101 : Groupe opérant sur un ensemble. Exemples d'applications.

Dans cette leçon, G désigne un groupe de neutre 1, et X désigne un ensemble.

I. Action d'un groupe sur un ensemble

A. Définitions et premiers exemples

Définition 1 ([R] 19, [U] 27). *Une* action *de G sur X est une application $G \times X \to X$ définie par $(g, x) \mapsto g \cdot x$ vérifiant*

1. $\forall (g, g') \in G^2, \forall x \in X, g' \cdot (g \cdot x) = (g'g) \cdot x$
2. $\forall x \in X, 1 \cdot x = x$

Pour signigier que G agit sur X, on note $G \circlearrowleft X$.

Exemple 2 ([R] 19, [U] 28).
- $\mathfrak{S}(X) \circlearrowleft X$ *par* $\sigma \cdot x = \sigma(x)$
- *Si E est un espace vectoriel, alors $GL(E) \circlearrowleft E$ par $\varphi \cdot x = \varphi(x)$*
- $(g, x) \mapsto x$ *est une action de G sur X, appelée* action triviale.

Proposition 3 ([R] 19, [U] 28). *La donnée d'une action $(g, x) \mapsto g \cdot x$ de G sur X équivaut à la donnée d'un morphisme $\varphi : G \to \mathfrak{S}(X)$, $g \mapsto [x \mapsto g \cdot x]$, appelé* morphisme associé à l'action de G sur X.

Définition 4 ([R] 19/21, [U] 29). *Soit $x \in X$. Alors :*
- *L'*orbite *de x est l'ensemble* $\mathrm{Orb}(x) = \{g \cdot x \mid g \in G\}$ *(aussi noté $G \cdot x$) ;*
- *Le* stabilisateur *de x est l'ensemble* $\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\}$.

Proposition 5 ([U] 34/37).
1. *$G \circlearrowleft G$ par $g \cdot h = ghg^{-1}$ (on l'appelle* action par conjugaison*). Le stabilisateur de $h \in G$ est appelé* centralisateur *de h, et est noté $C(h)$.*
2. *G agit sur l'ensemble de ses sous-groupes par $g \cdot H = gHg^{-1}$ (action par conjugaison). Le stabilisateur de $H \leq G$ est appelé* normalisateur *de H, et est noté $N(H)$.*

Définition 6 ([R] 20, [U] 29/31). *On dit que l'action de G sur X est* transitive *si elle n'a qu'une seule orbite,* i.e. *si $\forall (x, y) \in X^2, \exists g \in G : g = g \cdot x$.*

On dit que l'action de G sur X est fidèle *si φ est injective.*

Exemple 7 ([U] 31).
- $\mathfrak{S}_n \circlearrowleft [\![1, n]\!]$ *transitivement par $\sigma \cdot i = \sigma(i)$*
- *$G \circlearrowleft G$ fidèlement par $g \cdot h = gh$ (on l'appelle* action par translation à gauche*)*
- *Soit H un sous-groupe de G. L"'action de G sur G/H définie par $g \cdot xH = gxH$, appelée* action par translation à gauche*, est transitive.*

Proposition 8 ([R] 21). *Pour tout $x \in X$,* $\mathrm{Stab}(x)$ *est un sous-groupe de G.*

Proposition 9 ([U] 30). *$x \mathcal{R} y \iff \exists g \in G : g = g \cdot x$ définit une relation d'équivalence sur X dont les classes sont les orbites de l'action de G sur X.*

Corollaire 10 ([U] 30). *Les orbites partitionnent X.*

Exemple 11 ([U] 41). *Soit $\sigma \in \mathfrak{S}_n$. Le groupe $\langle \sigma \rangle$ agit sur $[\![1, n]\!]$ par $\sigma^k \cdot i = \sigma^k(i)$. Les orbites non ponctuelles sont les supports des cylckes dans la décomposition en produit de cycles à supports disjoints de σ.*

B. Cas d'un groupe et d'un ensemble finis

Dans ce paragraphe, on suppose G et X finis. On pose $n = \mathrm{Card}(G)$.

Théorème 12 (de Caylay - [R] 21, [U] 31). *G s'identifie à un sous-groupe de $\mathfrak{S}_n$.*

Proposition 13 ([R] ?, [U] ?). $\forall (x, y) \in X^2, y \in \mathrm{Orb}(x) \implies \exists g \in G : \mathrm{Stab}(y) = g\,\mathrm{Stab}(x) g^{-1}$.

Théorème 14 (Relation orbite-stabilisateur - [R] 21). *Pour tout $x \in X$, $G/\mathrm{Stab}(x)$ et $\mathrm{Orb}(x)$ sont équipotents (cela reste vrai si G est infini). Par conséquent,*

$$\mathrm{Card}(G) = \mathrm{Card}(\mathrm{Stab}(x))\,\mathrm{Card}(\mathrm{Orb}(x))$$

Théorème 15 (Équation aux classes - [R] 21). *Soit $\{x_1, \ldots, x_r\}$ un système de représentants pour les orbites. Alors,*

$$\mathrm{Card}\, X = \sum_{i=1}^{r} \mathrm{Card}(\mathrm{Orb}(x_i)) = \sum_{i=1}^{r} \frac{\mathrm{Card}\, G}{\mathrm{Card}(\mathrm{Stab}(x_i))}$$

Exemple 16 ([R] 22). *Si $\mathrm{Card}\, G$ est une puissance d'un nombre premier, alors son centre $Z(G) := \{g \in G \mid \forall h \in G, ghg^{-1} = h\}$ n'est pas réduit à $\{1\}$.*

Corrolaire ([R] 23) *: tout groupe d'ordre p^2 avec p premier est abélien.*

Théorème 17 (Formule de Burnside - [R] 35). *L'action de G sur X possède $\frac{1}{\mathrm{Card}\, G} \sum_{g \in G} \mathrm{Card}(\mathrm{Fix}(g))$ orbites, où $\mathrm{Fix}(g) = \{x \in X \mid g \cdot x = x\}$.*

Exemple 18 ([C] 132). *En moyenne, une permutation de $[\![1, n]\!]$ tirée aléatoirement a 1 point fixe.*

Exemple 19 ([C] 132). *Si G n'est pas abélien, alors la probabilité de tirer simultanément deux éléments qui commutent vaut $\frac{k}{n}$, avec k le nombre de classes de conjugaison de G.*

Théorème 20 (de Cauchy - [R] 23). *Soit p un nombre premier. Si $p \mid \mathrm{Card}\, G$, alors G admet un élément d'ordre p.*

II. Applications

A. En géométrie : les isométries des polytopes

Théorème 21 ([R] 94). *L'ensemble des isométries du plan conservant un triangle équilatéral est un groupe isomorphe à $\mathfrak{S}_3$.*

Proposition 22 ([R] 82). *Soit $\mathcal{C}$ un cube. L'ensemble des isométries de l'espace conservant $\mathcal{C}$ est un groupe, noté $Is(\mathcal{C})$. On note $Is^+(\mathcal{C})$ le sous-groupe de $\mathcal{C}$ formé de rotations.*

Théorème 23 ([R] 85). *$Is^+(\mathcal{C}) \cong \mathfrak{S}_4$ et $Is(\mathcal{C}) \cong \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.*

Théorème 24 ([R] 95). *En notant $\mathcal{T}$ le tétraèdre régulier, on a $Is^+(\mathcal{T}) \cong \mathcal{A}_4$ et $Is(\mathcal{T}) \cong \mathfrak{S}_4$.*

B. Du côté des matrices

Dans ce paragraphe, K désigne un corps. On fixe $(n, m) \in (\mathbb{N}^*)^2$.

Proposition 25 ([R] 184/185/199/195/206)**.** *Les applications suivantes sont des actions :*

1. *Translation à gauche :* $GL_n(K) \times \mathcal{M}_{n,m}(K) \to \mathcal{M}_{n,m}(K)$, $(P, A) \mapsto PA$
2. *Translation à droite :* $GL_n(K) \times \mathcal{M}_{n,m}(K) \to \mathcal{M}_{n,m}(K)$, $(P, A) \mapsto AP^{-1}$
3. *Similitude (ou conjugaison) :* $GL_n(K) \times \mathcal{M}_n(K) \to \mathcal{M}_n(K)$, $(P, A) \mapsto PAP^{-1}$
4. *Équivalence (ou* action de Steiniz*) :* $(GL_n(K) \times GL_m(K)) \times \mathcal{M}_{n,m}(K) \to \mathcal{M}_{n,m}(K)$, $((P, Q), A) \mapsto PAQ^{-1}$
5. *Congruence :* $GL_n(K) \times \mathcal{M}_n(K) \to \mathcal{M}_n(K)$, $(P, A) \to {}^tPAP$

Proposition 26 ([R] 184/185/ ?/195/207)**.** *Dans l'ordre de la proposition précédente, les orbites sont caractérisées par :*

1. *le noyau de A*
2. *l'image de A*
3. *les molynômes minimal et caractéristique de A*
4. *Ça dépend de K...*

Exemple 27. *$Diag(1, 2, 2)$ et $Diag(1, 1, 2)$ ont même polynôme minimal mais ne sont pas semblables : il faut donc bien les deux informations !*

C. Théorèmes de Sylow

Dans ce paragraphe, on se donne p premier, et on note $\operatorname{Card} G = p^\alpha m$, $m \wedge p = 1$.

Définition 28 ([U] 85)**.** *Un p-Sylow de G est un sous-groupe de G de cardinal p^α.*

$Syl_p(G)$ désigne l'ensemble des p-Sylow de G, et $n_p :=$ $\operatorname{Card}(Syl_p(G))$.

Théorème 29 (de Sylow - [U] 87)**.** *Soit G un groupe d'ordre $p^\alpha m$, $m \wedge p = 1$. Alors,*

1. *$Syl_p(G) \neq$*
2. *G agit transitivement sur $Syl_p(G)$ par conjugaison*
3. *$n_p \equiv 1\,[p]$*

Définition 30. *On dit que G est* simple *si les seuls sous-groupes de G distingués (*i.e. *fixe par l'action par conjugaison de G) sont $\{1\}$ et G.*

Théorème 31 ([S] 277)**.** *Si G est simple et d'ordre* 60*, alors $G \cong \mathcal{A}_5$.*

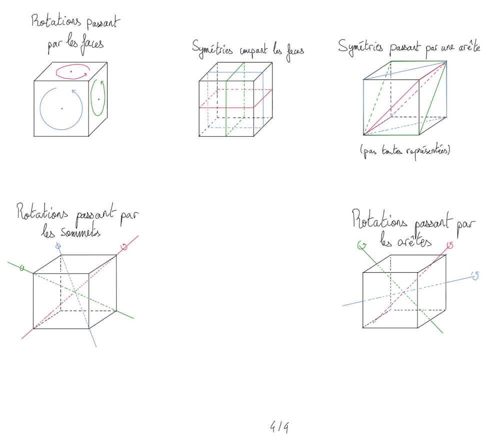
Développements

— Développement 1 : Théorème 23
— Développement 2 : Théorème 31

Références

U *Théorie des groupes*, Félix Ulmer
R *Mathématiques pour l'agrégation - Algèbre et géométrie*, Jean-Étienne Rombaldi, 2e édition
S *Algèbre pour la licence 3*, Szpirglas
C *Carnets de voyage en Algébrie*, Caldero

FIGURE : Isométries du cube



102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications.

I. Les nombres complexes de module 1

Définition 1. *L'ensemble des nombres complexes de module 1, aussi appelé* cercle unité, *est noté* $S^1 := \{z \in \mathbb{C} \mid |z| = 1\}$.

A. Autour de l'exponentielle

Définition 2 ([T] 43/44/45)**.** *Pour* $z \in \mathbb{C}$, *on définit :*

- $\exp(z) = e^z = \sum_{n=0}^{+\infty} \frac{z^n}{n!}$ *(l'*exponentielle *de z)*
- $\sin(z) = \sum_{n=0}^{+\infty} \frac{(-1)^n}{(2n+1)!}$ *(le* sinus *de z)*
- $\cos(z) = \sum_{n=0}^{+\infty} \frac{(-1)^n}{(2n)!}$ *(le* cosinus *de z)*

Proposition 3 ([T] 43/35/44)**.**
- exp, cos *et* sin *sont des séries entières de rayon de convergence infini. En particulier, elles sont entières. De plus,* $\exp' = \exp$.
- $\forall z \in \mathbb{C}$, $e^{iz} = \cos(z) + i\sin(z)$
- $\forall \theta \in \mathbb{R}$, $|e^{i\theta}| = 1$

Proposition 4 ([T] 44/44)**.**
- $\theta \mapsto e^{i\theta}$ *est périodique. On note* τ *sa période. C'est un morphisme de groupes surjectif de* $(\mathbb{R}, +)$ *dans* $(S^1, \times)$.
- exp *est un morphisme de groupes surjectif de* $(\mathbb{C}, +)$ *dans* $(\mathbb{C}^*, \times)$. *Son noyau est* $i\tau\mathbb{Z}$.

Définition 5 ([T] 44)**.** $\pi := \tau/2$. *On admet que* π *est transcendant sur* $\mathbb{Q}$.

Proposition 6 ([T] 45)**.**
- *Formules d'Euler :* $\forall z \in \mathbb{C}$, $\cos(z) = \frac{e^z + e^{-z}}{2} \in \mathbb{R}$, $\sin(z) = \frac{e^z - e^{-z}}{2i} \in \mathbb{R}$
- *Formule de Moivre :* $\forall \theta \in \mathbb{R}$, $\forall n \in \mathbb{N}$, $\left(e^{i\theta}\right)^n = e^{in\theta}$

Remarque 7 (c.f. Figure 1)**.**
- ▷ *La formule de Moivre est fausse pour n non entier :* $1 = \left(e^{2i\pi}\right)^{1/2} \neq e^{i\pi} = -1$
- ▷ $\cos^2 + \sin^2 = 1$
- ▷ $\forall \theta \in \mathbb{R}$, $\cos(\theta) = \Re(e^{i\theta})$ *et* $\sin(\theta) = \Im(e^{i\theta})$

Application 8. *Avec les formules de Moivre et d'Euler, pour tous* $\theta \in \mathbb{R}$ *et* $n \in \mathbb{N}$, $\cos(n\theta) \in \mathbb{R}[\cos(\theta)]$ *et* $\sin(n\theta) \in \mathbb{R}[\sin(\theta)]$.
(Appli : problème de trisection de l'angle - voir II. B)

Application 9 (Polynômes de Techebychev)**.** *Ce sont les polynômes tels que* $\forall n \in \mathbb{N}$, $\forall \theta \in \mathbb{R}$, $\cos(n\theta) = T_n(\theta)$ *et on a :* $T_0 = 1$, $T_1 = X$, *et* $\forall n \in \mathbb{N}$, $T_{n+2} = 2XT_{n+1} - Tn$.

Application 10 (Noyaux de Dirichlet et de Fejér)**.** $\forall \theta \in \mathbb{R}/2\pi\mathbb{Z}$, $\forall n \in \mathbb{N}^*$,

$$D_N(\theta) := \sum_{n=-N}^{N} e^{in\theta}$$

$$K_n(\theta) := \frac{1}{N} \sum_{n=0}^{N-1} D_N(\theta) = \left(\frac{\sin(N\theta/2)}{\sin(\theta/2)}\right)^2$$

Théorème 11 ([R] 101)**.** $\forall z \in S^1$, $\exists! \theta \in]-\pi, \pi] : z = e^{i\theta}$

Définition 12 ([R] 102)**.** *Soit* $z \in \mathbb{C}^*$. *D'après théorème 11, il existe un unique* $\theta \in]-\pi, \pi]$, *appelé* argument principal *de z, noté* $\arg(z)$, *tel que* $z = |z|e^{i\theta}$.
On appelle (un) argument *de z tout réel* θ *tel que* $z = |z|e^{i\theta}$. *Les arguments de z sont congrus à* $\arg(z)$ *modulo* 2π.

Définition 13 ([T] 63)**.** *On appelle* détermination principale du logarithme complexe *l'application :*

$$\begin{aligned} \log : \mathbb{C} \setminus \mathbb{R}^- &\longrightarrow B_\pi := \{z \in \mathbb{C} \mid |\Im(z)| < \pi\} \\ z &\longmapsto \ln(|z|) + i\arg(z) \end{aligned}$$

Proposition 14. exp *induit une bijection de* B_π *sur* $\mathbb{C} \setminus \mathbb{R}^-$, *de réciproque* log.

Théorème 15 (de relèvement - ADMIS)**.** *Soit* $I \subseteq \mathbb{R}$ *un intervalle et* $k \in \mathbb{N}$. *Pour tout* $f \in C^k(I, S^1)$, *il existe* $\varphi \in C^k(I, \mathbb{R})$ *telle que* $f = e^{i\varphi}$.

B. Les racines de l'unité

Définition 16 ([P] 80)**.** *Soient* $n \in \mathbb{N}^*$ *et* $z \in \mathbb{C}$. *On dit que z est une* racine *n*-ième de l'unité *sir* $z^n = 1$. *On note* $\mathbb{U}_n$ *l'ensemble des racines n-ièmes de l'unité. On dit que z est une racine de l'unité sur* $z \in \mathbb{U} := \cup_{n \in \mathbb{N}^*} \mathbb{U}_n$.

Proposition 17. $\mathbb{U}_n = \left\{e^{i\frac{2k\pi}{n}} \mid k \in \mathbb{N}\right\} = \left\{e^{i\frac{2k\pi}{n}} \mid 0 \leq k \leq n-1\right\} = \langle \omega_n \rangle$, *où* $\omega_n := e^{i\frac{2\pi}{n}}$. *En particulier,* $\mathbb{U}_n \cong \mathbb{Z}/n\mathbb{Z}$.

Proposition 18. $\forall n \geq 2$, $\sum_{\omega \in \mathbb{U}} \omega = 0$, $\omega^n = 1$, $\overline{\omega_n} = \omega_n^{n-1}$.

Définition 19 ([P] 80)**.** *Soit* $n \in \mathbb{N}^*$. *On dit que* $\zeta_n \in \mathbb{C}$ *est une* racine primitive *n-ième de l'unité si* $\mathbb{U}_n = \langle \zeta_n \rangle$. *On note* μ_n^* *l'ensemble des racine primitives n-ièmes de l'unité,* i.e. *des générateurs de* $\mathbb{U}_n$.

Proposition 20 ([P] 80, cf FIGURE 2)**.**

$$\mu_n^* = \{\omega_n^k \mid k \wedge n = 1\}$$

Exemple 21. $\mathbb{U}_2 = \{\pm 1\}$, $\mathbb{U}_3 = \left\{1, e^{2i\pi/3}, e^{-2i\pi/3}\right\} = \left\{1, \frac{1}{2} \pm i\frac{\sqrt{3}}{2}\right\}$, $\mathbb{U}_4 = \{\pm 1, \pm i\}$.

Proposition 22 ([P] 80, [Rb] 18)**.** *Soit* $(n, d) \in (\mathbb{N}^*)^2$.
- ▷ $\mathbb{U}_d \subseteq \mathbb{U}_n \iff d \mid n$
- ▷ Card $\mu_n^* = \varphi(n)$ *(indicatrice d'Euler)*
- ▷ $\mathbb{U}_n = \sqcup_{d \mid n} \mu_d^*$
- ▷ $n = \sum_{d \mid n} \varphi(d)$

Remarque 23. *Soient* $a \in \mathbb{C}^*$ *et* $n \in \mathbb{N}^*$. *Une racine n-ième de a est un nombre complexe z vérifiant* $z^n = a$. *Posons* $z_0 := |a|^{\frac{1}{n}} \exp(i\frac{\arg a}{n})$, *de sorte que* $z_0^n = a$. *Si* $z^n = a$, *alors* $\left(\frac{z}{z_0}\right)^n = 1$, i.e. $\frac{z}{z_0} \in \mathbb{U}_n$, *donc il existe* $k \in [\![0, n-1]\!]$ *tel que* $z = z_0 e^{i\frac{2k\pi}{n}}$.

Théorème 24 ([Rb] 114/132)**.** *Soit H un sous-groupe de* S^1. *Si H est fini d'ordre n, alors* $H = \mathbb{U}_n$. *Sinon, H est dense dans* S^1.

Application 25 ([Rb] 132). $\overline{\{\cos(n) \mid n \in \mathbb{N}\}} = \overline{\{\sin(n) \mid n \in \mathbb{N}\}} = [0, 1]$

Théorème 26 (de Niven). *Soit $r \in \mathbb{Q}$. Si $\cos(r\pi) \in \mathbb{Q}$, alors $r \in \{0, \frac{1}{3}, \frac{1}{2}\}$. Si $\sin(r\pi) \in \mathbb{Q}$, alors $r \in \{0, \frac{1}{6}, \frac{1}{2}\}$.*

Corollaire 27. $\mathbb{U} \cap \mathbb{Q}[i] = \{\pm 1, \pm i\}$

C. Polynômes cyclotomiques

Soit $n \in \mathbb{N}^*$.

Définition 28 ([P] 80). *On appelle* n-ième polynôme cyclotomique *le polynôme* $\Phi_n := \prod_{\zeta \in \mu_n^*} (X - \zeta)$.

Exemple 29 ([P] e81). $\Phi_1 = X - 1$, $\Phi_2 = X + 1$, $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$, ...

Proposition 30 ([P] 80-83). ▷ $\deg(\Phi_n) = \varphi(n)$

- ▷ $X^n - 1 = \prod_{d \mid n} \Phi_d$
- ▷ $\Phi_n \in \mathbb{Z}[X]$
- ▷ Φ_n *est irréductible sur* $\mathbb{Q}$
- ▷ Φ_n *est le polynôme minimal de* $\zeta \in \mu_n^*$ *sur* $\mathbb{Q}$

Proposition 31. *Pour tout p premier,*

$$\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1$$

D. Applications

Théorème 32 (de Wedderburn - [P] 82). *Tout corps fini est commutatif.*

Théorème 33 (de Kronecker - [FGN] 213). *Soit $P \in \mathbb{Z}[X]$ unitaire dont toutes les racines sont de module ≤ 1, et tel que $P(0) \neq 0$. Alors toutes les racines de P sont des racines primitives de l'unité.*

Corollaire 34 (théorème de Kronecker - [Go] 95). *Soit $P \in \mathbb{Z}[X]$ irréductible sur $\mathbb{Q}$. Si toutes les racines de P sont de module ≤ 1, alors $P = X$ ou P est cyclotomique.*

II. Liens avec la géométrie

A. Notion d'angle orienté

On note $S^1(0, 1)$ le cercle unité de $\mathbb{R}^2$ pour la norme euclidienne, qui s'identifie à S^1. Pour $z \in \mathbb{C}$, on note M_z le point de $\mathbb{R}^2$ d'affixe z.

On note $\mathcal{B}$ une base orthonormée de $\mathbb{R}^2$, que l'on décrète directe.

Proposition 35. $\forall (\overrightarrow{u}, \overrightarrow{v}) \in S^1(0, 1)^2, \exists ! r \in SO(\mathbb{R}^2) : \overrightarrow{v} = r(\overrightarrow{u})$

Théorème 36 ([P] 146). *On dispose des isomorphismes de groupes suivant :*

$$\begin{array}{cccc} \mathbb{R}/2\pi\mathbb{Z} \longrightarrow S^1 & \longrightarrow SO_2(\mathbb{R}) & \longleftarrow SO(\mathbb{R}^2) \\ \theta \longmapsto e^{i\theta} & \longmapsto R(\theta) & \longleftarrow r_\theta \end{array}$$

NB : $R(\theta)$ est la matrice de rotation 2D d'angle θ (cos, -sin // sin, cos).

Corollaire 37. *La relation $(\overrightarrow{u}, \overrightarrow{v}) \, \mathcal{R} \left(\overrightarrow{u'}, \overrightarrow{v'}\right) \iff \exists r \in SO(\mathbb{R}^2) : \overrightarrow{u'} = r(\overrightarrow{u})$ et $\overrightarrow{v'} = r(\overrightarrow{v})$ est une relation d'équivalence sur $\left(S^1\right)^2$.*

Définition 38 ([P] 146 - FIGURE 3). *Soit $(\overrightarrow{u}, \overrightarrow{v}) \in \left(S^2\right)^2$.*

- ▷ *On appelle* angle orienté de $\overrightarrow{u}$ à $\overrightarrow{v}$ *la classe d'équivalence de $(\overrightarrow{u}, \overrightarrow{v})$ dans $\left(S^1\right)^2 / \mathcal{R}$, que l'on note $\widehat{(\overrightarrow{u}, \overrightarrow{v})}$.*
- ▷ *Une* mesure *de $\widehat{(\overrightarrow{u}, \overrightarrow{v})}$ est un réel θ tel que $\overrightarrow{v} = r_\theta(\overrightarrow{u})$.*
- ▷ *La* mesure principale *de $\widehat{(\overrightarrow{u}, \overrightarrow{v})}$ est la mesure de $\widehat{(\overrightarrow{u}, \overrightarrow{v})}$ entre $-\pi$ et π.*

Définition 39. *On étend la définition aux couples de vecteurs non nuls $(\overrightarrow{u}, \overrightarrow{v})$ en posant :*

$$\widehat{(\overrightarrow{u}, \overrightarrow{v})} := \widehat{\left(\frac{\overrightarrow{u}}{\|\overrightarrow{u}\|}, \frac{\overrightarrow{v}}{\|\overrightarrow{v}\|}\right)}$$

Remarque 40. *Si $z_{\overrightarrow{u}}$ est l'affixe de $\overrightarrow{u} \in \mathbb{R}^2$, alors l'affixe de $r_\theta(\overrightarrow{u})$ est $e^{i\theta} z_{\overrightarrow{u}}$.*

Remarque 41. *En notant $\langle \cdot \mid \cdot \rangle$ le produit scalaire euclidien de $\mathbb{R}^2$, on appelle* écart angulaire *entre deux vecteurs non nuls $\overrightarrow{u}$ et $\overrightarrow{v}$ le réel $\alpha = \arccos\left(\frac{\langle \overrightarrow{u} \mid \overrightarrow{v} \rangle}{\|\overrightarrow{u}\| \cdot \|\overrightarrow{v}\|}\right)$. Si θ est la mesure principale de $\widehat{(\overrightarrow{u}, \overrightarrow{v})}$, alors $\alpha = |\theta|$.*

Plus précisément, si $\overrightarrow{u}$ et $\overrightarrow{v}$ sont colinéaires et de même sens (resp. de sens opposé), alors $\alpha = \theta = 0$ (resp. $\alpha = \theta = \pi$) et sinon, si $\widehat{(\overrightarrow{u}, \overrightarrow{v})}$ est directe, alors $\alpha = \theta$ et sinon $\alpha = -\theta$.

Proposition 42 ([Bu] 497). *Une mesure de $\widehat{(\overrightarrow{u}, \overrightarrow{v})}$ est un réel θ vérifiant*

$$e^{i\theta} = \frac{\langle \overrightarrow{u} \mid \overrightarrow{v} \rangle + i \det_{\mathcal{B}}(\overrightarrow{u}, \overrightarrow{v})}{\|\overrightarrow{u}\| \cdot \|\overrightarrow{v}\|}$$

Définition 43. *Soient $\overrightarrow{u}$ et $\overrightarrow{v}$ deux vecteurs non nuls d'écart angulaire α. On dit que $\widehat{(\overrightarrow{u}, \overrightarrow{v})}$ est* nul *si $\alpha = 0$,* plat *si $\alpha = \pi$,* droit *si $\alpha = \pi/2$,* aigu *si $\alpha < \pi/2$ et* obtus *si $\alpha > \pi/2$.*

B. Autour des polygônes réguliers - groupes diédraux, constructibilité

Soit $n \geq 3$.

Définition 44. *Le* polygône régulier à n côtés *est le polygône convexe P_n du plan dont les sommets sont, dans l'ordre, les points d'affixes $1, \omega_n, \omega_n^2, \ldots, \omega_n^{n-1}$.*

Proposition 45. *L'ensemble des isométries du plan conservant P_n est un groupe, appelé* groupe diédral d'ordre $2n$ *et noté D_{2n}. Il est engendré par la rotation d'angle $\frac{2\pi}{n}$ centrée à l'origine (correspondant à $z \mapsto \omega_n z$ en termes d'affixes) et la symétrie d'axe (Ox) (correspondant à la conjugaison en termes d'affixes).*

Définition 46 ([P] 68). *On dit que $z \in \mathbb{C}$ est* constructible *si on peut tracer l'image de z dans le plan uniquement avec un compas et une règle non graduée. On dit que P_n est constructible si ω_n l'est.*

Théorème 47 (de Gauss-Wantzel - FIGURES 2,4). *P_n est constructible si, et seulement si, n est de la forme $n = 2^m p_1 \ldots p_r$, avec $m \in \mathbb{N}$ et $p_1, \ldots, p_r$ des nombres premiers de Fermat (*i.e. $3, 5, 17, 257, 65537$*).*

C. Application : une caractérisation de 7

Théorème 48 (de Gauss-Lucas - [FGN] 225)**.** *Soit $P \in \mathbb{C}[X]$ non constant.*

$$Z - \mathbb{C}(P') \subset Conv(Z_{\mathbb{C}}(P))$$

où, si $Z_{\mathbb{C}}(P) = \{\alpha_1, \dots, \alpha_r\}$, alors :

$$Conv(Z_{\mathbb{C}}(P)) = \left\{ \sum_{k=1}^{r} \lambda_k \alpha_k \mid (\lambda_1, \dots, \lambda_r) \in [0,1]^r, \sum_{k=1}^{r} \lambda_k = 1 \right\}$$

Application 49. *7 est le plus grand entier $n \geq 2$ tel que :*

$$Z_{\mathbb{C}}((X+1)^n - X^n - 1) \subseteq \{z \in \mathbb{C} \mid |z| = 1\}$$

Développements

— Développement 1 : Théorème 33 et Corrolaire 34

— Développement 2 : Théorème 48 et Application 49

Références

Rb *Mathématiques pour l'agrégation - Algèbre et géométrie*, Jean-Étienne Rombaldi, 2e édition

Rb *Eléments d'analyse réelle*, Rombaldi

P Perrin

FGN *Oraux X-ENS, Algèbre 1*, 2è édition (Francinou)

T *Analyse complexe*, Tauvel

Bu Burg

105 : Groupe des permutations d'un ensemble fini. Applications.

I. Permutations d'un ensemble fini

A. Introduction

Définition 1 ([R] 37). *Soit E un ensemble. On note $\mathfrak{S}(E)$ l'ensemble des bijections de E dans E. On l'appelle* groupe symétrique *de E. On notera plus simplement $\mathfrak{S}_n = \mathfrak{S}([\![1,n]\!])$. On appelle* permutation *de E un élément de $\mathfrak{S}(E)$.*

Proposition 2. *$\mathfrak{S}(E)$ est un groupe pour la composition, de neutre l'identité de E.*

Proposition 3 ([R] 39). *Si E et F sont deux ensembles équipotents, alors $\mathfrak{S}(E)$ et $\mathfrak{S}(F)$ sont isomorphes (en tant que groupes).*

Proposition 4 ([R] 39). *Pour $n \geq 3$, $\mathfrak{S}_3$ n'est pas commutatif.*

Dans toute la suite, on étudiera $\mathfrak{S}_n$ pour $n \geq 3$.

Proposition 5 ([R] 40). $\#\mathfrak{S}_n = n!$

Notation ([U] 41). *Soit $\sigma \in \mathfrak{S}_n$. On représentera σ par la matrice $2 \times n$:*

$$\sigma = \left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{smallmatrix}\right)$$

B. Action naturelle de $\mathfrak{S}_n$ sur $[\![1,n]\!]$, conséquences

Proposition 6 ([U] 41). *$\mathfrak{S}_n$ agit naturellement sur $[\![1,n]\!]$ par $\sigma \cdot i = \sigma(i)$. Le morphisme associé est l'identité de $\mathfrak{S}_n$.*

Définition 7 ([U] 42). *On note* $\mathrm{Fix}(\sigma)$ *l'ensemble des points fixes de $\sigma \in \mathfrak{S}_n$. Son complémentaire dans $[\![1,n]\!]$ est appelé* support *de σ, et est noté* $\mathrm{Supp}(\sigma)$.

Proposition 8 ([U] 43). *Soit $\sigma \in \mathfrak{S}_n$. Le sous-groupe $\langle\sigma\rangle$ agit sur $[\![1,n]\!]$ par restriction de l'action de $\mathfrak{S}_n$. Les orbites de cette action sont appelées* σ-orbites. *La réunion des σ-orbites ponctuelles est* $\mathrm{Fix}(\sigma)$. *Les σ-orbites non ponctuelles partitionnent* $\mathrm{Supp}(\sigma)$.

Exemple 9. *Soit $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{smallmatrix}\right)$. On a* $\mathrm{Supp}(\sigma) = \{1,2\} \sqcup \{4,5\} = \langle\sigma\rangle \cdot \{1\} \sqcup \langle\sigma\rangle \cdot \{4\}$.

Définition 10 ([U] 43). *Un* k-cycle *($2 \leq k \leq n$) est une permutation n'ayant qu'une seule σ-orbite non ponctuelle $\{i_1, \ldots, i_k\}$. On la note $\sigma = (i_1, \ldots, i_k)$ pour signifier que $\forall j \notin \{i_1, \ldots, i_k\}$, $\sigma(j) = j$ et $\sigma(i_j) = i_{j+1}$ en regardant les indices modulo k.*

Un 2-cycle est appelé transposition.

Proposition 11 ([U] 43). $(i_1, i_2, \ldots, i_k) = (i_2, i_3, \ldots, i_k, i_1) = \cdots = (i_k, i_1, i_2, \ldots, i_{k-1})$

Proposition 12. *Un k-cycle est d'ordre k.*

C. Décomposition d'une permutation, conséquences

Proposition 13 ([U] 42). *Deux permutations à supports disjoints commutent.*

Théorème 14 ([U] 43). *Toute permutation se décompose de manière unique (à l'ordre des facteurs près) comme produit de cycles à supports disjoints.*

Algorithme 15 ([U] 43). *Pour trouver une telle décomposition, il suffit de trouver les r-orbites.*

1. *On calcule $\sigma(1), \sigma^2(1), \ldots$ justqu'à trouver $\sigma^{k_1}(1) = 1$ (NB : $k_1 \leq n$) ;*
2. *On pose $i_2 = \min [\![1,n]\!] \setminus (\langle\sigma\rangle \cdot \{1\})$, et de même on calcule $\sigma(i_2), \sigma^2(i_2), \ldots$ jusqu'à trouver $\sigma^{k_2}(i_2) = i_2$;*
3. *On itère jusqu'à épuiser $[\![1,n]\!]$.*

On a alors $\sigma = (1, \sigma(1), \ldots, \sigma^{k_1-1}(1)) \circ (i_2, \sigma(i_2), \ldots, \sigma^{k_2-1}(i_2)) \circ \cdots \circ (i_j, \sigma(i_j), \ldots, \sigma^{k_j-1}(i_j))$

Exemple 16. $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{smallmatrix}\right) = (1,3,4)(5,6)$

Proposition 17 ([R] 44). $(i_1, \ldots, i_k) = (i_1, i_2)(i_2, i_3) \ldots (i_{k-1}, i_k)$

Corollaire 18 ([R] 44). *Les transpositions engendrent $\mathfrak{S}_n$.*

Proposition 19 ([R] 45). $\mathfrak{S}_n = \langle (i, i+1),\, 1 \leq i \leq n \rangle = \langle (1,i),\, 2 \leq i \leq n \rangle = \langle (1,2),\, (1,2,\ldots,n) \rangle$

Définition 20 ([U] 45). *On appelle* type *de $\sigma \in \mathfrak{S}_n$ la liste croissante des cardinaux des σ-orbites.*

Exemple 21. *Le type de $(1,2,5)(3,4)(7,8) \in \mathfrak{S}_8$ est la liste* $[1,2,2,3]$.

Proposition 22 ([U] 46). *Deux permutations sont conjuguées dans $\mathfrak{S}_n$ si, et seulement si, elles ont le même type. Cela décrit donc les classes de conjugaison de $\mathfrak{S}_n$.*

Proposition 23 ([U] 45). *Si σ est du type $[l_1, \ldots, l_k]$, alors* $\mathrm{ord}(\sigma) = l_1 \vee \cdots \vee l_k$.

D. Signature dune permutation, groupe alterné

Proposition 24 ([R] 47). *Il existe un unique morphisme $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ qui envoie les transpositions sur -1. On appelle* signature *de σ la quantité $\varepsilon(\sigma)$.*

Corollaire 25. *La signature d'un k-cycle est $(-1)^{k+1}$.*

Proposition 26 ([R] 48). $\forall \sigma \in \mathfrak{S}_n$,

$$\varepsilon(\sigma) = \prod_{1 \leq i \leq j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

En particulier, la signature mesure le nombre d'inversions.

Définition 27 ([R] 48). *On appelle* n-ième groupe alterné *le sous-groupe $\mathcal{A}_n = \mathrm{Ker}(\varepsilon)$. C'est l'ensemble des permutations dîtes* paires.

Exemple 28. $\mathcal{A}_3 = \{\mathrm{id},\, (1,2,3),\, (1,3,2)\}$.

Proposition 29. $\#\mathcal{A}_n = \frac{n!}{2}$

Théorème 30 ([R] 49). *Pour $n \geq 3$, les 3-cycles engendrent $\mathcal{A}_n$, et y sont conjugués.*

Théorème 31 ([R] 50). *Pour $n \geq 5$, $\mathcal{A}_n$ n'admet pas de sous-groupe distingué non trivial.*

II. Quelques applications du groupe symétrique

A. En géométrie : les isométries des polytopes

Théorème 32 ([R] 94). *L'ensemble des isométries du plan conservant un triangle équilatéral est un groupe isomorphe à* $\mathfrak{S}_3$.

Proposition 33 ([R] 82). *Soit* $\mathcal{C}$ *un cube. L'ensemble des isométries de l'espace conservant* $\mathcal{C}$ *est un groupe, noté* $\mathrm{Is}(\mathcal{C})$. *On note* $\mathrm{Is}^+(\mathcal{C})$ *le sous-groupe de* $\mathrm{Is}(\mathcal{C})$ *formé des rotations.*

Théorème 34 ([R] 85). $\mathrm{Is}^+(\mathcal{C}) \cong \mathfrak{S}_4$ *et* $\mathrm{Is}(\mathcal{C}) \cong \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

Théorème 35 ([R] 95). *En notant* $\mathcal{T}$ *le tétraèdre régulier, on a :* $\mathrm{Is}(\mathcal{T}) \cong \mathfrak{S}_4$ *et* $\mathrm{Is}^+(\mathcal{T}) \cong \mathcal{A}_4$.

Chez les (actions de) groupes

Théorème 36 (de Cayley - [R] 53). *Tout groupe fini d'ordre* n *est isomorphe à un sous-groupe de* $\mathfrak{S}_n$.

Proposition 37. *Comme pout tout corps (commutatif)* K, $\mathfrak{S}_n \circlearrowleft GL_n(K)$, *tout groupe de garde* n *est isomorphe à un sous-groupe de* $GL_n(K)$.

Exemple 38. *Soit* $D_{2\times 4}$ *le groupe des isométries du carré. Comme* $\#D_{2\times 4} = 8$, $D_{2\times 4}$ *est isomorphe à un sous-groupe de* $\mathfrak{S}_8$. *Noton* φ *un tel isomorphisme. Comme* $D_{2\times 4} = \langle r, s\rangle$ *où* $\mathrm{ord}(r) = 4$, $\mathrm{ord}(s) = 2$ *et* $\mathrm{ord}(rs) = 2$, *on a* $\varepsilon \circ \varphi(s) = \varepsilon \circ \varphi(rs) = -1$, *donc* $\varepsilon \circ \varphi(r) = 1$.

C. Polynômes symétriques

Définition 39 ([R] 55). *Un* polynôme symétrique *est un polynôme* $P \in K[X_1, \dots, X_n]$ *tel que* $\forall \sigma \in \mathfrak{S}_n$, $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$.

Définition 40 ([R] 55). *Les* polynômes symétriques élémentaires *sont les*

$$\Sigma_{k,n} = \sum_{1\leq i_1 \leq \dots \leq i_k \leq n} X_{i_1} \dots X_{i_k} \in K[X_1, \dots, X_n]$$

Théorème 41 (ADMIS - [R] 55). *Pour tout polynôme symétrique* $P \in K[X_1, \dots, X_n]$, *il existe un unique polynôme* $Q \in K[X_1, \dots, X_n]$ *tel que* $P(X_1, \dots, X_n) = Q(\Sigma_{1,n}, \dots, \Sigma_{n,n})$.

D. En algèbre (multi-)linéaire

Dans ce paragraphe, E est un $\mathbb{K}$-espace vectoriel de dimension finie n. On fixe une base $\mathcal{B} = (e_1, \dots, e_n)$ de E.

Définition 42 ([R] 545). *Une* forme k-linéaire *sur* E *est une application* $\varphi : E^k \to \mathbb{K}$ *telle que pour tout* $i \in [\![1, n]\!]$, *pour tout* $(x_1, \dots, x_k) \in E^k$, $\varphi(x_1, \dots, x_{i-1}, \cdot, x_{i+1}, \dots, x_k)$ *est linéaire.*

On note $\bigotimes^k E^*$ *l'ensemble des formes* k*-linéaires sur* E.

Proposition 43 ([R] 546). $(e_{i_1}^* \otimes \dots \otimes e_{i_k}^*)_{1\leq i_1 < \dots < i_k \leq n}$ *est une base de* $\bigotimes^k E^*$, *où pour* $(x_1, \dots, x_k) \in E^k$, $e_{i_1}^* \otimes \dots \otimes e_{i_k}^*(x_1, \dots, x_k) = e_{i_1}^*(x_1) \dots e_{i_k}^*(x_k)$.

Définition 44 ([R] 546). *Une forme* k*-linéaire* alternée *est une forme* k*-linéaire* $\varphi \in \bigotimes^k E^*$ *telle que* $\forall \sigma \in \mathfrak{S}_k$, $\forall (x_1, \dots, x_k) \in E^k$, $\varphi(x_{\sigma(1)}, \dots, x_{\sigma(k)}) = \varepsilon(\sigma)\varphi(x_1, \dots, x_k)$.

On note $\bigwedge^k E^*$ *l'espace des formes* k*-linéaires alternées sur* E.

Proposition 45. $(e_{i_1}^* \wedge \dots \wedge e_{i_k}^*)_{1\leq i_1 < \dots < i_k \leq n}$ *est une base de* $\bigwedge^k E^*$, *où pour* $(x_1, \dots, x_k) \in E^k$, $e_{i_1}^* \wedge \dots \wedge e_{i_k}^*(x_1, \dots, x_k) = \sum_{\sigma \in \mathfrak{S}_k} \varepsilon(\sigma) e_{i_1}^*(x_{\sigma(1)}) \dots e_{i_k}^*(x_{\sigma(k)})$.

Corollaire 46. *On a* $\dim\left(\bigwedge^k E^*\right) = \binom{n}{k}$.

Définition 47. *On appelle* déterminant *dans la base* $\mathcal{B}$ *l'unique forme* n*-linéaire alternée* $\det_{\mathcal{B}}$ *sur* E *vérifiant* $\det_{\mathcal{B}}(\mathcal{B}) = 1$. *(La fammille* $(\det_{\mathcal{B}})$ *est une base de* $\bigwedge^n E^*$.*)*

Proposition 48 ([R] 547). $\forall (x_1, \dots, x_n) \in E^n$, $\det_{\mathcal{B}}(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) e_1^*(x_{\sigma(1)}) \dots e_n^*(x_{\sigma(n)})$.

E. Résultats en probabilités

Définition 49 ([R] 51). *On appelle* dérangement *une permutation sans point fixes.*

Proposition 50. *Notons* d_n *le nombre de dérangements de* $[\![1, n]\!]$. *Alors* $d_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$. *En particulier, la probabilité de choisir un dérangement en tiant au hasard une permutation de* $[\![1, n]\!]$ *tend vers* $\frac{1}{e}$ *quand* $n \to +\infty$.

Proposition 51 ([C]). *Soit* X *la variable aléatoire qui compte le nombre de points fixes d'une permutation aléatoirement choisie dans* $\mathfrak{S}_n$. *Alors* $\mathbb{E}[X] = \mathbb{V}[X] = 1$.

F. Groupes simples d'ordre 60

Dans ce paragraphe, on se donne p premier, et on note $\#G = p^\alpha m$, $m \wedge p = 1$.

Définition 52 ([U] 85). *Un* p-Sylow *de* G *est un sous-groupe de* G *de cardinal* p^α.

Notation. $\mathrm{Syl}_p(G)$ *désigne l'ensemble des* p*-Sylow de* G, *et* $n_p = \# \mathrm{Syl}_p(G)$.

Théorème 53 (de Sylow - [U] 87). *Soit* G *un groupe d'ordre* $p^\alpha m$, p *premier et* $m \wedge p = 1$.

1. $\mathrm{Syl}_p(G) \neq \emptyset$
2. G *agit transitivement sur* $\mathrm{Syl}_p(G)$ *par conjugaison*
3. $n_p \equiv 1\,[p]$ *(donc* $n_p \mid m$*).*

Définition 54. *On dit que* G *est* simple *si les seuls sous-groupes de* G *distingués (*i.e. *fixe par l'action par conjugaison de* G*) sont* $\{1\}$ *et* G.

Théorème 55 ([S] - 277). *Si* G *est simple et d'ordre* 60, *alors* $G \cong \mathcal{A}_5$.

Développements

— Développement 1 : Théorème 34

— Développement 2 : Théorème 55

Références

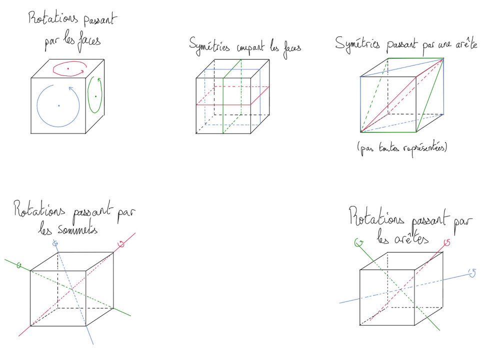
R *Mathématiques pour l'agrégation - Algèbre et géométrie*, Jean-Étienne Rombaldi, 2e édition

U *Théorie des groupes*, Félix Ulmer

S *Algèbre pour la licence 3*, Szpirglas

C *Carnets de voyage en Algébrie*, Caldero

FIGURE : Isométries du cube



4/4