PRÉPARATION À L'AGRÉGATION EXTERNE : ENTIERS DE GAUSS

TONY LIMAGNE

Ce développement est adapté pour les leçons 122 et 127. Cette fiche se base essentiellement sur [P, Chap.2].

1. Préliminaires

On aura besoin d'un lemme de théorie des anneaux :

Lemme 1. Soient A un anneau commutatif et $a, b \in A$. On note $\pi : A \to A/(a)$ la surjection canonique. L'anneau $\mathrm{A}/(a, b)$ est isomorphe à $(A/(a))/(\pi(b))$.

Démonstration. Comme $(a) \subseteq (a, b)$ alors $A/(a, b)$ est un idéal de $A/(a)$. Notons $\rho : A \to A/(a, b)$ la surjection canonique. Par la propriété universelle de l'anneau quotient on a le diagramme

$$\begin{array}{ccc} A & \xrightarrow{\rho} & A/(a,b) \\ {\scriptstyle\pi}\downarrow & \nearrow_{\exists \overline{\rho}} & \\ A/(a) & & \end{array}$$

Le morphisme $\overline{\rho}$ est surjectif car ρ l'est. Le morphisme ρ est aussi injectif car

$$\overline{x} \in \ker(\overline{\rho}) \quad \Leftrightarrow \quad x \in \ker(\rho) \quad \Leftrightarrow \quad x \in (a, b) \quad \Leftrightarrow \quad \overline{x} \in \pi(bA) = (\pi(b)).$$

□

2. Le développement

L'objectif est d'étudier l'anneau des entiers de Gauss

$$\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}.$$

La proposition suivante dit formellement que décrire $\mathbb{Z}[i]$ revient à déterminer ses inversibles et ses éléments irréductibles.

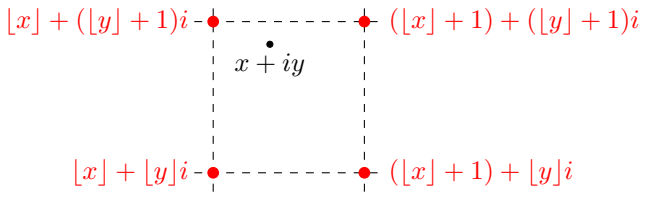
Proposition 2. L'anneau $\mathbb{Z}[i]$ est euclidien (et donc en particulier $\mathbb{Z}[i]$ est principal, donc factoriel).

Démonstration. Fixons $z, t \in \mathbb{Z}[i]$ avec $t \neq 0$. En regardant z et t comme éléments de $\mathbb{C}$ on peut écrire

$$\frac{z}{t} = x + iy,$$

où x et y sont deux nombres réels (x et y sont mêmes rationnels). Les relations $\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1$ et $\lfloor y \rfloor \leqslant y < \lfloor y \rfloor + 1$ permettent d'encadrer le nombre complexe $x + iy$ dans un carré du réseau $\mathbb{Z}[i]$ à savoir

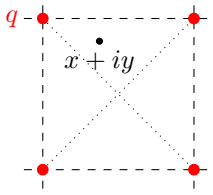
Date: Année 2025.



Parmi les quatre sommets du carré, il y en a au moins un, d'affixe $q \in \mathbb{Z}[i]$, qui vérifie

$$\left|\frac{z}{t} - q\right| \leqslant \frac{\sqrt{2}}{2} < 1.$$

de sorte que l'éément $r = z - qt \in \mathbb{Z}[i]$ vérifie $|r| < |t|$. Ainsi on a la division



euclidienne $z = qt + r$ associée au stathme $N : \mathbb{Z}[i] \to \mathbb{N}, z \mapsto |z|^2$. □

Pour décrire $\mathbb{Z}[i]$ il s'avère commode d'étudier en parallèle l'ensemble des entiers qui s'écrivent comme somme de deux carrés d'entiers :

$$\Sigma = \{N(z) : z \in \mathbb{Z}[i]\} = \{n \in \mathbb{N} : \exists (a,b) \in \mathbb{Z}, n = a^2 + b^2\}.$$

Proposition 3. (1) On a $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

(2) Un nombre premier p est réductible dans $\mathbb{Z}[i]$ si et seulement si $p = 2$ ou $p = 1 \mod 4$.

(3) Les éléments irréductibles de $\mathbb{Z}[i]$ sont, aux inversibles près : les nombres premiers p tels que $p = 3 \mod 4$ et les éléments de $\mathbb{Z}[i]$ dont la norme est un nombre premier.

Démonstration. (1) Lorsque $z, z' \in \mathbb{Z}[i]$ sont non nuls et vérifient $zz' = 1$ alors $N(z)N(z') = 1$. Et puisque N est à valeurs entières positives et multiplicative l'équation précédente entraine $N(z) = N(z') = 1$. Réciproquement, si $z \in \mathbb{Z}[i]$ est non nul et vérifie $N(z) = 1$ alors son inverse dans $\mathbb{C}$ est $\frac{\overline{z}}{N(z)} = \overline{z}$ qui est bien dans $\mathbb{Z}[i]$. Ainsi on vient de prouver l'équivalence

$$z \in \mathbb{Z}[i]^\times \quad \Leftrightarrow \quad N(z) = 1.$$

Pour déterminer $\mathbb{Z}[i]^\times$ il suffit alors de résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation diophantienne

$$x^2 + y^2 = 1.$$

Fixons (x, y) un couple solution. On ne peut avoir $|x| \geqslant 2$ ou $|y| \geqslant 2$ de sorte que $x \in \{0, \pm 1\}$ et $y \in \{0, \pm 1\}$. On a alors quatre possibilités : $(x, y) = (-1, 0)$, $(x, y) = (1, 0)$, $(x, y) = (0, -1)$ ou $(x, y) = (0, 1)$. Ces couples sont au passage bien solutions de l'équation en question. Ces couples forment les parties réelles et imaginaires des éléments de $\mathbb{Z}[i]^\times$ qui sont maintenant entièrement déterminés : $\mathbb{Z}[i]^\times = \{-1, 1, -i, i\}$.

(2) Fixons p un nombre premier. Soit z un diviseur de p dans $\mathbb{Z}[i]$: $p = zz'$. Par multiplicativité de la fonction N, les entiers $N(z)$ et $N(z')$ divisent p^2. On a donc

$$N(z), N(z') = 1, p \text{ ou } p^2.$$

Si z et $z' \in \mathbb{Z}[i]$ ne sont pas inversibles alors $N(z) > 1$ et $N(z') > 1$ et il reste alors

$$N(z) = N(z') = p.$$

On en déduit que si p est réductible dans $\mathbb{Z}[i]$ alors $p \in \Sigma$. Réciproquement, soit $p \in \Sigma$ écrit $p = a^2 + b^2$ avec $a, b \in \mathbb{Z}$. On a $p = (a + ib)(a - ib)$ qui est une factorisation de p dans $\mathbb{Z}[i]$ faisant intervenir deux facteurs non inversibles (car $N(a + ib) = N(a - ib) = a^2 + b^2 > 1$). En résumé on a l'équivalence

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

Montrons qu'alors

$$p \in \Sigma \quad \Leftrightarrow \quad p = 2 \quad \text{ou} \quad p = 1 \mod 4.$$

Le cas $p = 2$ est clair car $2 = 1 + 1$. Supposons p impair. Le morphisme d'évaluation $\mathbb{Z}[X] \to \mathbb{Z}[i], P \to P(i)$ en i et la réduction $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ modulo p induisent les isomorphismes d'anneaux

$$\mathbb{Z}[X]/(X^2 + 1) \cong \mathbb{Z}[i] \qquad \text{et} \qquad \mathbb{Z}[X]/p\,\mathbb{Z}[X] \cong \mathbb{F}_p[X].$$

Par le lemme 1, on a les isomorphismes d'anneaux suivants

$$\begin{aligned} \mathbb{Z}[i]/p\,\mathbb{Z}[i] &\cong (\mathbb{Z}[X]/(X^2 + 1))/p\,\mathbb{Z}[X] \cong \mathbb{Z}[X]/(X^2 + 1, p), \\ &\cong (\mathbb{Z}[X]/p\,\mathbb{Z}[X])/(X^2 + 1) \cong \mathbb{F}_p[X]/(X^2 + 1). \end{aligned}$$

On a donc

$$\begin{aligned} p \in \Sigma \quad &\Leftrightarrow \quad p \text{ réductible dans } \mathbb{Z}[i], \\ &\Leftrightarrow \quad p\,\mathbb{Z}[i] \text{ non premier dans } \mathbb{Z}[i] \text{ car } \mathbb{Z}[i] \text{ est principal}, \\ &\Leftrightarrow \quad \mathbb{Z}[i]/p\,\mathbb{Z}[i] \text{ non intègre}, \\ &\Leftrightarrow \quad \mathbb{F}_p[X]/(X^2 + 1) \text{ non intègre}, \\ &\Leftrightarrow \quad (X^2 + 1) \text{ non premier dans } \mathbb{F}_p[X], \\ &\Leftrightarrow \quad X^2 + 1 \text{ réductible dans } \mathbb{F}_p[X] \text{ car } \mathbb{F}_p[X] \text{ est principal}, \\ &\Leftrightarrow \quad X^2 + 1 \text{ a une racine sur } \mathbb{F}_p, \\ &\Leftrightarrow \quad -1 \in \mathbb{F}_p^{*2}. \end{aligned}$$

Or les éléments de $\mathbb{F}_p^{*2}$ sont exactement les racines de $X^{(p-1)/2} - 1$. On peut donc conclure

$$p \in \Sigma \quad \Leftrightarrow \quad (-1)^{(p-1)/2} = 1 \quad \Leftrightarrow \quad p = 1 \mod 4.$$

(3) On a déjà montrer que les nombres premiers p tels que $p \equiv 3 \mod 4$ sont irréductibles dans $\mathbb{Z}[i]$. Soit $t = a + ib$ un entier de Gauss tel que $a^2 + b^2$ est un nombre premier. Soient z, z' dans $\mathbb{Z}[i]$ tels que $zz' = t$. On a $N(z)N(z') = a^2 + b^2$. Et puisque $a^2 + b^2$ est premier, l'un des entiers $N(z), N(z')$ vaut 1, et donc l'un des éléments z, z' est inversibles dans $\mathbb{Z}[i]$: t est donc irréductible.

Réciproquement, soit $z \in \mathbb{Z}[i]$ irréductible. Comme z n'est pas nul, ni inversible alors $N(z) \geqslant 2$. Soit p un facteur premier de $N(z)$. Si $p \equiv 3 \mod 4$ alors p est irréductible dans sur $\mathbb{Z}[i]$. Et puisque p divise $z\overline{z}$ dans $\mathbb{Z}[i]$ alors d'après le lemme d'Euclide :

(1) soit p divise z et dans ce cas $z = \pm p$ ou $z = \pm ip$;

(2) soit p divise $\overline{z}$ et dans ce cas $z = \pm p$ ou $z = \pm ip$ car $\overline{z}$ est encore irréductible ;

Si $p \equiv 1 \mod 4$ alors $p \in \Sigma$ et s'écrit $p = a^2 + b^2$ avec $a, b \in \mathbb{Z}$. L'entier de Gauss $s = a + ib$ est donc irréductible (voir ci-dessus) et divise z ou $\overline{z}$ si bien que $z \in \{\pm s, \pm\overline{s}, \pm is, \pm i\overline{s}\}$. □

Remarque 4. On peut utiliser la factorialité de $\mathbb{Z}[i]$ pour résoudre certaines équations diophantiennes (voir `https://math.univ-lyon1.fr/~caldero/TD3-Algebre.pdf`, Exercice 13).

De la preuve de la proposition 3.(2) on déduit de façon immédiate le

Corollaire 5. Un nombre premier p est dans Σ si et seulement si $p = 2$ ou $p \equiv 1 \mod 4$.

3. Description des éléments de Σ

Le lemme suivant est une vérification quasi-immédiate :

Lemme 6. L'ensemble Σ est stable par multiplication.

Étant donné un entier $n \geqslant 2$ et un facteur premier p de n, on rappelle qu'il existe un unique entier strictement positif k tel que p^k divise n et p^{k+1} ne divise n. L'entier k s'appelle la *valuation p-adique de n* et on note $k = v_p(n)$.

Théorème 7 (des deux carrés)**.** Soit $n \geqslant 2$ un entier. On a $n \in \Sigma$ si et seulement si pour tout facteur premier p de n tel que $p = 3 \mod 4$, l'entier $v_p(n)$ est pair.

Démonstration. $\boxed{\Leftarrow}$ Décomposons n en facteurs premiers

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)} = 2^{v_2(n)} \left(\prod_{p \equiv 1 \mod 4} p^{v_p(n)} \right) \left(\prod_{p \equiv 3 \mod 4} p^{v_p(n)} \right).$$

On sait que $2 \in \Sigma$ et que les nombres premiers p tels que $p \equiv 1 \mod 4$ sont aussi dans Σ. Comme Σ est stable par multiplication, il existe $N \in \Sigma$ tel que

$$n = N \prod_{p \equiv 3 \mod 4} p^{v_p(n)}.$$

Par hypothèse, pour tout facteur premier p de n tel que $p \equiv 3 \mod 4$ il existe $k_p \in \mathbb{N}$ tel que $v_p(n) = 2k_p$. Pour les nombres premiers p ne divisant pas n mais tels que $p \equiv 3 \mod 4$ on a encore $v_p(n) = 0 = 2 \times 0$, et on pose dans ce cas $k_p = 0$.

On a donc $n = N \left(\prod_{p \equiv 3 \mod 4} p^{k_p} \right)^2$. Écrivons $N = a^2 + b^2$ avec $a, b \in \mathbb{Z}$ et $c = \prod_{p \equiv 3 \mod 4} p^{k_p}$. On a finalement $n = (a^2 + b^2)c^2 = (ac)^2 + (bc)^2 \in \Sigma$.

$\boxed{\Rightarrow}$ Soit p un facteur premier de n tel que $p \equiv 3 \mod 4$. On montre d'abord que p^2 divise n. D'après la proposition 3.(3) on sait que p est irréductible dans $\mathbb{Z}[i]$. Par hypothèse on a $n \in \Sigma$. Écrivons $n = a^2 + b^2$ avec $a, b \in \mathbb{Z}$. L'entier p divise donc

$$n = (a + ib)(a - ib),$$

dans $\mathbb{Z}[i]$. Et puisque p est irréductible dans $\mathbb{Z}[i]$ il divise l'un des deux facteurs, disons $a + ib$ par conjugaison. Mais p divise aussi $a - ib$ et donc en retour p^2 divise n.

Pour tout $l \in \mathbb{N}^*$ posons $N_l = \frac{n}{p^{2l}}$. Tant que $2l \leqslant v_p(n)$ on a $N_l \in \Sigma$ car $n \in \Sigma$. Par l'absurde, supposons que $v_p(n)$ soit impair, écrit $v_p(n) = 2k+1$ avec $k \in \mathbb{N}^*$. Puisque p^2 divise n on a $k \geqslant 1$ et donc $N_k \in \Sigma$. En remplaçant n par N_k au sein du raisonnement prédédent, on trouve que p^2 divise N_k, et donc p^{2k+2} divise n, ce qui implique que $2k+2 \leqslant v_p(k) = 2k+1$. Absurde. □

La preuve précente est assez constructive pour qu'on puisse dégager un algorithme de calcul.

Exercice 8. L'entier 1210 est-il somme de deux carrés ? Si oui, donner une décomposition de 260 en somme de deux carrés.

Solution. On commence par décomposer 1210 en facteurs premiers

$$1210 = 121 \cdot 10 = 11^2 \cdot 2 \cdot 5.$$

On a $5 \equiv 1 \mod 4$ et $11 \equiv 3 \mod 4$ avec $v_{11}(1210) = 2$. L'entier 1210 est donc dans Σ. Maintenant on a aussi

$$2 = 1^2 + 1^2 = (1+i)(1-i) \qquad \text{et} \qquad 5 = 4^2 + 1 = (2+i)(2-i).$$

On travaille alors dans $\mathbb{Z}[i]$ en réarrangeant les facteurs :

$$\begin{aligned} 1210 &= 11^2(1+i)(1-i)(2+i)(2-i), \\ &= 11^2(1+i)(2+i)(1-i)(2-i), \\ &= 11^2(1+3i)(1-3i), \\ &= 11^2(1^2+3^2) = 11^2 + 33^2. \end{aligned}$$

□

Remarque 9. La décomposition d'un élément de Σ en somme de deux carrés d'entiers n'est pas unique. Cependant, il est assez difficile de trouver un contre-exemple.

4. Quelques questions auxquelles il faut absolument savoir répondre rapidement

(1)

(2)

(3)

Références

[P] D. Perrin, *Cours d'algèbre*, Ellipses, 1996.