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 $\{x_1, \dots, x_r\}$ 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.*

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

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

1. $\mathrm{Syl}_p(G) \neq$
2. *G agit transitivement sur $\mathrm{Syl}_p(G)$ 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

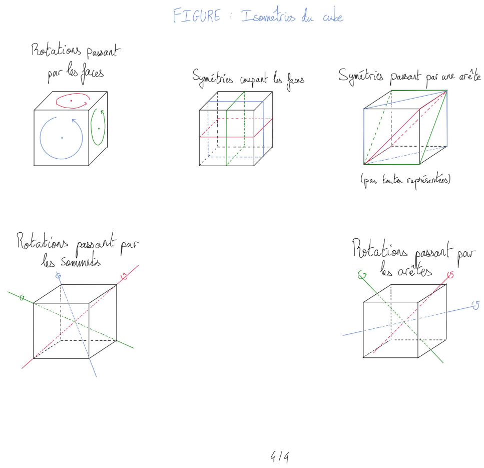
Références

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



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 $\{i_1, \dots, i_k\}$. On la note $\sigma = (i_1, \dots, i_k)$ pour signifier que $\forall j \notin \{i_1, \dots, i_k\}$, $\sigma(j) = j$ et $\sigma(i_j) = i_{j+1}$ en regardant les indices modulo k.*

Un 2-cycle est appelé transposition.

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

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 $\sigma(1), \sigma^2(1), \dots$ 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 $\sigma(i_2), \sigma^2(i_2), \dots$ jusqu'à trouver $\sigma^{k_2}(i_2) = i_2$;*
3. *On itère jusqu'à épuiser $[\![1,n]\!]$.*

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

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)**.** $(i_1, \dots, i_k) = (i_1, i_2)(i_2, i_3) \dots (i_{k-1}, i_k)$

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

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

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 $[l_1, \dots, l_k]$, 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

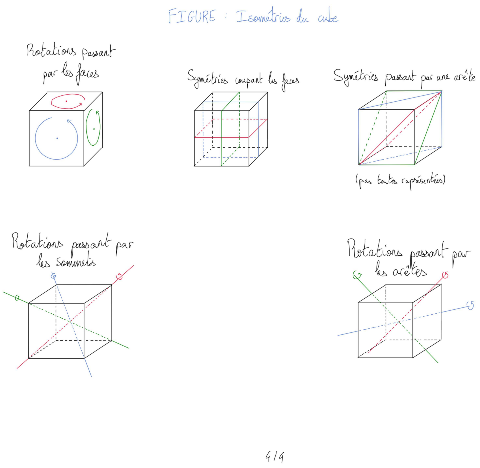


FIGURE 1.1 – Isométries du cube

106 : Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications

Dans cette leçon, K est un corps commutatif, et E est un K-espace vectoriel de dimension finie $n \geq 1$.

I. Endomorphismes inversibles d'un espace vectoriel

A. Introduction au groupe linéaire

Théorème 1 ([Rb] 139). — *L'ensemble $\mathcal{L}(E)$ des endomorphismes de E est un anneau pour $+$ et $\circ$, dont le groupe des inversibles est noté $GL(E)$, et est appelé* groupe linéaire *de E.*

— *Similairement, l'ensemble $\mathcal{M}_n(K)$ des matrices carrées de taille $n \times n$ est un anneau pour $+$ et $\times$, dont le groupe des inversibles est noté $GL_n(K)$, appelé* groupe linéaire d'ordre n sur K.

Remarque 2 ([Rb] 140). *Étant donnée une base $\mathcal{B}$, l'application $u \mapsto \mathrm{Mat}_{\mathcal{B}}(u)$ induit un isomorphisme entre $GL(E)$ et $GL_n(K)$.*

Définition 3 ([Rb] 141). *On note $SL(E)$ (resp. $SL_n(K)$) le noyau du morphisme* det *de $GL(E)$ (resp. $GL_n(K)$) dans $K^\times$. On l'appelle* groupe spécial linéaire de E *(resp.* groupe spécial linéaire d'ordre n sur K*).*

Théorème 4 ([Rb] 140). *Soit $u \in \mathcal{L}(E)$. Comme $\dim E < +\infty$, sont équivalentes :*

1. $u \in GL(E)$
2. (a) *u est injectif*
   (b) $\mathrm{Ker}\, u = \{0\}$
   (c) $\exists v \in \mathcal{L}(E) : v \circ u = \mathrm{id}_E$
3. (a) *u est surjectif*
   (b) $\mathrm{Im}\, u = E$
   (c) $\exists v \in \mathcal{L}(E) : u \circ v = \mathrm{id}_E$
4. *L'image par u d'une base de E est une base de E*
5. $\det(u) \neq 0$

Remarque 5. *Un matrice A est inversible si, et seulement si, ses colonnes forment une base de K^n, et si, et seulement si, ses lignes forment une base de K^n.*

Définition 6. *On dit que $u \in \mathcal{L}(E)$ est une* homothétie de rapport $\lambda \in K^\times$ *si $\forall x \in E$, $u(x) = \lambda x$.*

Proposition 7. *Une homothétie de rapport $\lambda \in K^\times$ est inversible, d'inverse l'homothétie de rapport $1/\lambda$.*

Proposition 8 ([Rb] e168). *Les homothéties sont les seuls endomorphismes à stabiliser toute droite.*

B. Opérations élémentaires

Soit $A \in \mathcal{M}_n(K)$. On note $L_1, \ldots, L_p$ les lignes de A, et $C_1, \ldots, C_n$ ses colonnes.

Définition 9 ([Bu] 315-317). *Soient $\alpha \in K^\times$, $(i,j) \in [\![1,n]\!]^2$ tel que $i \neq j$ et $\sigma \in \mathfrak{S}_n$. On définit les matrices suivantes :*

— *Matrice de* dilatation $D_i(\alpha) = \mathrm{diag}(1, \ldots, 1, \alpha, 1, \ldots, 1) \in GL_n(K)$ *(α est à la i-ième position)*

— *Matrice de* transvection $T_{i,j}(\alpha) = I_n + \alpha E_{i,j} \in GL_n(K)$

— *Matrice de* permutation $P_\sigma = \left(\delta_{i,\sigma(j)}\right)_{1 \leq i,j \leq n} \in GL_n(K)$

Définition 10. *On définit les* opérations élémentaires *sur les colonnes :*

— $C_i \longleftarrow \alpha C_i$ *: on remplace C_i par αC_i*

— $C_i \longleftarrow C_i + \alpha C_j$ *: on remplace C_i par $\alpha C_i + \alpha C_j$*

— $C_i \longleftrightarrow C_j$ *: on échange C_i et C_j*

Théorème 11 ([Bu] 315-318). *On a les correspondances suivantes entre opérations élémentaires et multiplication matricielle :*

— $D_i(\alpha)A \iff L_i \longleftarrow \alpha L_i$

— $T_{i,j}(\alpha)A \iff L_i \longleftarrow L_i \alpha L_j$

— $P_{(i,j)}A \iff L_i \longleftrightarrow L_j$

et

— $AD_i(\alpha) \iff C_i \longleftarrow \alpha C_i$

— $AT_{i,j}(\alpha) \iff C_i \longleftarrow C_i \alpha C_j$

— $AP_{(i,j)} \iff C_i \longleftrightarrow C_j$

Proposition 12. *$\sigma \mapsto P_\sigma$ est un morphisme de groupes injectif de $\mathfrak{S}_n$ dans $GL_n(K)$.*

II. Structure de $GL(E)$, sous-groupe orthogonal

A. Structure de groupe

Théorème 13 (Pivot de Gauss - [Rb] 191). *Pour toute matrice de rang r, il existe une suite d'opérations élémentaires qui transforme cette matrice en la matrice $J_{n,r} = \mathrm{diag}(I_r, O_{n-r})$. Plus précisément, si $\mathrm{rg}\, A = n$, alors il existe $\sigma \in \mathfrak{S}_n$ et des matrices de transvection $T_1, \ldots, T_p$ telles que $A = P_\sigma T_1 \ldots T_p D_\alpha$ où D_α est la matrice de dilatation D_α de rapport $\alpha = \det A$.*

Corollaire 14 ([Rb] 154, 153). — *Les matrices de transvection et de dilatation engendrent $GL_n(K)$;*

— *Les matrices de transvection engendrent $SL_n(K)$.*

Corollaire 15 ([Rb] 141). $GL(E)/SL(E) \cong K^\times$

Corollaire 16 ([Rb] 141). — *$Z(GL(E)) = K^\times \mathrm{id}_E$ (c'est l'ensemble des homothéties) ;*

— *$Z(SL(E)) = \mathbb{U}_n(K)\, \mathrm{id}_E$, où $\mathbb{U}_n(K) \{\lambda \in K^\times \mid \lambda^n = 1\}$.*

B. Le groupe spécial orthogonal

Soit q une forme quadratique sur E, de forme polaire φ. Supposons car $K \neq 2$.

Définition 17 ([P] 123-124). — *Le* groupe orthogonal *de (E, q) est $O(q) = \{u \in \mathcal{L}(E) \mid q \circ u = q\}$*

— *Le groupe spécial orthogonal de* (E, q) *est* $SO(q) = \{u \in O(q) \mid \det u = 1\}$

— *Lorsque* φ *est le produit scalaire canonique relativement à une base donnée, on note* $O(E) = O(q) = \{u \in \mathcal{L}(E) \mid {}^t u \circ u = \mathrm{id}_E\}$ *et* $SO(E) = SO(q) = \{u \in O(E) \mid \det u = 1\}$.

— *On note également* $O_n(K) = \{M \in \mathcal{M}_n(K) \mid {}^t M M = I_n\}$ *et* $SO_n(K) \{M \in O_n(K) \mid \det M = 1\}$.

Proposition 18 ([Rb] 722)**.** *Si* $\mathcal{B}$ *est une base orthonormale de* E*, alors* $u \in O(E) \iff \mathrm{Mat}_{\mathcal{B}}(u) \in O_n(K)$.

Théorème 19 (de réduction des isométries - [Rb] 727)**.** *Soit* $u \in O(\mathbb{R}^n)$*. Il existe une base orthonormale* $\mathcal{B}$ *de* $\mathbb{R}^n$ *telle que* $\mathrm{Mat}_{\mathcal{B}}(u) = \mathrm{diag}(R(\theta_1), \ldots, R(\theta_r), \varepsilon_1, \ldots, \varepsilon_p)$ *où* $R(\theta_i) = \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix}$ *et* $\varepsilon_i = \pm 1$.

Remarque 20 ([P] 146)**.** $SO_2(\mathbb{R}) = \{R(\theta) \mid \theta \in \mathbb{R}\} \cong \mathbb{R}/2\pi\mathbb{Z}$.

Théorème 21 ([C] 50)**.** *Soient* p *premier,* $r \geq 1$ *et* $q = p^r$.

$$SO_2(\mathbb{F}_q) \cong \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & \text{si } -1 \text{ est un carré mod } q \\ \mathbb{Z}/(q+1)\mathbb{Z} & \text{sinon} \end{cases}$$

Définition 22 ([P] 125)**.** *Soit* $u \in O(q)$ *telle que* $u^2 = \mathrm{id}_E$.

On dit que u *est une* réflexion *si* $\dim(\mathrm{Ker}(u + \mathrm{id}_E)) = 1$, i.e. *si* u *est une symétrie par rapport à un hyperplan.*

On dit que u *est une* renversement *si* $\dim(\mathrm{Ker}(u + \mathrm{id}_E)) = 2$, i.e. *si* u *est une symétrie par rapport à un plan.*

On suppose désormais que E est un $\mathbb{R}$-espace vectoriel de dimension finie $n \geq 1$, et que q est définie positive.

Théorème 23 ([P] 143)**.** *Tout élément de* $O(q)$ *est produit d'au plus* n *réflexions.*

Lemme 24. *Si* $n \geq 3$*, alors pour toutes réflexions* τ_1 *et* τ_2*, il existe deux renversements* σ_1 *et* σ_2 *tels que* $\tau_1\tau_2 = \sigma_1\sigma_2$.

Théorème 25. *Pour* $n \geq 3$*, tout élément de* $SO(q)$ *est produit d'au plus* n *renversements.*

Remarque 26. *Ces théorèmes restent vrais si* E *est un espace vectoriel de dimension finie sur un corps* K *de caractéristique* $\neq 2$*, et si* q *est non dégénérée (Cartan, Dieudonné).*

III. Topologie dans $GL(E)$

Dans ce paragraphe, K désigne $\mathbb{R}$ ou $\mathbb{C}$.

Proposition 27 ([Rb] 160-161)**.** $GL(E)$ *est ouvert dans* $(\mathcal{L}(E), |||\cdot|||)$ *et* $u \mapsto u^{-1}$ *est continue.*

Proposition 28.
— $GL_n(\mathbb{C})$ *et* $SL_n(K)$ *sont connexes ;*
— $GL_n(\mathbb{R})$ *a deux composantes connexes.*

Proposition 29. $O_n(\mathbb{R})$ *et* $SO_n(\mathbb{R})$ *sont compacts.*

Théorème 30 (Décomposition polaire - [Rb] 740)**.**

$$\begin{aligned} O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R}) &\to GL_n(\mathbb{R}) \\ (H, S) &\mapsto HS \end{aligned}$$

est un homéomorphisme.

Développements

— Développement 1 : Théorème 21

— Développement 2 : Théorème 23, Lemme 24 et Théorème 25

Références

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

P *Cours d'algèbre*, Perrin

B *Algèbre et géométrie : CAPES et Agrégation*, Pierre Burg

C *Nouvelles histoires hédonistes de groupes et géométries*, P. Caldero, J. Germoni

120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

Dans toute la leçon, $n \in \mathbb{N} \setminus \{0,1\}$ et p est un nombre premier.

I. L'anneau $\mathbb{Z}/n\mathbb{Z}$

A. Rappels d'arithmétique des entiers

Théorème 1 (division euclidienne - [R] 279)**.** $\forall (a,b) \in \mathbb{Z}^2$, $\exists ! (q,r) \in \mathbb{Z}^2$:

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

Définition 2 ([R] 279)**.** *Soit $(a,b) \in \mathbb{Z}^2$. On dit que a est* congru *à b modulo n, et on note $a \equiv b\,[n]$ si n divise $b-a$.*

Proposition 3 ([R] 280)**.** *Soit $(a,b,c,d) \in \mathbb{Z}^4$ tel que $a \equiv b\,[n]$ et $c \equiv d\,[n]$. Alors $a+c \equiv b+d\,[n]$ et $ac \equiv bd\,[n]$.*

B. Construction

Lemme 4. *Tout idéal de $\mathbb{Z}$ est principal, et admet un unique générateur positif.*

Définition 5 ([R] 280)**.** *Le quotient de l'anneau $(\mathbb{Z},+,\times)$ par son idéal $n\mathbb{Z}$ est l'anneau noté $\mathbb{Z}/n\mathbb{Z}$. On note $\overline{a}$ l'image de $a \in \mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.*

Remarque 6. $\overline{a} = \overline{b} \iff a \equiv b\,[n]$

Proposition 7 ([R] 280)**.** $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$, *et les lois sont données par Prop 3 et Rq 6.*

Exemple 8. $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\} = \{\overline{9}, \overline{64}, \overline{-7}\}$, *et on a* $\overline{1} + \overline{2} = \overline{1+2} = \overline{3} = \overline{0}$, *mais aussi* $\overline{1} \times \overline{2} = \overline{1 \times 2} = \overline{2}$.

C. Structure d'anneau

Proposition 9 ([R] 283)**.** *L'ensemble des inversibles $\mathbb{Z}/n\mathbb{Z}$ est :*

$$(\mathbb{Z}/n\mathbb{Z})^{\times} = \left\{\overline{k} \in \mathbb{Z}/n\mathbb{Z} \mid k \wedge n = 1\right\}$$

L'ensemble des diviseurs de O de $\mathbb{Z}/n\mathbb{Z}$ est :

$$D_0\left(\mathbb{Z}/n\mathbb{Z}\right) = \mathbb{Z}/n\mathbb{Z} \setminus \left[(\mathbb{Z}/n\mathbb{Z})^{\times} \cup \{0\}\right]$$

Exemple 10. $(\mathbb{Z}/8\mathbb{Z})^{\times} = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, *et* $D_0\left(\mathbb{Z}/8\mathbb{Z}\right) = \{\overline{2}, \overline{4}, \overline{6}\}$.

Proposition 11 ([R] 241 et 281)**.** *Les idéaux propres de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$ avec $d \mid n$, $d \notin \{1,n\}$. De plus,* $(d\mathbb{Z}/n\mathbb{Z},+) \cong \left(\mathbb{Z}/\frac{n}{d}\mathbb{Z},+\right)$.

Corollaire 12. *$\mathbb{Z}/n\mathbb{Z}$ est principal.*

Corollaire 13. *L'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$ est $(\mathbb{Z}/n\mathbb{Z})^{\times}$.*

Exemple 14. *Les idéaux propres de $\mathbb{Z}/6\mathbb{Z}$ sont $2\mathbb{Z}/6\mathbb{Z}$ et $3\mathbb{Z}/6\mathbb{Z}$, respectivement isomorphes à $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$.*

Proposition 15 ([R] 295-282)**.** $\forall n, m \geq 2$,

$$\mathrm{Hom}_{gr}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n \wedge m)\mathbb{Z},$$

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^{\times},$$

$$\mathrm{Hom}_{Ann}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \begin{cases} \{k \textit{ mod } n \mapsto k \textit{ mod } m\} & \textit{si } m \mid n \\ \emptyset \quad \textit{sinon} \end{cases}$$

D. Le corps $\mathbb{Z}/p\mathbb{Z}$

Théorème 16. *Les assertions suivantes sont équivalentes :*

1. *$\mathbb{Z}/n\mathbb{Z}$ est un corps ;*
2. *$\mathbb{Z}/n\mathbb{Z}$ est intègre ;*
3. *n est premier.*

Corollaire 17 ([R] 292)**.** $(\mathbb{Z}/p\mathbb{Z})^{\times} \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Contre-exemple 18. *C'est très faux pour n non premier !* $(\mathbb{Z}/8\mathbb{Z})^{\times} = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ *n'a même pas 7 éléments !*

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

A. Préambule : le théorème des restes chinois

Théorème 19 (des restes chinois - [R] 285)**.** *Soit $(a_1, \dots, a_d) \in (\mathbb{N} \setminus \{0,1\})^d$. Les entiers, $a_1, \dots, a_d$ sont deux à deux premiers si, et seulement si, les anneaux $\mathbb{Z}/a_1 \dots a_d\mathbb{Z}$ et $\mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_d\mathbb{Z}$ sont isomorphes.*
Le cas échéant, il existe $(u_1, \dots, u_d) \in \mathbb{Z}^d$ tel que $\sum_{i=1}^d a_i b_i = 1$, où $b_i = \frac{a_1 \dots a_d}{a_i}$. L'application :

$$\begin{aligned} \overline{\varphi} : \mathbb{Z}/a_1 \dots a_d\mathbb{Z} &\to \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_d\mathbb{Z} \\ x \,\mathrm{mod}\, a_1 \dots a_d &\mapsto (x \,\mathrm{mod}\, a_1, \dots, x \,\mathrm{mod}\, a_d) \end{aligned}$$

est un isomorphisme d'anneaux, de réciproque :

$$\overline{\varphi}^{-1} : (x_1 \,\mathrm{mod}\, a_1, \dots, x_d \,\mathrm{mod}\, a_d) \mapsto \sum_{i=1}^d x_i a_i b_i \,\mathrm{mod}\, a_1 \dots a_d$$

B. Fonction indicatrice d'Euler

Définition 20 ([R] 283)**.** L'indicatrice d'Euler *est :* $\varphi : n \mapsto \#\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times} = \#\left\{k \in [\![1,n]\!] \mid k \wedge n = 1\right\}$.

Exemple 21. $\varphi(8) = 4$ *d'après Exemple 10.*

Proposition 22 ([R] 288)**.** *Si $a \wedge b = 1$, alors $\varphi(ab) = \varphi(a)\varphi(b)$. Pour tout $\alpha \in \mathbb{N}^*$, $\varphi(p^{\alpha}) = p^{\alpha-1}(p-1)$.*

Corollaire 23 ([R] 288)**.** *Si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ est la décomposition de n en produit de facteurs premiers, alors :*

$$\varphi(n) = \prod_{i=1}^r p^{\alpha_i - 1}(p-1) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

Exemple 24. $\varphi(90) = \varphi(3^2)\varphi(2)\varphi(5) = 3(3-1)(2-1)(5-1) = 24$

Théorème 25 (d'Euler - [R] 283)**.** *Si $a \wedge n = 1$, alors $a^{\varphi(n)} \equiv 1\,[n]$.*

Théorème 26 (de Fermat - [R] 284)**.** *Si $a \wedge p = 1$, alors $a^{p-1} = 1\,[p]$. De manière générale, $a^p \equiv a\,[p]$.*

Proposition 27 ([R] 284)**.**

$$n = \sum_{d \mid n} \varphi(d)$$

Théorème 28 ([R] 292)**.** *Si $p \geq 3$, alors $\forall \alpha \geq 1$, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.*

Théorème 29 (ADMIS - [R] 294)**.** *$(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si, et seulement si, $n \in \{2, 4, p^\alpha, 2p^\alpha\}$ avec $p \geq 3$ (premier) et $\alpha \geq 1$.*

III. Applications

A. Résolution de systèmes de congruence

Théorème 30 ([R] 290)**.** *L'équation $ax \equiv b\,[n]$ d'inconnue $x \in \mathbb{Z}$ admet des solutions si, et seulement si, $a \wedge n \mid b$.*

Le cas échéant, $S(ax \equiv b\,[n]) = \frac{b}{a\wedge n}x_0 + \frac{n}{a\wedge n}\mathbb{Z}$, où x_0 est une solution particulière de l'équation.

Remarque 31. *Le théorème des restes chinois permet de résoudre des systèmes de congruences.*

Exemple 32 ([R] 291)**.** $S\left(\begin{cases} x \equiv 2\,[4] \\ x \equiv 3\,[5] \\ x \equiv 1\,[9] \end{cases}\right) = 118 + 180\mathbb{Z}$

Remarque 33 ([R] 291)**.** $S\left(\begin{cases} x \equiv x_1\,[a_1] \\ x \equiv x_2\,[a_2] \end{cases}\right) = \begin{cases} \emptyset & \text{si } a_1 \wedge a_2 \nmid x_1 - x_2 \\ x_0 + (a_1 \vee a_2)\mathbb{Z} & \text{sinon} \end{cases}$

B. Carrés de $\mathbb{Z}/p\mathbb{Z}$

Soit $c : \overline{x} \in \mathbb{Z}/p\mathbb{Z} \mapsto \overline{x}^2$. On s'intéresse à $\operatorname{Im} c$.

Proposition 34. *Tous les éléments de $\mathbb{Z}/2\mathbb{Z}$ sont des carrés.*

On supposera désormais $p \geq 3$.

Proposition 35 ([R] 426)**.** *Soit $l : \overline{x} \in \mathbb{Z}/p\mathbb{Z} \mapsto \overline{x}^{\frac{p-1}{2}}$.*

- *$\forall \overline{x} \in \mathbb{Z}/p\mathbb{Z}$, $c \circ l(\overline{x}) = l \circ c(\overline{x}) = \overline{1}$*
- *$\operatorname{Ker} c = \operatorname{Im} l = \{\pm 1\}$ et $\operatorname{Im} c = \operatorname{Ker} l$.*

Corollaire 36. *Il y a $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$.*

Théorème 37 (de Wilson - [R] 325)**.** *n est premier $\iff (n-1)! \equiv -1\,[n]$*

Proposition 38 ([P] 75)**.** *-1 est un carré modulo p si, et seulement si, $p \equiv 1\,[4]$. Le cas échéant $-1 \equiv (2 \times 3 \times \cdots \times \frac{p-1}{2})^2\,[p]$.*

Théorème 39 (des deux carrés de Fermat - [P] 56)**.** *p s'écrit comme somme de deux carrés d'entiers si, et seulement si, $p = 2$ ou $p \equiv 1\,[4]$.*

C. Algorithme de chiffrement RSA

Algorithme 40 ([G] 37)**.** *Alice veut envoyer à Bob un message représenté par un nombre entier m, en tout sécurité.*

- *Bob choisit en secret deux nombres premiers distincts p et q et calcule leur produit $n = pq$.*
- *Il choisit ensuite un entier $c < \varphi(n) = (p-1)(q-1)$ premier à $\varphi(n)$.*
- *Il trouve ensuite un entier d tel que $cd \equiv 1\,[\varphi(n)]$.*
- *La clé publique de Bob est (n, c), qu'il donne à Alice, et sa clé privée est (n, d), qu'il garde secrète.*
- *Alice envoie à Bob le message $m^c \bmod n$.*
- *Pour décoder le message, Bob calcule $(m^c)^d \equiv m\,[n]$.*

Développements

- Développement 1 : Théorème 19 (restes chinois) et exemple 32
- Développement 2 : Théorème 28 (cyclicité des inversibles de $\mathbb{Z}/p^\alpha\mathbb{Z}$)

Références

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

P *Cours d'algèbre*, Perrin

G *Les maths en tête - Algèbre et probabilités*, Xavier Gourdon, 3e édition

121 : Nombres premiers. Applications.

Pour un entier n, $\mathrm{Div}(n)$ désigne l'ensemble des diviseurs positifs de n.

I. Résultats fondamentaux sur les nombres premiers

A. Notion de nombre premier, propriétés élémentaires

Définition 1 ([R] 303). *On dit que $p \in \mathbb{N}$ est* premier *si* $\mathrm{Div}(p) = \{1, p\}$. *On dit que n est* composé *si $n \neq 0$ et si $\exists a \in \mathbb{N} \setminus \{1, n\} : a \mid n$.*

Dans la suite, $\mathcal{P}$ désignera l'ensemble des nombres premiers.

Lemme 2 (d'Euclide). *$\forall (a,b) \in \mathbb{N}^2$, $\forall p \in \mathcal{P}$, $p \mid ab \implies (p \mid a)$ ou $(p \mid b)$.*

Lemme 3 ([R] 303). *$\forall n \geq 2$, $\exists p \in \mathcal{P} : p \mid n$*

Proposition 4 ([R] 304). *Tout entier composé n admet un facteur premier entre 2 et $\sqrt{n}$.*

Théorème 5 (fondamental de l'Arithmétique - [R] 306). *$\forall n \in \mathbb{N}^*$, $\exists! \left(v_p(n)\right)_{p \in \mathcal{P}} \in \mathbb{N}^{\mathcal{P}}$:*

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

Cette écriture est appelée "(la) décomposition en produit de facteurs premieres de n"*.*

Définition 6 ([R] 306). *Dans la décomposition en produit de facteurs premiers de n, l'entier $v_p(n)$ ($p \in \mathcal{P}$) est appelé* valuation p-adique de n*.*

Proposition 7 ([R] 307). *$\forall (a,b) \in (\mathbb{N}^*)^2$, $a \mid b \iff \forall p \in \mathcal{P}$, $v_p(a) \leq v_p(b)$*

Proposition 8 ([R] 319). *$\forall (a,b) \in (\mathbb{N}^*)^2$, $v_p(ab) = v_p(a) + v_p(b)$*

Proposition 9 ([R] 307). *$\forall (a,b) \in (\mathbb{N}^*)^2$, $\forall p \in \mathcal{P}$,*

$$v_p(a \vee b) = \max(v_p(a), v_p(b))$$
$$v_p(a \wedge b) = \min(v_p(a), v_p(b))$$

B. Répartition des nombres premiers

Théorème 10 (Euclide - [R] 305). *Il existe une infinité de nombres premiers.*

Théorème 11 (de la progression arithmétique, Dirichlet, ADMIS). *Pour tout $(a,b) \in (\mathbb{N}^*)^2$ tel que $a \wedge b = 1$, il existe une infinité de nombres premiers congrus à a modulo b.*

Conjecture 12 (des nombres premiers jumaux). *Il existe une infinité de nombres premiers p tels que $p+2$ est premier.*

Proposition 13. *Il existe des intervalles de longueur arbitrairement grande ne contenant aucun nombre premier.*

Théorème 14 (Bertrand - ADMIS - [R] 325). *Il existe toujours un nombre premier compris entre n'importe quel entier naturel non nul et son double.*

Théorème 15 (des nombres premiers - ADMIS - [R] 308).

$$\#\mathcal{P} \cap [\![1, n]\!] \sim_{x \to +\infty} \frac{n}{\ln n}$$

II. Tests de primalité

Proposition 16 (Crible d'Ératosthène - ANNEXE). *Le procédé suivant permet de trouver la liste croissante des nombres premiers : on part de la liste des entiers plus grands que 2. À chaque itération, on garde le plus petit nombre, et on supprime tous ses multiples.*

Proposition 17. *n est premier si, et seulement si, $\forall d \leq \lfloor \sqrt{n} \rfloor$, $d \nmid n$. La complexité au pire de ce test est donc en $O(\sqrt{n})$.*

Théorème 18 (de Fermat). *Si p est premier, alors $\forall a \in \mathbb{N}$, $a \wedge p = 1 \implies a^{p-1} \equiv 1\,[p]$.*

Remarque 19. *On en déduit donc un test de non primalité.*

Définition 20 ([R] 329). *Un nombre n composé satisfaisant le test du théorème de Fermat est appelé* nombre de Carmichaël.

Exemple 21 ([R] 329). *561 est un nombre de Carmichaël.*

Théorème 22 (de Korselt - [R] 330). *n est un nombre de Carmichaël si, et seulement si, pour tout diviseur premier p de n, $(p-1) \mid (n-1)$ et $p^2 \nmid n$.*

Théorème 23 (de Wilson - [R] 326). *n est premier si, et seulement si, $(n-1)! \equiv -1\,[n]$. C'est un test de primalité qui requiert $n-1$ multiplications dans $\mathbb{Z}/n\mathbb{Z}$.*

III. Applications des nombres premiers

A. Fonctions spéciales

Définition 24 ([R] 283). L'indicatrice d'Euler *est : $\varphi : n \mapsto \#\left(\mathbb{Z}/n\mathbb{Z}\right)^\times = \#\{k \in [\![1, n]\!] \mid k \wedge n = 1\}$.*

Proposition 25 ([R] 288). *$\forall (a,b) \in (\mathbb{N}^*)^2$, $a \wedge b = 1$, alors $\varphi(ab) = \varphi(a)\varphi(b)$. Pour tout $\alpha \in \mathbb{N}^*$, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.*

Corollaire 26 ([R] 288). *$\forall n \in \mathbb{N}^*$,*

$$\varphi(n) = \prod_{\substack{p \in \mathcal{P} \\ v_p(n) \geq 1}} p^{v_p(n)-1}(p-1) = n \prod_{\substack{p \in \mathcal{P} \\ v_p(n) \geq 1}} \left(1 - \frac{1}{p}\right)$$

Définition 27. *La* fonction ζ de Riemann *est définie par :*

$$\zeta : \{z \in \mathbb{C} \mid \Re(z) > 1\} \to \mathbb{C}$$
$$s \mapsto \sum_{n=0}^{+\infty} \frac{1}{n^s}$$

Proposition 28 ([KG] 461). *On a :*

$$\zeta(s) = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^s}}$$

Cette écriture est appelé "produit eulérien"*.*

Théorème 29 ([KG] 461, [R] 343). $\sum_{p \in \mathcal{P}} \frac{1}{p} = +\infty$

Définition 30 ([R] 331). *La* fonction de Moëbius *est définie par :*

$$\mu : n \in \mathbb{N}^* \mapsto \begin{cases} 1 & si\ n = 1 \\ (-1)^r & si\ n = p_1 \dots p_r,\ avec\ p_1, \dots, p_r\ distincts \\ 0 & sinon \end{cases}$$

Théorème 31 (Cesàro - ADMIS [R] 334). *La probabilité de choisir au hasard $r \geq 2$ entiers entre 1 et n qui sont premiers entre eux vaut $\frac{1}{\zeta(r)}$.*

B. Algorithme de chiffrement RSA

Théorème 32 (d'Euler - [R] 283). *$\forall (a,b) \in (\mathbb{N}^*)^2$, si $a \wedge n = 1$, alors $a^{\varphi(n)} \equiv 1\,[n]$.*

De la complexité des tests de primalité découle la grande difficulté de la recherche de la décomposition en produit de facteurs premiers d'un entier donné. Ce principe est à la base de la sécurité de l'algorithme de chiffrement RSA, détaillé ci-dessous :

Algorithme 33 ([G] 37). *Alice veut envoyer à Bob un message représenté par un nombre entier m, en tout sécurité.*

- *Bob choisit en secret deux nombres premiers distincts p et q et calcule leur produit $n = pq$.*
- *Il choisit ensuite un entier $c < \varphi(n) = (p-1)(q-1)$ premier à $\varphi(n)$.*
- *Il trouve ensuite un entier d tel que $cd \equiv 1\,[\varphi(n)]$.*
- *La clé publique de Bob est (n, c), qu'il donne à Alice, et sa clé privée est (n, d), qu'il garde secrète.*
- *Alice envoie à Bob le message m^c mod n.*
- *Pour décoder le message, Bob calcule $(m^c)^d \equiv m\,[n]$.*

C. Corps finis

Définition 34 ([R] 415). *La* caractéristique *d'un anneau A est l'unique générateur positif du noyau du morphisme $\varphi : \mathbb{Z} \to A$, $n \mapsto n1_A$.*

Lemme 35 ([R] 415). *La caractéristique d'un corps est nulle ou première.*

Exemple 36. *$\mathbb{Z}/p\mathbb{Z}$ est un corps de caractéristique p.*

Théorème 37 ([R] 421). *Il existe un corps fini de cardinal q si, et seulement si, q est une puissance d'un nombre premier. Le cas échéant, un tel corps est unique à isomorphisme près, et on note $\mathbb{F}_q$ le corps fini à q éléments. Par ailleurs, $p = \operatorname{car} \mathbb{F}_q$ est un nombre premier, et q est une puissance de p.*

D. Le théorème des deux carrés de Fermat

Lemme 38 ([P] 75). *-1 est un carré dans $\mathbb{F}_p$ si, et seulement si, $p \equiv 1\,[4]$.*

Théorème 39 (des deux carrés de Fermat - [P] 56). *Soit $E = \left\{ n \in \mathbb{N}^* \mid \exists (a,b) \in \mathbb{N}^2 : n = a^2 + b^2 \right\}$ Alors, $n \in E \iff \forall p \in \mathcal{P},\, p \equiv 3\,[4] \implies v_p(n)$ est pair.*

E. En théorie des groupes

Définition 40 ([R] 22). *Un p-groupe est un groupe de cardinal une puissance de p.*

Proposition 41 ([R] 22). *Si un p-groupe G agit sur un ensemble fini X, alors $\#X \equiv \#X^G\,[p]$ où X^G est l'ensemble des éléments de X fixes par l'action de G.*

Corollaire 42 ([R] 23). *Le centre d'un p-groupe n'est pas trivial.*

Définition 43 ([U] 85). *Soit G un groupe fini de cardinal $p^\alpha m$, $m \wedge p = 1$. Un p-Sylow de G est un sous-p-groupe de G de cardinal p^α.*

Théorème 44 (de Sylow - ADMIS [U] 87). *Soit G un groupe d'ordre $p^\alpha m$, $m \wedge p = 1$. Alors,*

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

Théorème 45 ([R] 292). *Si $p \geq 3$, alors $\forall \alpha \geq 1$, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.*

Proposition 46 ([R] 23). *Tout groupe d'ordre p^2 est abélien.*

Développements

- Développement 1 : Lemme 38, et théorème 39
- Développement 2 : Théorème 45 (cyclicité des inversibles de $\mathbb{Z}/p^\alpha\mathbb{Z}$)

Références

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

U *Théorie des groupes*, Félix Ulmer

G *Les maths en tête - Algèbre et probabilités*, Xavier Gourdon, 3e édition

KG *De l'intégration aux probabilités*, Olivier Garet, Aline Kurtzmann, 2e édition augmentée

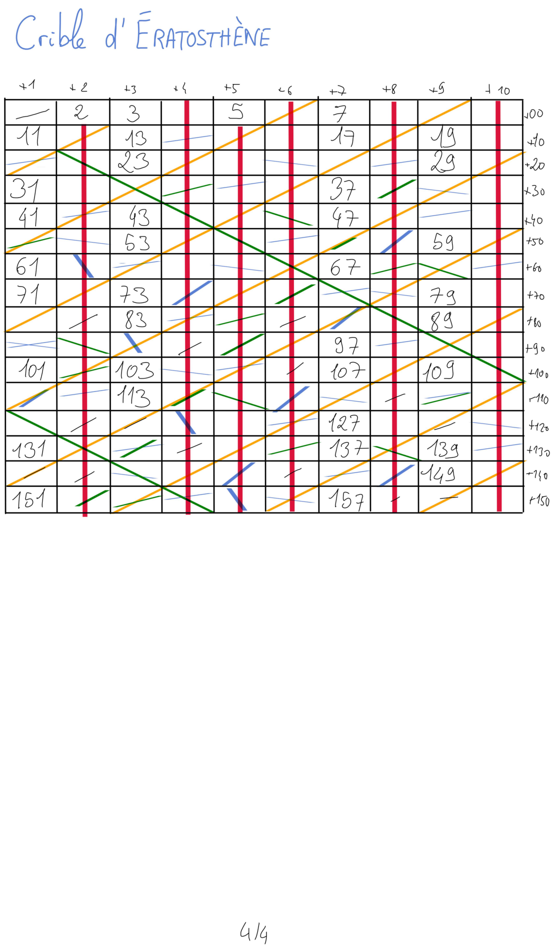


FIGURE 1.2 – Crible d'Eratosthène