[Rau] I.3

Définition 1 : Soit $(G;\cdot)$ groupe, $X \subseteq G$. On dit que X engendre G si $X = \{x_1; \dots; x_n\}$ et si tout élément de G s'écrit comme produit fini d'éléments de X. Noté $G = \langle X \rangle$

I] Groupes abéliens finis

1] Groupes monogènes et cycliques

[Rau] I.4

Définition 2 : On dit que G est monogène s'il existe $g \in G$ tel que $G = \langle g \rangle$. Si en plus G est fini, alors on dit que G est cyclique.

Exemples 3 : (1) $(\mathbb{Z};+)$ est monogène engendré par 1
(2) $\forall n \in \mathbb{N}$, $(\frac{\mathbb{Z}}{n\mathbb{Z}};+)$ est cyclique d'ordre n
(3) $\forall n \in \mathbb{N}$, $(\mu_n;\times)$ est cyclique d'ordre n

Remarque 4 : Si G est cyclique, alors il est commutatif

Proposition 5 : Soit G groupe monogène
Alors : (1) Si G est infini, alors il est isomorphe à $(\mathbb{Z};+)$
(2) S'il est cyclique d'ordre n, alors il est isomorphe à $(\frac{\mathbb{Z}}{n\mathbb{Z}};+)$

Proposition 6 : Soit $G = \langle g \rangle$ groupe cyclique d'ordre n.
Alors : ses générateurs sont : $\{g^k \mid k \in [\![1, n-1]\!],\ k \wedge n = 1\}$

Remarque 7 : Le nombre de générateurs de G groupe cyclique d'ordre n est donné par $\varphi(n)$.

Théorème 8 : Soit $p \neq q$ premiers, G groupe abélien d'ordre pq
Alors : G est cyclique

Contre-exemple 9 : L'hypothèse $p \neq q$ est vitale !
Pour p premier $(\frac{\mathbb{Z}}{p\mathbb{Z}})^2$ est d'ordre p^2 non-cyclique car tout élément non-neutre sont d'ordre p.

Théorème 10 : Soit $G = \langle g \rangle$ groupe cyclique d'ordre n
Alors : (1) Les sous-groupes de G sont cycliques d'ordre diviseur de n
(2) $\forall d \mid n$, $\exists ! H < G \mid H = \langle g^{\frac{n}{d}} \rangle$ d'ordre d, et on a :
$H = \{g \in G \mid \mathrm{ord}(g) \mid d\} = \langle \{g \in G \mid \mathrm{ord}(g) = d\} \rangle$

[Rau] I.5

2] Groupes abéliens finis

Théorème 11 : (de Cauchy) Soit G groupe abélien fini cyclique d'ordre n
Alors : $\forall p \mid n$, p premier, $\exists g \in G \mid \mathrm{ord}(g) = p$

Contre-exemple 12 : L'hypothèse de cyclicité est vitale !
$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ n'a pas d'élément d'ordre 4.

[Rau] I.3

Définition 13 : Soit G groupe abélien fini. On appelle exposant de G : $e(G) = \max_{g \in G} \{\mathrm{ord}(g)\} = \mathrm{PPCM}(\{\mathrm{ord}(g) \mid g \in G\})$.
Un caractère d'un groupe G est un morphisme de groupes de G dans $\mathbb{C}^*$.

Exemple 14 : $G \to \mathbb{C}^*$, $g \mapsto 1$ est le caractère trivial

Proposition 15 : Soit $H < G$ et $\varphi : H \to \mathbb{C}^*$ caractère.
Alors : φ se prolonge en un caractère sur G.

Lemme 16 : Soit $g_0 \in G$ tel que : $\mathrm{ord}(g_0) = e(G)$, $n \leq n-1$, $K = \langle g_0 \rangle$
Alors : (1) $\exists ! \varphi_0 : K \to \mathbb{C}^*$ caractère tel que : $\varphi_0(g_0) = \omega = e^{\frac{2i\pi}{n}}$
(2) En prolongeant φ_0 en $\varphi : G \to \mathbb{C}^*$, l'application :
$\theta : \langle g_0 \rangle \times \ker(\varphi) \to G$, $(g_0^k; h) \mapsto g_0^k h$ est un isomorphisme de groupes.

Théorème 17 : (de Kronecker) $\exists ! (n_k)_{k=1}^r \in \mathbb{N}^r \mid 2 \leq n_1 \mid \dots \mid n_r$,
G est isomorphe à $\Gamma = \prod_{k=1}^r \mu_{n_k}$

[Rau] I.5

II] Exemples de groupes non-abéliens finis

1] Groupe symétrique

Soit E ensemble à au moins 2 éléments, $n = |E|$.

II.1

Définition 18: On note $S(E) = \mathrm{Bij}(E;E)$. Soit $r \in [\![2; \mathrm{card}(E)]\!]$. On appelle cycle d'ordre r toute permutation $\sigma \in S(E)$ telle que: $\exists \{x_1;\dots;x_r\} \subset E \setminus \forall k \in [\![1;r-1]\!], \sigma(x_k) = x_{k+1}$; $\sigma(x_r) = x_1$ et $\forall x \in E \setminus \{x_1;\dots;x_r\}, \sigma(x) = x$. On appelle transposition un 2-cycle.

II.4 [Rom]

Théorème 19: Toute permutation $\sigma \in S(E) \setminus \{id_E\}$ se décompose en produit de cycles 2 à 2 disjoints de manière unique à l'ordre des facteurs près.

Remarque 20: Si $\sigma = \gamma_1 \circ \dots \circ \gamma_p$ est une telle décomposition, alors $\mathrm{Supp}(\sigma) = \bigcup_{k=1}^{p} \mathrm{Supp}(\gamma_k)$ et $\mathrm{ord}(\sigma) = \mathrm{PPCM}(\mathrm{ord}(\gamma_1);\dots;\mathrm{ord}(\gamma_p))$.

II.5

Corollaire 21: Toute permutation $\sigma \in S(E)$ se décompose en produit de transpositions i.e. le groupe $S(E)$ est engendré par les transpositions.

Exemple 22: $(1\,2\,3\,4\,5)(6\,7) = (1\,2)(2\,3)(3\,4)(4\,5)(6\,7)$ d'ordre $\mathrm{PPCM}(5;2) = 10$.

Proposition 23: S_n est engendré par les $n-1$ transpositions $(1\,k)$.

Exemple 24: $(1\,2)(2\,3)(3\,4)(4\,5)(6\,7) = (1\,2)[(1\,2)(1\,3)(1\,2)][(1\,3)(1\,4)(1\,3)][(1\,4)(1\,5)(1\,4)][(1\,6)(1\,7)(1\,6)] = (1\,3)(1\,2)(1\,3)(1\,4)(1\,3)(1\,4)(1\,5)(1\,4)(1\,6)(1\,7)(1\,6)$

Proposition 25: S_n est engendré par les $n-1$ transpositions $(k\;k+1)$.

Exemple 26: $(1\;k) = (k-1\;k)(1\;k-1)(k-1\;k)$

Proposition 27: S_n est engendré par $(1\,2)$ et $(1\,2\,\cdots\,n)$.

Exemple 28: $(k\;k+1) = (1\,2\cdots n)^{k-1}(1\,2)[(1\,2\cdots n)^{k-1}]^{-1}$

2] Sous-groupe alterné et application à l'algèbre linéaire

II.6 [Rom]

Théorème 29: Les seuls morphismes de groupes de $(S(E);\circ)$ dans $(\mathbb{R}^*;\cdot)$ sont l'application constante 1 et la signature:

$$\varepsilon : \begin{array}{l} S(E) \to \{\pm 1\} \\ \sigma \mapsto \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i} \end{array}$$

Définition 30: On appelle groupe alterné $A(E) = \mathrm{Ker}(\varepsilon)$.

II.7

Proposition 31: $A(E) \lhd S(E)$ et $|A(E)| = \frac{n!}{2}$

Proposition 32: Pour $n \geq 3$, $A(E)$ est engendré par les 3-cycles.

[Isen]

Définition 33: Une matrice de dilatation de $GL_n(\mathbb{K})$ est de la forme $\begin{pmatrix} 1 & & \\ & \ddots & \\ & & \lambda \end{pmatrix}$ avec $\lambda \in \mathbb{K}^*$ dans une certaine base.

Soit H hyperplan de E espace vectoriel et G son supplémentaire: $E = H \oplus G$. La dilatation f de base H, direction G et rapport $\lambda \in \mathbb{K}^*$ est telle que: $\forall h, u \in H \times G$, $f(h+u) = h + \lambda u$.

Théorème 34: Soit $\mathbb{K}$ à au moins 3 éléments et V un $\mathbb{K}$-ev. Alors: les dilatations engendrent $GL(V)$.

Lemme 35: (1) L'application $\varphi : \begin{array}{l} \mathbb{F}_p^* \to \{\pm 1\} \\ a \mapsto \left(\frac{a}{p}\right) \end{array}$ est un morphisme

(2) Soit p premier impair. Alors il y a $\frac{p+1}{2}$ carrés et $\frac{p-1}{2}$ non-carrés dans $\mathbb{F}_p$.

Théorème 36: Soit $\mathbb{K}$ corps fini. Alors: $\exists a \in \mathbb{K}^* \setminus \mathbb{K}^* = \langle a \rangle$

Théorème 37: (de Frobenius-Zolotarev) Soit p premier impair, V un $\mathbb{F}_p$-espace vectoriel de dimension n. Alors: $\forall u \in GL(V)$, $\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$.

3] Groupe diédral

II.4.3 [Rom]

Définition 38: On dit qu'un groupe multiplicatif G est diédral de type D_{2n} s'il est dicyclique engendré par un élément ρ d'ordre n

III.4.3 [Rou]

et un élément $\sigma \neq \rho$ d'ordre 2 tel que $\rho\sigma\rho\sigma = id$.

Théorème 39: (1) Si G est diédral de type $\mathbb{D}_{2n}$, alors: $G = \{id; \rho; \dots; \rho^{n-1}\} \cup \{\sigma; \sigma\rho; \dots; \sigma\rho^{n-1}\}$ est d'ordre $2n$.
(2) Deux groupes diédraux de type $\mathbb{D}_{2n}$ sont isomorphes.

Exemple 40: Dans le plan, la rotation ρ d'angle $\frac{2\pi}{n}$ et σ la réflexion d'axe $\mathbb{R}e_1$ forment un groupe $\langle \rho; \sigma \rangle$ diédral $\mathbb{D}_{2n}$.

Définition 41: On note $\Gamma_n = \{A_k = \rho^k(e_1) \mid k \in [\![0; n-1]\!]\}$ les sommets d'un polygône régulier à n côtés et $Is(\Gamma_n) = \{u \in O(E) \mid u(\Gamma_n) = \Gamma_n\}$

Théorème 42: $Is(\Gamma_n) = \langle \rho; \sigma \rangle = \{id; \rho; \dots; \rho^{n-1}\} \cup \{\sigma; \sigma\rho; \dots; \sigma\rho^{n-1}\}$

Exemple 43: S_3 est isomorphe au groupe du triangle équilatéral, il est alors de type $\mathbb{D}_6$.

III] Parties génératrices en algèbre linéaire

1] Générateurs de $GL(E)$ et $SL(E)$.

Soit E un $\mathbb{K}$-espace vectoriel de dimension n.

IV.2 [Per]

Lemme 44: Soit $x, y \in E^*$.
Alors: $\exists$ un transvection ou $\exists$ un produit de deux transvections tels que: $u(x) = y$ ou $u \circ u(x) = y$

Théorème 45: Les transvections engendrent $SL(E)$

Corollaire 46: Les transvections et les dilatations engendrent $GL(E)$.

Remarque 47: Matriciellement, pour tout $A \in GL_n(\mathbb{K})$, il existe $P_1, \dots, P_r, Q_1, \dots, Q_s$ matrices de transvections telles que:
$$A = P_1 \times \dots \times P_r \begin{pmatrix} \det(A) & & \\ & 1 & \\ & & \ddots \end{pmatrix} Q_1 \times \dots \times Q_s$$

Application 48: La méthode du pivot de Gauss est similaire à la démonstration du résultat précédent.

Plutôt mettre Frobenius-Zolotarev ici.

2] Groupe orthogonal

Définition 49: Une isométrie de E est une application $u: E \to E$ qui conserve le produit scalaire
ie $\forall x, y \in E$, $\langle u(x) | u(y) \rangle = \langle x | y \rangle$
On note $O(E)$ le groupe des isométries de E.

Exemple 50: Les seules homothéties $x \mapsto \lambda x$ isométriques sont Id et $-Id$.

Théorème 51: $O(E)$ est engendré par des réflexions orthogonales. Plus précisément, si $u \in O(E)$, alors u est produit d'au plus n réflexions.

Théorème 52: Pour $n \geq 3$, $SO_n(\mathbb{R})$ est engendré par des renversements. Plus précisément, tout $u \in SO_n(\mathbb{R})$ est produit d'au plus n renversements.

Définition 53: Le corps gauche des quaternions $\mathbb{H}$ est une $\mathbb{R}$-algèbre non-abélienne engendrée par i, j, k tels que:
$i^2 = j^2 = k^2 = -1$; $ij = k$; $jk = i$; $ki = j$.
La norme de $q = a + ib + jc + kd \in \mathbb{H}$ est: $N(q) = \sqrt{a^2 + b^2 + c^2 + d^2}$
On note $Sp(1) = \{q \in \mathbb{H} \mid N(q) = 1\}$ et $Im(\mathbb{H}) = \{q \in \mathbb{H} \mid Re(q) = 0\}$
Un retournement de $\mathbb{R}^3$ pour $v \in \mathbb{R}^3$ est: $r_v : \mathbb{R}^3 \to \mathbb{R}^3$, $z \mapsto z - 2\frac{\langle z | v \rangle}{\|v\|^2} v$

Proposition 54: Soit $q = a + ib + jc + kd \in \mathbb{H}$, $q_1, q_2 \in \mathbb{H}$
Alors: (1) $2Re(q) = q + \bar{q}$ avec $\bar{q} = a - ib - jc - kd$
(2) $\overline{q_1 q_2} = \bar{q_2}\,\bar{q_1}$
(3) $N(q)^2 = q\bar{q}$
(4) $Z(\mathbb{H}) = \{q \in \mathbb{H} \mid \forall q' \in \mathbb{H}, qq'q^{-1} = q'\} = \mathbb{R}$
(5) $Z(\mathbb{H}) \cap Sp(1) = \{\pm 1\}$

Théorème 55: Les ensembles $SO_3(\mathbb{R})$ et $Sp(1)/\{\pm 1\}$ sont isomorphes.

VI.1 [Per] VI.2 [Esseu]

Références :

[Rou] Mathématiques pour l'agrégation Algèbre et Géométrie – Rombaldi

[Per] Cours d'algèbre – Perrin

[Isen] L'oral à l'agrégation de mathématiques – Isenmann