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 $\dfrac{a}{b} = x + iy$, 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 :
$$\left|\frac{a}{b} - q\right| \leq \sqrt{(1/2)^2 + (1/2)^2} = \frac{1}{\sqrt{2}}.$$

   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 Σ. Les p_i congrus à 1 modulo 4 sont dans Σ 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 Σ.

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

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.

2 Ordres dans un groupe

2.1 Théorème de Lagrange

1. cf. exercice 14, feuille de TD. (*Attention ! Ce n'est pas la même relation d'équivalence, on a inversé gauche et droite.*)

2. Soit $x \in G$, soit $y \in G$. On a les équivalences :

$$y \in \mathrm{cl}_{\mathscr{R}}(x) \iff x^{-1}y \in H \iff y \in xH.$$

   Donc, $\mathrm{cl}_{\mathscr{R}}(x) = xH$. L'application $\tau : H \to \mathrm{cl}_{\mathscr{R}}(x), h \mapsto xh$ est alors une bijection (de réciproque $y \mapsto x^{-1}y$).

3. On a une partition de G en classes d'équivalence de la relation $\mathscr{R}$. Chacune de ces classes a $|H|$ éléments d'après la question précédente. Donc, s'il y a N classes, le principe de division donne : $|G| = N|H|$. En particulier, $|H|$ divise $|G|$.

4. On redonne l'argument, déjà vu en cours. L'ensemble $\{x^n, n \in \mathbb{N}^*\}$ est fini puisque G est fini. On peut donc trouver deux indices $1 \leq p < q$ tels que $x^p = x^q$. Alors, $x^{q-p} = e_G$. Donc, x est d'ordre fini. Notons $\omega(x)$ son ordre. L'argument précédent montre de plus que les éléments x^i, pour $i \in [\![0, \omega(x)-1]\!]$ sont deux à deux distincts (sinon on trouverait un $n < \omega(x)$ tel que $n \geq 1$ et $x^n = e_G$).
   Montrons alors que $\langle x \rangle = \{x^i, i \in [\![0, \omega(x)-1]\!]\}$. On sait que $\langle x \rangle = \{x^n, n \in \mathbb{Z}\}$. Donc, l'inclusion droite-gauche est évidente. Soit $n \in \mathbb{Z}$. Par division euclidienne, on peut trouver $q \in \mathbb{Z}$ et $r \in [\![0, \omega(x)-1]\!]$ tel que $n = q\omega(x) + r$. Alors, $x^n = \left(x^{\omega(x)}\right)^q \times \omega^r = \omega^r$; ce qui montre l'inclusion gauche-droite.
   Donc, $\langle x \rangle = \{x^i, i \in [\![0, \omega(x)-1]\!]\}$. Donc, $|\langle x \rangle| = \omega(x)$.

5. D'après la question 3, appliquée au sous-groupe $\langle x \rangle$, $|\langle x \rangle|$ divise $|G|$. Avec la question précédente, on a donc $\omega(x) \mid |G|$.

6. Soit G un groupe de cardinal p. Soit $x \in G$ un élément différent de l'élément neutre. D'après le théorème de Lagrange, $\omega(x)$ divise p ; comme $\omega(x) \neq 1$ (puisque x n'est pas l'élément neutre), $\omega(x) = p$. Donc, $\langle x \rangle$ est de cardinal p, et c'est un sous-groupe de G. Par égalité des cardinaux, $\langle x \rangle = G$. Donc, G est un groupe monogène, donc il est cyclique (donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$).

7. Soit $a \in \mathbb{N}^*$. On cherche à savoir quand $a\overline{k} = \overline{0} \in \mathbb{Z}/n\mathbb{Z}$. Or $a\overline{k} = \overline{ak}$; cette classe est nulle (dans $\mathbb{Z}/n\mathbb{Z}$) ssi n divise ak. Or $n \mid ak \iff \dfrac{n}{n \wedge k} \mid a\dfrac{k}{n \wedge k} \iff \dfrac{n}{n \wedge k} \mid a$ (la dernière équivalence par lemme de Gauss). Donc, le plus petit entier $a \in \mathbb{N}^*$ tel que $a\overline{k} = \overline{0}$ est $\dfrac{n}{n \wedge k}$.
   Donc, c'est l'ordre de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$. (*on retrouve par exemple que si n est premier, $\overline{k}$ est d'ordre n si n ne divise pas k ; plus généralement, on voit qu'il y a $\phi(n)$ éléments d'ordre n dans $\mathbb{Z}/n\mathbb{Z}$.*)

8. **Exemple des groupes symétriques.** Soit $n \geq 1$. On note S_n le groupe des permutations de $[\![1, n]\!]$.

   (a) On sait que $|S_n| = n!$. Soit $k \in [\![1, n]\!]$. On note c la permutation de $[\![1, n]\!]$ telle que $c(1) = 2$, $c(2) = 3$,...,$c(k) = 1$ et, pour tout $i \in [\![k+1, n]\!]$, $c(i) = i$. Alors, un calcul direct montre

que $c^k = \mathrm{id}_{[\![1,n]\!]}$ et que k est le premier entier avec cette propriété (*considérer p. ex. l'image de* 1 *pour le deuxième point*). *Évidemment, la puissance k désigne ici la k-ème composée.* Donc, c est d'ordre k.

(b)
- Pour $n = 3$, $|S_3| = 6$. Les ordres possibles sont *a priori* 1, 2, 3 et 6. La question précédente donne un exemple pour 1, 2 et 3 mais il n'y a pas d'élément d'ordre 6 (sinon S_3 serait cyclique, donc commutatif, ce qui n'est pas).
- Pour $n = 4$, $|S_4| = 24$. Les ordres possibles sont *a priori* 1, 2, 3, 4, 6, 8, 12, 24. Les ordre 1, 2, 3 et 4 ont été traités par la question précédente et on se convainc que ce sont les seuls ordres possibles (*Une justification plus rigoureuse pourra être obtenue après le théorème de décomposition des permutations en produits de cycles à supports disjoints ; plus tard dans l'année.*)

(c) La permutation σ envoyant 1 sur 2, 2 sur 3, 3 sur 1 et échangeant 4 et 5 convient.

2.2 Théorème de Cauchy

9.
- Réflexivité. Soit $(g_c) \in E$. Alors, pour tout $c \in \mathbb{Z}/p\mathbb{Z}$, $g_c = g_{0+c}$. Donc, $(g_c)\mathscr{R}(g_c)$.
- Symétrie. Soient (g_c) et (g'_c) dans E tels que $(g_c)\mathscr{R}(g'_c)$. Alors, il existe $a \in \mathbb{Z}/p\mathbb{Z}$ tel que $\forall c \in \mathbb{Z}/p\mathbb{Z}, g_c = g'_{c+a}$. Avec $b = -a$, on a donc $\forall c \in \mathbb{Z}/p\mathbb{Z}, g'_c = g_{c+b}$. Donc, $(g'_c)\mathscr{R}(g_c)$.
- Transitivité. Soient (g_c), (g'_c) et (g''_c) dans E tels que $(g_c)\mathscr{R}(g'_c)$ et $(g'_c)\mathscr{R}(g''_c)$. Alors, il existe a et b dans $\mathbb{Z}/p\mathbb{Z}$ tels que pour tout $c \in \mathbb{Z}/p\mathbb{Z}$, $g_c = g'_{c+a}$ et $g'_c = g''_{c+b}$. Avec $d = a + b$, on a $\forall c \in \mathbb{Z}/p\mathbb{Z}$, $g_c = g''_{c+d}$. Donc, $(g_c)\mathscr{R}(g''_c)$.

10. D'abord, $H_{(g_c)}$ contient la classe $0 \in \mathbb{Z}/p\mathbb{Z}$. Soient $x, y \in H_{(g_c)}$. On a donc,

$$\forall c \in \mathbb{Z}/p\mathbb{Z}, g_{a+x-y} = g_{a-y} = g_a,$$

en utilisant successivement que x et y sont dans $H_{(g_c)}$ (dans un sens et dans l'autre). Donc, $H_{(g_c)}$ est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$.

11. Les seuls sous-groupes de $\mathbb{Z}/p\mathbb{Z}$ sont $\{0\}$ et $\mathbb{Z}/p\mathbb{Z}$ lui-même (car le cardinal d'un tel sous-groupe doit diviser p).

- Si $H_{(g_c)} = \mathbb{Z}/p\mathbb{Z}$, (g_c) est égal à tous ses translatés ; donc $\mathrm{cl}_{\mathscr{R}}((g_c))$ a pour cardinal 1.
- Si $H_{(g_c)} = \{0\}$, alors l'application $f : \mathbb{Z}/^p\mathbb{Z} \to \mathrm{cl}_{\mathscr{R}}((g_c)), a \mapsto (g_{c+a})$, qui est surjective par définition, est aussi injective. En effet, si elle ne l'était pas, et si on avait $f(a) = f(b)$ avec a et b distincts dans $\mathbb{Z}/p\mathbb{Z}$, on aurait $a - b \in H_{(g_c)}$. Donc, dans ce cas, $\mathrm{cl}_{\mathscr{R}}((g_c))$ a pour cardinal p.

12. D'après ce qui précède, les $\mathscr{R}$-classes d'équivalence sont de cardinal 1 ou p. Notons r le nombre de classes de cardinal 1 et ℓ le nombre de classes de cardinal p. On a donc $|E| = r + \ell p$.

13. Remarquons déjà que $|E| = |G|^{p-1}$ (en effet, l'élément $g_{\overline{p-1}}$ est déterminé de façon unique par les éléments $g_{\overline{k}}$ pour $k \in [\![0, p-2]\!]$ et ces éléments sont quelconques). On en déduit que $p||E|$. D'après la question précédente, on a donc aussi $p \mid r$. Or, un élément de E dont la classe d'équivalence est de cardinal 1 est simplement une famille $(g_c)_{c\in\mathbb{Z}/p\mathbb{Z}}$ où tous les g_c sont les mêmes. L'ensemble de ces éléments est donc en bijection avec l'ensemble des $x \in G$ tels que $x^p = e$ (vu la définition de E). Or, si x vérifie cette équation, son ordre divise p :

c'est donc 1 (et $x = e$) ou p. Autrement dit, le nombre N recherché vaut $N = r - 1$. Donc, $N \equiv -1\,[r]$.

14. Absolument pas ! l'existence d'un élément d'ordre n dans un groupe de cardinal n caractérise les groupes cycliques !