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

Les parties 1.4 et 2.2 sont facultatives.

1 Entiers de Gauss et sommes de deux carrés

Dans ce problème, on étudie l'anneau $\mathbb{Z}[i] = \{a + ib, (a,b) \in \mathbb{Z}^2\}$ des entiers de Gauss. En guise d'application, on caractérise l'ensemble Σ des entiers naturels qui s'écrivent comme somme de deux carrés d'entiers. On adopte les définitions suivantes :

- Si a et b sont des éléments de $\mathbb{Z}[i]$, on dit que a divise b s'il existe $c \in \mathbb{Z}[i]$ tel que $b = ac$.
- Un élément $a \in \mathbb{Z}[i]$ est irréductible s'il n'est pas inversible et si, dans une décomposition $a = bc$, avec $b, c \in \mathbb{Z}[i]$, b ou c est un inversible de $\mathbb{Z}[i]$.

Pour tout $z \in \mathbb{Z}[i]$, on note $N(z) = |z|^2$.

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

1. Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.
2. Montrer que $\forall z, z' \in \mathbb{Z}[i], N(zz') = N(z)N(z')$.
3. Soit $z \in \mathbb{Z}[i]$. Montrer que z est inversible dans $\mathbb{Z}[i]$ ssi $N(z) = 1$.
   En déduire les inversibles de $\mathbb{Z}[i]$.
4. Montrer que $\mathbb{Z}[i]$ est un anneau euclidien, de stathme N, au sens suivant :

   $$\forall a \in \mathbb{Z}[i], \forall b \in \mathbb{Z}[i] - \{0\}, \exists (q,r) \in \mathbb{Z}[i]^2 : a = bq + r \text{ et } N(r) < N(b).$$

   Considérer pour q un élément de $\mathbb{Z}[i]$ proche de $\frac{a}{b} \in \mathbb{C}$.
5. Y a-t-il unicité du couple (q,r) en général ?

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

Soit a un irréductible de $\mathbb{Z}[i]$, soient $x, y \in \mathbb{Z}[i]$. On suppose que a divise xy et on cherche à montrer que a divise x ou a divise y. On suppose que a ne divise pas x et on note

$$I = a\mathbb{Z}[i] + x\mathbb{Z}[i] = \{au + xv, (u,v) \in \mathbb{Z}[i]^2\}.$$

6. Montrer qu'il existe $d \in I - \{0\}$ tel que $N(d) = \min\{N(z), z \in I - \{0\}\}$.
7. Montrer que d divise a ; en déduire que d est un inversible de $\mathbb{Z}[i]$, puis que a divise y.

1.3 Nombres premiers sommes de deux carrés

Dans cette partie, on montre qu'un nombre premier impair p est somme de deux carrés d'entiers ssi il est congru à 1 modulo 4.

8. On suppose que p est congru à 3 modulo 4. Montrer que p n'est pas somme de deux carrés d'entiers.

On suppose désormais que p est congru à 1 modulo 4. On sait[1] qu'on peut trouver $x \in \mathbb{Z}$ tel que $x^2 \equiv -1\,[p]$. Dans $\mathbb{Z}[i]$, on a la décomposition $x^2+1 = (x-i)(x+i)$.

9. Montrer que, dans $\mathbb{Z}[i]$, p divise x^2+1, mais qu'il ne divise ni $x+i$, ni $x-i$.
10. En déduire qu'il existe $b, c \in \mathbb{Z}[i]$, non inversibles, tels que $p = bc$.
11. Montrer que $N(b) = p$. En déduire que p est somme de deux carrés d'entiers.

1.4 Théorème de Fermat de Noël

Notons $\Sigma = \{n \geq 1 \mid \exists (a,b) \in \mathbb{N}^2 : n = a^2+b^2\}$. Dans cette partie, on montre que pour tout entier $n \geq 1$, n appartient à Σ ssi pour tout premier p congru à 3 modulo 4, $v_p(n)$ est pair.[2]

12. Soit $n \geq 1$. Montrer que $n \in \Sigma$ ssi il existe $z \in \mathbb{Z}[i]$ tel que $n = N(z)$.
13. En déduire que si $u, v \in \Sigma$, alors $uv \in \Sigma$.
14. En déduire que si pour tout premier p congru à 3 modulo 4, $v_p(n)$ est pair, alors $n \in \Sigma$.

Pour la réciproque, on fixe un nombre premier p congru à 3 modulo 4.

15. Soient u, v deux entiers. Montrer que u^2+v^2 divise $u^{p-1}+v^{p-1}$.
16. En déduire que p divise u^2+v^2 ssi p divise u et p divise v.
17. **Conclusion :** Soit $n \in \Sigma$. On écrit $n = a^2+b^2$, avec $(a,b) \in \mathbb{N}^2$. On note

$$d = a \wedge b,\ a' = \frac{a}{d},\ b' = \frac{b}{d},\ n' = a'^2 + b'^2 = \frac{n}{d^2}.$$

Montrer que n' n'est divisible par aucun nombre premier congru à 3 modulo 4. Conclure.

[1] Par un exercice du TD ou par le dernier DM

[2] Théorème énoncé par Girard en 1625. Dans une lettre à Mersenne datée du jour de Noël 1640, Fermat discute des outils nécessaires à sa résolution.

2 Ordres dans un groupe

Soit G un groupe d'élément neutre e, soit x un élément de G. On dit que x est d'ordre fini s'il existe un entier $k > 0$ tel que $x^k = e$, et d'ordre infini sinon. Si x est d'ordre fini, le plus petit tel entier k est l'ordre de g ; on le note $\omega(g)$.

2.1 Théorème de Lagrange

Soit H un sous-groupe de G. On note $\mathscr{R}$ la relation sur G définie par

$$\forall x, y \in G, x \mathscr{R} y \iff x^{-1}y \in H.$$

1. Montrer que $\mathscr{R}$ est une relation d'équivalence sur G.
2. Soit $x \in G$. Montrer que $\mathrm{cl}_{\mathscr{R}}(x) = xH$. En déduire qu'il existe une bijection de H dans $\mathrm{cl}_{\mathscr{R}}(x)$.

On suppose désormais que G est un groupe fini.

3. Déduire de ce qui précède que $|H| \,|\, |G|$.
4. Soit x un élément de G. Montrer que x est d'ordre fini et que $\omega(x) = |\langle x \rangle|$.
5. En déduire le théorème de Lagrange :

$$\forall x \in G, \omega(x) \,|\, |G|.$$

6. **Application.** Soit p un nombre premier. Montrer que tout groupe fini de cardinal p est cyclique.
7. **Exemple des groupes cycliques.** Soit $n \geq 1$, soit $k \in \mathbb{Z}$. On note $\overline{k}$ la classe de k dans $\mathbb{Z}/n\mathbb{Z}$. Déterminer $\omega(\overline{k})$.
8. **Exemple des groupes symétriques.** Soit $n \geq 1$. On note S_n le groupe des permutations de $[\![1, n]\!]$.
   (a) Que vaut $|S_n|$? Déterminer pour $k \in [\![1, n]\!]$, un élément d'ordre k de S_n.
   (b) Pour $n = 3$ et $n = 4$, quels sont les ordres possibles des éléments de S_n ? Donner pour chaque ordre un élément ayant cet ordre.
   On n'attend pas de justification.
   (c) Donner un élément d'ordre 6 de S_5.

2.2 Théorème de Cauchy

On suppose que G est fini et on note p un diviseur premier de $|G|$. On souhaite montrer qu'il existe un élément x de G tel que $\omega(x) = p$.

On note E l'ensemble des familles $(g_c)_{c \in \mathbb{Z}/p\mathbb{Z}}$ d'éléments de G indexées par $\mathbb{Z}/p\mathbb{Z}$, telles que

$$\prod_{k=0}^{p-1} g_{\overline{k}} = e.$$

9. On définit une relation[3] $\mathscr{R}$ sur E par

$$(g_c)_{c\in\mathbb{Z}/p\mathbb{Z}}\,\mathscr{R}\,(g'_c)_{c\in\mathbb{Z}/p\mathbb{Z}} \iff \exists a\in\mathbb{Z}/p\mathbb{Z} : \forall c\in\mathbb{Z}/p\mathbb{Z}, g_c = g'_{c+a}.$$

   Montrer que $\mathscr{R}$ est une relation d'équivalence sur E.

Soit $(g_c)_{c\in\mathbb{Z}/p\mathbb{Z}} \in E$. On note $H_{(g_c)} = \left\{a\in\mathbb{Z}/p\mathbb{Z} \mid \forall c\in\mathbb{Z}/p\mathbb{Z}, g_c = g_{a+c}\right\}$.

10. Montrer que $H_{(g_c)}$ est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$.

11. En déduire l'alternative suivante :

    - Ou bien $H_{(g_c)} = \{\overline{0}\}$ et $\mathrm{cl}_{\mathscr{R}}\left((g_c)\right)$ a pour cardinal p.
    - Ou bien $H_{(g_c)} = \mathbb{Z}/p\mathbb{Z}$ et $\mathrm{cl}_{\mathscr{R}}\left((g_c)\right)$ a pour cardinal 1.

12. En considérant la partition de E associée à $\mathscr{R}$, montrer que le nombre de $\mathscr{R}$-classes d'équivalence de cardinal 1 est divisible par p.

13. En déduire que le nombre N d'éléments x de G tels que $\omega(x) = p$ vérifie $N \equiv -1\,[p]$.
    En particulier, $N \neq 0$.

14. Si n est un diviseur quelconque de $|G|$, existe-t-il toujours un élément d'ordre n dans G ?

[3] De façon informelle, deux familles sont en relation si l'une s'obtient en faisant tourner l'autre.