Groupes et anneaux II

Ivan Lejeune*

29 janvier 2024

1 Introduction

1.1 Informations importantes

- CC1 : Début mars
- CC2 : Fin avril
- Examen final : En mai

$$\text{Note finale} = \max\left(\text{note finale}, \frac{\text{examen} \;+ \frac{\text{CC1 CC2}}{2}}{2}\right)$$

1.2 Références

Voir le cours de Joao Pedro dos Santos

2 Exemples importants de groupes

Exemple 2.1. Le groupe des inversibles dans $\mathbb{C}$ avec la multiplication entre nombres complexes :

$$\mathbb{C} = \mathbb{C} \setminus \{0\}$$

Le sous-groupe des racines n-ièmes de l'unité :

$$\mu_n := \{z \in \mathbb{C}^\times | z^n = 1\}$$

Remarque 2.1. On obtient $\mu_n \approx \mathbb{Z}/n\mathbb{Z}$ via

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\to \mu_n \\ [k] &\mapsto e^{\frac{2k\pi i}{n}} \end{aligned}$$

Exemple 2.2. Le groupe général linéaire des matrices inversibles de taille $n \times n$ à coefficients dans $\mathbb{K}$ avec multiplication matricielle :

$$GL_n(()\mathbb{K})$$

Remarque 2.2. Si $\mathbb{K} = \mathbb{F}_p$ alors $|GL_n(()\mathbb{K})|$ est fini.

*Cours inspiré de M. Charlier et M. De Renzi

Pour calculer $|GL_n(()\mathbb{F}_p)|$, considérons $X \in GL_n(()\mathbb{F}_p)$

$$\begin{aligned} X &= (X_1|X_2|\cdots|X_n), X_i \in \mathbb{F}_p^n \\ X_1 &\neq 0 \\ X_2 &\notin \mathbb{F}_p X_1 \\ X_3 &\notin \mathsf{Vect}_{\mathbb{F}_p}(X_1, X_2) \\ &\vdots \end{aligned}$$

On a alors

$$\begin{aligned} |\mathbb{F}_p^n \smallsetminus \{0\}| &= p^n - 1 \text{ choix pour } X_1 \\ |\mathbb{F}_p^n \smallsetminus \mathbb{F}_p X_1| &= p^n - p \text{ choix pour } X_2 \\ |\mathbb{F}_p^n \smallsetminus \mathsf{Vect}_{F_p}(X_1, X_2)| &= p^n - p^2 \text{ choix pour } X_3 \\ &\vdots \end{aligned}$$

Soit

$$|GL_n(()\mathbb{F}_p)| = \prod_{i=0}^{n-1} (p^n - p^i)$$

En particulier, pour $p = n = 2$, on a

$$|GL_2(\mathbb{F}_2)| = (2^2 - 1)(2^2 - 2^1) = 6$$

Exemple 2.3. Pour $n > 1$, on a

- $R \in GL_2(\mathbb{R})$ la rotation d'angle $\frac{2\pi}{n}$ dans le sens anti-horlogique
- $S \in GL_2(\mathbb{R})$ réflexion par rapport à l'axe des abscisses.

Si on identifie $\mathbb{R}^2 \approx \mathbb{C}$, alors

$$R(z) = e^{\frac{2\pi i}{n}} z, \quad S(z) = \overline{z}$$

On a alors

$$\forall k \in \mathbb{Z}, SR^k S = R^{-k}$$

Preuve 2.1.

$$\begin{aligned} S(R^k(S(z))) &= S(R^k(\overline{z})) \\ &= S(e^{\frac{2k\pi i}{n}} \overline{z}) \\ &= e^{-\frac{2k\pi i}{n}} z \\ &= R^{-k}(z) \end{aligned}$$

Proposition 2.1. On note

$$\mathfrak{D}_n := I_2, R, \cdots, R^{n-1}$$

le groupe diédral, alors

$$\{S, RS, \cdots, R^{n-1}S\} \subset \mathfrak{D}_n$$

est un sous-groupe de $GL_2(\mathbb{R})$ (le groupe diédral à $2n$ éléments)

Preuve 2.2.

$$\begin{aligned} R^iR^j &= R^{i+j} && \text{(a)}\\ R^i(R^jS) &= R^{i+j}S \\ (R^iS)R^j &= R^iSR^jSS = R^{i-j}S \\ \underbrace{(R^iS)(R^jS)}_{\substack{\Rightarrow \mathfrak{D}_n \text{ est clos}\\ \text{par multiplication}}} &= R^{i-j} && \text{(b)}\\ (R^i)^{-1} &= R^{-i} \text{ grâce à (a)} \\ (R^iS)^{-1} &= R^iS \text{ grâce à (b)} \end{aligned}$$

Remarque 2.3. Si $n > 2$, on a $\mathfrak{D}_n$ non commutatif

3 Actions

Soit X un ensemble et G un groupe.

Définition 3.1. Une **action** de G sur X est une fonction

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

telle que

(i) $\forall x \in X, e \cdot x = x$

(ii) $\forall g, h \in G, \forall x \in X, (gh) \cdot x = g \cdot (h \cdot x)$

Remarque 3.1. "G agit sur X" sera noté $G \circlearrowleft X$.
Un G-ensemble est un ensemble muni d'une action de G.

Exercice 3.1.

$$G \circlearrowleft X \Rightarrow \rho : G \to \mathsf{Bij}(X)$$

Avec ρ définie par

$$\rho(g)(x) := g \cdot x, \quad \forall g \in G, x \in X$$

Montrer que ρ est un morphisme de groupes.

Réciproquement, montrer que si $\rho: G \to \mathsf{Bij}(X)$ est un morphisme de groupes, alors $g \cdot x := \rho(g)(x), \quad \forall g \in G, \forall x \in X$ définit une action de G.

4 Exemples importants d'Actions

Exemple 4.1. $\mathfrak{S}_n \circlearrowleft \{1, \ldots, n\}$ naturellement $(\sigma \cdot k = \sigma(k))$

Exemple 4.2. $GL_n(\mathbb{K}) \circlearrowleft \mathbb{K}^n$ par produit matriciel

$$A \cdot v = Av \quad \forall A \in GL_n(()\mathbb{K}), \forall v \in \mathbb{K}^n$$

(v vecteurs colonnes)

Exemple 4.3. $\mathcal{D}_n \circlearrowleft \mu_n$ car

$$\zeta^n = 1 \Rightarrow g(\zeta)^n = 1, \quad \forall g \in \mathcal{D}_n$$

En effet, il suffit de le vérifier pour les générateurs $R, S \in \mathcal{D}_n$:

$$\begin{aligned}
R(\zeta)^n &= \left(e^{\frac{2\pi i}{n}}\zeta\right)^n \\
&= e^{\frac{2n\pi i}{n}}\zeta^n \\
&= 1 \\
S(\zeta)^n &= \left(\overline{\zeta}\right)^n = \zeta^{-n} = 1
\end{aligned}$$

Exemple 4.4. $H < G$ (notation pour "H est un sous-groupe de G")

(a) Action par translation à gauche : $H \circlearrowleft G$ par

$$\begin{aligned}
\rho_L \colon H \to &\quad \mathsf{Bij}(G) \\
\rho_L(h)(g) := &\quad hg \qquad \forall h \in H, \forall g \in G
\end{aligned}$$

(b) Action par translation à droite : $H \circlearrowleft G$ par

$$\begin{aligned}
\rho_R \colon H \to &\quad \mathsf{Bij}(G) \\
\rho_R L(h)(g) := &\quad gh^{-1} \qquad \forall h \in H, \forall g \in G
\end{aligned}$$

Remarque 4.1. Le réflexe $h \cdot g = gh$ ne définit pas une action en général

Exercice 4.1. Vérifier que ce n'est pas le cas uniquement si $H < Z(G)$.

Définition 4.1. Soient X, Y, G des ensembles. On a $f \colon X \to Y$ G-**équivariante** (ou une G-fonction) si

$$\forall g \in G, \forall x \in X, \quad f(g \cdot x) = g \cdot f(x)$$

Exercice 4.2. Soit $H < G$ (un sous-groupe) de G et G_L(resp. G_R) l'ensemble G munit de l'action de H par translation à gauche(resp. translation à droite).
Montrer que

$$\begin{aligned}
_^{-1} \colon G_L &\to G_R \\
g &\mapsto g^{-1}
\end{aligned}$$

est une bijection H-équivalente

Définition 4.2. On pose G un groupe, Γ un groupe et V un espace vectoriel sur $\mathbb{K}$. Les assertions des points suivants sont équivalentes :

(i) $G \circlearrowleft \Gamma$ par homomorphismes si
- $\forall g \in G, \gamma, \gamma' \in \Gamma$ on a $g \cdot (\gamma\gamma') = (g \cdot \gamma)(g \cdot \gamma')$
- $\rho \colon G \to \mathsf{Aut}(\Gamma) < \mathfrak{S}$
- $\rho(g)$ est un morphisme de groupes $\forall g \in G$

(ii) $G \circlearrowleft V$ de manière linéaire si
- $\forall g \in G, v, v' \in V, \lambda, \lambda' \in \mathbb{K}$ on a $g \cdot (\lambda v \lambda' v') = \lambda(g \cdot v) + \lambda'(g \cdot v')$
- $\rho \colon G \to \mathrm{GL}_{\mathbb{K}}(V) < \mathfrak{S}_V$
- $\rho(g)$ est une application linéaire $\forall g \in G$

Exemple 4.5. Soient H et G des groupes avec $H < G$. Les assertions suivantes sont équivalentes :
- L'action de H sur G par translation à gauche est une action par homomorphismes
- $H = \{e\}$

En effet :

$$\begin{aligned}\forall h \in H \quad & h\cdot(gg') = (h\cdot g)(h\cdot g') \\ & \Longleftrightarrow hgg' = hghg' \\ & \Longleftrightarrow (hg)^{-1}hgg'(g')^{-1} = (hg)^{-1}hghg'(g')^{-1} \\ & \Longleftrightarrow e = h\end{aligned}$$

Soit que $\forall h \in H, h = e$ et donc $H = \{e\}$

Exemple 4.6. L'action de $GL_n(\mathbb{K})$ sur $\mathbb{K}^n$ qu'on a vu l'autre fois est linéaire.

Exemple 4.7. L'action par conjugaison :
Soient H et G des groupes, si $H < G$ alors $H \circlearrowleft G$ par $\rho_C\colon H \to \mathsf{Aut}(G) < \mathfrak{S}_G$ avec

$$\rho_C(h)(g) \coloneqq hgh^{-1} \quad \forall h \in H, g \in G$$

Il s'agit d'une action par homomorphismes car

$$\begin{aligned} h\cdot(gg') = hgg'h^{-1} & = hgh^{-1}hg'h^{-1} \\ & = (h\cdot g)(h\cdot g') \\ & = \rho_C(h)(g)\rho_C(h)(g') \\ & \quad \forall h \in H, g, g' \in G\end{aligned}$$

Théorème 4.1 Cayley.
Si G est un groupe d'ordre $n \in N$ alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Preuve 4.1. G agit sur lui-même par translation à gauche par

$$\rho_L\colon G \to \mathfrak{S}_G \simeq \mathfrak{S}_n$$

$$g \in \mathsf{Ker}(\rho_L) \Longrightarrow \rho_L(g)(e) = (e) \Longrightarrow ge = e$$

Donc ρ_L est injectif et $\rho_L\colon G \to \mathsf{Im}(\rho_L) < \mathfrak{S}_n$ est un isomorphisme.

Exemple 4.8. On considère $\zeta = e^{\frac{2\pi i}{5}}$ et

$$\mu_5 = \{\zeta^1, \zeta^2, \dots, \zeta^5\} \simeq \{1, 2, \dots, 5\}$$

$$\begin{aligned}\rho_L\colon \mu_5 & \to \mathfrak{S}_{\mu_5} \simeq \mathfrak{S}_5 \\ \zeta^k & \mapsto (1\ 2\ 3\ 4\ 5)^k\end{aligned}$$

Définition 4.3. Soit G un groupe et X un ensemble avec $G \circlearrowleft X$. On a alors

(i) $Y \in X$ est **stable** par G si $G\cdot Y \subset Y$. En particulier, Y est un sous-G ensemble.

(ii) L'**orbite** de $x \in X$ notée $\mathsf{orb}(x)$ ou $G\cdot x$ est

$$G\cdot x = \{g\cdot x \mid g \in G\}$$

> **Remarque 4.2.** $\mathsf{orb}(x)$ est stable par G.

(iii) Le **stabilisateur** de $x \in X$ est $\mathsf{st}(x)$ ou G_x est

$$G_x = \{g \in G \mid g\cdot x = x\}$$

Remarque 4.3. $\mathsf{st}(x) < G, e \in \mathsf{st}(x)$

$$g, g' \in \mathsf{st}(x) \implies g \cdot (g' \cdot x) = g \cdot x = x$$

(iv) $x \in X$ est un **point fixe** si

$$g \cdot x = x \quad \forall g \in G$$

Soit, si

$$G_x = G \qquad \text{ou} \qquad G \cdot x = x$$

L'ensemble des points fixes est noté X^G.

(v) L'action est **transitive** si

$$\exists x \in X : G \cdot x = X$$

Dans ce cas, on dit que X est un **espace homogène**

(vi) L'action est **libre** si

$$\forall x \in X, G_x = \{e\}$$