Agrégation Interne – Poitiers – 2012/2013

Congruences – Anneaux principaux et euclidiens – Groupes et géométrie

rédigé par Anne Moreau

Première partie

Congruences

On supposera connues les notions d'anneaux, idéaux, morphismes d'anneaux, corps...

1 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Proposition 1.1. *Les sous-groupes de $\mathbb{Z}$ (resp. idéaux de $\mathbb{Z}$) sont les ensembles $n\mathbb{Z}$, avec $n \in \mathbb{N}$.*

Démonstration. Le point clé est l'existence d'une division euclidienne (DE) : pour tout $(a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$, il existe un couple $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et ($r = 0$ ou $0 < |r| < |b|$).
Remarque : on a l'unicité si on impose $r \geqslant 0$.

Les ensembles $n\mathbb{Z}$ ($n \in \mathbb{N}$) sont clairement des sous-groupes (resp. idéaux) de $\mathbb{Z}$. Réciproquement, soit H un sous-groupe de $\mathbb{Z}$ non réduit à $\{0\}$, et n le plus petit élément non nul de H en valeur absolue. Un tel élément existe et on peut supposer que $n > 0$ (prendre son opposé sinon). On a $n\mathbb{Z} \subset H$ car H est un sous-groupe de $\mathbb{Z}$. Pour établir l'autre inclusion, soit $a \in H$. On fait la DE de a par n ; il existe $(q, r) \in \mathbb{Z}^2$ tel que $a = nq + r$ et ($r = 0$ ou $0 < |r| < |b|$). Alors r est nécessairement nul d'après le choix de n (car $r = a - nq \in H$). En conclusion, $H = n\mathbb{Z}$. □

Remarque 1.2.

1) $\mathbb{Z}$ *est un exemple d'anneau* euclidien *(i.e., un anneau intègre qui possède une DE ; cf. Définition 7.11) avec pour « norme » la valeur absolue.*

2) *Un anneau euclidien est* principal *(i.e., tout idéal est engendré par un élément ; cf. Définition 7.8) : cela se démontre comme ci-dessus grâce à l'existence d'une DE.*

3) *L'anneau $\mathbb{k}[X]$, où $\mathbb{k}$ est un corps commutatif, est un autre exemple d'anneau euclidien avec le degré pour « norme » (= fonction ν dans la Définition 7.11). Nous verrons un autre exemple d'anneau euclidien : l'anneaux des* entiers de Gauss $\mathbb{Z}[i]$ *(cf. section 8).*

4) *Les inversibles (ou* unités*) de* $\mathbb{Z}$ *sont* -1 *et* 1.

On va désormais s'intéresser aux anneaux quotients $\mathbb{Z}/n\mathbb{Z}$, pour $n \in \mathbb{N}^*$.

Lemme 1.3. *Soient A un anneau commutatif (resp. G un groupe) et I un idéal de A (resp. H un sous-groupe distingué de G). Alors il existe une correspondance bijective entre les idéaux (resp. sous-groupes) de A/I (resp. G/H) et les idéaux (resp. sous-groupes) de A (resp. G) contenant I (resp. H) :*

$$\{ \text{ idéaux de } A/I \} \leftrightarrow \{ \text{ idéaux de } A \text{ contenant } I \}$$

$$(\text{resp. } \{ \text{ sous-groupes de } G/H \} \leftrightarrow \{\text{sous-groupes de } G \text{ contenant } H \}).$$

Démonstration. On considère l'application quotient $\alpha : A \to A/I$. Si $J \supset I$ est un idéal de A contenant I, alors $\alpha(J)$ est un idéal de A/I (exercice). Réciproquement, si $K \subset A/I$ est un idéal de A/I, alors $\alpha^{-1}(K)$ est un idéal de A contenant I (exercice).

On fait de même dans le cas des groupes...

□

On applique le lemme à $G = A = \mathbb{Z}$ et $H = I = n\mathbb{Z}$, $n \in \mathbb{N}^*$. Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ coïncident avec les idéaux de $\mathbb{Z}/n\mathbb{Z}$ et sont en bijection avec les idéaux (=sous-groupes) de $\mathbb{Z}$ contenant $n\mathbb{Z}$, donc en bijection avec les diviseurs positifs de n.

Plus précisément, si d divise n, alors $\langle \overline{d} \rangle \subset \mathbb{Z}/n\mathbb{Z}$ est l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre $\frac{n}{d}$ et on a

$$\langle \overline{d} \rangle = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} \mid \frac{\overline{n}}{d}\,\overline{x} = 0\}.$$

Explications. C'est en effet un sous-groupe d'ordre $\frac{n}{d}$ car c'est l'ordre de d. Réciproquement, si H est un sous-groupe d'ordre $\frac{n}{d}$ de $\mathbb{Z}/n\mathbb{Z}$, alors $\alpha^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$ contenant $n\mathbb{Z}$ donc $\alpha^{-1}(H) = d'\mathbb{Z}$ où d' divise n. Or $\alpha(d'\mathbb{Z}) = H = \{\overline{d'k} \mid k \in \mathbb{Z}\}$ est d'ordre $\frac{n}{d'}$. Par suite $d = d'$ et $H = \langle \overline{d} \rangle$.

□

Corollaire 1.4. *Soit G un groupe* cyclique *(i.e., un groupe monogène d'ordre fini) d'ordre n, $G = \langle g \rangle$ (G est ici noté multiplicativement). Les sous-groupes de G sont cycliques et il y en a un par diviseur de n. Ils sont de la forme $\langle g^d \rangle = \{h \in G \mid h^{\frac{n}{d}} = 1_G\}$.*

Démonstration. Considérer l'applicaton $\mathbb{Z}/n\mathbb{Z} \to G$, $\overline{k} \mapsto g^k$.

□

Exemples 1.5. *Le groupe $\mathbb{U}_n$ des racines n-ième de l'unité est cyclique. L'isomorphisme est donné par $\mathbb{Z}/n\mathbb{Z} \to \mathbb{U}_n$, $\overline{k} \mapsto e^{\frac{2ik\pi}{n}}$.*

Remarque 1.6. *Si $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ ($a \in \mathbb{Z}$), alors $\langle \overline{a} \rangle = \langle \overline{d} \rangle$ où $d = \operatorname{pgcd}(a, n)$. Cela résulte de la relation $a\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ qui découle (presque) de la définition du pgcd (c'est la définition dans un anneau principal, cf. Définition 7.9).*

2 Application : résolution de l'équation $y = \overline{k}x$ dans $\mathbb{Z}/n\mathbb{Z}$ d'inconnue x ($y \in \mathbb{Z}/n\mathbb{Z}$, $k \in \mathbb{Z}$ fixés)

On considère l'application $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $t \mapsto \overline{k}t$. On a : $\operatorname{im}\phi = \langle \overline{k} \rangle = \langle \overline{d} \rangle$ où $d = \operatorname{pgcd}(n, k)$ d'après la remarque 1.6. Par suite, $|\operatorname{im}\phi| = \frac{n}{d}$ et $\operatorname{im}\phi = \{\overline{u} \in \mathbb{Z}/n\mathbb{Z} \mid \frac{\overline{n}}{d}\overline{u} = 0\}$. On en déduit que le cardinal de $\ker\phi$ est $d = \frac{|\mathbb{Z}/n\mathbb{Z}|}{|\operatorname{im}\phi|}$. En effet, d'après le Théorème de factorisation (cf. Théorème 8.4), le morphisme ϕ induit un isomorphisme $\overline{\phi} : (\mathbb{Z}/n\mathbb{Z})/\ker\phi \to \operatorname{im}\phi$, d'où l'égalité sur les cardinaux.

Conclusion : l'équation $y = \overline{k}x$ admet une solution dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement $y \in \operatorname{im}\phi$, i.e., $\frac{\overline{n}}{d}y = 0$ (dans $\mathbb{Z}/n\mathbb{Z}$), et dans ce cas il y a exactement d solutions.

En utilisant le Corollaire 1.4, on en déduit :

Corollaire 2.1. *Soient G un groupe cyclique d'ordre n, $k \in \mathbb{Z}$ et $y \in G$. L'équation $y = x^k$ admet une solution dans G si et seulement si $y^{\frac{n}{d}} = 1_G$ où $d = \operatorname{pgcd}(n, k)$ et dans ce cas il y a exactement d solutions.*

3 Unités (ou inversibles) de $\mathbb{Z}/n\mathbb{Z}$

Proposition 3.1. *Soit $m \in \mathbb{Z}$. On a $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement si $\operatorname{pgcd}(n, m) = 1$, ou encore si et seulement si $\overline{m}$ engendre $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration. Cela vient de de l'identité de Bézout : on a $\operatorname{pgcd}m, n = 1$ (i.e., m et n sont premiers entre eux) si et seulement si $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ ou encore si et seulement si m est inversible dans $\mathbb{Z}/n\mathbb{Z}$. D'autre part, $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si l'application $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\overline{k} \to \overline{m}\overline{k}$ est bijective, d'où la deuxième assertion.

□

On note $\varphi(n)$ le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$. L'application φ est appelée la *fonction indicatrice d'Euler*. On a :

$$n = \sum_{d|n} \varphi(d). \tag{3.1}$$

Explication de la formule (3.1). Les éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$, pour d parcourant l'ensemble des diviseurs de n, forment une partition de $\mathbb{Z}/n\mathbb{Z}$. Or il y a exactement $\varphi(d)$ éléments d'ordre

d d'après la Proposition 3.1. En effet, ces éléments engendrent l'unique sous-groupe d'ordre $\frac{n}{d}$ de $\mathbb{Z}/n\mathbb{Z}$. La formule est alors claire.

□

Corollaire 3.2. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.*

Quelques applications (de la Proposition 3.1 et du Corollaire 3.2) :

1) Soit $a \in \mathbb{Z}$ tel que $\text{pgcd}(a, n) = 1$. Alors $a^{\varphi(n)} \equiv 1 \mod n$. En particulier, si $n = p$ est premier, alors $\varphi(p) = p - 1$ et $a^{p-1} \equiv 1 \mod p$ pour tout $p \nmid a$ (petit Théorème de Fermat). On en déduit que pour tout $a \in \mathbb{Z}$, on a $a^p \equiv a \mod p$.

2) Théorème de Wilson ([Francinou-Gianella, page 81 et plus]). Soit $n \in \mathbb{N}^*$. Alors n est premier si et seulement si $(n-1)! \equiv -1 \mod n$.

(Si $n = p$ est premier, avec $p \geqslant 3$ (pour $p = 2$, le résultat est clair), on regroupe les éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$ avec leur inverse. L'équation $x^2 = 1$ a au plus deux solutions car $\mathbb{Z}/p\mathbb{Z}$ est un corps. Elle en a exactement deux puisque $\overline{1} \neq -\overline{1}$ ($p \neq 2$) or ce sont deux solutions de $x^2 = 1$. On en déduit que $\overline{2} \cdots \overline{p-2} = 1$ dans $\mathbb{Z}/p\mathbb{Z}$, d'où $(p-1)! \equiv p - 1 \equiv -1 \mod p$. Réciproquement, supposons $n \mid (n-1)! + 1$. Si n n'est pas premier, alors il existe $0 < a < n$ tel que $a \mid n$. Donc a divise $(n-1)!$ et par hypothèse a divise $(n-1)! + 1$ d'où la contradiction.)

4 Théorème Chinois

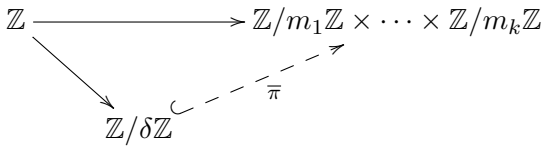
Théorème 4.1 (Théorème Chinois)**.** *Soient $m_1, \ldots, m_k$ des entiers > 0, et*

$$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$$

le morphisme naturel d'anneaux. On a

$$\ker \pi = \langle m_1 \rangle \cap \ldots \cap \langle m_k \rangle = \langle \text{ppcm}(m_1, \ldots, m_k) \rangle = \langle \delta \rangle,$$

d'où une factorisation (cf. Théorème 8.4),



Si $m_1, \ldots, m_k$ sont deux à deux premiers entre eux, alors $\delta = m_1 \cdots m_k$, et les cardinaux de $\mathbb{Z}/\delta\mathbb{Z}$ et $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$ coïncident. Par suite, $\overline{\pi}$ est un isomorphisme.

En pratique, c'est l'existence de $\overline{\pi}^{-1}$ qui est utile. Explicitons $\overline{\pi}^{-1}$.

Soient $x_1, \ldots, x_k$ des entiers. Il s'agit de chercher $x \in \mathbb{Z}$ tel que $x \equiv x_i \mod m_i$ pour tout $i = 1, \ldots, k$ On a $\text{pgcd}(m_i, \prod_{j \neq i} m_j) = 1$. D'après Bézout, il existe donc $(a_i, b_i) \in \mathbb{Z}^2$ tels que

$a_i m_i + b_i \prod_{j \neq i} m_j = 1$ (algorithme d'Euclide). Posons $c_i := b_i \prod_{j \neq i} m_j$. On a $c_i \equiv 0 \mod m_j$ pour tout $j \neq i$ et $c_i \equiv 1 \mod m_i$. On pose alors

$$x := \sum_{i=1}^{k} x_i c_i, \quad \text{on a } x \equiv x_i \mod m_i \text{ pour tout } i.$$

Corollaire 4.2. *Si $\delta = m_1 \cdots m_k$, alors $\overline{\pi}$ induit un isomorphisme sur les groupes des unités :*

$$(\mathbb{Z}/\delta\mathbb{Z})^\times \simeq (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})^\times.$$

En particulier, φ est multiplicative.

Soit $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \in \mathbb{N}$, avec p_i premier pour tout $i \in \{1, \ldots, k\}$. Alors

$$\varphi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i^{\alpha_i}})$$

(exercice : montrer d'abord que $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ si p est premier). En particulier, on voit que $\varphi(n) \to +\infty$ lorsque $n \to +\infty$.

5 Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$

D'après le Théorème Chinois 4.1, on est ramenés au cas où $n = p^\alpha$.

- 1er cas : $\alpha = 1$.

Théorème 5.1. *Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$, i.e., $((\mathbb{Z}/p\mathbb{Z})^\times, \times) \simeq (\mathbb{Z}/(p-1)\mathbb{Z}, +)$. Plus généralement, si $\Bbbk$ est un corps (commutatif), alors tout sous-groupe fini de $\Bbbk^\times$ est cyclique (e.g. $\mathbb{U}_n \subset \mathbb{C}^\times$). En particulier, si $\Bbbk$ est fini, alors $\Bbbk^\times$ est cyclique.*

Démonstration. Le théorème sera une conséquence de :

Lemme 5.2. *Soit G un groupe d'ordre n. Pour tout diviseur d de n, on pose $G(d) := \{x \in G \mid x^d = 1\}$. Supposons que pour tout $d|n$, on ait $|G(d)| \leqslant d$. Alors G est cyclique d'ordre n.*

Le lemme implique le théorème puisque dans un corps, l'équation $x^d = 1$ a au plus d solutions.

Démonstration du lemme. Soit $x \in G$; alors l'ordre d de x divise n. Donc $|\langle x \rangle| = d$. Or $\langle x \rangle \subset G(d)$, d'où $\langle x \rangle = G(d)$. Par suite, $G(d)$ est un groupe cyclique d'ordre d. De plus, il y a exactement $\varphi(d)$ éléments d'ordre d s'il y en a un (qui sont les générateurs de $\langle x \rangle$ si x est d'ordre d).

Pour tout diviseur d de n, notons $\psi(d)$ le nombre d'éléments de G d'ordre d. D'après ce qui précède, ou bien $\psi(d) = \varphi(d)$ (s'il y a des éléments d'ordre d dans G), ou bien $\psi(d) = 0$. Par ailleurs,

$$\sum_{d|n} \psi(d) = n = \sum_{d|n} \varphi(d).$$

La première égalité vient de ce que les éléments d'ordre d de G, pour d parcourant l'ensemble des diviseurs de n, forment une partition de G ; la deuxième résulte de (3.1). On en déduit que $\psi(d) = \varphi(d)$ pour tout $d|n$. En particulier, $\psi(n) = \varphi(n) \neq 0$. Donc $G = G(n)$ est cyclique (puisqu'il possède un élément d'ordre n).

□

□

En général, il est difficile de trouver un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. Un tel élément est appelé une *racine primitive modulo p*. Une conjecture (d'Artin) stipule que 2 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ pour une infinité de p premier...

• 2ème cas : $\alpha > 1$ et $p \neq 2$. Ici, l'étude est plus délicate (on peut omettre la lecture !) mais on montre de même que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique. Précisément :

Proposition 5.3. *Si p est premier impair et $\alpha \geqslant 2$, alors*

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z} \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}.$$

Idée de la démonstration. Les principales étapes sont les suivantes.
1) On considère le morphisme de groupes $\pi : (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ induit par le morphisme d'anneaux $\mathbb{Z}/p^\alpha\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$.

> *Le morphisme d'anneaux $\mathbb{Z}/p^\alpha\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ est bien défini car $p^\alpha\mathbb{Z} \subset \ker(\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z})$ donc le théorème de factorisation s'applique. De plus, comme* $\mathrm{pgcd}(n, p^\alpha) = 1$ *implique* $\mathrm{pgcd}(n, p) = 1$*, il induit le morphisme de groupes π.*

On en déduit que le noyau H de π est de cardinal $p^{\alpha-1}$ ($|(\mathbb{Z}/p^\alpha\mathbb{Z})^\times|/|(\mathbb{Z}/p\mathbb{Z})^\times| = \frac{p^{\alpha-1}(p-1)}{p-1} = p^{\alpha-1}$).

2) On montre que H est cyclique d'ordre $p^{\alpha-1}$. Précisément, on montre grâce au lemme qui suit que $a := \overline{1+p}$ est d'ordre $p^{\alpha-1}$ dans H :

Lemme 5.4. *Pour tout $k \geqslant 0$ et $p \neq 2$, on a* $(1+p)^{p^k} \equiv 1 + p^{k+1} \mod p^{k+2}$.

Le lemme se démontre à l'aide de la formule du binôme de Newton...

3) On construit un élément b d'ordre $p-1$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$: cette étape est un peu technique...

4) On en déduit alors que le produit $ab \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est d'ordre $p^{\alpha-1}(p-1)$ car $\mathrm{pgcd}(p^{\alpha-1}, p-1) = 1$. Ceci provient d'un résultat plus général dans un groupe quelconque :

Proposition 5.5. *Soit G un groupe. Si a et b sont d'ordre m et n respectivement, avec* $\text{pgcd}(m,n)=1$ *et a et b commutent, alors ab est d'ordre* $\text{ppcm}(m,n)=mn$.

Démonstration. Comme a et b commutent, $(ab)^{mn}=(a^n)^m(b^m)^n=1_G$ donc l'ordre $\text{ord}(ab)$ de ab divise mn ; ou bien il est égal à mn, ou bien il divise m ou n puisque $\text{pgcd}(m,n)=1$. Mais $(ab)^m=a^m\neq 1_G$ (car $n\nmid m$). De même $(ab)^n\neq 1_G$. Par suite $\text{ord}(ab)$ ne peut diviser m ou n, d'où $\text{ord}(ab)=mn$.

□

Conclusion : comme $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est d'ordre $p^{\alpha-1}(p-1)$, on a $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times=\langle ab\rangle$ et $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

□

• 3ème cas : $p=2$. Énonçons seulement les conclusions dans ce cas (voir [Perrin] pour plus de détails). On a $(\mathbb{Z}/2\mathbb{Z})^\times=\{1\}$, $(\mathbb{Z}/4\mathbb{Z})^\times=\{\pm 1\}$ (facile !). Pour $\alpha\geqslant 3$, on a $\mathbb{Z}/2^\alpha\mathbb{Z}\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^{\alpha-2}\mathbb{Z}$ (difficile !) ; en particulier, dans ce dernier cas, le groupe n'est pas cyclique.

Remarque 5.6. *On a un isomorphisme* $\text{Aut}(\mathbb{Z}/n\mathbb{Z})\simeq(\mathbb{Z}/n\mathbb{Z})^\times$ *donné par* $\alpha\mapsto\alpha(1)$. *Son application inverse est donnée par* $s\mapsto(x\mapsto sx)$.

6 Applications

Cryptage RSA

Référence : [Schwartz, page 106]

L'objectif de la cryptographie est de permettre de communiquer par des messages codés, qui ne pourront être lus que par leur destinataire. Pour cela, un "superviseur" donne à chaque receveur potentiel un "décodeur" et une "clé". La clé est quelque chose qui peut être diffusé à tout le monde.

L'algorithme RSA (1977), du nom de ses inventeurs Rivest, Shamir et Adleman, est basé sur la difficulté de factoriser un nombre entier en nombres premiers. Le principe est le suivant. Supposons que A souhaite envoyer des messages cryptés RSA à B. Alors B se donne deux grands nombres premiers distincts p et q.

> *(Maple permet de construire de tels nombres à l'aide des fonctions* `isprime` *et* `nextprime`*. Par exemple* `isprime(12345678901234567890123456 7)` *renvoie* `false` *donc 12345678901234567890123456 7 n'est pas premier, et* `nextprime(12345678901234567890123456 7)` *renvoie* `12345678901234567890123465 1`*, qui est donc le nombre premier le plus petit plus grand que celui-ci.)*

Ces deux nombres premiers seront notés p et q. La première partie de la **clé publique**, notée $c := pq$, sera le produit de p et q.

B choisit alors un nombre d, premier avec $\varphi(c) = (p-1)(q-1)$ (il est facile de choisir un nombre qui soit premier avec un autre : il suffit d'en piocher un au hasard, et de recommencer jusqu'à ce que l'algorithme de Bezout confirme que ces deux nombres sont premiers entre eux.) Cet entier sera connu de A.

On peut aussi déterminer facilement d^{-1}, inverse de d dans $(\mathbb{Z}/c\mathbb{Z})^\times = \mathbb{Z}/\varphi(c)\mathbb{Z}$ (pour celui qui connaît $\varphi(c)$!). Cet entier ne sera connu que de B (qui connaît p, q et donc $\varphi(c)$). Il y a bien un isomorphisme car $(\mathbb{Z}/c\mathbb{Z})^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ puisque $(p,q) = 1$, et un isomorphisme entre $(\mathbb{Z}/p\mathbb{Z})^\times$ et $\mathbb{Z}/(p-1)\mathbb{Z}$ (resp. $(\mathbb{Z}/q\mathbb{Z})^\times$ et $\mathbb{Z}/(q-1)\mathbb{Z}$) : cf. Théorème Chinois 4.1 et ses conséquences.

Cryptage :

- On suppose le message suffisamment court pour être codable par un élément inversible de $\mathbb{Z}/c\mathbb{Z}$, ce qui est possible en remplaçant le message par des tranches successives suffisamment petites (si on a un alphabet de taille α, il suffit de prendre des tranches de longueur l avec $\alpha^l < \varphi(c)$). Cette méthode de codage n'a pas à être compliquée ni à être cachée. Il suffit donc d'avoir une injection de $[1; \alpha^l]$ dans $(\mathbb{Z}/c\mathbb{Z})^\times$.
- Chaque message de A est donc remplacé (par A) par un élément n inversible dans $\mathbb{Z}/c\mathbb{Z}$.
- A envoie alors à B le nombre $e := n^d$ dans $\mathbb{Z}/c\mathbb{Z}$.

Décryptage :

- B, qui dispose de d et de d^{-1}, effectue simplement le calcul de $e^{d^{-1}}$, qui lui donne n, et donc le message initial.

Équations diophantiennes

Par définition, on appelle *équations diophantiennes* toute équation de la forme $P(x_1, \ldots, x_k) = 0$ où $P \in \mathbb{Z}[X_1, \ldots, X_k]$.

• Exemple des équations diophantiennes d'ordre 1 (avec deux inconnues) : $ax + by = c$, avec $a, b, c \in \mathbb{Z}$. Si le pgcd de a et b ne divise pas c, il n'y a pas de solution. Sinon, l'ensemble des solutions est $\{(c'u + kb', c'v - ka'),\ k \in \mathbb{Z}\}$ où $\delta = \text{pgcd}(a,b)$, $a = \delta a'$, $b = \delta b'$, $c = \delta c'$ et où (u,v) vérifie $a'u + bv' = 1$ (un tel couple existe d'après l'identité de Bézout).

• Pour les équations diophantiennes d'ordre plus élevé, il n'y a pas de résultat général. On peut néanmoins étudier certaines familles d'exemples, notamment pour les équations d'ordre 2, à l'aide de l'étude des corps finis (voir plus tard dans le cours).
Exemple : l'équation $x^2 + y^2 = p$ n'a pas de solution dans $\mathbb{Z}$ si p est un nombre premier, $p \equiv 3 \mod 4$ (cf. Théorème des deux carrés, Section 8).

Nous rencontrerons d'autres exemples (e.g. $x^2+y^2=7z^2$, $x^2-5y^2=3$, cas particuliers de l'équation de Fermat $x^n+y^n=z^n$, équation de Pell $x^2-dy^2\pm 1$).

Références : [Monier] (pour les équations d'ordre 1), [Samuel] (pour des exemples d'équations d'ordre $\geqslant 2$).

Deuxième partie

Anneaux principaux et euclidiens

Référence : [Perrin, pages 45 et plus].
Remarque : les anneaux *noethériens* et *factoriels* ne sont pas au programme de l'Agrégation Interne.

Les anneaux considérés ici seront supposés commutatifs, intègres (i.e., $A\neq\{0\}$ et $(ab=0\Leftrightarrow a=0$ ou $b=0)$), et unitaires. Dans tout ce qui suit, A est un tel anneau.

7 Définitions

Définition 7.1. *Soient $a,b\in A$.*

1) *On dit que a* divise *b s'il existe $c\in A$, tel que $b=ac$, i.e., $(b)\subset(a)$.*

2) *On dit que a* et *b* sont associés *si a divise b et b divise a, i.e., $(a)=(b)\iff(\exists\, u\in A^\times, b=ua)$.*

La propriété « intègre » est essentielle pour établir la deuxième équivalence de (2). Cependant, il n'existe pas d'exemple simple d'anneau non intègre où l'équivalence n'a pas lieu. Par exemple, dans $\mathbb{Z}/n\mathbb{Z}$ qui n'est pas intègre en général, l'équivalence $(a)=(b)\iff(\exists\, u\in A^\times, b=ua)$ reste vraie.

En revanche, elle est fausse dans $\Bbbk[X,Y,Z]/X(1-YZ)$; on a $(x)=(xy)$ mais x et xy ne sont pas associés (exercice). Ici, $x=\overline{X}$ et $y=\overline{Y}$.

Définition 7.2. *Soit $p\in A$. On dit que p est* irréductible *si*

1) *$p\notin A^\times$;*

2) *$p=ab\Rightarrow a$ ou $b\in A^\times$.*

Remarque : 0 n'est pas irréductible car $0=0\times 0$ et $0\notin A^\times$.

Exemple 7.3 (non traité en cours !)**.** *Considérons l'anneau $A=\mathbb{Z}[\sqrt{10}]=\{a+\sqrt{10}b\,|\,a,b\in\mathbb{Z}\}$, qui est* l'anneau des entiers *de $\mathbb{Q}(\sqrt{10})$, i.e., l'anneau $\{x\in\mathbb{Q}(\sqrt{10})\,|\,\exists P\in\mathbb{Z}[X], P(x)=0\}$. Il existe un unique isomorphisme non trivial $\sigma:\mathbb{Q}(\sqrt{10})\to\mathbb{Q}(\sqrt{10})$; il envoie $a+\sqrt{10}b$ sur $a-\sqrt{10}b$ (exercice). On définit alors la* norme *$N(x)$ d'un élément $x\in A$ par $N(x):=$*

$x\sigma(x) = a^2 - 10b^2$. Remarquons que $N(x)$ est un entier relatif pour tout $x \in A$ et que la norme est multiplicative, i.e., $N(xy) = N(x)N(y)$ pour tout $x, y \in A$. On vérifie alors que $A^\times = \{x \in A \mid N(x) = \pm 1\}$ (si $xy = 1$, alors $N(x)N(y) = 1$ donc $N(x) = \pm 1$; réciproquement, si $N(x) = \pm 1$ alors $\sigma(x)$ ou $-\sigma(x)$ est un inverse de x dans A...). On en déduit que

$$A^\times = \{a + \sqrt{10}b \mid a, b \in \mathbb{Z},\ a^2 - 10b^2 = \pm 1\}.$$

On est donc ramenés à étudier l'équation de Pell *: $a^2 - 10b^2 = \pm 1$. On obtient*

$$A^\times = \{(\pm(3 + \sqrt{10})^n,\ n \in \mathbb{Z}\}$$

(les solutions de cette équations sont connues).

Exercice : montrer que 2 est un élément irréductible de A.

(solution : si 2 était réductible, alors $2 = xy$, $4 = N(2) = N(x)N(y)$, avec $x, y \notin A^\times$. Donc $N(x) = \pm 2 = a^2 - 10b^2$. On en déduit que 2 est un carré modulo 10, donc modulo 5, ce qui est impossible puisque dans $\mathbb{Z}/5\mathbb{Z}$ les seuls carrés sont 1 et 4 ; voir l'étude des carrés dans un corps finis.)

Définition 7.4. *Soit I un idéal de A.*

1) *On dit que I est* premier *si l'anneau A/I est intègre.*

2) *On dit que I est maximal si I est maximal pour l'inclusion, i.e., si $J \supset I$ et $J \neq I$, alors $I = A$.*

Proposition 7.5. *Soit I un idéal de A. Alors I est maximal si et seulement si A/I est un corps. En particulier, tout idéal maximal est premier.*

Exemple 7.6. *Les idéaux premiers de $\mathbb{Z}$ sont (0) et $p\mathbb{Z}$ avec p premier. Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$ avec p premier.*

Proposition 7.7. *Soit $p \in A$, $p \notin A^\times$ et $p \neq 0$. Alors*

$$(p) \text{ est premier (i.e., } p|ab \Rightarrow p|a \text{ ou } p|b) \Longrightarrow p \text{ est irréductible.}$$

Définition 7.8. *On dit qu'anneau A est* principal *si tout idéal de A est principal, i.e., engendré par un seul élément.*

La réciproque de la Proposition 7.7 est vraie lorsque A est principal. En fait, elle reste vraie lorsque A est seulement *factoriel* (notion hors programme !). Lorsque l'implication inverse est vraie (par exemple dans un anneau principal), on dit que l'anneau *vérifie la condition d'Euclide.*

Exemple : dans $\mathbb{Z}[\sqrt{10}]$, 2 est irréductible mais (2) n'est pas premier. En effet $2 \times 3 = (4 + \sqrt{10})(4 - \sqrt{10})$ donc $2|(4+\sqrt{10})(4-\sqrt{10})$ mais 2 ne peut diviser $4+\sqrt{10}$ ou $4-\sqrt{10}$. L'anneau $\mathbb{Z}[\sqrt{10}]$ n'est donc pas principal.

Dans un anneau principal, on peut faire de l'arithmétique « classique ». Les notions de *pgcd*, *ppcm*, d'éléments *premiers entre eux* existent néanmoins dès que A est intègre. Attention aux définitions du pgcd et du ppcm dans le cas général : elles diffèrent un peu de celles données ci-dessous :

Définition 7.9. *On dit que a et b sont* premiers entre eux *si on a*

$$\forall\, d \in A, \quad d|a \text{ et } d|b \Rightarrow d \in A^\times.$$

Autrement dit, a et b n'ont pas de diviseurs communs non triviaux. Lorsque A est principal, on peut définir un pgcd *et* un ppcm *comme suit :*

$$\mathrm{ppcm}(a,b) = c \ \text{ où } \ (a)\cap(b) = (c), \quad \mathrm{pgcd}(a,b) = d \ \text{ où } \ (a)+(b) = (d).$$

Attention : le ppcm et le pgcd sont définis aux inversibles près (cf. définition 7.1) !

Si A est principal, on dispose de l'existence de la « propriété universelle de l'arithmétique », c'est-à-dire la factorisation, unique à l'ordre des facteurs près et multliplication des inversibles près, d'un élément à l'aide d'éléments irréductibles. Précisément, pour tout $a \in A$, il existe $u \in A^\times$ et $p_1, \dots, p_r$ des éléments irréductibles de A tels que

$$a = up_1 \cdots p_r.$$

Si $a = vq_1 \cdots p_s$ est une autre telle décomposition, alors $r = s$ et il existe une permutation σ de $\{1, \dots, r\}$ telle que p_i et $q_{\sigma(i)}$ soient associés.

De plus, si A est principal, alors la condition d'Euclide (ou Lemme d'Euclide) et le Lemme de Gauss (i.e., si a divise bc et si a et b sont premiers entre eux, alors a divise c) s'appliquent. L'égalité donnant le pgcd dans la Définition 7.9 est connue sous le nom de *Théorème de Bézout* :

Théorème 7.10 (Bézout)**.** *Si $a, b \in A \setminus \{0\}$, alors il existe $\lambda, \mu \in A$ tels que $\lambda a + \mu b = d$ où d est un* pgcd *de a et b.*

Définition 7.11. *Un anneau A est dit* euclidien *si A est intègre et si A est muni d'une application $\nu : A \setminus \{0\} \to \mathbb{N}$ telle que si $a, b \in A \setminus \{0\}$, alors il existe $q, r \in A$ avec $a = bq + r$ et ($r = 0$ ou $0 < \nu(r) < \nu(b)$).*

Un anneau euclidien est principal. La démonstration a déjà été vue dans le cas de $\mathbb{Z}$ (cf. Proposition 1.1). Les mêmes arguments s'appliquent pour un anneau euclidien quelconque.

Exemples 7.12. 1) *Si $\Bbbk$ est un corps, alors $\Bbbk[X]$ est euclidien donc principal.*

2) *Plus généralement, si A est un anneau, alors $A[X]$ est principal si et seulement si A est un corps. En particulier, $\mathbb{Z}[X]$ n'est pas principal (on peut le voir directement en remarquant que l'idéal engendré par 2 et X n'est pas principal).*

3) *Nous verrons que $\mathbb{Z}[i]$ est euclidien (cf. prochain cours).*

4) *L'anneau des séries formelles $\Bbbk[[X]]$, l'anneau D des nombres décimaux (i.e., le sous-anneau de $\mathbb{Q}$ engendré par $\mathbb{Z}$ et $1/10$) sont des exemples d'anneaux euclidiens.*

5) *Il existe des anneaux principaux non euclidiens. Exemple : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ (voir [Perrin, page 54])*

8 Application : l'anneau $\mathbb{Z}[i]$ et le théorème des deux carrés

Référence : [Perrin, page 56] ou [Francinou-Gianella].

L'anneau $\mathbb{Z}[i]$ est explicitement au programme de l'Agrégation Interne. Cette application sera l'occasion de rappeler quelques résultats sur les corps finis.

Le problème est de déterminer quels entiers $n \in \mathbb{N}$ sont sommes de deux carrés. On pose

$$\Sigma := \{n \in \mathbb{N} \,|\, n = a^2 + b^2,\, a, b \in \mathbb{N}\}.$$

Remarque : Si $n \equiv 3 \mod 4$, alors $n \notin \Sigma$. En effet, si a est pair, alors $a^2 \equiv 0 \mod 4$ et si a est impair, alors $a \equiv 1 \mod 4$, donc $a^2 + b^2 \equiv 0, 1$ ou $2 \mod 4$.

L'idée pour étudier Σ est de remarquer que pour $n \in \Sigma$, on a $n = (a + ib)(a - ib)$ dans $\mathbb{C}$, avec $a, b \in \mathbb{Z}$. D'où l'idée d'introduire l'anneau des entiers, dit *de Gauss*,

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

et de considérer une norme (comme pour $\mathbb{Z}[\sqrt{10}]$). La norme permettra de montrer que Σ est multiplicatif. Il suffira alors essentiellement de déterminer les entiers premiers qui sont dans Σ.

Étude de $\mathbb{Z}[i]$

On remarque tout d'abord que l'anneau $\mathbb{Z}[i]$ est intègre (car inclus dans $\mathbb{C}$). On définit une norme (au sens de l'arithmétique) sur $\mathbb{Z}[i]$ en posant

$$N(a + ib) = a^2 + b^2, \quad a, b \in \mathbb{Z}.$$

(elle provient, comme pour $\mathbb{Z}[\sqrt{10}]$, de l'unique automorphisme non trivial de $\mathbb{Z}[i]$ qui est $\sigma : \mathbb{Z}[i] \to \mathbb{Z}[i]$, $a + ib \mapsto a - ib$). La norme est clairement multiplicative : $N(zz') = N(z)N(z')$ pour tout $z, z' \in \mathbb{Z}[i]$. Remarquons aussi que $N(z)$ est un entier naturel pour tout $z \in \mathbb{Z}[i]$.

Proposition 8.1. (i) *L'ensemble Σ est stable par multiplication.*

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

(iii) *L'anneau $\mathbb{Z}[i]$ est euclidien (relativement à N), donc principal.*

Démonstration. (i) il suffit de remarquer que pour $n \in \mathbb{N}^*$, $n \in \Sigma$ si et seulement s'il existe $z \in \mathbb{Z}[i]$ tel que $n = N(z)$.

(ii) On raisonne comme pour $\mathbb{Z}[\sqrt{10}]$. Ici, $z \in \mathbb{Z}[i]^\times$ implique $N(z) = 1$ car $N(z) \in \mathbb{N}$. Réciproquement, $N(a+ib) = 1$ implique que $a = \pm 1$ et $b = 0$ ou $a = 0$ et $b = \pm 1$.

(iii) Soient $z, t \in \mathbb{Z}[i] \smallsetminus \{0\}$. Écrivons $z/t = x + iy$ dans $\mathbb{C}$. On choisit un entier de Gauss $q = a+ib$ le "plus proche" possible de z/t. Précisément, on chosit $a, b \in \mathbb{Z}$ de sorte que $|x-a| \leqslant \frac{1}{2}$ et $|y-b| \leqslant \frac{1}{2}$, d'où $|z/t - q|^2 \leqslant \frac{1}{2}$. Posons $r := z - tq$. Alors $r \in \mathbb{Z}[i]$ et, ou bien $r = 0$, ou bien $N(r) = |t(z/t-q)|^2 = N(t)|z/t-q|^2 < N(t)$.

□

Résultat principal

Théorème 8.2. *Soit $p \in \mathbb{N}$ un nombre premier. Alors*

$$p \in \Sigma \iff p = 2 \text{ ou } p \equiv 1 \mod 4.$$

Du théorème, on déduit une caractérisation plus générale pour n'importe quel entier (à l'aide de la factorisation d'un entier en produit de nombres premiers).

Démonstration. La condition est nécessaire (déjà vue). Pour la réciproque, on montre d'abord :

Lemme 8.3. *On a $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.*

Démonstration. Si $p \in \Sigma$, alors $p = (a+ib)(a-ib)$, avec $a, b \in \mathbb{Z}$, et a ou b non nul ; donc p n'est pas irréductible dans $\mathbb{Z}[i]$.

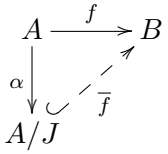
Réciproquement, si p n'est pas irréductible dans $\mathbb{Z}[i]$, alors $p = zz'$ avec $z, z' \notin A^\times$, i.e., $N(z) \neq 1$ et $N(z') \neq 1$. On a $p^2 = N(p) = N(z)N(z')$. Comme p est premier, $N(z)$ ou $N(z')$ est égal à p. Par suite $p \in \Sigma$.

□

Revenons à la démonstration du Théorème 8.2. D'après le lemme, on est conduits à caractériser les entiers premiers p dans $\mathbb{Z}$ qui ne sont pas irréductibles dans $\mathbb{Z}[i]$. Comme $\mathbb{Z}[i]$ est euclidien, donc principal, il résulte de la Proposition 7.7 que p n'est pas irréductible dans $\mathbb{Z}[i]$ si et seulement si (p) n'est pas premier dans $\mathbb{Z}[i]$ ou encore, si et seulement si le quotient $\mathbb{Z}[i]/(p)$ n'est pas intègre (cf. Définition 7.4).

Nous allons donc décrire l'anneau quotient $\mathbb{Z}[i]/(p)$. Rappelons le Théorème d'isomorphisme (déjà utilisé) :

Théorème 8.4 (Théorème d'isomorphisme)**.** *Soit $f : A \to B$ un morphisme d'anneaux et $I = \ker f$. Soit J un idéal de A contenu dans I et $\alpha : A \to A/J$ la projection canonique. Alors il existe un unique morphisme $\overline{f} : A/J \to B$ tel que $f = \overline{f} \circ \alpha$.*



De plus, $\overline{f}$ est injectif si et seulement si $J = I$ et $\overline{f}$ est surjectif si et seulement si f l'est. En particulier, on a $\operatorname{im} f \simeq A/\ker f$.

À l'aide du Théorème d'isomorphisme, on établit les isomorphismes suivants :

$$\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1), \qquad (\mathbb{Z}[X]/(X^2+1))/(p) \simeq \mathbb{Z}[X]/(X^2+1,p),$$

$$\mathbb{Z}[X]/(X^2+1,p) \simeq (\mathbb{Z}[X]/(p))/(X^2+1), \qquad \mathbb{Z}[X]/(p) \simeq \mathbb{Z}/p\mathbb{Z}[X].$$

D'où,

$$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}/p\mathbb{Z}[X]/(X^2+1).$$

Ainsi, p n'est pas irréductible dans $\mathbb{Z}[i]$ si et seulement si $\mathbb{Z}/p\mathbb{Z}[X]/(X^2+1) = \mathbb{F}_p[X]/(X^2+1)$ n'est pas intègre. Ici, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ désigne le corps fini à p éléments. Dire que l'anneau $\mathbb{F}_p[X]/(X^2+1)$ n'est pas intègre équivaut à dire que X^2+1 n'est pas irréductible dans $\mathbb{F}_p[X]$ (car $\mathbb{F}_p[X]$ est principal). Comme X^2+1 est de degré $\leqslant 3$, cette dernière condition équivaut encore à dire que X^2+1 a une racine dans $\mathbb{F}_p$, ou encore que -1 est un carré dans $\mathbb{F}_p$.

En conclusion,

$$p \in \Sigma \iff -1 \in (\mathbb{F}_p^\times)^2, \tag{8.1}$$

où $(\mathbb{F}_p^\times)^2 := \{x^2 \mid x \in \mathbb{F}_p^2\}$ est l'ensemble des carrés non nuls de $\mathbb{F}_p$.

Attention : pour un polynôme P de $\Bbbk[X]$, $\Bbbk$ un corps commutatif, de degré $\geqslant 4$, il est faux en général de dire que P est irréductible dans $\Bbbk$ si et seulement si P a une racine dans $\Bbbk$. Par exemple, $P(X) = (X^2+1)^2$ est réductible dans $\mathbb{R}[X]$ mais n'a pas de racines dans $\mathbb{R}$.

Compte tenu de l'équivalence (8.1), nous allons faire quelques rappels sur l'étude des carrés dans un corps finis.

Digression sur les carrés dans un corps finis. Soient $q = p^n$, p premier impair, et $\mathbb{F}_q$ *le* corps fini à q éléments (le cardinal d'un corps fini est une puissance de sa *caractéristique*, qui est toujours un nombre premier).

Proposition 8.5. *Rappelons que $p \neq 2$. Pour tout $a \in \mathbb{F}_q$,*

$$a \text{ est un carré dans } \mathbb{F}_q \quad \iff \quad a^{\frac{q-1}{2}} = 1.$$

En particulier, -1 est un carré modulo p si et seulement si $p \equiv 1 \mod 4$.

D'après l'équation (8.1) et la Proposition 8.5 ci-dessus, l'implication réciproque du Théorème 8.2 s'ensuit.

Démonstration. Notons $\mathbb{F}_q^2 = \{x^2 \,|\, x \in \mathbb{F}_q\}$ l'ensemble des carrés de $\mathbb{F}_q$, et $(\mathbb{F}_q^\times)^2 := \mathbb{F}_q^2 \cap \mathbb{F}_q^\times$. On a un morphisme de groupes $\mathbb{F}_q^\times \to (\mathbb{F}_q^\times)^2$, $x \mapsto x^2$. Comme $p \neq 2$, l'équation $x^2 = 1$ a exactement deux solutions : 1 et -1. Le noyau du morphisme est donc de cardinal 2. Par suite $|(\mathbb{F}_q^\times)^2| = \frac{q-1}{2}$.

Montrons alors la proposition. Il est clair que si $a = x^2$, $x \in \mathbb{F}_q$, est un carré de $\mathbb{F}_q$, alors $a^{\frac{q-1}{2}} = x^{q-1} = 1$. Réciproquement, comme l'équation $y^{\frac{q-1}{2}} = 1$ a au plus $\frac{q-1}{2}$ solutions et que tous les éléments de $(\mathbb{F}_q^\times)^2$ sont solutions, on en déduit $(\mathbb{F}_q^\times)^2$ est exactement l'ensemble des solutions de l'équation $y^{\frac{q-1}{2}} = 1$.

□

Remarque 8.6. *Grâce à la discussion sur les cardinaux dans la preuve précédente, on montre que* $|\mathbb{F}_q^2| = \frac{q-1}{2} + 1 = \frac{q+1}{2}$.

□

Troisième partie

Groupes et géométrie

Nous étudierons ici des exemples d'utilisation des groupes en géométrie. Ce sera l'occasion de rappeler des résultats généraux sur les groupes (e.g., sur le produit semi-direct) et sur le groupe symétrique en particulier.

Contexte : on se place dans un espace affine euclidien $(E, \mathcal{E})$ de dimension 2 ou 3. On note $\langle\ ,\ .\ ,\ \rangle$ le produit scalaire et $\|.\|$ la norme associée. On notera $GA(\mathcal{E})$ le *groupe affine* de $\mathcal{E}$, c'est-à-dire le groupe des transformations affines inversibles.

9 Introduction

Nous allons essentiellement étudier dans ce cours des sous-groupes finis de

$$O(E) := \{u \in \mathrm{L}(E) \,|\, \|u(x)\| = \|x\|, \forall\, x \in E\}$$

et donner une interprétation géométrique de certains de ces groupes (tous dans le cas de la dimension 2). Les sous-finis de $O(E)$ apparaissent naturellement en géométrie compte tenu des deux remarques importantes qui suivent.

2) En géométrie, il est naturel de s'intéresser aux transformations du plan (resp. de l'espace) qui préservent un polygone régulier (resp. un polyèdre régulier) $\mathcal{P}$, c'est-à-dire qui laisse globalement invariant $\mathcal{P}$.

Remarque : il y a une infinité de polygones réguliers du plan (carré, pentagone, hexagone,..., n-gone) et seulement 5 polyèdres réguliers convexes (9 si on compte les non convexes) de l'espace : le *tétraèdre* (4 faces), le cube ou *hexaèdre* (6 faces), l'*octaèdre* (8 faces), le *dodécaèdre* (12 faces) et l'*icosaèdre* (20 faces), voir Figure 1.

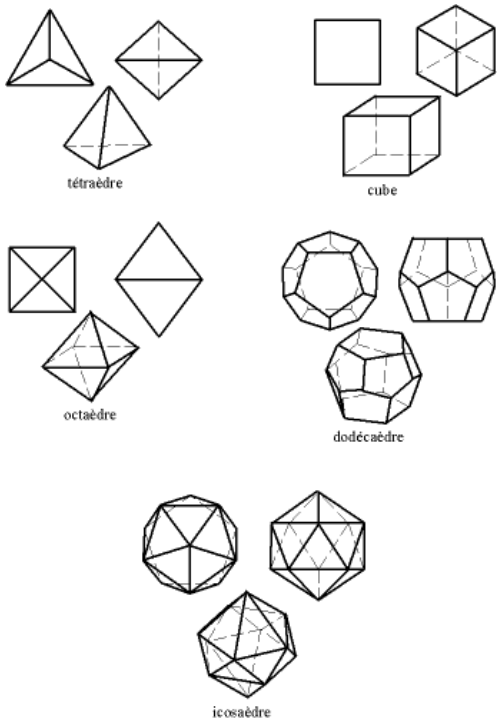


FIGURE 1 – Polyèdres réguliers convexes

L'ensemble de ces transformations, que nous noterons $\mathcal{I}s(\mathcal{P})$, forme un sous-groupe fini de $GA(\mathcal{E})$.

Explication. Tout d'abord, remarquons que $\mathcal{I}s(\mathcal{P})$ est contenu dans $GA(\mathcal{E})$. En effet, les éléments de $\mathcal{I}s(\mathcal{P})$ permutent les sommets de $\mathcal{P}$. Or des sommets $S_1, \ldots, S_n$ de $\mathcal{P}$, on peut extraire un repère affine de $\mathcal{E}$. Ensuite, on vérifie facilement que $\mathcal{I}s(\mathcal{P})$ forme un sous-groupe de $GA(\mathcal{E})$.

Il reste à voir que ce sous-groupe est fini. Comme les éléments de $\mathcal{I}s(\mathcal{P})$ permutent les sommets de $\mathcal{P}$, on a une action du groupe $\mathcal{I}s(\mathcal{P})$ dans l'ensemble $X := \{S_1, \ldots, S_n\}$, d'où une application $\mathcal{I}s(\mathcal{P}) \to \mathfrak{S}(X) \simeq \mathfrak{S}_n$, où $\mathfrak{S}_n$ est le *groupe symétrique* d'ordre n. L'action est fidèle (si une application fixe tous les sommets, alors c'est l'identité car, des sommets, on peut extraire un repère affine de $\mathcal{E}$). Nous reviendrons sur ce point dans les exemples. Cela montre que $\mathcal{I}s(\mathcal{P})$ s'injecte dans le groupe $\mathfrak{S}_n$; en particulier, il est fini !

□

1) Si $G \subset GA(\mathcal{E})$ est un sous-groupe fini de $GA(\mathcal{E})$, alors G s'identifie à un sous-groupe fini de $O(E)$.

Explication. Remarquons que, si M est un point quelconque de $\mathcal{E}$, alors l'isobarycentre A des points $g(M)$, pour $g \in G$, est fixé par tous les éléments de G car les transformations affines préservent le barycentre. L'étude se réduit donc à celle des sous-groupe finis de $GL(E)$. Précisément, l'isomorphisme est induit par le morphisme de groupes

$$\phi : G \hookrightarrow GL(E),\ f \longmapsto (\vec{v} \mapsto \overrightarrow{f(A)f(A+\vec{v})}).$$

On peut donc supposer que G est un sous-groupe fini de $GL(E)$. Il existe alors un produit scalaire φ sur E tel que G soit contenu dans $O(E, \varphi)$. En effet, il suffit de poser

$$\forall\, (x, y) \in E^2, \quad \varphi(x, y) := \sum_{g \in G} \langle g(x), g(y) \rangle.$$

Comme $O(E)$ et $O(E, \varphi)$ sont isomorphes, on est donc conduits à étudier les sous-groupes finis de $O(E)$ comme annoncé.

□

D'après les remarques 1) et 2), on peut identifier $\mathcal{I}s(\mathcal{P})$ à un sous-groupe fini de $O(E)$. Nous nous placerons donc désormais dans ce cadre.

10 Sous-groupes finis de $O(2, \mathbb{R})$

Référence : [Tauvel2, page 14]

On suppose ici que $E = \mathbb{R}^2$ et que E est muni du produit scalaire canonique.

Sous-groupes de $SO(2, \mathbb{R})$

Rappelons que le *groupe spécial orthogonal* $SO(2, \mathbb{R})$ est commutatif et que l'on a

$$SO(2, \mathbb{R}) = \{R(\theta) := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},\ \theta \in \mathbb{R}\}.$$

Théorème 10.1. *On a un isomorphisme entre $SO(2,\mathbb{R})$ et $\mathbb{U}$, le groupe des complexes de module 1. L'isomorphisme est donné par $R(\theta) \mapsto e^{i\theta}$.*

Rappel : soit $\phi : \mathbb{R}/2\pi\mathbb{Z} \to \mathbb{U}$ l'isomorphisme induit par $\theta \mapsto e^{i\theta}$. On dit que la classe de $\phi^{-1}(\cos\theta + i\sin\theta)$ dans $\mathbb{R}/2\pi\mathbb{Z}$ est la *mesure de θ*. Tout représentant de cette classe dans $\mathbb{R}$ est appelé, par abus, *une mesure de la rotation $r(\theta)$*, où $r(\theta)$ est la rotation dont la matrice dans la base canonique est $R(\theta)$.

Il résulte du Théorème 10.1 que les sous-groupes finis de $SO(2,\mathbb{R})$ sont cycliques et isomorphes à $\mathbb{U}_n$ (car $\mathbb{U} \subset \mathbb{C}^\times$ et $\mathbb{C}$ est un corps, cf. Théorème 5.1) :

Corollaire 10.2. *Les sous-groupes finis de $SO(2,\mathbb{R})$ sont cycliques et isomorphes à $\mathbb{U}_n$ pour un certain $n \in \mathbb{N}$.*

Il est facile de comprendre l'isomorphisme : si r est une rotation d'angle $2\pi/n$, alors le sous-groupe de $SO(2,\mathbb{R})$ engendré par r est cyclique d'ordre n. De plus, le Corollaire 10.2 assure que tout sous-groupe fini de $SO(2,\mathbb{R})$ est de cette forme.

Cas général et interprétation géométrique

Rappelons que notre motivation est d'étudier les transformations du plan qui préservent un polygone régulier $\mathcal{P}_n$ (à $n \geqslant 3$ côtés). On notera $S_1, \ldots, S_n$ les sommets de $\mathcal{P}_n$. L'isobarycentre des sommets est préservé par de telles transformations ; on peut supposer que c'est l'origine. Le groupe $\mathcal{I}s(\mathcal{P}_n)$ des isométries de $\mathcal{P}_n$ s'identifie donc à un sous-groupe fini de $O(2,\mathbb{R})$ (cf. Introduction).

On commence par décrire le sous-groupe $\mathcal{I}s^+(\mathcal{P}_n) = \mathcal{I}s(\mathcal{P}_n) \cap SO(2,\mathbb{R})$ des isométries positives (i.e., des rotations) qui préservent le polygone $\mathcal{P}_n$.

Proposition 10.3. *Le groupe $\mathcal{I}s^+(\mathcal{P}_n)$ est un groupe cyclique engendré par la rotation de mesure d'angle $\frac{2\pi}{n}$. En particulier, il est de cardinal n.*

Démonstration. Le groupe $\mathcal{I}s^+(\mathcal{P}_n)$ est un sous-groupe fini de $SO(2,\mathbb{R})$; il est donc cyclique (cf. Corollaire 10.2). Si ρ est une rotation qui préservent $\mathcal{P}_n$, alors sa mesure d'angle est $\frac{2k\pi}{n}$ avec $k \in \mathbb{Z}$. Son ordre divise donc n (car $\rho^n = \mathrm{Id}_E$). Réciproquement, toutes ces rotations appartiennent à $\mathcal{I}s^+(\mathcal{P}_n)$. En particulier, la rotation r de mesure d'angle $\frac{2\pi}{n}$, qui est d'ordre exactement n, est dans $\mathcal{I}s^+(\mathcal{P}_n)$. Par suite $\mathcal{I}s^+(\mathcal{P}_n)$ est le groupe cyclique engendré par r. Comme r est d'ordre n, le cardinal de $\mathcal{I}s^+(\mathcal{P}_n)$ est n.

□

On notera désormais r la rotation de mesure d'angle $\frac{2\pi}{n}$. D'après la Proposition 10.3, on a $\mathcal{I}s^+(\mathcal{P}_n) = \langle r \rangle$.

Il existe des isométries indirectes qui préservent $\mathcal{P}_n$. Par exemple, la symétrie orthogonale d'axe la bissectrice formée par les vecteurs $\overrightarrow{S_1S_2}$ et $\overrightarrow{S_1S_n}$ (voir la Figure 2). Le groupe $\mathcal{I}s(\mathcal{P}_n)$ n'est donc certainement pas contenu dans $SO(2,\mathbb{R})$ et $\mathcal{I}s^+(\mathcal{P}_n)$ ne suffit pas à décrire $\mathcal{I}s(\mathcal{P}_n)$!

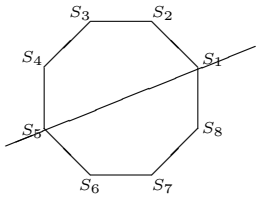


FIGURE 2 – Octogone, $n = 8$

Notons s la symétrie d'axe la bissectrice formée par les vecteurs $\overrightarrow{S_1S_2}$ et $\overrightarrow{S_1S_n}$.

Proposition 10.4. *Le groupe $\mathcal{I}s(\mathcal{P}_n)$ est de cardinal $2n$ et On a*

$$\mathcal{I}s(\mathcal{P}_n) = \{\mathrm{Id}_E, r, r^2, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s\}.$$

Démonstration. Considérons le morphisme de groupes $\varphi : \mathcal{I}s(\mathcal{P}_n) \to \{1,-1\}$, $u \mapsto \det(u)$. Comme $\varphi(r) = 1$ et $\varphi(s) = -1$, φ est surjective. D'autre part, le noyau de φ est $\mathcal{I}s^+(\mathcal{P}_n)$ (presque par définition de $\mathcal{I}s^+(\mathcal{P}_n)$!). D'après le Théorème d'isomorphisme (Théorème 8.4), on en déduit que $\mathcal{I}s(\mathcal{P}_n)/\mathcal{I}s^+(\mathcal{P}_n) \simeq \{1,-1\}$. En particulier, le cardinal du quotient $\mathcal{I}s(\mathcal{P}_n)/\mathcal{I}s^+(\mathcal{P}_n)$ est 2. Or, d'après la Proposition 10.3, le cardinal de $\mathcal{I}s^+(\mathcal{P}_n)$ est n, d'où $|\mathcal{I}s(\mathcal{P}_n)| = 2n$.

Les éléments $\mathrm{Id}_E, r, r^2, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s$ sont clairement dans $\mathcal{I}s(\mathcal{P}_n)$ (puisque r et s le sont !) et on vérifie sans difficulté qu'ils sont deux à deux distincts. Ce sont donc les seuls éléments de $\mathcal{I}s(\mathcal{P}_n)$ puisqu'ils sont au nombre de $2n = |\mathcal{I}s(\mathcal{P}_n)|$.

□

Le groupe $\mathcal{I}s(\mathcal{P}_n)$ contient les deux sous-groupes $\langle r\rangle$ et $\langle s\rangle$. Le premier est cyclique d'ordre n (déjà vu) et le second est (cyclique) d'ordre 2 car $s^2 = \mathrm{Id}_E$.

Notons aussi que $\langle r\rangle = \mathcal{I}s^+(\mathcal{P}_n)$ est *distingué* dans $\mathcal{I}s(\mathcal{P}_n)$, i.e., $\forall (g,n) \in \mathcal{I}s(\mathcal{P}_n) \times \mathcal{I}s^+(\mathcal{P}_n)$, $gng^{-1} \in \mathcal{I}s^+(\mathcal{P}_n)$ (en effet, $\det(gng^{-1}) = \det(n) = 1$ donc $gng^{-1} \in \mathcal{I}s^+(\mathcal{P}_n)$).
Attention : $\langle s\rangle$ n' est pas distingué dans $\mathcal{I}s(\mathcal{P}_n)$! Par exemple $rsr^{-1} \notin \langle s\rangle = \{\mathrm{Id}_E, s\}$ (exercice).

En tant qu'ensemble, on a $\mathcal{I}s(\mathcal{P}_n) = \langle r\rangle\langle s\rangle$ (cf. Proposition 10.4). Pour décrire le groupe $\mathcal{I}s(\mathcal{P}_n)$, il reste à expliciter la loi produit dans $\mathcal{I}s(\mathcal{P}_n)$. Remarquons que r et s ne commutent pas (voir la remarque ci-dessus). Par conséquent, en tant que groupe, $\mathcal{I}s(\mathcal{P}_n) \not\simeq \langle r\rangle \times \langle s\rangle = \mathbb{Z}/n\mathbb{Z} \times \{-1,1\}$.

Les éléments de $\mathcal{I}s(\mathcal{P}_n)$ sont de la forme $r^k s^\varepsilon$ avec $k \in \mathbb{Z}$ et $\varepsilon \in \{0,1\}$ (cf. Proposition 10.4). Pour décrire le produit dans $\mathcal{I}s(\mathcal{P}_n)$, calculons $r^k s^\varepsilon r^{k'} s^{\varepsilon'}$ avec $(k,k') \in \mathbb{Z}^2$ et $(\varepsilon,\varepsilon') \in \{0,1\}^2$.

On a

$$r^k s^\varepsilon r^{k'} s^{\varepsilon'} = r^k (s^\varepsilon r^{k'} s^{-\varepsilon}) s^\varepsilon s^{\varepsilon'}$$

Comme $\langle r \rangle$ est distingué dans $\mathcal{I}s(\mathcal{P}_n)$, l'élément $s^\varepsilon r^{k'} s^{-\varepsilon}$ appartient à $\langle r \rangle$.

Ainsi, la structure dans $\mathcal{I}s(\mathcal{P}_n)$ se décrit comme suit. On a $\mathcal{I}s(\mathcal{P}_n) = \langle r \rangle \langle s \rangle$ en tant qu'ensemble et le produit est donné par : $(r^k s^\varepsilon).(r^{k'} s^{\varepsilon'}) = (r^k (s^\varepsilon r^{k'} s^{-\varepsilon}) s^\varepsilon s^{\varepsilon'}) \in \langle r \rangle \langle s \rangle$. On dit que $\mathcal{I}s(\mathcal{P}_n)$ est le *produit semi-direct* de $\langle r \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ par $\langle s \rangle \simeq \{-1, 1\}$, et on note $\mathcal{I}s(\mathcal{P}_n) \simeq \langle r \rangle \rtimes \langle s \rangle$.

La notation $\rtimes$ rappelle que $\mathcal{I}s(\mathcal{P}_n) = \langle r \rangle \langle s \rangle$ et que $\langle r \rangle$ est distingué dans le groupe $\mathcal{I}s(\mathcal{P}_n)$, ce qui s'écrit $\langle r \rangle \lhd \mathcal{I}s(\mathcal{P}_n)$.

Plus généralement, on a un produit semi-direct dans la situation suivante :

Définition-Proposition 10.5. *Soient G un groupe, N un sous-groupe distingué de G et H un sous-groupe de G (non nécessairement distingué dans G) tel que la restriction de la projection $G \to G/N$ à H induise un isomorphisme de H sur G/N.*

Alors le morphisme quotient $\varphi : G \to G/N$ est surjectif et son noyau est N. On a $N \cap H = \{1_G\}$ et $G = NH = \{nh \,|\, n \in H,\, h \in H\}$ en tant qu'ensemble. La loi produit dans G est donnée par :

$$\forall\, (n, n') \in N^2,\, \forall\, (h, h') \in H^2, \quad nhn'h' = n \underbrace{(hn'h^{-1})}_{\in N \text{ car } N \lhd G} hh' = (nhn'h^{-1})hh' \in NH.$$

On dit que G est le produit semi-direct *de N par H, et on note $G = N \rtimes H$.*

Pour une définition (encore) plus abstraite du produit semi-direct, voir par exemple [Perrin, Ch. I, §6, page 20]. Donnons ici seulement la définition suivante :

Définition 10.6. *On appelle* groupe diédral d'ordre n ($n \geqslant 2$), *que l'on note D_n, le* produit semi-direct *de $\mathbb{Z}/n\mathbb{Z}$ par $\{1, -1\}$, c'est-à-dire le groupe dont l'ensemble sous-jacent est $\mathbb{Z}/n\mathbb{Z} \times \{1, -1\}$ et dont produit est donné par :*

$$\forall\, (x, x') \in (\mathbb{Z}/n\mathbb{Z})^2,\, \forall\, (\tau, \tau') \in \{-1, 1\}^2, \quad (x + x', \tau\tau') = (x + \varphi(\tau)(x'), \tau\tau').$$

Ici, $\varphi : \{1, -1\} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est défini par : $\varphi(1)(x) = x$ et $\varphi(-1)(x) = -x$ pour tout $x \in \mathbb{Z}/n\mathbb{Z}$.

D'après ce qui précède, le groupe $\mathcal{I}s(\mathcal{P}_n)$ est isomorphe au groupe diédral D_n.

Remarque 10.7. *On définit parfois le* groupe diédral d'ordre n *comme le groupe des isométries du plan qui préservent un polygone régulier à n côtés, ce qui est légitime compte tenu de l'isomorphisme $\mathcal{I}s(\mathcal{P}_n) \simeq D_n$. On pourra prendre cette définition pour le groupe diédral si on veut éviter d'introduire la Définition 10.6 ci-dessus.*

On peut maintenant décrire tous les sous-groupes finis de $SO(2, \mathbb{R})$:

Proposition 10.8. *Soit G un groupe fini de $O(E)$ d'ordre n, $n \geqslant 2$.*

(i) *Si $G \subset SO(E)$, alors $G \simeq \mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$.*

(ii) *Si $G \not\subset SO(E)$, alors G est d'ordre pair et $G \simeq D_{\frac{n}{2}}$ (si $n = 2$, alors $G \simeq \mathbb{Z}/2\mathbb{Z}$).*

Démonstration. Le point (i) a déjà été vu (cf. Corollaire 10.2).

(ii) si $n = 2$, le résultat est clair. Supposons $n > 2$. Alors, d'après (i), $G^+ := G \cap SO(E) = \langle r \rangle$ est isomorphe à $\mathbb{U}_m$ pour un certain m et une certaine rotation $r \in SO(E)$. De plus G^+ est distingué dans G (si $n \in G^+$, alors pour tout $g \in G$, $\det(gng^{-1}) = 1$ donc $gng^{-1} \in G^+$). Comme $G \not\subset SO(E)$, il existe $\tau \in G$ telle que $\tau \notin SO(E)$; on a $\tau^2 = \mathrm{Id}_E$. Par suite, $H := \{\mathrm{Id}_E, \tau\} \simeq \{-1, 1\}$ est un sous-groupe de G dont la restriction de la projection $G \to G/G^+$ à H induit un isomorphisme de H sur G/G^+ (remarquer que $G/G^+ = G^+ \sqcup \tau G^+$). On en déduit que le cardinal de G est $2 \times |G^+| = 2m$, d'où $m = \frac{n}{2}$ (en particulier, n est pair). De plus, G est le produit semi-direct de $G^+ \simeq \mathbb{Z}/\frac{n}{2}\mathbb{Z}$ par $H \simeq \{-1, 1\}$ d'après la Définition-Proposition 10.5 ; il est donc isomorphe au groupe diédral d'ordre $\frac{n}{2}$ (cf. Définition 10.6).

□

11 Groupe des isométries du tétraèdre

Référence : [Tauvel2, page 465].

Nous allons décrire ici les isométries du tétraèdre. Soit $\mathcal{T}$ un tétraèdre de sommets $\{S_1, S_2, S_3, S_4\}$. Remarquons tout d'abord que $\mathcal{I}s(\mathcal{T})$ s'identifie à un sous-groupe de $\mathfrak{S}_4$ (on fait agir $\mathcal{I}s(\mathcal{T})$ sur les sommets et l'action est fidèle). D'autre part, pour tout $\sigma \in \mathfrak{S}_4$, on a

$$\|\overrightarrow{S_iS_j}\| = |\overrightarrow{S_{\sigma i}S_{\sigma j}}\|, \qquad \forall\, (i,j) \in \{1,2,3,4\}^2.$$

Par suite, il existe un unique $f \in O(E)$ telle que $f(S_i) = S_{\sigma i}$. On en déduit que $\mathcal{I}s(\mathcal{T})$ et $\mathfrak{S}_4$ sont isomorphes.

> *(Si f vérifie cette condition, alors f envoie le repère affine (S_1, S_2, S_3, S_4) sur le repère affine $(S_{\sigma 1}, S_{\sigma 2}, S_{\sigma 3}, S_{\sigma 4})$ et préserve la norme, il est donc dans $O(E)$. Réciproquement, une telle application existe et elle est unique : une application affine est entièrement déterminée par l'image d'un repère affine.)*

Proposition 11.1. *Le groupe des isométries du tétraèdre est isomorphe à $\mathfrak{S}_4$ et le groupe $\mathcal{I}s^+(\mathcal{T})$ des isométries positives du tétraèdre est isomorphe à $\mathfrak{A}_4$. (Ici, $\mathfrak{A}_n$ désigne le* groupe alterné d'ordre n.*)*

Démonstration. La première partie de la proposition vient d'être établie. Pour la seconde partie, remarquons que $\mathcal{I}s^+(\mathcal{T})$ et d'indice 2 dans $\mathcal{I}s(\mathcal{T})$ (et distingué). La proposition résulte alors de :

Lemme 11.2. *Soit $n \geqslant 3$. Si H est un sous-groupe d'indice 2 de $\mathfrak{S}_n$, alors $H = \mathfrak{A}_n$.*

Idée de la démonstration. 1) Comme H est d'indice 2, il est distingué dans $\mathfrak{S}_n$ et le quotient $\mathfrak{S}_n/H$ est commutatif (exercice).

2) On en déduit que $xyx^{-1}y^{-1} \in H$ pour tout $x, y \in \mathfrak{S}_n$. Or $(a,b)(a,c)(a,b)^{-1}(a,c)^{-1} = (a,b,c)$. Dès que $n \geqslant 3$, on peut choisir a, b, c distincts. Comme les 3-cycles engendrent $\mathfrak{A}_n$, on en déduit que $\mathfrak{A}_n \subset H$.

3) Comme $|\mathfrak{A}_n| = |H|$, on obtient $\mathfrak{A}_n = H$.

Remarque : si $n \geqslant 5$, le lemme vient de ce que $\mathfrak{A}_n$ est simple.

□

□

Description géométrique de $\mathcal{I}s^+(\mathcal{T})$

Appelons *hauteur* toute droite passant par un sommet et orthogonal à la face opposée à ce sommet. Appelons *médiane* toute droite contenant le milieu de deux arrêtes opposées. On voit que $\mathcal{I}s^+(\mathcal{T})$, qui est de cardinal $|\mathfrak{A}_4| = 12$, est composé de :

∗ $2 \times 4 = 8$ rotations d'odre 3 d'axe les 4 hauteurs de $\mathcal{T}$; elles correspondent aux 3-cycles de $\mathfrak{A}_4$.

∗ 3 retournements d'axes les 3 médianes de $\mathcal{T}$; ils correspondent aux 3 doubles transpositions de $\mathfrak{A}_4$.

∗ l'identité.

12 Groupe des isométries du cube

Soient $\mathcal{C}$ un cube de sommets $S_1, \ldots, S_8$, $\mathcal{I}s(\mathcal{C})$ le groupe des isométries du cube et $\mathcal{I}s^+(\mathcal{C})$ le groupe des isométries positives du cube. En faisant agir $\mathcal{I}s(\mathcal{C})$ sur les sommets du cube, on voit que $\mathcal{I}s(\mathcal{C})$, et $\mathcal{I}s^+(\mathcal{C})$, s'injectent dans $\mathfrak{S}_8$. Mais cette action n'est clairement pas assez « fine » pour décrire $\mathcal{I}s(\mathcal{C})$. Toute permutation des sommets ne correspond pas à une isométrie du cube !

Groupe des isométries positives du cube

Le groupe $\mathcal{I}s^+(\mathcal{C})$ agit également sur les 4 diagonales du cube et l'action est fidèle (une rotation qui conservent les 4 diagonales est l'identité). Ainsi, $\mathcal{I}s^+(\mathcal{C})$ s'injecte dans $\mathfrak{S}_4$.

Proposition 12.1. *Le groupe $\mathcal{I}s^+(\mathcal{C})$ des isométries positives du cube est isomorphe à $\mathfrak{S}_4$.*

Démonstration. 1ère méthode (voir par exemple [Tauvel2, Calais2]) : on considère l'action de $\mathcal{I}s^+(\mathcal{C})$ sur les sommets et on considère le stabilisateur d'un sommet. On écrit enfin l'équation des classes pour obtenir que $|\mathcal{I}s^+(\mathcal{C})| = 24$.

2ème méthode : on montre que $\mathcal{I}s^+(\mathcal{C})$ contient au moins $24 = |\mathfrak{S}_4|$ éléments ; comme $|\mathcal{I}s^+(\mathcal{C})| \leqslant 24$, on obtient l'isomorphisme. Nous allons faire ainsi ! $\mathcal{I}s^+(\mathcal{C})$ est composé de (au moins, et donc exactement) :

∗ 9 rotations d'odre 2 ou 4, d'axes contenant les centres de deux faces opposées (elles correspondent aux 3 doubles transpositions et aux 6 4-cycles de $\mathfrak{S}_4$).

∗ 6 rotations d'ordre 2, d'axes contenant les milieux d'arrêtes opposées (elles correspondent aux 6 transpositions de $\mathfrak{S}_4$).

∗ 8 rotations d'ordre 3 d'axes contenant 2 sommets opposés (elles correspondent aux 3-cycles de $\mathfrak{S}_4$).

∗ l'identité.

Attention : dans l'identification avec $\mathfrak{S}_4$, on agit ici sur les diagonales et non sur les sommets !

□

Proposition 12.2. *On a* $\mathcal{I}s(\mathcal{C}) \simeq \{-1, 1\} \times \mathfrak{S}_4$.

Démonstration. On considère la symétrie centrale $-\mathrm{Id}_E$: c'est un élément de $\mathcal{I}s(\mathcal{C})$ qui n'est pas dans $\mathcal{I}s^+(\mathcal{C})$. Soit alors le morphisme $\varphi : \{\mathrm{Id}_E, -\mathrm{Id}_E\} \times \mathcal{I}s^+(\mathcal{C}) \to \mathcal{I}s(\mathcal{C})$, $\pm\mathrm{Id}_E \times u \mapsto \pm\mathrm{Id}_E\, u$. Ici, le produit est direct car $-\mathrm{Id}_E$ commute avec $\mathcal{I}s(\mathcal{C})$. Le morphisme φ est injectif et $|\{\mathrm{Id}_E, -\mathrm{Id}_E\} \times \mathcal{I}s^+(\mathcal{C})| = 2 \times 24 = 48 = |\mathcal{I}s(\mathcal{C})|$, d'où l'isomorphisme souhaité (notons que $|\mathcal{I}s(\mathcal{C})| = 48$ car $|\mathcal{I}s^+(\mathcal{C})| = 24$ est d'indice 2).

□

Remarque 12.3. *Deux sous-groupes finis de* $O(3, \mathbb{R})$ *isomorphes ne sont pas nécessairement conjugués dans* $O(3, \mathbb{R})$. *Par exemple, le groupe des isométries positives du cube et le groupe des isométries du tétraèdre sont isomorphes* ($\simeq \mathfrak{S}_4$) *mais ce sont pas conjugués dans* $O(3, \mathbb{R})$. *En effet, tous les conjugués du premier sont contenus dans* $SO(3, \mathbb{R})$ *car* $SO(3, \mathbb{R})$ *est distingué dans* $O(3, \mathbb{R})$ *mais le deuxième contient des isométries indirectes !*

13 Étude des groupes $O(E)$ et $SO(E)$

Références : [Tauvel1, Perrin].

Dans ce paragraphe, E désigne un espace vectoriel euclidien de dimension $n \geqslant 2$; on notera comme précédemment $\langle\ ,\ \rangle$ le produit scalaire et $\|\,.\,\|$, la norme associée. Rappelons que

$$\begin{aligned} O(E) &= \{u \in \mathrm{L}(E) \,|\, \|u(x)\| = \|x\|,\ \forall\, x \in E\} \subset GL(E) \\ &= \{u \in \mathrm{L}(E) \,|\, u \circ u^* = u^* \circ u = \mathrm{id}_E\} \end{aligned}$$

et que $SO(E) = O(E) \cap SL(E)$. Les ensembles $O(E)$ et $SO(E)$ sont des sous-groupes de $GL(E)$. Nous allons nous intéresser ici aux propriétés topologiques (connexité, compacité, etc.) et algébriques (centre, générateurs, etc.) de ces groupes.

Propriétés topologiques

Rappelons que si $u \in O(E)$, alors les seules valeurs propres possibles de u sont 1 et -1. Posons $E^+(u) = \ker(u - \mathrm{id}_E)$ et $E^-(u) = \ker(u + \mathrm{id}_E)$.

Proposition 13.1. *Il existe une base orthonormée (b.o.n) de E dans laquelle la matrice de u est de la forme*

$$\begin{pmatrix} +I_r & & & & & \\ & -I_s & & & 0 & \\ & & R(\theta_1) & & & \\ & & & R(\theta_2) & & \\ & 0 & & & \ddots & \\ & & & & & R(\theta_t) \end{pmatrix},$$

où $r, s, t \in \mathbb{N}$ et, pour $i \in \{1, \dots, t\}$, $R(\theta_i)$ est la matrice de rotation d'ordre 2 d'angle θ_i (cf. Section 10).

Démonstration. On raisonne par récurrence sur la dimension n. Nous savons que la proposition est vraie pour $n = 2$ (et même $n = 3$). Supposons qu'elle soit vraie pour tout sous-espace E' de E de dimension $< N$ et tout $u' \in SO(E')$ pour un certain $N \in \{1, \dots, n-1\}$, et montrons la proposition pour $u_0 \in SO(E_0)$, où E_0 est-un sous-espace de E de dimension N. Du cas $N = n$ et $u_0 = u$, la proposition s'ensuivra.

Si u_0 admet une valeur propre réelle, on pose $F_0 := E_0^+(u_0) \oplus E_0^-(u_0)$. Comme F_0 est stable par u, son orthogonal $E' := F_0^\perp$ l'est aussi, et $\dim E' < \dim E_0$. L'hypothèse de récurrence s'applique alors à E' et l'endomorphisme induit $u' : E' \to E'$, $x \mapsto u_0(x)$. On conclut alors aisément dans ce cas.

Supposons désormais que u_0 n' admet aucune valeur propre réelle. r Remarquons que l'endomorphisme $v := u_0 + u_0^{-1}$ de E_0 est auto-adjoint (en effet $(u_0 + u_0^{-1})^* = u_0^* + (u_0^{-1})^* = u_0^{-1} + u_0$). Par conséquent, d'après le Théorème fondamental, il admet une valeur propre réelle. Soit $e \in E_0$ un vecteur propre de v. Le plan P engendré par e et $u_0(e)$ (c'est bien un plan car u_0 n'a pas de valeur propre) est stable par u_0. En effet, $u_0(e) \in P$ et $u_0(u_0(e)) \in P$ car, $v(e) = (u_0 + u_0^{-1})(e) \in \mathbb{R}e$ implique $u_0(e) \in \mathbb{R}e + \mathbb{R}u_0^{-1}(e)$. De plus, l'endomorphisme induit $P \to P$, $x \mapsto u_0(x)$ n'a pas de valeur propre. On en déduit que c'est une rotation (cf. Section 10). On applique alors l'hypothèse de récurrence à $E' := P^\perp$, qui est de dimension $< \dim E_0$, et l'endomorphisme induit $u' : E' \to E'$, $x \mapsto u_0(x)$ comme précédemment.

□

Application : le groupe $SO(E)$ est connexe par arcs.

Explication. Soit $u \in SO(E)$. Il s'agit de construire un chemin continu entre u et Id_E dans $SO(E)$. Il existe une b.o.n dans laquelle la matrice de u est comme décrite dans la Proposition 13.1.

Puisque $\det(u) = 1$, $s = \dim E^-(u)$ est pair. On peut donc écrire le bloc $-I_s$ sous forme d'une matrice diagonale par blocs dont tous les blocs sont identiques égaux à la matrice de rotation $R(\pi) = -I_2$. On conclut en observant que l'application $[0,1] \to SO(2)$, $t \mapsto R(t\theta)$ est un chemin continu de I_2 à $R(\theta)$ pour tout $\theta \in \mathbb{R}$.

□

Gram-Schmidt et la décompostion d'Iwasawa. On omettra ici certains détails. Soit $\underline{e} = (e_1, \ldots, e_n)$ une base quelconque de E.

Théorème 13.2 (Procédé d'othonormalisation de Gram-Schmidt)**.** *Il existe une unique base orthonormée $\underline{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_n)$ de E telle que la matrice de passage $P_{\underline{e}}^{\underline{\varepsilon}}$ de $\underline{e}$ à $\underline{\varepsilon}$ soit triangulaire supérieure à coefficients diagonaux > 0. De plus, les coefficients de $P_{\underline{e}}^{\underline{\varepsilon}}$ sont des fonctions continues de $\langle e_i, e_j \rangle$.*

Idées de la démonstration. On construit les éléments ε_k par récurrence sur $k \in \{1, \ldots, n\}$.
$*$ $\underline{k = 1}$. On pose $\varepsilon_1 = \frac{e_1}{\|e_1\|}$. Seul ce choix est convenable pour ε_1.
$*$ On suppose avoir construit $(\varepsilon_1, \ldots, \varepsilon_{k-1})$ « convenablement » pour un certain k de $\{1, \ldots, n-1\}$. D'après l'hypothèse de récurrence, la famille $(\varepsilon_1, \ldots, \varepsilon_{k-1})$ est une b.o.n de $\mathrm{Vect}(e_1, \ldots, e_{k-1})$. On cherche ε_k tel que :

1) ε_k soit orthogonal à $(\varepsilon_1, \ldots, \varepsilon_{k-1})$;
2) ε_k soit de norme 1 ;
3) sa coordonnée selon e_k dans la base $(e_1, \ldots, e_k)$ de $\mathrm{Vect}(e_1, \ldots, e_k)$ soit > 0.

On considère le projeté orthogonal de ε_k sur $\mathrm{Vect}(e_1, \ldots, e_{k-1})$ que l'on normalise ; ce choix est uniquement déterminé par les conditions ci-dessus :

$$\varepsilon_k := \frac{e_k - \sum_{i=1}^{k-1} \langle e_k, \varepsilon_i \rangle \varepsilon_i}{\| e_k - \sum_{i=1}^{k-1} \langle e_k, \varepsilon_i \rangle \varepsilon_i \|}.$$

De plus, les coordonées de ε_k sont clairement des fonctions continues en les $\langle e_i, e_j \rangle$ d'après l'hypothèse de récurrence.

□

Notons $\mathcal{T}^{>0}$ l'ensemble des matrices triangulaires supérieures à coefficients diagonaux > 0. On a $\mathcal{T}^{>0} \simeq (\mathbb{R}^{+*})^n \times \mathbb{R}^{\frac{n(n-1)}{2}}$ (homéomorphisme). On note $O(n, \mathbb{R})$ le groupe orthogonal d'ordre n, i.e., le sous-groupe de $GL(n, \mathbb{R})$ formée des matrices orthogonales d'ordre n, $O(n, \mathbb{R}) = \{A \in \mathrm{M}(n, \mathbb{R}) \mid A\,{}^tA = I_n\}$.

Corollaire 13.3 (Décomposition d'Iwasawa)**.** *L'application*

$$\begin{array}{ccc} O(n, \mathbb{R}) \times \mathcal{T}^{>0} & \longrightarrow & GL(n, \mathbb{R}) \\ (O, T) & \longmapsto & OT \end{array}$$

est un homéomorphisme.

Démonstration. L'application est bien définie et elle est continue. Montrons qu'elle est bijective et que son application inverse est continue. Soit $A \in GL(n,\mathbb{R})$. Alors A est la matrice de passage $P^{\underline{e}}_{\underline{e}_0}$ de la base canonique à une certaine base $\underline{e}$ de E. D'après le procédé d'othonormalisation de Gram-Schmidt (Théorème 13.2) il existe une (unique) b.o.n $\underline{\varepsilon}$ telle que $P^{\underline{\varepsilon}}_{\underline{e}}$ soit triangulaire supérieure à coefficients diagonaux > 0. On a $A = P^{\underline{e}}_{\underline{e}_0} = OT$, où $O = P^{\underline{\varepsilon}}_{\underline{e}_0} \in O(n,\mathbb{R})$ (car $\underline{e}_0$ et $\underline{\varepsilon}$ sont des b.o.n) et $T = P^{\underline{e}}_{\underline{\varepsilon}} \in \mathcal{T}^{>0}$ (d'après le Théorème 13.2). D'après l'unicité dans le Théorème 13.2, le choix de (O,T) est unique.

Il reste à montrer que l'application $A \mapsto (O,T)$ est continue (point non traité en cours !). Il s'agit de montrer que l'application $A \mapsto (AT^{-1},T)$ est continue, ou encore que l'application $A \mapsto T$ est continue ($A \mapsto AT^{-1}$ l'étant clairement). Le résultat sera une conséquence de :

Lemme 13.4. *Soit $S^{++}(n,\mathbb{R})$ l'ensemble des matrices symétriques réelles définies positives. Pour tout $S \in S^{++}(n,\mathbb{R})$, il existe une unique matrice $T \in \mathcal{T}^{>0}$ telle que $S = {}^tTT$. De plus, l'application $S^{++}(n,\mathbb{R}) \to \mathcal{T}^{>0}$, $S \mapsto T$ ainsi définie est continue.*

Démonstration. Pour la première partie, il suffit d'observer que S s'écrit de façon unique $S = H^2 = {}^tHH$ avec $H \in S^{++}(n,\mathbb{R})$ (cf. Lemme 13.6 plus loin !) et d'appliquer la décomposition d'Iwasawa à H.

Pour la seconde partie, comme S est une matrice symétrique définie positive, S est la matrice d'un produit scalaire ; elle s'écrit donc sous la forme $S = \big(\varphi(e_i,e_j)\big)_{i,j}$ où $\underline{e} = (e_1,\dots,e_n)$ est une base (quelconque) de E et $\varphi : E \times E \to E$ un produit scalaire sur E. L'application $S \mapsto T$ est alors continue d'après le Théorème 13.2 relativement à (E,φ) (car $T = P^{\underline{\varepsilon}}_{\underline{e}}$ dans les notations du Théorème 13.2, d'après la construction précédente).

□

Revenons à la preuve du théorème. Remarquons que ${}^tAA$ est une matrice symétrique définie positive ; le Lemme 13.4 s'applique donc à $S = {}^tAA$. Précisément, on montre sans difficulté que ${}^tAA = (\langle e_i,e_j\rangle)_{i,j}$ où $\underline{e}$ est la base considérée au début de la démonstration. L'application $A \mapsto T$ est donc continue d'après le Lemme 13.4.

□

Remarque : une variante du résultat précédent établit que l'application $SO(n,\mathbb{R}) \times \mathcal{T}^{>0} \to GL^+(n,\mathbb{R})$ est un homéomorphisme.

La décomposition polaire. On note $\mathcal{S}$ (resp. $\mathcal{S}^+$, $\mathcal{S}^{++}$) l'ensemble des endomorphismes symétriques (resp. positifs, définis positifs) de E. Rappelons que $h \in \mathcal{S}$ si et seulement si $h = h^*$ et que, $h \in \mathcal{S}^+$ (resp. $\mathcal{S}^{++}$) si et seulement si $h = h^*$ et $\langle h(x),x\rangle \geqslant 0$ (resp. > 0) pour tout $x \in E \smallsetminus \{0\}$ ou encore, si et seulement si $h = h^*$ et toutes ses valeurs propres sont $\geqslant 0$ (resp. > 0).

Théorème 13.5. (i) *Soit $u \in \mathrm{L}(E)$. Il existe un couple $(\rho, h) \in O(E) \times \mathcal{S}^+$ tel que $u = \rho \circ h$. Si $u \in GL(E)$, on a de plus l'unicité.*

(ii) *L'application*

$$\begin{array}{ccc} O(E) \times \mathcal{S}^{++} & \longrightarrow & GL(E) \\ (\rho, h) & \longmapsto & \rho \circ h \end{array}$$

est un homéomorphisme.

Ce résultat est une généralisation de l'écriture $z = re^{i\theta}$, avec $r \geqslant 0$ et $\theta \in \mathbb{R}$, pour tout $z \in \mathbb{C}$.

Pour la partie (ii), l'application est bijective et clairement continue. Il est plus délicat de montrer que son inverse est une application continue. Nous admettrons ce point ; voir par exemple [Tauvel1, page 416] pour les détails.

Avant de démontrer le théorème, rappelons le lemme suivant (déjà utilisé !) :

Lemme 13.6 (racine carré dans $\mathcal{S}^+$)**.** *Soit $u \in \mathcal{S}^+$ (resp. $\mathcal{S}^{++}$). Alors il existe un unique $v \in \mathcal{S}^+$ (resp. $\mathcal{S}^{++}$) tel que $v^2 = h$.*

Démonstration. Pour l'existence, on choisit une b.o.n $\underline{b}$ dans laquelle la matrice D de u est diagonale, $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. Les coefficients diagoanaux λ_i sont $\geqslant 0$. L'endomorphisme v dont la matrice dans la b.o.n $\underline{b}$ est $\mathrm{diag}(\sqrt{\lambda_1}, \ldots, \sqrt{\lambda_n})$ est symétrique positif (défini si u l'est) et vérifie $v^2 = u$.

Le choix de v est uniquement déterminé par la condition $v^2 = h$ et $v \in \mathcal{S}^+$ (remarquer que u et v commutent et considérer les espaces propres...).

□

Démonstration du Théorème 13.5. Comme annoncé, on démontre seulement (i). Commençons par le cas, plus simple, où $u \in GL(E)$. Alors $u^* \circ u$ est un endomorphisme symétrique défini positif (exercice !). D'après le Lemme 13.6, il existe un unique élément $h \in \mathcal{S}^{++}$ tel que $h^2 = u^* \circ u$. On pose $\rho := u \circ h^{-1}$. On a $\rho \in O(E)$ car $\rho \circ \rho^* = (u \circ h^{-1}) \circ (h^{-1} \circ u^*) = u(u^* \circ u)^{-1} u^* = \mathrm{id}_E$. Enfin, $u = \rho \circ h$.

Supposons maintenant que u est quelconque, plus nécessairement inversible. Comme précédemment, on construit (de façon unique jusqu'ici !) $h \in \mathcal{S}^+$ comme étant la « racine carré » de $u^* \circ u$ (cf. Lemme 13.6).

Attention : comme h n'est pas inversible en général, on ne peut plus poser $\rho := u \circ h^{-1}$!!!

Soit $(e_1, \ldots, e_r)$ une b.o.n de $\ker u$, et soit $(e_{r+1}, \ldots, e_n)$ une base de $S := (\ker u)^\perp$. Observons que $\ker u = \ker h$. Cela vient de ce que $\ker u = \ker(u^* \circ u)$ (exercice). Par suite, S est stable par h et, quitte à changer les e_i pour $i \geqslant r+1$, on peut supposer que $(h(e_r + 1), \ldots, h(e_n))$ est une b.o.n de S car $S \to S, x \mapsto h(x)$ est un endomorphisme symétrique défini positif de S.

On cherche $\rho \in O(E)$ tel que $u(e_i) = \rho(h(e_i))$ pour tout $i \in \{1, \dots, n\}$. On construit ρ comme suit. On pose $\rho(h(e_i)) = u(e_i)$ pour tout $i \in \{r+1, \dots, n\}$. Il restera à définir ρ sur le noyau $\ker u$ de sorte que ρ soit orthogonal. On aura alors $u = \rho \circ h$.

La famille $(e_1, \dots, e_r, h(e_r+1), \dots, h(e_n))$ est une b.o.n de E d'après le choix des e_i. Pour tout $(i,j) \in \{r+1, \dots, n\}^2$, on a

$$\langle \rho(h(e_i)), \rho(h(e_j)) \rangle = \langle u(e_i), u(e_j) \rangle = \langle u^* \circ u(e_i), e_j \rangle = \langle h^2(e_i), e_j \rangle = \langle h(e_i), h(e_j) \rangle = \delta_{i,j}.$$

On définit alors $\rho(e_i)$ pour $i \in \{1, \dots, r\}$ de sorte que $(\rho(e_1), \dots, \rho(e_r))$ soit une b.o.n de $(u(S))^\perp$; cette construction est possible car $\dim u(S) = \dim E - \dim \ker u$, donc $\dim(u(S))^\perp = \dim \ker u$. Pour tout $(i,j) \in \{1, \dots, r\}^2$, on a alors

$$\langle \rho(e_i), \rho(e_j) \rangle = \delta_{i,j}.$$

Enfin, pour tous $i \in \{1, \dots, r\}$ et $j \in \{r+1, \dots, n\}$, on a

$$\langle \rho(e_i), \rho(h(e_j)) \rangle = \langle \rho(e_i), u(e_j) \rangle = \delta_{i,j}.$$

Finalement, ρ ainsi construit est bien en endomorphisme orthogonal d'après la discussion précédente, ce qui achève la démonstration.

Remarque : ici, le choix de ρ n'est pas unique. Penser au cas où u est nul !

□

Proposition 13.7. *Le groupe $O(E)$ est un sous-groupe compact maximal de $GL(E)$, i.e., il n'y a pas de sous-groupe compact de $GL(E)$ contenant strictement E.*

Ce résultat généralise celui-ci : $\mathbb{U}$ est un sous-groupe compact maximal de $\mathbb{C}^\times$.

Démonstration. Rappelons brièvement pourquoi $O(E)$ est en effet compact : c'est un sous-ensemble fermé ($O(E) = \Phi^{-1}(\{\mathrm{id}_E\})$ où Φ est l'application continue $L(E) \to L(E), u \mapsto u^* \circ u$, or $\{\mathrm{id}_E\}$ est fermé dans $L(E)$), et borné (si $u \in O(E)$, alors $|||u||| \leqslant 1$) de l'espace vectoriel de dimension finie $L(E)$.

Pour la seconde partie de la proposition, supposons qu'il existe un sous-groupe compact K de $GL(E)$ contenant strictement $O(E)$. Soit alors $u \in K \setminus O(E)$ et écrivons sa décomposition polaire (Théorème 13.5(i)) : $u = \rho \circ h$, avec $\rho \in O(E)$ et $h \in \mathcal{S}^{++}$. Comme $u \in K$ et $\rho \in O(E) \subset K$, on a $h = \rho^{-1} \circ u \in K$ car K est un groupe. D'autre part, comme $u \notin O(E)$, on a $h \neq \mathrm{id}_E$. Soient $\lambda_1, \dots, \lambda_n$ les valeurs propres de h ; on a $\lambda_i > 0$ pour tout i. Comme $h \neq \mathrm{id}_E$, il existe i tel que $\lambda_i \neq 1$; d'où $\lambda_i^r \to 0$ ou $\lambda_i^r \to +\infty$ quand $r \to \infty$. Par conséquent, la suite $(h^r)_{r \in \mathbb{N}}$ de $K^{\mathbb{N}}$ n'admet pas de sous-suite convergente dans K, ce qui contredit la compacité de K.

□

Propriétés algébriques : centre et générateurs

Les éléments de $O(E)$ et de $SO(E)$ qui ont « beaucoup de points fixes » jouent un rôle crucial dans l'étude de $O(E)$ et de $SO(E)$ (ce sont les analogues des transpositions dans l'étude du groupe symétrique et du groupe alternée, ou encore des transvections pour l'étude de $SL(E)$). Pour $O(E)$, on s'intéressera donc particulièrement aux *réflexions* (i.e., les symétries orthogonales par rapport à une droite qui ont un hyperplan de points fixes) et pour $SO(E)$, aux *renversements* ou *retournements* (i.e., les symétries orthogonales par rapport à un plan qui ont un sous-espace de codimension 2 de points fixes). Remarquons que les réflexions ne sont jamais dans $SO(E)$!

De manière générale, on appellera *symétrie orthogonale de sous-espace F* la symétrie orthogonale s_F de E telle que $E^-(s_F) = \ker(s_F + \mathrm{Id}_E) = F$.

Lemme 13.8 ([Perrin, Chap. V, Proposition 4.8])**.** *Soient F un sous-espace de E et $u \in O(E)$. Alors $us_Fu^{-1} = s_{u(F)}$. Autrement dit, us_Fu^{-1} est la symétrie orthogonal de sous-espace $u(F)$. De plus, on a $E^+(s_{u(F)}) = u(E^+(s_F))$.*

Démonstration. Comme us_Fu^{-1} est une involution, c'est une symétrie. De plus, c'est un élément de $O(E)$. Par conséquent, c'est une symétrie orthogonale. On vérifie alors sans difficulté que $E^+(s_{u(F)}) = u(E^+(s_F))$ et $E^-(s_{u(F)}) = u(E^-(s_F))$, d'où le lemme.

□

Théorème 13.9. (i) *Le centre de $O(E)$ est $Z = \{\mathrm{id}_E, -\mathrm{id}_E\}$. En particulier, $O(E)$ n'est pas commutatif.*

(ii) *Pour $n \geqslant 3$, le centre de $SO(E)$ est $Z \cap SO(E)$, c'est-à-dire $\{\mathrm{id}_E\}$ si n est impair, et $\{\mathrm{id}_E, -\mathrm{id}_E\}$ si n est pair.*

Rappelons que $SO(E)$ est commutatif si $n = 2$ (cf. Section 10) ; dans ce cas, le centre de $SO(E)$ est lui-même !

Démonstration. i) Il est clair que $\{\mathrm{id}_E, -\mathrm{id}_E\}$ est contenu dans le centre de $O(E)$. Réciproquement, soit $u \in O(E)$ dans le centre de $O(E)$. Alors u commute avec toute réflexion s_D de droite D. On a donc

$$s_{u(D)} = us_Du^{-1} = s_D.$$

Par suite $u(D) = D$, et ceci est vrai pour tout droite D de E. On en déduit que u est une homothétie (exercice classique !). Comme u appartient à $O(E)$, on en déduit que $u \in \{\mathrm{id}_E, -\mathrm{id}_E\}$.

ii) Tout d'abord, $-\mathrm{id}_E$ est dans $SO(E)$ si et seulement si n est pair. Une inclusion est donc claire. Comme pour (i), soit $u \in SO(E)$ dans le centre de $SO(E)$. Alors u commute avec tout renversement de plan P. On a ainsi

$$s_{u(P)} = us_Pu^{-1} = s_P,$$

d'où $u(P) = P$ pour tout plan P de E. Comme $n \geqslant 3$, toute droite est une intersection de deux plans. On en déduit alors que u stabilise toutes les droites de E et on conclut comme en (i).

□

Théorème 13.10 ([Perrin, Théorème 2.4])**.** *Le groupe $O(E)$ est engendré par les réflexions orthogonales. Plus précisément, si $u \in O(E)$, alors u est la composée d'au plus n réflexions.*

Démonstration. Rappelons que pour $u \in O(E)$, $E^+(u) = \{x \in E \mid u(x) = x\}$ est l'ensemble des points fixes de u.

On montre le théorème par récurrence sur la dimension de $E^+(u)$, ou plus exactement sur $n - \dim E^+(u)$. Si $n = \dim E^+(u)$, alors $u = \mathrm{id}_E$ est le résultat est clair.

Supposons que tout élément $v \in O(E)$ tel que $n - \dim E^+(v) < p$ s'écrivent comme au plus $n - \dim E^+(v)$ réflexions orthogonales pour un certain $p \in \{1, \dots, n-1\}$, et montrons le théorème pour $u \in O(E)$ tel que $n - \dim E^+(u) = p$.

Soit $F := (E^+(u))^\perp$ l'orthogonal de $E^+(u)$; il est stable par u car $E^+(u)$ l'est. Soit $x \in F$, et $y = u(x)$. Alors $y \neq u(x)$ (puisque $x \notin E^+(u)$) et comme $\|y\| = \|x\|$, on a $\langle x - y, x + y\rangle = 0$. Soit s la réflexion orthogonal de droite $\mathrm{Vect}(x-y)$. Alors $s(x-y) = -x+y$ et $s(x+y) = x+y$, d'où $s(y) = x$. Par suite $su(x) = x$. D'autre part, remarquons que $E^+(u) \subseteq E^+(s)$. En effet, puisque $x - y \in (E^+(u))^\perp$, on a $E^+(s) = (x-y)^\perp \supseteq E^+(u)$. En conclusion, $E^+(su) \supsetneq E^+(u)$. D'après l'hypothèse de récurrence, on en déduit qu'il existe r réflexions $s_1, \dots, s_r$, avec $r < p$, telles que $su = s_1 \cdots s_r$, i.e., $u = ss_1 \cdots s_r$. Comme $r + 1 \leqslant p$, la propriété au rang p s'ensuit. Par récurrence, le théorème est ainsi démontré.

□

Théorème 13.11 ([Perrin, Théorème 2.6])**.** *Pour $n \geqslant 3$, le groupe $SO(E)$ est engendré par les renversements. Précisément, si $u \in SO(E)$, alors u est la composée d'au plus n renversements.*

Démonstration. 1er cas : supposons $n = 3$. Si $u \neq \mathrm{id}_E$, alors $u = s_1 s_2$ où s_i sont des réflexions (voir la preuve précédente). Mais $\sigma_i = -s_i$ est un renversement, et $u = (-s_1)(-s_2)$, d'où le résultat dans ce cas.
2ème cas : $n > 3$. D'après le Théorème 13.10, u s'écrit $u = s_1 \cdots s_r$, avec $r \leqslant n$. Comme $u \in SO(E)$, r est pair. Il suffit donc de démontrer le lemme suivant :

Lemme 13.12. *Soient $n \geqslant 3$ et s_1, s_2 deux réflexions orthogonales. Alors $s_1 s_2$ est le produit de deux renversements.*

Démonstration. Posons $u = s_1 s_2$. Soient H_1 et H_2 les hyperplans de s_1 et s_2 respectivement, i.e., $s_i = s_{H_i^\perp}$, et soit V un sous-espace de $H_1 \cap H_2$ de dimension $n-3$ (un tel sous-espace existe car $n \geqslant 3$). On a $u|_V = \mathrm{id}_V$ et donc $u(V^\perp) \subset V^\perp$. De plus, $\dim V^\perp = 3$. D'après le premier cas, il existe deux renversements σ_1 et σ_2 de $V^\perp$ tels que $u|_{V^\perp} = \sigma_1\sigma_2$. On obtient le résultat le résultat en prolongeant σ_i par l'identité sur V.

□

□

Références

[Calais1] J. Calais, *Éléments de théorie des anneaux*, PUF.

[Calais2] J. Calais, *Éléments de théorie des groupes*, PUF.

[Francinou-Gianella] S. Francinou et H. Gianella, *Exercices de Mathématiques Algèbre I*, Masson.

[Monier] J.-M. Monier, *Cours de mathématiques, Algèbre I MPSI, PCSI, PTSI*, Dunod.

[Perrin] P. Perrin, *Cours d'algèbre*, École Normale Supérieure de Jeunes Filles, Paris, 1982 (ou Ellipses).

[Samuel] P. Samuel, *Théorie algébrique des nombres*, Hermann.

[Schwartz] L. Schwartz, *Mathématiques pour la licence - Algèbre*, Hermann.

[Tauvel1] P. Tauvel, *Cours d'algèbre*, Dunod.

[Tauvel2] P. Tauvel, *Cours de géométrie*, Dunod.