Leçon 108 : Exemple de parties génératrices de groupes. Applications.

[Perr] : Daniel Perrin : Cours d'algèbre [F. GNAP 3] Oraux X-ENS Algèbre 3
[Gou1] : Xavier Gourdon : Algèbre
[Cal] : Josette Calais : Eléments de théorie des groupes
[Comb] : Combe : Algèbre et géométrie

I Partie génératrice et relations

I.1 Sous groupe engendré par une partie

[Perr] p10

Def. 1 Soit G groupe $A \subset G$, le sous groupe H est le plus petit sous groupe de G contenant A on le note $\langle A \rangle$

Def 2 $\langle A \rangle = \{a_1 \dots a_n \mid n \in \mathbb{N}\ a_i \in A \cup A^{-1}\}$
avec $A^{-1} = \{x \in G \mid x^{-1} \in A\}$ (def par l'intérieur)

Def 3 $\langle A \rangle$ = intersection des sous groupe contenant A

[Gou1] p28

Ex 4 : $\langle 1 \rangle = \mathbb{Z}$, $\langle \bar{1} \rangle = \mathbb{Z}/n\mathbb{Z}$, $\langle \{e^{i\frac{2\pi}{n}} \mid n \in \mathbb{N}^*\} \rangle = \mathbb{U}$

[Perr] p13

Ex 5 : $D(G)$: le groupe dérivée sous groupe engendrée par les commutateur $(xyx^{-1}y^{-1}\ x, y \in G)$

Rq 6 : $G/D(G)$ est le plus grand quotient abélien de G

App 7 : Si G commutatif $D(G) = \{1\}$
Pour $G = \mathfrak{S}_3$ $D(G) = \{1, \sigma, \sigma^2\}$
Pour $G = \mathfrak{A}_5$ $D(G) = \mathfrak{A}_5$

I.2 Groupe libre et présentation

[Cal] p338 p344

Def 8 F est un groupe libre sur X si pour $X \xrightarrow{\alpha} F$ on a pour tout groupe G et application $\sigma : X \to G$ il existe un unique morphisme $f : F \to G$ tq $f \circ \alpha = \sigma$

Ex 9 : $\mathbb{Z}$ est libre sur $\{1\}$
$\mathbb{Z}/n\mathbb{Z}$ n'est pas libre sur $\{1\}$

Def 10 : G engendrée par un ensemble X et vérifiant un ensemble de relation $R = \{r_k = 1, k \in K\}$
$\langle R \rangle$ est un sous groupe distingué du groupe libre F_X et on dit que $\langle X \mid R \rangle$ est une présentation de G si $G \simeq \frac{F_X}{\langle R \rangle}$

Ex 11 : $\langle x \mid x^n \rangle$ présentation du groupe cyclique d'ordre n
$\langle 1 \mid n.1 = 0 \rangle$ présentation de $\mathbb{Z}/n\mathbb{Z}$
$\langle X \mid \emptyset \rangle$ présentation de F_X

App 13 : $\langle X \mid [a, b]\ a, b \in X \rangle$ presentation de G alors $G \simeq \frac{F_X}{D(F_X)}$ groupe abelien libre

II Groupes abéliens

II.1 Groupes monogènes et cycliques

[Gou1] p19

Def 14 : G est dit "monogène" s'il existe $a \in G$ $\langle a \rangle = G$
Si de plus G est fini il est "cyclique". G est de type fini s'il a un nombre fini de générateur $a_1, \dots, a_n$ $\langle a_1, \dots, a_n \rangle = G$

Rq 15 : un groupe monogène est abélien

Prop 16 Toute image par un morphisme d'un groupe monogène est un groupe monogène

Prop 17 $\mathbb{Z}/n\mathbb{Z}$ est cyclique

[Cal] p89 p95

Th 18 Si G monogène
G infini $\iff G \simeq \mathbb{Z}$
G fini $\iff G$ cyclique $\iff G \simeq \mathbb{Z}/n\mathbb{Z}$
$o(G) = n$ avec $o(G) = n$

Ex 19 $\mathbb{U}_n$ groupe des racine n-eme engendré par les racine n-ième primitive de l'Unité
$\mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$

Cor 20 : deux groupes monogène infini ou cyclique de même ordre sont isomorphe

Th 21 :
- Tout sous groupe non réduit au neutre d'un groupe monogène infini est monogène infini
- Tout sous groupe d'un groupe cyclique est cyclique

[Cal] p95

Cor 22 le nombre de sous groupe de $\mathbb{Z}/n\mathbb{Z}$ est le nombre de diviseur de n dans $\mathbb{N}^*$

Ex 23 : $\mathbb{Z}/6\mathbb{Z}$ à pour sous groupe $\langle \bar{1} \rangle = \mathbb{Z}/6\mathbb{Z}$, $\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{6}\}$
$\langle \bar{3} \rangle = \{\bar{3}, \bar{0}\}$ et $\langle \bar{6} \rangle = \{\bar{0}\}$ cyclique

[Gou] p7

Prop 24 $\langle m, n \rangle = m\mathbb{Z} + n\mathbb{Z} = (m \wedge n)\mathbb{Z}$

[Perr] p24 p74

Prop 25 $G = \langle a \rangle$ groupe cyclique d'ordre n
alors (i) k premier à n
(ii) $\bar{k}$ générateur de $\mathbb{Z}/n\mathbb{Z}$
(iii) $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ pour la multiplication

Prop 26 il y a $\varphi(n)$ générateur de $\mathbb{Z}/n\mathbb{Z}$
avec $\varphi(n) = \mathrm{card}\{0 \leq k \leq n \ k \wedge n = 1\}$ fonction d'euler

Prop 27 $\mathrm{Aut}\, \mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

Th 28 $\mathbb{F}_q^\times$ est cyclique

Cor 29 Tout sous groupe fini du groupe multiplicatif d'un corps est cyclique.

II.2 Groupes abéliens fini

[Perr]

Th 30 (reste chinois) p, q premier entre eux
alors on a $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

Ex 31 : $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$

Ex 32 : Attention si $p \wedge q \neq 1$ alors on ne peut pas conclure $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas isomorphe à $\mathbb{Z}/4\mathbb{Z}$

[Com] p66

Th 33 (Théorème de structure)
Soit G groupe abélien fini d'ordre $n \geq 2$
Il existe $q_1, \dots, q_k \in \mathbb{Z}$ avec $2 \leq q_1 | q_2 | \dots | q_k$ uniquement déterminé tel que $G \simeq \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_k\mathbb{Z}$

Cor 34 $q_1, \dots, q_k$ sont appelé les invariants de G

Ex 35 si $|G| = 600$ alors les invariants possible sont
(600) $(5, 120)$, $(10, 60)$ $(2, 2, 150)$, $(2, 10, 30)$

III Groupes symétriques et diédraux

III.1 Groupes symétriques

Def 36 On appelle groupe symétrique de l'ensemble E.
le groupe des bijections de E. si $E = [\![1, n]\!]$ on le note $\mathfrak{S}_n$ et $|\mathfrak{S}_n| = n!$

[Perr] p10 p28

Def 37 : la permutation $\sigma = (a_1, \dots, a_k)$ avec $a_i \neq a_j \ \forall i \neq j$
et $\sigma(a_{[i]}) = a_{[i+1]}$ avec $[i]_k = i \bmod k$ (et $\sigma(a_{k-1}) = a_k$
cette permutation est le cycle d'ordre k
pour $k = 2$ on parle de transposition

Def 38 : On munit $\mathfrak{S}_n$ d'un morphisme surjective $\varepsilon : \mathfrak{S}_n \to \{1, -1\}$
pour un cycle σ d'ordre k $\varepsilon(\sigma) = (-1)^{k+1}$

Def 39 : Le noyau de cette application forme un groupe $\mathfrak{A}_n$ appelé le groupe Alterné

Th 40 : toute permutation se décompose de manière unique en cycle à support disjoint

Prop 41 : Les transpositions engendrent $\mathfrak{S}_n$ les $(1, i)$ $i \in [\![2, n]\!]$ suffisent

Prop 42 : $(12), (1, \dots n)$ engendrent $\mathfrak{S}_n$

Prop 43 : $\mathfrak{A}_n$ est engendré par les 3-cycle pour $n \geq 3$

Appli 44 : $\mathfrak{A}_n$ est simple pour $n \geq 5$ DVP

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

III.2 Groupes diédraux

[Cal1] p120 **Def46** : D_n est le groupe formés par les isométries qui conservent les sommets d'un polygone à n sommets

Prop47 : D_n est d'ordre $2n$

p342 **Prop48** : $D_n := \langle r, s \mid r^n, s^2, (rs)^2 \rangle$ est une présentation du groupe diédral

[ULm] **Appli 49** : $D(D_n) = \langle r^2 \rangle$ $D(D_{2n}) = \langle r^2 \rangle$ $D(D_{2n+1}) = \langle r \rangle$

IV Générateur en algèbre linéaire

IV.1 Groupes linéaires et spéciaux linéair

[Perr] p95-p99

Soit K un corps E un K espace vectoriel de dimension n

Def50 : L'existence d'une base défini un isomorphisme de $GL(E)$ le groupe linéaire (i.e groupe des automorphisme de E) dans $GL_n(K)$ le groupe des matrices $n \times n$ inversible $SL_n(K) = \{A \in GL_n(K) \mid \det A = 1\}$

Prop 51 : Soit H hyperplan de E et soit $u \in GL(E)$ tq $u_{|H} = Id_H$ alors les assertions suivantes sont équivalentes :

1) on a $\det u = \lambda \neq 1$ ($u \notin SL(E)$)
2) u admet une valeur propre $\lambda \neq 1$ (donc une droite propre D pour λ) et u diagonalisable
3) on a $Im(u - Id) \not\subset H$
4) Dans une base bien choisi la matrice de u est Fig 1

u est une dilatation d'hyperplan H, de droite D, de rapport λ

Prop 52 : H hyperplan d'équation $f \in E^*$ ($H = \ker f$) alors les assertions suivantes sont équivalentes :

1) $\det u = 1$ $u \in SL(E)$
2) u n'est pas diagonalisable
3) on a $D = Im(u - Id) \subset H$
4) le morphisme $\bar{u} : E/H \to E/H$ est l'identité de E/H
5) $\exists a \in H \setminus \{0\}$ tel que $\forall x \in E$ $u(x) = x + f(x)a$
6) la matrice de u est Fig 2

[Perr]

Th53 Les transvections engendrent $SL(E)$

Cor54 Les dilatations et les transvection engendrent $GL(E)$

IV Groupe orthogonal

$\dim E = n$

Def55 Soit f forme bilinéaire symétrique sur E les isométries sont les automorphismes $u \in GL(E)$ tel que $f(u(x), u(y)) = f(x, y)$ ils forment un groupe qu'on appelle le groupe orthogonal $O(f)$

[Perr]

Def56 : le sous groupe des isométrie de determinant 1 est distingué on l'appelle le groupe special orthogonal $SO(f)$

p120 ..125

Def57 : q forme quadratique associé à f une forme bilinéaire symétrique $\forall x \in E$ $q(u(x)) = f(u(x), u(x)) = q(x)$ pour $u \in GL(E)$ isométrie.

Prop 58 Soit $u \in GL(E)$ tel que $u^2 = Id$ alors il existe deux sous espace E^+, E^- tel que

1) $E = E^+ \oplus E^-$
2) $u_{|E^+} = Id_{E^+}$ $u_{|E^-} = -Id_{E^-}$

En choisissant convenablement les base on obtient que la matrice de u est Fig 3

p142 ..144

Def59 si $\dim E^- \neq 0$ u est une symétrie si $\dim E^- = 1$ on dit que u est une reflexion si $\dim E^- = 2$ on parle de renversement

Th60 $O(q)$ est engendré par les reflexions orthogonales plus précisément si u est dans $O(q)$ il est produit d'au-plus n reflexion

Cor61 $SO(q)$ est engendré par les renversement si $u \in SO(q)$ u est produit d'au plus n renversement

Appli62 $SO_3^+(\mathbb{R})$ est simple DVP

[FGNAP3] p67

Prop 63 : $D(O(q)) = D(SO(q)) = SO(q)$

Fig 1

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

Fig 2

$$\begin{pmatrix} 1 & & 0 & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \\ 0 & & & 1 \\ & & & 1 \end{pmatrix}$$

Fig 3

$$\begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & 1 & & \\ & & & -1 & \\ & & & & \ddots \\ 0 & & & & & -1 \end{pmatrix}$$