Exemples de parties génératrices d'un groupe. Applications.

Soit G un groupe et $\mathbb{K}$ un corps.

I/ Généralités

1) Définition :

Proposition 1 : L'intersection d'une famille quelconque $(H_i)_{i\in I}$ de sous-groupes de G est un sous-groupe de G.

Définition 2 : Si X est une partie de $(G,\cdot)$, le sous-groupe de G engendré par X est l'intersection de tous les sous-groupe de G qui contiennent X. On note $\langle X\rangle$ le sous-groupe de G engendré par X.

Définition 3 : Si X est une partie de G, on dit que X engendre G si $G=\langle X\rangle$

Proposition 4 : En notant, pour X non vide, $X^{-1}=\{x^{-1}\mid x\in X\}$, les éléments de $\langle X\rangle$ sont de la forme $x_1\cdots x_r$ où $r\in\mathbb{N}^*$, et les $x_k\in X\cup X^{-1}$ $\forall k\in[\![1,r]\!]$

Proposition 5 : $\forall p\in\mathbb{N}^*$ et $\forall(g_1,\dots,g_p)\in G^p$ qui commutent 2 à 2, on a $\langle g_1,\dots,g_p\rangle=\left\{\prod_{k=1}^{p} g_k^{\alpha_k}\mid(\alpha_1,\dots,\alpha_p)\in\mathbb{Z}^p\right\}$ et ce groupe est commutatif

2) Groupes monogènes et cycliques :

Définition 6 : On dit que G est monogène s'il existe un élément g de G tel que $G=\langle g\rangle$. Si de plus G est fini, on dit alors qu'il est cyclique.

Exemple 7 : Le groupe $(\mathbb{Z},+)$ est monogène et $\mathbb{Z}=\langle 1\rangle$
Le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ est cyclique et $\mathbb{Z}/n\mathbb{Z}=\langle\bar{1}\rangle$

Proposition 8 : Soit G un groupe monogène. S'il est infini, il est isomorphe à $(\mathbb{Z},+)$, s'il est cyclique d'ordre n, il est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$

Exemple 9 : Le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité est cyclique d'ordre n, est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Proposition 10 : Si $G=\langle g\rangle$ est cyclique d'ordre n, ses générateurs sont les g^k où $k\wedge n=1$, $k\in[\![1,n-1]\!]$

Exemple 11 : $\mathbb{Z}/n\mathbb{Z}$ possède $\varphi(n)$ générateur où $\varphi(n)$ est $\#\{k\in[\![1,n]\!]\mid k\wedge n=1\}$

Proposition 12 : Soit $G=\langle a\rangle$, cyclique d'ordre n.
1) Les sous-groupe de G sont cycliques d'ordre divisant n.
2) Pour tout diviseur positif d de n, il existe un unique sous groupe d'ordre d de G. Ce sous-groupe est le groupe cyclique $H=\langle a^{\frac{n}{d}}\rangle$.

II/ Le groupe symétrique.

1) Étude de S_n.

Définition 13 : S_n, est le groupe des bijections de $[\![1,n]\!]$ dans $[\![1,n]\!]$, appelé groupe symétrique.

Proposition 14 : $\mathrm{Card}(S_n)=n!$

Définition 15 : Le support d'une permutation $\sigma \in \mathfrak{S}_n$ est l'ensemble $Supp(\sigma) = \{x \in E \mid \sigma(x) \neq x\}$

Proposition 16 : Si $Supp(\sigma) \cap Supp(\sigma') = \emptyset$ alors $\sigma \circ \sigma' = \sigma' \circ \sigma$.

Définition 17 : On dit que deux cycles σ et σ' dans $\mathfrak{S}_n$ sont disjoints si leurs supports le sont dans $[\![1, n]\!]$.

Proposition 18 : Toute permutation $\sigma \in \mathfrak{S}_n \setminus \{Id\}$ se décompose en produit de cycles deux à deux disjoints i.e $\mathfrak{S}_n$ est engendré par les cycles.

Corollaire 19 : Toute permutation $\sigma \in \mathfrak{S}_n$ se décompose en produit de transpositions i.e les transpositions engendrent $\mathfrak{S}_n$.

Exemple 20 : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} = (1\,2\,3\,4\,5)(6\,7)$
$= (1\,2)(2\,3)(3\,4)(4\,5)(6\,7)$

Proposition 21 : $\mathfrak{S}_n$ est engendré par :

i) Soit les $n-1$ transpositions $(1\,k)$ où $k \in [\![2, n]\!]$

ii) Soit les $n-1$ transpositions $(k\;k+1)$ où $k \in [\![1, n-1]\!]$

iii) Soit $(1,2)$ et $(1\,2\,3 \dots n)$

Théorème 22 : Soit $n \in \mathbb{N}^* \setminus \{6\}$. Les automorphismes de $\mathfrak{S}_n$ sont intérieurs i.e de la forme $s \mapsto \sigma s \sigma^{-1}$ où $\sigma \in \mathfrak{S}_n$

2) Le groupe Alterné.

Définition 23 : Soient $1 \leq n$ un entier et $\sigma \in \mathfrak{S}_n$. On appele signature $\sigma \in \mathfrak{S}_n$, et on note $\varepsilon(\sigma)$, le nombre
$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Exemple 24 : $\varepsilon(Id) = 1$ et $\varepsilon((1,2)) = -1$

Proposition 25 : L'application ε est un morphisme de groupe et si $\#(\sigma)$ désigne le nombre de transpositions qui apparait dans une décomposition de σ, en produit de transposition alors $\varepsilon(\sigma) = (-1)^{\#(\sigma)}$

Définition 26 : Pour $n \geq 2$, on définit le groupe alterné, noté $\mathcal{A}_n$ comme le noyau du morphisme signature.

Proposition 27 : $Card(\mathcal{A}_n) = \frac{n!}{2}$

Proposition 28 : Soit $n \geq 3$, le groupe $\mathcal{A}_n$ est engendré par les cycles de la forme $(1, i, j)$ avec $i \neq j \in [\![2, n]\!]$. En particulier $\mathcal{A}_n$ est engendré par les 3-cycles.

Théorème 29 : Pour $n \geq 5$, $\mathcal{A}_n$ est simple.

III / Le groupe linéaire.

Définition 30 : On définit le groupe linéaire de $\mathbb{K}$, noté $GL_n(\mathbb{K})$, l'ensemble $GL_n(\mathbb{K}) = \{A \in \mathcal{M}_n(\mathbb{K}) \mid det(A) \neq 0\}$ et le groupe $SL_n(\mathbb{K}) = \{A \in \mathcal{M}_n(\mathbb{K}) \mid det(A) = 1\}$.

Proposition 31 : $SL_n(\mathbb{K})$ est un sous-groupe de $GL_n(\mathbb{K})$.

Proposition 32 : Les assertions suivantes sont équivalentes :

i) $A \in GL_n(\mathbb{K})$

ii) $Ker(A) = \{0\}$

iii) $rg(A) = n$

D1 | D2

Théorème 33 : (Burnside) Soit G un sous-groupe de de $GL_n(\mathbb{C})$ d'exposant fini. Alors G est fini.

Définition 34 : On définit les matrices de :

- Transvection de la forme $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$ où $i \neq j$, $\lambda \in \mathbb{K}$
- Dilatation de la forme $D_i(\alpha) = I_n + (\alpha - 1) E_{i,i}$ où $\alpha \in \mathbb{K} \setminus \{0\}$

Proposition 35 : Soit $A \in \mathcal{M}_n(\mathbb{K})$, on note L_i la $i$ème ligne et C_j la j-ième colonne.

* $D_i(\alpha) A$ revient à faire $L_i \to \alpha L_i$
* $A D_j(\alpha)$ revient à faire $C_j \to \alpha C_j$.
* $T_{i,j}(\lambda) A$ revient à faire $L_i \to L_i + \lambda L_j$
* $A T_{i,j}(\lambda)$ revient à faire $C_j \to C_j + \lambda C_i$.

Théorème 36 : i) Le groupe $SL_n(\mathbb{K})$ est engendré par les matrices de transvections

ii) Le groupe $GL_n(\mathbb{K})$ est engendré par les matrices de transvection et de dilatations.

Rombaldi
Ulmer.