

Groupes et Anneaux II — Cours

Ivan Lejeune

5 février 2025

Table des matières

Chapitre 1 — qqch	2
1 Exemples importants de groupes.	2
2 Action de groupe	2

Chapitre 1 — qqch

1 Exemples importants de groupes

A^\times

Soit A un anneau et A^\times l'ensemble des éléments inversibles de A . L'ensemble A^\times est un groupe pour la multiplication.

Si $A = \mathbb{K}$ est un corps, alors pour tout $n \in \mathbb{N}$, l'ensemble

$$\mu_n(\mathbb{K}) = \{z \in \mathbb{K} \mid z^n = 1\}$$

est un groupe pour la multiplication.

Remarque. On a $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$ via l'isomorphisme de groupes

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\rightarrow \mu_n \\ \bar{k} &\mapsto e^{2i\pi k/n} \end{aligned}$$

$\mathrm{GL}_n(\mathbb{K})$

Soit \mathbb{K} un corps et $\mathrm{GL}_n(\mathbb{K})$ l'ensemble des matrices carrées inversibles de taille n à coefficients dans \mathbb{K} . L'ensemble $\mathrm{GL}_n(\mathbb{K})$ est un groupe pour la multiplication des matrices.

Remarque. Si $\mathbb{K} = \mathbb{F}_p$, c'est-à-dire un $\mathbb{Z}/p\mathbb{Z}$ avec p premier, alors $|\mathrm{GL}_n(\mathbb{F}_p)|$ est fini. Pour le calculer, considérons $X \in \mathrm{GL}_n(\mathbb{F}_p)$. On a

$$X = \begin{pmatrix} X_1 & X_2 & \cdots & X_n \end{pmatrix}$$

avec $X_i \in \mathbb{F}_p^n$. On a $X_1 \neq 0$, donc on a $p^n - 1$ choix pour X_1 .

Ensuite, on a $X_2 \notin \mathbb{F}_p X_1 = \mathrm{Vect}_{\mathbb{F}_p}(X_1)$, donc on a $p^n - p$ choix pour X_2 .

En général, on a $p^n - p^{i-1}$ choix pour X_i .

On a donc

$$|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) = \prod_{k=0}^{n-1} (p^n - p^k)$$

\mathcal{S}_n

Considérons les éléments suivants :

- $n > 1$ un entier naturel,
- $R \in \mathrm{GL}_n(\mathbb{R})$ la rotation d'angle $\frac{2\pi}{n}$ dans le plan (dans le sens anti-horaire),
- $S \in \mathrm{GL}_n(\mathbb{R})$ la réflexion par rapport à l'axe des abscisses.

Si on identifie \mathbb{R}^2 à \mathbb{C} , alors pour tout $z \in \mathbb{C}$,

$$R(z) = e^{\frac{2i\pi}{n}} z \quad \text{et} \quad S(z) = \bar{z}$$

et alors pour tout $k \in \mathbb{Z}$,

$$SR^k S = R^{-k}$$

Alors, le groupe

$$\mathcal{D}_n = \{\mathrm{Id}, R, \dots, R^{n-1}, S, SR, \dots, SR^{n-1}\}$$

est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$, c'est le groupe diédral à $2n$ éléments.

2 Action de groupe

Soit G un groupe et X un ensemble.

Définition 2.1. Une **action** de G sur X est une application

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

telle que

- (i) pour tout $x \in X$, on a $e \cdot x = x$,
- (ii) pour tout $g, h \in G$ et $x \in X$, on a $g \cdot (h \cdot x) = (gh) \cdot x$.

Notation.

- On notera $g \cdot x$ pour signifier $\alpha(g, x)$.
- On notera $G \curvearrowright X$ pour signifier que G agit sur X .

Définition 2.2. Un **G -ensemble** est un ensemble muni de l'action de G .

Définition 2.3. Une **représentation** de G dans X est un morphisme de groupes

$$\rho : G \rightarrow \mathfrak{S}_X$$

où \mathfrak{S}_X est le groupe des permutations/bijections de X .

Notation. On notera alors pour tout $g \in G$

$$\rho_g := \rho(g)$$

et pour tout $x \in X$

$$\rho_g(x) := \rho(g(x))$$

Exercice.

- Montrer que si $\alpha : G \times X \rightarrow X$ est une action alors il existe $\rho : G \rightarrow \mathfrak{S}_X$ telle que, pour tout $g \in G$, on a

$$\begin{aligned}\rho(g) : X &\rightarrow X \\ x &\mapsto g \cdot x\end{aligned}$$

- Réciproquement, montrer que si $\rho : G \rightarrow \mathfrak{S}_X$ est une représentation alors $\alpha : G \times X \rightarrow X$ définie pour tout $g \in G$ et $x \in X$ par

$$\alpha(g, x) := \rho_g(x)$$

est une action.

Exemple.

- Soit $n \in \mathbb{N}$. Le groupe symétrique \mathfrak{S}_n agit sur $\{1, \dots, n\}$ par permutation, c'est-à-dire

$$\begin{aligned}\mathfrak{S}_n \times \{1, \dots, n\} &\rightarrow \{1, \dots, n\} \\ (\sigma, k) &\mapsto \sigma(k)\end{aligned}$$

- Soit \mathbb{K} un corps. Le groupe $\mathrm{GL}_n(\mathbb{K})$ agit sur \mathbb{K}^n par multiplication, c'est-à-dire

$$\begin{aligned}\mathrm{GL}_n(\mathbb{K}) \times \mathbb{K}^n &\rightarrow \mathbb{K}^n \\ (A, x) &\mapsto Ax\end{aligned}$$

- Soit $n \in \mathbb{N}$. Le groupe diédral \mathcal{D}_n agit sur μ_n par multiplication, c'est-à-dire

$$\begin{aligned}\mathcal{D}_n \times \mu_n &\rightarrow \mu_n \\ (g, \zeta) &\mapsto g(\zeta)\end{aligned}$$

On peut vérifier que cette action est bien définie pour les générateurs R et S .

- Soit $H < G$ (sous-groupe de G). On a
 1. L'action par translation à gauche :

$$H \subset G \quad \text{par} \quad \rho^L : H \rightarrow \mathfrak{S}_G$$

$$\text{avec } \rho_h^L(g) = hg$$

2. L'action par translation à droite :

$$H \subset G \quad \text{par} \quad \rho^R : H \rightarrow \mathfrak{S}_G$$

$$\text{avec } \rho_h^R(g) = gh^{-1}$$

Remarque. Attention, en général $\rho_h(g) := gh$ ne définit pas une action de H sur G .

Définition 2.4. Soient X et Y des G -ensembles. On dit que

$$f : X \rightarrow Y$$

est **G -équivariante** si pour tout $x \in X$ et tout $g \in G$, on a

$$f(g \cdot x) = g \cdot f(x)$$

Exercice. On considère G un groupe et H un sous-groupe de G . On note G^L (respectivement G^R) l'ensemble G muni de l'action de H par translation à gauche (respectivement à droite). Montrer que

$$\begin{aligned}(\cdot)^{-1} : G^L &\rightarrow G^R \\ g &\mapsto g^{-1}\end{aligned}$$

est une bijection H -équivariante.

Définition 2.5. Soient G et Γ des groupes et V un \mathbb{K} -espace vectoriel.

- (i) Si $G \subset \Gamma$, les assertions suivantes sont équivalentes :

- G agit par homomorphismes sur Γ ,
- pour tout $g \in G$ et tout $\gamma_1, \gamma_2 \in \Gamma$, on a

$$g \cdot (\gamma_1 \gamma_2) = (g \cdot \gamma_1)(g \cdot \gamma_2)$$

- Il existe un morphisme de groupes

$$\rho : G \rightarrow \text{Aut}(\Gamma) < \mathfrak{S}_\Gamma$$

tel que pour tout $g \in G$, on a ρ_g est un morphisme de groupes.

- (ii) Si $G \subset V$, les assertions suivantes sont équivalentes :

- G agit linéairement sur V (l'action est linéaire),
- pour tout $g \in G$ et tout $v_1, v_2 \in V$ et tout $\lambda_1, \lambda_2 \in \mathbb{K}$, on a

$$g \cdot (\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 (g \cdot v_1) + \lambda_2 (g \cdot v_2)$$

- Il existe un morphisme de groupes

$$\rho : G \rightarrow \mathrm{GL}_{\mathbb{K}}(V) < \mathfrak{S}_V$$

tel que pour tout $g \in G$, on a ρ_g est une application linéaire.

Exemple.

1. Avec $H < G$, l'action de H par translation à gauche sur G est une action par homomorphismes si et seulement si $H = \{e\}$.

En effet, si $H = \{e\}$, alors l'action est triviale. Réciproquement, si l'action est par homomorphismes, on a

$$\begin{aligned} h \cdot (gg') &= (h \cdot g)(h \cdot g') \\ \iff hgg' &= hghg' \\ \iff e &= h \end{aligned}$$

pour tout $g, g' \in G$, donc $H = \{e\}$.

2. L'action de $\mathrm{GL}_n(\mathbb{K})$ sur \mathbb{K}^n est linéaire.

3. L'action par conjugaison :

Si $H < G$ alors $H \subset G$ par $\rho^C : H \rightarrow \mathrm{Aut}(G) < \mathfrak{S}_G$ et $\rho_h^C(g) = hgh^{-1}$.

Il s'agit d'une action par homomorphismes.

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

Démonstration. On sait que G agit sur lui même par translation à gauche $\rho^L : G \rightarrow \mathfrak{S}_G \simeq \mathfrak{S}_n$.
Donc

$$g \in \mathrm{Ker}(\rho^L) \implies \rho_g^L(e) = g \cdot e = e \implies g = e$$

Donc ρ^L est injectif et

$$\rho^L : G \rightarrow \rho^L(G) < \mathfrak{S}_G$$

est un isomorphisme de groupes. □

Exemple. μ_n est isomorphe au sous-groupe de \mathfrak{S}_n engendré par $(1 \ 2 \ \dots \ n)$.

$$\zeta_n = e^{2i\pi/n}, \quad \mu_n = \{\zeta^1, \dots, \zeta^n\} \simeq \{1, 2, \dots, n\}$$

et

$$\begin{aligned} \rho^L : \mu_n &\rightarrow \mathfrak{S}_{\mu_n} \simeq \mathfrak{S}_n \\ \zeta_n^k &\mapsto (1 \ 2 \ \dots \ n)^k \end{aligned}$$

Définition 2.6. On prend $G \subset X$.

1. On dit que $Y \subset X$ est **stable** par G si

$$\{g \cdot y \mid g \in G, y \in Y\} = G \cdot Y = Y$$

2. L'**orbite** de $x \in X$ est

$$\mathrm{orb}(x) = G \cdot x = \{g \cdot x \mid g \in G\}$$

qui est stable par G .

3. Le **stabilisateur** de $x \in X$ est

$$\mathrm{st}(x) = G_x = \{g \in G \mid g \cdot x = x\}$$

qui est un sous-groupe de G .

4. On dit que $x \in X$ est un **point fixe** de $g \in G$ si

$$g \cdot x = x$$

c'est à dire si $g \in \text{st}(x)$. L'ensemble des points fixes de g est noté

$$X^g = \{x \in X \mid g \cdot x = x\}$$

De plus, $x \in X$ est un point fixe de G si et seulement si

$$x \in X^g, \quad \forall g \in G$$

c'est à dire si et seulement si $G_X = G$. L'ensemble des points fixes de G est noté

$$X^G = \{x \in X \mid g \cdot x = x, \quad \forall g \in G\}$$

5. L'action est **transitive** si il existe $x \in X$ tel que $\text{orb}(x) = G \cdot x = X$ (dans ce cas, $X = G \cdot x, \forall x \in X$) Dans ce cas, on dit que X est un **G -espace homogène**.

Proposition. Soit X un G -ensemble et Y un ensemble.

Pour toute application $f : X \rightarrow Y$ constante sur les orbites, il existe une unique fonction $\bar{f} : X/G \rightarrow Y$ telle que

$$\forall x \in X, \quad \bar{f}(\text{orb}(x)) = f(x)$$

Démonstration. Par définition du quotient. □

Lemme. Soit X un G -ensemble et $x \in X$. On a les propriétés suivantes :

(i) Il existe une bijection

$$\begin{aligned} \bar{\alpha}_x : G/G_x &\rightarrow G \cdot x \\ gG_x &\mapsto g \cdot x \end{aligned}$$

(ii) $\bar{\alpha}_x$ est G -équivariante. C'est-à-dire que $G \curvearrowright G/G_x$ par translation à gauche, soit $g \cdot g'G_x := gg'G_x$.

(iii) Pour tout $g \in G$, on a

$$G_{g \cdot x} = gG_xg^{-1}$$

Démonstration.

(i) L'application $\bar{\alpha}_x$ est bien définie :

$$\begin{aligned} g'G_x = gG_x &\implies s \in G_x : g' = gs \\ &\implies g' \cdot x = (gs) \cdot x = g \cdot (s \cdot x) \\ &\qquad\qquad\qquad g \cdot x \end{aligned}$$

L'application $\bar{\alpha}_x$ est aussi surjective par définition de l'orbite

L'application $\bar{\alpha}_x$ est injective :

$$\begin{aligned} \bar{\alpha}_x(gG_x) &= \bar{\alpha}_x(g'G_x) \\ \iff g \cdot x &= g' \cdot x \\ \iff g^{-1} \cdot (g \cdot x) &= g^{-1} \cdot (g' \cdot x) \\ \iff g^{-1}g' \in G_x &\iff gG_x = g'G_x \end{aligned}$$

(ii) On a

$$\begin{aligned} \bar{\alpha}_x(g \cdot g'G_x) &= \bar{\alpha}_x(gg'G_x) \\ &= (gg') \cdot x \\ &= g \cdot (g' \cdot x) \\ &= g \cdot \bar{\alpha}_x(g'G_x) \end{aligned}$$

(iii) Soit $s \in G_{g \cdot x}$ Alors

$$\begin{aligned} s \cdot (g \cdot x) &= g \cdot x \\ \iff g^{-1} \cdot (s \cdot (g \cdot x)) &= g^{-1} \cdot (g \cdot x) \\ \iff (g^{-1} s g) \cdot x &= x \\ \iff g^{-1} s g &\in G_x \\ \iff s &\in g G_x g^{-1} \end{aligned}$$

□

Corollaire. Soit X un G -espace homogène (c'est à dire qu'il n'y a qu'une seule orbite). Alors, il existe $H < G$ et $f : G/H \rightarrow X$ une bijection G -équivariante.

Démonstration. Soit $x \in X$, on pose $G = G_x$ et on applique le Lemme précédent. □

Exemple. On sait que $\mathrm{GL}_n(\mathbb{K}) \curvearrowright \mathbb{P}^{n-1}(\mathbb{K})$ transitivement et donc on obtient une application

$$\mathrm{GL}_n(\mathbb{K})/H \rightarrow \mathbb{P}^{n-1}(\mathbb{K})$$

bijective et G -équivariante où

$$H = (\mathrm{GL}_n(\mathbb{K}))_{[e_1]} = \left\{ \begin{pmatrix} a & b \\ 0 & D \end{pmatrix} \middle| \begin{matrix} a \in \mathbb{K}^\times \\ b^T \in \mathbb{K}^{n-1} \\ D \in \mathrm{GL}_{n-1}(\mathbb{K}) \end{matrix} \right\}$$

Corollaire : Formule des classes. Soient G, X finis et $G \curvearrowright X$. Alors, les propriétés suivantes sont vraies :

- (i) Pour tout $x \in X$, on a $|G \cdot x| = [G : G_x] = |G/G_x|$.
- (ii) Si on a $X = (G \cdot x_1) \sqcup \dots \sqcup (G \cdot x_n)$ alors

$$|X| = \sum_{i=1}^n |G \cdot x_i| = \sum_{i=1}^n \frac{|G|}{|G_{x_i}|}$$

Démonstration.

(i) On a

$$\begin{aligned} \bar{\alpha}_x : G/G_x &\rightarrow G \cdot x \\ gG_x &\mapsto g \cdot x \end{aligned}$$

bijective donc

$$|G \cdot x| = |G/G_x| = [G : G_x]$$

(ii) On a $X = \bigsqcup_{i=1}^n (G \cdot x_i)$ donc

$$\begin{aligned} |X| &= \sum_{i=1}^n |G \cdot x_i| \\ &= \sum_{i=1}^n |G/G_{x_i}| \\ &= \sum_{i=1}^n \frac{|G|}{|G_{x_i}|} \end{aligned}$$

□

Définition 2.7. Soit $p \in \mathbb{N}$ premier. Un groupe G est un **p -groupe fini** si $|G| = p^n$ avec $n > 0$.

Lemme. Si G est un p -groupe fini et X un G -ensemble fini. Alors

$$|X| \equiv |X^G| \pmod{p}$$

où X^G est l'ensemble des points fixes de $G \curvearrowright X$.

Démonstration. Soit $x \in X \setminus X^G$. Alors

$$1 < |G \cdot x| = |G/G_x| = \frac{|G|}{|G_x|}$$

qui divise $|G|$. Alors $|G \cdot x| \equiv 0 \pmod{p}$

Si $X = (G \cdot x_1) \sqcup \cdots \sqcup (G \cdot x_n)$ et $X = (G \cdot x_1) \sqcup \cdots \sqcup (G \cdot x_m)$ avec $1 \leq m \leq n$. Alors la formule des classes donne

$$|X| = \sum_{i=1}^m |G \cdot x_i| + \sum_{j=m+1}^n |G \cdot x_j| \equiv m = |X^G| \pmod{p}$$

□

Corollaire. Soit G un p -groupe fini. Alors, le centre de G noté $Z(G) \neq \{e\}$.

Démonstration. On a $G \curvearrowright G$ par conjugaison, donc

$$|G| \equiv |G^G| = |Z(G)| \pmod{p}$$

et donc $|Z(G)| > 1$.

□

Théorème de Cauchy. Soit $p \in \mathbb{N}$ premier qui divise $|G|$. Alors G admet un élément d'ordre p .

Démonstration. A voir sur le Moodle.

□

Lemme de Burnside. Soit G un groupe fini et X un G -ensemble fini. Alors

$$|X/G| = \frac{1}{|G|} \times \sum_{g \in G} |X^g|$$