

Théorème des 2 carrés: Kern p. 56 121-122-126

$$\Sigma = \{ n \in \mathbb{N} \setminus \{0, 1\} \mid n = a^2 + b^2, a, b \in \mathbb{N} \} = \{ n \in \mathbb{N} \mid n = \prod_{p \in P} p^{r_p(n)} \mid r_p(n) \text{ est pair si } p \equiv 3 \pmod{4} \}$$

(admis)

Lemme 1: $\mathbb{Z}[i]$ est euclidien par le Norme $N: \mathbb{Z}[i] \rightarrow \mathbb{N}$
 $z = a+ib \mapsto z\bar{z} = a^2 + b^2$

Lemme 2: p premier; $p \in \Sigma \iff p$ est non irréductible dans $\mathbb{Z}[i]^\times$

$$\Leftrightarrow -1 \text{ est un carré de } \mathbb{F}_p \iff p = 2 \text{ ou } p \equiv 1 \pmod{4}$$

(b) $\Leftrightarrow$

Remarque: $\mathbb{Z}[i]$ est donc principal et donc factoriel (1)

(2) Σ est stable par multiplication

$\bullet N$ est multiplicatif

$$\bullet n \in \Sigma \iff \exists z \in \mathbb{Z}[i] \mid n = N(z)$$

$$\bullet n \equiv 3 \pmod{4} \rightarrow n \notin \Sigma.$$

Lemme 1. Soient $s, t \in \mathbb{Z}[i] \setminus \{0\}$; on considère $\frac{s}{t} \in \mathbb{C}$ qui a écrit sous la forme $\frac{s}{t} = a+ib$; $a, b \in \mathbb{R}$. On pose $q = x+iy \in \mathbb{Z}[i]$ où x et y sont les entiers les plus proches de a, b respectivement.

$$\text{On pose } r = s - qt \text{ alors } |r| = |t| \left| \frac{s}{t} - q \right| \leq |t| \sqrt{(a-x)^2 + (b-y)^2} \leq |t| \frac{\sqrt{2}}{2} < |t|$$

$$\text{donc } N(r) < N(t) \text{ et } s = qt + r. \quad \square \quad (1)$$

est non inversible dans $\mathbb{Z}[i]$ donc $p \neq \pm 1, \pm i$

Lemme 2: (a) $\Rightarrow$ si $p \in \Sigma$ alors $p = a^2 + b^2 = (a+ib)(a-ib)$ avec a et $b \neq 0$ donc $a+ib, a-ib \notin \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ donc p n'est pas irréductible. (3)

$$\Leftrightarrow \text{si } p = z\bar{z} \text{ avec } z, \bar{z} \notin \mathbb{Z}[i]^\times, \text{ alors } N(p) = p^2 = N(z)N(\bar{z}) \text{ avec } N(z), N(\bar{z}) \neq 1 \text{ donc } N(z) = N(\bar{z}) = p \text{ donc } p \in \Sigma.$$

(c) $\nexists \delta: p \neq 2$

$$\text{On note } \mathbb{F}_p^\times = \{ \text{carrés de } \mathbb{F}_p^\times \}. \text{ On pose } X = \{ x \in \mathbb{F}_p^\times \mid x^{\frac{p-1}{2}} = 1 \}$$

Alors $|X| \leq \frac{p-1}{2}$ car $x^{p-1/2} = 1$ admet au plus $\frac{p-1}{2}$ racines.

Et $x \in \mathbb{F}_p^{*2} \Leftrightarrow \exists y \in \mathbb{F}_p^* \mid x = y^2 \Rightarrow x^{p-1/2} = y^{p-1} = 1$

donc $\mathbb{F}_p^{*2} \subset X$ donc $\mathbb{F}_p^{*2} = X$, car $|\mathbb{F}_p^{*2}| = \frac{p-1}{2}$ (4)

Et $-1 \in \mathbb{F}_p^{*2} \Leftrightarrow (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow \frac{p-1}{2}$ pair $\Leftrightarrow p \equiv 1 \pmod{4}$.

* si $p = 2$; ~~$\mathbb{Z} = \mathbb{Z}^2 + \mathbb{Z}^2 \oplus \mathbb{Z}$~~ $-1 = i^2$ dans $\mathbb{F}_2$ donc ok un carré.

(b) Comme $\mathbb{Z}[i]$ est principal: p non irréductible $\Leftrightarrow (p)$ non premier

$\Leftrightarrow \mathbb{Z}[i]/(p)$ non intègre. (5)

Or $\mathbb{Z}[i]/(p) \cong \mathbb{F}_p[x]/(x^2+1)$ (6)

donc p non irréductible $\Leftrightarrow x^2+1$ admet une racine dans $\mathbb{F}_p$

$\Leftrightarrow -1 \in \mathbb{F}_p^{*2}$ $\square$

démonstration: $\mathbb{Z}[i]$ est factoriel donc: $n = \prod_{p \in P} p^{v_p(n)}$

(c) $n = \underbrace{\prod_{\substack{p \in P \\ p \equiv 1,2 \pmod{4}}} p^{v_p(n)}}_{\in \Sigma \text{ par stabilité et par la ligne 2}} \cdot \underbrace{\prod_{\substack{p \in P \\ p \equiv 3 \pmod{4}}} (p^k)^2}_{\in \Sigma \text{ par stabilité et } (p^k)^2 \text{ est un carré}}$

(c) $n = \prod_{p \in P} p^{v_p(n)}$. Soit $p \in P$ tel que $p \equiv 3 \pmod{4}$.
~~récurse sur $v_p(n)$ que $v_p(n)$ est pair.~~ Supposons que pour les $n-1$ 1^{ers} éléments de Σ , $\forall p \equiv 3 \pmod{4} \Rightarrow v_p(k)$ pair $\forall k \in \{0, \dots, n-1\}$
 Soit $p \nmid n$ alors $v_p(n) = 0$ et c'est ok.
 * si non, $p \mid n$ alors $p \mid n$ l'élément suivant $p \mid n = a^2 + b^2 = (a+bi)(a-bi)$. Or $p \equiv 3 \pmod{4} \Rightarrow p \nmid \Sigma \Rightarrow$

p est irréductible. donc $p \mid a+bi$ par exemple.

p étant entier, $p \mid a$ et $p \mid b$ donc $p^2 \mid n$ et $a = pa'$; $b = pb'$

donc $\frac{n}{p^2} = a'^2 + b'^2 \in \Sigma$ $\downarrow \frac{n}{p^2} < n$

Par hypothèse de récurrence: $v_p(\frac{n}{p^2})$ est pair, donc $v_p(n) = 2 + v_p(\frac{n}{p^2})$ aussi $\square$

Initialisation: $n = 2 = 1^2 + 1^2 = 2'$
 $v_2(2) = 1$

① p. 50 * euclidien $\Rightarrow$ pp

Soit I idéal de A ; $I \neq \{0\}$; soit $b \in I \setminus \{0\}$ / $\forall b$ soit min parmi les éléments de $I \setminus \{0\}$

Soit $a \in I$; $a = bq + r$ avec $r = 0$ ou $\nu(r) < \nu(b)$

Alors $r = a - bq \in I$ avec $\nu(r) < \nu(b)$ donc $r = 0$

donc $a \in (b)$ donc $I = (b)$

* pp $\Rightarrow$ factoriel

pp $\Rightarrow$ noethérien $\Rightarrow \forall a \in A \setminus \{0\}$, $a = u \prod_{p \in P} p^{\nu_p(a)}$, $u \in A^\times$, $\nu_p(a) \in \mathbb{N}$

p pr dans $A \Rightarrow (p)$ max parmi les idéaux $p \neq A \Rightarrow (p)$ max tout court

$\Rightarrow (p)$ premier

donc p pr $\Leftrightarrow p$ premier $\Leftrightarrow p$ factoriel.

③ Soit $z \in \mathbb{Z}[i]^\times$ alors $\exists z' \in \mathbb{Z}[i]^\times$ / $zz' = 1$

Alors $N(zz') = N(z)N(z') = 1 \Rightarrow N(z) = N(z') = 1 = a^2 + b^2$

intr dans $\mathbb{N}$

donc $a = 0$ et $b = \pm 1$ ou $a = \pm 1$ et $b = 0$ donc $z = \pm 1, \pm i$

la réciproque est évidente.

④ p. 74 $q = p^n$; $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q \mid x = y^2\}$

* $p = 2 \Rightarrow \mathbb{F}_q^2 = \mathbb{F}_q$

En effet: $f: \mathbb{F}_q \rightarrow \mathbb{F}_q$ est un automorphisme

$x \mapsto x^2$

- $f(xy) = f(x)f(y)$ • $(x+y)^2 = x^2 + y^2$
- Un sous-corps est toujours intègre / on vérifie qu'un idéal I de A est un idéal de K car $1 \mapsto 1$

* $p > 2$; $1 \neq -1$ dans $\mathbb{F}_q$; on a la suite exacte

$$1 \rightarrow \{\pm 1\} \xrightarrow{i} \mathbb{F}_q^\times \xrightarrow{\pi} \mathbb{F}_q^{\times 2} \rightarrow 1$$

$x \mapsto x^2$

i injectif / $\text{Im}(i)$
 π surjectif / $\text{Ker}(\pi)$

Par th' d'ire: $\mathbb{F}_9^{\times} / \{ \pm 1 \} \simeq \mathbb{F}_9^{\times 2}$ donc $\frac{p-1}{2} = |\mathbb{F}_9^{\times 2}|$

⑥ ~~Disy~~: $\left[a) A/I / J/I \simeq A/J \text{ où } I \subset J \subset A \text{ idéaux} \right]$

b) $f: B \rightarrow C$ isomorphisme; $I \subset B$ idéal $\Rightarrow B/I \simeq C/f(I)$

Aci: On a $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[x]/(x^2+1)$

$\varphi: \mathbb{Z}[x] \rightarrow \mathbb{Z}[i]$ induit un iso $\bar{\varphi}: \mathbb{Z}[x]/(x^2+1) \rightarrow \mathbb{Z}[i]$
 $p \mapsto p(i)$

donc par b): $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[x]/(x^2+1) / \bar{\varphi}((p)) = \mathbb{Z}[x]/(x^2+1) / (p) = \mathbb{Z}[x]/(p) / (x^2+1)$

$\psi: \mathbb{Z}[x] \rightarrow \mathbb{Z}/p\mathbb{Z}[x]$ induit un iso $\mathbb{Z}[x]/(p) \simeq \mathbb{Z}/p\mathbb{Z}[x]$
 $p \mapsto \bar{p}$

donc par b): $\mathbb{Z}[x]/(p) / (x^2+1) \simeq \mathbb{Z}/p\mathbb{Z}[x] / \tilde{\psi}((x^2+1)) = \mathbb{Z}/p\mathbb{Z}[x] / (x^2+1)$

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