108
Exemples de parties génératrices d'un groupe. Applications.

**Refs.** [Perr] Perrin, cours d'Algèbre [Cal 1] Calais, Théorie des groupes. [Gou 1] Gourdon, Algèbre, [Ulm] Ulmer, Théorie des groupes [FGNA2] Oraux X-Ens 2. [FGNA3] Oraux X-Ens 3 [Aud] Audin, Géométrie.

**Devt:**
Générateurs $GL$ $SL$ ($SO_3(\mathbb{R})$ simple. (64).
Générateurs $O$, $O^+$ (62, 63)

Par défaut, $X$ désignera un ensemble non vide, et $G$ un groupe.

# I. Parties génératrices, relations.

## 1) Sous groupe engendré par une partie.

[Perr] 10

**Def 1**: Soit $A \subseteq G$ une partie de $G$, on appelle sous groupe de $G$ engendré par $A$ l'intersection des sous groupes de $G$ contenant $A$. On le note $\langle A\rangle$.

**Prop 2**: Le groupe $\langle A\rangle$ est le plus petit sous groupe de $G$ contenant $A$. Ses éléments sont les produits finis d'éléments de $A$ et de leurs inverses.

**Def 3** On dit que $A \subseteq G$ engendre $G$ si $\langle A\rangle = G$. On dit que $G$ est de type fini s'il possède une partie génératrice finie.

**Ex 4**: $\langle 1\rangle = \mathbb{Z}$, $\langle \bar{1}^n\rangle = \mathbb{Z}/n\mathbb{Z}$.

[Perr] 13

**Ex 5**: Le groupe dérivé $D(G)$ de $G$ est le sous-groupe de $G$ engendré par les commutateurs : les éléments de $G$ de la forme $xyx^{-1}y^{-1}$ $x, y \in G$.

**Rq 6**: Le groupe dérivé de $G$ est le plus petit sous groupe de $G$ tel que $G/D(G)$ soit un groupe abélien ($G/D(G)$ est l'abélianisé de $G$).
On a $D(G) = \{1\}$ ssi $G$ est abélien. $D(\mathfrak{S}_n) = \mathfrak{A}_n$ pour $n \geq 5$.

## 2) Notion de groupe libre.

[Cal1] 329 341

**Def 8**: Soit $F$ un groupe. On dit que $F$ est libre sur $X$ si l'on a une injection $X \xrightarrow{i} F$ et si les applications $X \xrightarrow{f} G$ correspondent bijectivement aux morphismes $F \xrightarrow{\varphi} G$ avec $\varphi \circ i = f$.

**Ex 8**: $\mathbb{Z}$ est libre sur $\{1\}$. $\mathbb{Z}/n\mathbb{Z}$ n'est pas libre sur $\{\bar{1}\}$.

**Prop 9** Deux groupes libres sur un même ensemble sont canoniquement isomorphes.

**Théo 10**: Il existe un groupe libre pour tout ensemble $X$.

**Théo 11**: Tout groupe s'écrit comme quotient d'un groupe libre

**Rq 12** Une telle écriture n'est pas unique, on notera en général $G = (H|N)$ où $H$ est un ensemble de générateurs et $N$ le quotienteur, $N$ sont les relations satisfaites par les éléments de $H$.

**Appli 13** produit libre et somme amalgamée de groupes.

**Ex 14**: $\mathbb{Z}/n\mathbb{Z} = \langle 1 \mid n.1 = 0\rangle$.

# II Cas des groupes abéliens

Dans cette partie, $G$ est supposé abélien

## 1) Groupes monogènes et cycliques.

[Gou 1] 19.

**Def 15**: $G$ est dit monogène s'il admet un singleton pour partie génératrice. Si $G$ est de plus fini, on dit que $G$ est cyclique.

**Prop 16**: Tout groupe monogène est abélien, la classe d'isomorphisme est entièrement caractérisée par son cardinal.

**Ex 17**: Tout sous groupe de $\mathbb{Z}$ est monogène et isomorphe à $\mathbb{Z}$.

**Rq 18**: Si $G$ est monogène, alors
- Si $G$ infini, $G = \langle 1\rangle$ (groupe libre
- Si $G$ est d'ordre $n$, $G = (a \mid a^n = 1) \simeq \mathbb{Z}/n\mathbb{Z}$.

[Cal 1] 83.

**Prop 19**: L'image d'un groupe monogène par un morphisme de groupes est un groupe monogène.

[Gou 1]

**Prop 20**: Dans $\mathbb{Z}$, $(m,n) = m\mathbb{Z} + n\mathbb{Z} = (n,m)\mathbb{Z}$.

**Prop 21**: Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les classes d'entiers premiers avec $n$. On a donc $\varphi(n)$ générateurs.

**Appl 22** $\mathbb{U}_n$ le groupe des racines de l'unité est engendré par les racines primitives de l'unité.

[Perr] 24, 74

**Prop 23**: Les automorphismes de $\mathbb{Z}/n\mathbb{Z}$ sont les multiplications par des classes d'entiers premiers avec $n$ : on a $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}$.

**Théo 24**: Tout sous groupe fini de $K^{\times}$ ou $K$ est un corps est cyclique.

## 2) Groupes abéliens finis, de type fini.

[Cal 1] 293.

**Théo 25**: (Restes chinois) Si $p$ et $q$ sont des entiers premiers entre eux on a un isomorphisme $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Dans la suite, on fixe $G$ abélien de type fini

**Def 26**: Un élément de $G$ sera dit de torsion s'il est d'ordre fini

**Prop 27** L'ensemble des éléments de torsion de $G$ forme un sous groupe noté $T(G)$, $G/T(G)$ est abélien sans éléments de torsion

**Théo 28** Si $G$ est sans torsion, alors $G$ est isomorphe à un produit de $n$ copie de $\mathbb{Z}$, on dit que $n$ est le rang de $G$ et que $G$ est un groupe abélien libre

**Rq 29**: Un groupe abélien libre de rang $n$ n'est pas un groupe libre, mais donné par $(a_1 \dots a_n \mid a_i a_j = a_j a_i \ \forall i, j)$.

[Cal1] 293-310.

Prop 30 : Soient $G, G'$ de type fini abélien, on a $T(G) \simeq T(G')$ et $G/T(G) \simeq G'/T(G')$ ssi $G \simeq G'$.

Théo 31 : Un sous groupe d'un groupe abélien de type fini est de type fini.

Théo 32 (Structure des groupes abéliens de type fini)
Si $G$ est abélien de type fini, il existe $r, d_1, \dots, d_s \in \mathbb{N}$ tels que

$$G \simeq \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$$

$d_i > 1$

avec $d_i \mid d_{i+1}$ pour $i \leq s-1$, les $d_i$ et $r$ sont uniques avec ces propriétés.

Ex 33 : $\mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/360\mathbb{Z}$ (restes chinois).

Ex 34 : Si $|G| = 600$, la liste des invariants possibles est donnée par :
$(600)$, $(5,120)$, $(10,60)$, $(2,2,150)$, $(2,10,30)$.

# II Groupes symétriques, diédraux

## 1) Groupe symétrique.

[Ulm] 41-48.

Déf 35 : Pour $n \geq 1$ un entier, on pose $\mathfrak{S}_n$ le groupe des bijections de l'ensemble $[\![1,n]\!]$ (la classe d'iso ne dépend que de $n$). C'est le groupe symétrique sur $n$ éléments. On a $|\mathfrak{S}_n| = n!$.

Déf 36 : Soit $\sigma \in \mathfrak{S}_n$. On appelle support de $\sigma$ l'ensemble $\{k \leq n \mid \sigma(k) \neq k\}$.

Déf 37 : Soit $1 \leq l \in \mathbb{N}$, et $i_1 \dots i_l$ des éléments distincts de $[\![1,n]\!]$. La permutation $\gamma$ définie par

$$\gamma(j) = \begin{cases} j & \text{si } j \notin \{i_1 \dots i_l\} \\ i_{k+1} & \text{si } j = i_k \text{ avec } k < l \\ i_1 & \text{si } j = i_l \end{cases}$$

est appelée cycle (de longueur $l$) et notée $(i_1\, i_2 \dots i_l)$. Un cycle de longueur 2 est une transposition. + les $n$-cycles sont conjugués dans $\mathfrak{S}_n$

Théo 38 : Les cycles engendrent $\mathfrak{S}_n$, plus précisément toute permutation se décompose en produit de cycles à supports disjoints, cette décomposition est unique à permutation des facteurs près.

Appli 39 Classes de conjugaison de $\mathfrak{S}_n$.

Théo 40 Les transpositions engendrent $\mathfrak{S}_n$, plus précisément les transpositions $(1,i)$ pour $1 \leq i \leq n$ suffisent.

$(i, i+1)$ + Tri à bulle + exemple décompo.

[Ulm] 48-53

Prop déf 41 Il existe un unique morphisme $\mathfrak{S}_n \to \mathbb{C}^*$, la signature, on note $\mathfrak{A}_n$ le noyau de ce morphisme, on a $|\mathfrak{A}_n| = n!/2$.

Prop 42 : Le groupe $\mathfrak{A}_n$ est engendré par les 3-cycles pour $n \geq 3$.

Appli 43 Le groupe $\mathfrak{A}_n$ est simple pour $n \geq 5$.

Prop 44 : Le groupe $\mathfrak{S}_n$ est engendré par $(1,2)$, $(1,2,\dots,n)$.

Cor 45 : Pour $n \geq 5$, $D(\mathfrak{A}_n) = \mathfrak{A}_n$ et $D(\mathfrak{S}_n) = \mathfrak{A}_n$.

## 2) Groupe diédral.

[Cal1] 120-125.

Déf 46 : On note $D_n$ le sous groupe des isométries affines du plan euclidien préservant un $n$-gone régulier.

Prop 47 : $D_n$ est d'ordre $2n$, et engendré par $s$ et $r$, où $s$ est une symétrie axiale et $r$ une rotation d'angle $2\pi/n$. On a en fait la présentation

$$D_n = \langle s, r \mid s^2 = 1,\ r^n = 1,\ (sr)^2 = 1 \rangle$$

Rq 48 On a également $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

Rq 49 : Pour donner un morphisme $D_n \to GL_n(\mathbb{C})$, il suffit de trouver des matrices respectant la présentation de $D_n$ (utile pr les tables de caractères).

# III. Générateurs en algèbre linéaire.

## 1) Groupes linéaires et spéciaux linéaires.

[Per] 95-96.

On fixe $k$ un corps et $E$ un $k$-espace vectoriel de dimension $n$. On rappelle que $GL(E)$ est le groupe des $k$-automorphismes de $E$, il s'identifie non canoniquement à $GL_n(k)$.

Prop 50 : L'application déterminant $GL(E) \to k^\times$ est un morphisme de groupes, on note $SL(E)$ son noyau, le groupe spécial linéaire, on a $GL(E) \simeq SL(E) \rtimes k^*$.

Prop déf 51 : Soit $H$ un hyperplan de $E$, et $u \in GL(E)$ tel que $u_{|H} = Id_H$. Les conditions suivantes s'équivalent

(i) On a $\det u = \lambda \neq 1$ (ie $u \notin SL(E)$)

(ii) $u$ admet une valeur propre $\lambda \neq 1$ (donc une droite propre $D$ pour $\lambda$) et $u$ est diago

(iii) On a $\mathrm{Im}(u - Id) \not\subset H$

(iv) Dans une bonne base, $u$ a pour matrice celle de Fig 1 ($\lambda \in k^*$, $\lambda \neq 1$).

On dit alors que $u$ est une dilatation d'hyperplan $H$, de droite $D$, de rapport $\lambda$. On a alors $D = \mathrm{Im}(u - Id)$, $H = \mathrm{Ker}(u - Id)$. Quand $\lambda = -1$ et $\mathrm{car}(k) \neq 2$, on dit que $u$ est une réflexion.

Prop def 52. Soit $H$ un hyperplan de $E$, d'équation $f \in E^*$, $u \in Gl(E)$, $u \neq Id$ tel que $u_{|H} = Id_H$. Les conditions suivantes sont équivalentes

(i) On a $\det u = 1$ (i.e $u \in SL(E)$)

(ii) $u$ n'est pas diagonalisable

[Perr] 96-99 101-102

(iii) on a $\underbrace{Im(u-Id)}_{=D} \subseteq H$

(iv) Le morphisme induit $E/H \to E/H$ est l'identité

(v) $\exists a \in H \setminus \{0\}$ tel que l'on ait $\forall x \in E$, $u(x) = x + f(x)a$.

(vi) Dans une base convenable, $u$ a pour matrice celle de Fig 2.

On dit alors que $u$ est une transvection d'hyperplan $H$ et de droite $D$, avec les notations ci-dessus, $D = (a)$ et $D \subseteq H$.

Prop 53 : Soit $\tau$ une transvection de droite $D$ et d'hyperplan $H$, et soit $u \in Gl(E)$. Alors $u \tau u^{-1}$ est une transvection de droite $u(D)$ et d'hyperplan $u(H)$.

Théo 54 : Le centre de $Gl(E)$ est constitué des homothéties, donc isom à $k^*$. Le centre de $Sl(E)$ et $Z(Gl(E)) \cap Sl(E)$, isom à $\mu_n(k) = \{\lambda \in k \mid \lambda^n = 1\}$.

Prop 55. Soit $u \in Gl(E)$, si $u$ fixe toutes les droites vectorielles alors $u$ est une homothétie.

Théo 56 : Les transvections engendrent $Sl(E)$, les transvections et dilatations engendrent $Gl(E)$. • Ex : Pivot de Gauss. • Ex de découpe DVP

Prop 57 : Deux dilatations sont conjuguées dans $Gl(E)$ ssi elles ont m̂ rapport. Deux transvections sont conjuguées dans $Gl(E)$, si $n \geq 3$, elles le sont aussi dans $Sl(E)$.

Théo 58 : 1) $D(Gl_n(k)) = Sl_n(k)$ sauf si $n=2$ et $k = \mathbb{F}_2$

2) $D(Sl_n(k)) = Sl_n(k)$ sauf si $n=2$ et $k = \mathbb{F}_2$ ou $n=2$ et $\mathbb{F}_3 = k$.

[FGNA2] 177

Appl 59 : $Sl_n(k)$ est connexe par arcs pour $k \in \{\mathbb{R}, \mathbb{C}\}$.

## 2) Groupe orthogonal.

[Perr] 125.

Def 60 : Soit $u \in Gl(E)$, telle que $u^2 = Id_E$, il existe $E^+$, $E^-$ des sous-espaces de $E$ avec

1) $E = E^+ \oplus E^-$ 2) $u_{|E^+} = Id_{E^+}$ $u_{|E^-} = -Id_{E^-}$ Dans une certaine base, la matrice de $u$ est donnée par Fig 3

Si $\dim E^- = 1$, on retrouve les réflexions.

Si $\dim E^- = 2$, on parle de renversement.

Si $\dim E^- > 0$, on parle de symétrie.

On se fixe un $n$ $K$ev ($K = \mathbb{R}$ ou $\mathbb{C}$) muni du prod scal usuel.

[Perr] 143

Théo 61 : Le centre de $O(q)$ est $Z = \{\pm Id\}$, en particulier, pour $n \geq 2$, $O(q)$ n'est pas abé.

Pour $n \geq 3$, $Z(O^+(q)) = Z(O(q)) \cap O^+(q)$ : $\{I_n\}$ si $n$ impair, $\{\pm I_n\}$ si $n$ pair

Théo 62 : Le groupe $O(q)$ est engendré par les réflexions orthogonales, plus prec, si $u \in O(q)$, $u$ est produit d'au plus $n$ réflexions.

Théo 63 : Pour $n \geq 3$, $O^+(q)$ est engendré par les renversements (au + $n$). DVP

[FGNA3] 67

Appl 64 $O_3^+(\mathbb{R})$ est simple. DVP

[Perr] 144

Prop 65 : Pour $n \geq 2$, $D(O(q)) = O^+(q)$

$n \geq 3$ $D(O^+(q)) = O^+(q)$.

## 3) Homographies sur la droite projective $PGl(E)$, $PSl(E)$.

[Perr] 99

Def 66 : Le quotient $Gl(E)/Z(Gl(E))$ est noté $PGl(E)$, de même, le quotient de $Sl(E)$ par son centre est noté $PSl(E)$.

[Aud] 201

Prop 67 : $PGl_2(\mathbb{C})$ est isomorphe au groupe des homographies constituées des transformations de la forme $z \longmapsto \frac{az+b}{cz+d}$ avec $ad-bc \neq 0$.

Prop 68 : Le groupe $PGl_2(\mathbb{C})$ est engendré par les similitudes directes de la forme $z \longmapsto az+b$ $a \neq 0$ et l'application $z \longmapsto \frac{1}{z}$.

Fig 1. $\begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ & & & 1 & \\ 0 & & & & \lambda \end{pmatrix}$

Fig 2 $\begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ 0 & & 1 & 1 \\ & & & 1 \end{pmatrix}$

Fig 3 $\begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & 1 & & \\ & & & -1 & \\ 0 & & & & \ddots \\ & & & & & -1 \end{pmatrix} = \begin{pmatrix} I_p & 0 \\ 0 & -I_{m-p} \end{pmatrix}$