Résolution de systèmes de congruence dans $\mathbb{Z}$

2) FACTORIALITÉ DES ANNEAUX PRINCIPAUX

Déf 35 : - $a; b \in A$ sont associés ssi $a | b$ et $b | a$ ssi $\exists u \in A^\times$ $a = ub$ c'est une relation d'équivalence : $a \sim b$

- Un système de représentants d'irréductibles est un ensemble $\mathcal{P}$ d'irréductibles tel que $\forall p$ irréductible $\exists q \in \mathcal{P}$ $q \sim p$
- A est factoriel s'il est intègre et pour tout système d'irréductibles $\mathcal{P}$ $\forall a \in A \setminus \{0\}$ a s'écrit de manière unique $u \prod_{p \in \mathcal{P}} p^{v_p(a)}$ avec $v_p(a) \in \mathbb{N}$, $u \in A^\times$ et $\{p ; v_p(a) \neq 0\}$ est fini

Thm 36 : Un anneau principal est factoriel

Ex 37 : La décomposition en nombres premiers dans $\mathbb{Z}$, et en polynômes irréductibles unitaires dans $k[X]$, avec k un corps

III MODULE DE TYPE FINI SUR UN ANNEAU PRINCIPAL

Soit A principal (toujours supposé unitaire et commutatif)

Prop 38 : Soit n un entier, M un A-module libre de rang m et soit $N \subseteq M$ un sous-module, alors N est libre de rang n, $n \leq m$

Lemme 39 : Soit M un A-module sans torsion et $x \neq 0$ dans M. Alors Ax admet un supplémentaire dans M si et seulement si il existe une forme A-linéaire φ sur M, telle que $\varphi(x) = 1$

Lemme 40 : Soit M un A-module, libre de base $(e_1 \cdots e_m)$; soit $x \in M$. Le pgcd des coordonnées de x vaut 1 si et seulement si il existe une forme A-linéaire φ, telle que $\varphi(x) = 1$

Théorème 41 : (de la base adaptée) Soit $N \subseteq M$ des A-modules avec M libre de rang m. Alors il existe $r \leq m$, $d_1 \dots d_r \in A \setminus \{0\}$ $d_1 | d_2 \cdots | d_r$ et une base $(\ell_1 \cdots \ell_m)$ de M tel que $(d_1\ell_1, d_2\ell_2 \cdots d_r\ell_m)$ soit une base de N

Théorème 42 : (de structure des modules) Soit V un A-module de type fini. $\exists n \geq 0$ et $d_1 \dots d_n \in A \setminus A^\times$ tels que $d_1 | d_2 \cdots | d_n$ et $V \simeq A/(d_1) \oplus A/(d_2) \oplus \cdots \oplus A/(d_n)$ de plus les (d_i) sont uniques à inversibles près

Rem 43 : Un groupe abélien est trivialement un $\mathbb{Z}$-module. On obtient ainsi le théorème de structure des groupes abéliens finis

Rem 44 : Un espace vectoriel muni de $u \in End(E)$ est muni d'une structure de $k[X]$-module (par la formule $P.x = P(u)(x)$) En dimension finie, on obtient le théorème de réduction de Frobenius

IV EXEMPLES ET APPLICATIONS

1) ANNEAUX DES SÉRIES FORMELLES

Prop 45 : Soit $P = \sum_{i \geq 0} a_i X^i \in k[[X]]$ alors P inversible ssi $a_0 \neq 0$

Prop 46 : Tous les idéaux de $k[[X]]$ non-nuls sont de la forme (X^p), $p \in$ En particulier cet anneau est principal, tous ses irréductibles sont associés à X, et il est même euclidien.

2) ANNEAU DES ENTIERS DE GAUSS

Déf 47 : On note $\mathbb{Z}[i]$ l'anneau des entiers de Gauss i.e $\{a+ib \in \mathbb{C},\ a \in \mathbb{Z}\ b \in \mathbb{Z}\}$ On définit $N : \mathbb{Z}[i] \to \mathbb{N}$, $a+ib \mapsto (a+ib)(\overline{a+ib}) = a^2+b^2$
N est multiplicative

Prop 48 : $\mathbb{Z}[i]^\times = \{\pm 1 ; \pm i\}$

DEV2 **Prop 49** : $\mathbb{Z}[i]$ est euclidien pour le stathme N

Thm 50 : (des deux carrés) Soit p premier dans $\mathbb{N}$ p est la somme de deux carrés ssi $p = 2$ ou $p \equiv 1 [4]$ et si $n \in \mathbb{N}$ il est somme de deux carrés ssi $\forall p \in \mathcal{P}$ $p \equiv 3[4] \Rightarrow v_p(n)$ pair

3) Application à l'algèbre linéaire

Prop 51 : Soit E un k-ev $End_k(E)$ l'algèbre des endomorphismes de E $\forall x \in E$ $\forall u \in End_k(E)$ les applications suivantes sont des morphismes d'anneaux :
$$\varphi : k[X] \to End_k(E), \quad P \mapsto P(u)$$
$$\psi_x : k[X] \to E, \quad P \mapsto P(u)(x)$$
Comme $k[X]$ est principal $\exists! \pi_u$ $\exists! \pi_{u,x}$, tels que $(\pi_u) = Ker(\varphi)$ $(\pi_{u,x}) = Ker(\psi_x)$. Ce sont respectivement le polynôme minimal de u et le polynôme minimal ponctuel de u en x.

__Lemme 52 :__ (des noyaux) Soit $u \in End_k(E)$ et $P = P_1 P_2 \cdots P_k \in k[X]$ avec $\forall i,j$ $P_i \wedge P_j = 1$ alors $Ker(P(u)) = Ker(P_1(u)) \oplus Ker(P_2(u)) \cdots \oplus Ker(P_k(u))$

__Appli 53 :__ $u \in End_k(E)$ est diagonalisable si et seulement si $\exists P \in k[X]$ tel que $P(u) = 0$ et P scindé à racines simples sur k.

__Appli 54 :__ $u \in End_k(E)$ et P scindé annulant u, alors il existe un unique couple $(d,n) \in End_k(E)^2$ avec d diagonalisable et n nilpotente tels que $u = d+n$, $dn = nd$.
C'est la décomposition de Dunford de u.

[FG] Exercices de mathématiques pour l'agrégation : Algèbre 1

[PER] Cours d'algèbre, Daniel Perrin

[GOU] Algèbre, Xavier Gourdon

[COL] Eléments d'analyse et d'algèbre, Pierre Colmez

Cours d'Antoine Ducros : Modules de type fini sur un anneau principal

$\mathbb{C}[X,Y]/(Y-X^2)$ 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 $\varphi : \begin{array}{rcl} \mathbb{C}[X,Y] & \longrightarrow & \mathbb{C}[T] \\ P(X,Y) & \longmapsto & P(T,T^2) \end{array}$ est un morphisme

* 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

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

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

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

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

$$:= F^{-1}\mathbb{C}[T]$$

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 (intégrité degré)
- (Inversibles de $\mathbb{Z}[X]$ ... $c(P) = 1$.
 [illegible] éléments? $\mathbb{Z}/_{2\mathbb{Z}}[X]/(X^2+X+1)$
 Démontrer $a \wedge b = 1$, $a | c$, $b | c$ ... valable dans un anneau factoriel.

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 $|\alpha| \leq \frac{1}{2}$ et $|\beta| \leq \frac{1}{2}$

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

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

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

$(\Longrightarrow)$ * $p = 1 + 1 = 2 \in \Sigma$

* 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 $p \equiv 1 [4]$

$(\Longleftarrow)$ On commence par introduire un lemme.

<u>Lemme</u> : Soit p un nombre premier.
$p \in \Sigma \iff p$ 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 $\iff X^2 + 1$ réductible dans $\mathbb{F}_p[X]$
$\iff X^2 + 1$ a une racine dans $\mathbb{F}_p$

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

Donc d'après le lemme, $p \in \Sigma \iff (-1)$ 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 $n\geq 2$, $n=\prod_{p\in\mathcal{P}} p^{v_p(n)}$, $n\in\Sigma \Leftrightarrow v_p(n)$ pair pour $p\equiv 3[4]$

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

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

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

Donc $v_p(n) = v_p\left(\frac{n}{p^2}\right) + 2$ 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 dans $\mathbb{Z}$, c'est il dans [illegible] ?

$\mathbb{Z}[i\sqrt{5}]$ décomp unique en [illegible] ?

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

[illegible] irréductible [illegible] $1 + i\sqrt{5}$?

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

Connaître [illegible] isomorphismes entre les [illegible]

→ Mettre la divisibilité comment