# DM 9 - Sommes de deux carrés – Ordres dans un groupe

## 1 Entiers de Gauss et sommes de deux carrés

### 1.1 $\mathbb{Z}[i]$ est un anneau euclidien.

1. Soient $z, z' \in \mathbb{Z}[i]$. On note $z = a + ib$ et $z' = c + id$ avec $a, b, c, d \in \mathbb{Z}$. Alors $z - z' = (a - c) + i(d - c)$ donc $z - z' \in \mathbb{Z}[i]$. Comme $\mathbb{Z}[i]$ est non vide (il contient 0), c'est un sous-groupe de $(\mathbb{C}, +)$. De plus, $1 \in \mathbb{Z}[i]$ et $zz' = (ac - bd) + i(ad + bc)$ ; donc $\mathbb{Z}[i]$ est stable par produit et contient l'élément neutre pour la multiplication. Donc $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.

2. Soient $z, z' \in \mathbb{Z}[i]$. On a
$$N(zz') = |zz'|^2 = |z|^2|z'|^2 = N(z)N(z').$$

3. Soit $z = a + ib \in \mathbb{Z}[i]$. On a $N(z) = a^2 + b^2 \in \mathbb{N}$. Si $z$ est inversible, il existe $z' \in \mathbb{Z}[i]$ : $zz' = 1$. Par la question précédente, $N(z)N(z') = 1$. Comme $N(z)$ et $N(z')$ sont des entiers naturels, les deux valents 1. Donc $N(z) = 1$.

   Réciproquement, si $N(z) = 1$, on a $z\bar{z} = |z|^2 = 1$. Comme $\bar{z} \in \mathbb{Z}[i]$, $z$ est inversible, d'inverse $\bar{z}$.

4. Soient $a \in \mathbb{Z}[i], b \in \mathbb{Z}[i] - \{0\}$. On écrit $\frac{a}{b} = x + iy$, avec $x$ et $y$ réels. On peut trouver des entiers $x'$ et $y'$ tels que $|x - x'| \leq 1/2$ et $|y - y'| \leq 1/2$. Notons $q = x' + iy' \in \mathbb{Z}[i]$. On a donc :
$$|\frac{a}{b} - q| \leq \sqrt{(1/2)^2 + (1/2)^2} = \frac{1}{\sqrt{2}}.$$

   On multiplie par $|b|$ et on prend le carré :
$$|a - qb|^2 \leq \frac{1}{2}|b|^2.$$

   Donc $N(a - qb) < N(b)$ (car $b \neq 0$). En posant $r = a - qb$, on a bien
$$a = bq + r \text{ et } N(r) < N(b).$$

5. On considère $a = 1 + i$ et $b = 2$. Alors $1 + i = 2 \times 0 + (1 + i)$ et $1 + i = 2 \times +(-1 + i)$. Et $N(1 + i) = N(-1 + i) < N(2)$. Il n'y a donc pas unicité.

   *Cela n'a rien de surprenant. Déjà dans $\mathbb{Z}$, la division euclidienne n'est unique que si on décide de façon (arbitraire) de prendre un reste positif. Si on demande seulement que $|r| < |b|$, il y aura en général deux choix possibles (avec deux quotients différant de 1).*

### 1.2 Lemme d'Euclide dans $\mathbb{Z}[i]$

6. Notons $X$ l'ensemble $\{N(z), z \in I - \{0\}\}$. On a vu que $N$ est à valeurs dans $\mathbb{N}$. Donc $X$ est une partie de $\mathbb{N}$, évidemment non vide. Elle admet donc un plus petit élément. Cet élément est donc de la forme $N(d)$, pour un $d \in I - \{0\}$.

7. On écrit une division euclidienne de $a$ par $d$ : $a = qd + r$, avec $q, r \in \mathbb{Z}[i]$ et $N(r) < N(d)$. Comme $d$ est dans $I$, il est de la forme $d = au + xv$, avec $u, v \in \mathbb{Z}[i]$. Ainsi,

$$r = a - qd = a(1 - qu) + x(-qv).$$

Donc, $r \in I$. Comme $N(r) < N(d)$, on a nécessairement $r = 0$, par construction de $d$. Donc $d$ divise $a$. Comme $d = au + xv$, on a aussi que $d$ divise $x$.

On écrit donc $a = dd'$, avec $d' \in \mathbb{Z}[i]$. Comme $a$ est irréductible, $d$ ou $d'$ est inversible. Mais si $d'$ était inversible, on aurait que $a$ divise $d$ et que $d$ divise $x$, ce qui est contraire à l'hypothèse. Donc, c'est $d$ qui est inversible.

En multipliant $d = au + xv$ par l'inverse de $d$, on obtient une relation $1 = au' + xv'$, avec $u', v' \in \mathbb{Z}[i]$. On multiplie par $y$ : $y = ayu' + xyv'$. Comme $a$ divise $ay$ et $xy$ (par hypothèse), il divise le membre de droite. Donc $a$ divise $y$ (le membre de gauche). Le lemme d'Euclide est démontré.

### 1.3 Nombres premiers somme de deux carrés

8. Dans $\mathbb{Z}/4\mathbb{Z}$, on a $\bar{0}^2 = \bar{2}^2 = \bar{0}$ et $\bar{1}^2 = \bar{3}^2 = \bar{1}$. Donc 0 et 1 sont les seuls carrés modulo 4. Ainsi, si $p = x^2 + y^2$, $p$ vaut $0 + 0 = 1$ ou $1 + 0 = 0 + 1 = 1$ ou $1 + 1 = 2$ modulo 4. En particulier, un nombre premier $p$ congru à 3 modulo 4 n'est pas somme de deux carrés.

9. Comme $x^2 \equiv 1\,[p]$, $p$ divise $x^2 + 1$ dans $\mathbb{Z}$, donc aussi dans $\mathbb{Z}[i]$. Si $p$ divisait $x + i$, on aurait l'existence de $a, b \in \mathbb{Z}$ tels que $p(a + ib) = x + i$, d'où $ap = x$ et $bp = 1$. La deuxième égalité est absurde. Donc $p$ ne divise pas $x + i$ ; de même il ne divise pas $x - i$.

10. Si $p$ était irréductible dans $\mathbb{Z}[i]$, comme il divise $x^2 + 1$, le lemme d'Euclide impliquerait qu'il divise $x + i$ ou $x - i$, ce qui n'est pas. Donc $p$ n'est pas irréductible ; il existe don une décomposition $p = bc$, avec $b$ et $c$ dans $\mathbb{Z}[i]$ non inversibles.

11. On prend la norme dans l'égalité précédente : $N(p) = N(b)N(c)$. Or $N(p) = p^2$ et $N(b)$ et $N(c)$ sont des entiers naturels. De plus, $N(b)$ et $N(c)$ sont différents de 1 car $b$ et $c$ ne sont pas inversibles. Nécessairement, $N(b) = N(c) = p$.

On écrit $b = u + iv$, avec $u, v \in \mathbb{Z}$. Alors,

$$p = N(b) = u^2 + v^2$$

est une somme de deux carrés d'entiers.

### 1.4 Théorème de Fermat de Noël

12. Soit $n \geq 1$. On a les équivalences suivantes :

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

13. Soient $u, v \in \Sigma$. On peut donc trouver $z, z' \in \mathbb{Z}[i]$ tels que $N(z) = u$ et $N(z') = v$. Alors $uv = N(zz')$. Donc $uv \in \Sigma$.

    *En pratique, cela donne un éclairage par les complexes à*

    $$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2,$$

    *qu'on appelle l'identité de Diophante, ou de Lagrange.*

14. Soit $n$ un entier dont toutes les valuations $v_p(n)$ sont paires, si $p$ est congru à 3 modulo 4. Alors, $n$ est le produit d'un certain nombre de facteurs 2, d'un certain nombre de facteurs $p_i$, avec $p_i$ congru à 1 modulo 4, et d'un certain nombre de facteurs $q_j^2$, avec $q_j$ congru à 3 modulo 4.

    Or $2 = 1^2 + 1^2$ est dans $\Sigma$. Les $p_i$ congrus à 1 modulo 4 sont dans $\Sigma$ d'après la partie précédente. Les $q_j^2$, pour $q_j$ congru à 3 modulo 4, vérifient $q_j^2 = q_j^2 + 0^2$, donc sont dans $\Sigma$.

    Une récurrence immédiate utilisant la question précédente montre qu'un produit d'un nombre quelconque de facteurs dans $\Sigma$ est encore dans $\Sigma$. Donc, $n$ est dans $\Sigma$.

15. On écrit $u^{p-1} + v^{p-1} = (u^2)^{\frac{p-1}{2}} + (v^2)^{\frac{p-1}{2}} = (u^2)^{\frac{p-1}{2}} - (-v^2)^{\frac{p-1}{2}}$. La première égalité vient de ce que $p-1$ est pair, la deuxième du fait que $\dfrac{p-1}{2}$ est impair (car $p \equiv 3\,[4]$). Par l'identité de Bernoulli, on a donc :

    $$u^{p-1} + v^{p-1} = (u^2 + v^2) \sum_{k=0}^{\frac{p-1}{2}-1} (u^2)^k (-v^2)^{\frac{p-1}{2}-k}.$$

    Donc $u^2 + v^2$ divise $u^{p-1} + v^{p-1}$.

16. Supposons que $p$ divise $u^2 + v^2$. D'après la question précédente, on a donc $u^{p-1} + v^{p-1} \equiv 0\,[p]$. Or, par le petit théorème de Fermat, $u^{p-1} \equiv 1\,[p]$ (si $u \wedge p = 1$) ou $u^{p-1} \equiv 0\,[p]$ (si $p \mid u$) ; de même pour $v$. Donc si $p$ ne divise pas $u$ ou $v$, on trouve $u^{p-1} + v^{p-1} \equiv 1$ ou $2\,[p]$. Comme $p \geq 3$, c'est absurde. Donc, $p$ divise $u$ et $p$ divise $v$.

    La réciproque est évidente.

17. **Conclusion :** Supposons par l'absurde que $n'$ soit divisible par un nombre premier $p$ congru à 3 modulo 4. Comme $n' = a'^2 + b'^2$, on a alors, d'après la question précédente, que $n$ divise $a'$ et $b'$. Comme $a'$ et $b'$ sont premiers entre eux, c'est absude. Donc $n'$ n'est divisible par aucun nombre premier congru à 3 modulo 4.

    Or, $n = n'd^2$. Si $p$ est congru à 3 modulo 4, on a donc $v_p(n) = v_p(n') + 2v_p(d) = 2v_p(d)$. Donc, toutes les valuations $v_p(n)$ sont paires, si $p$ est congru à 3 modulo 4.

    Ceci conclut la réciproque.