Séance n° 2

Thème : Groupes (II)

Table des matières

1 Notes de cours

1.1 Conjugaison

Soient X et X' sont deux ensembles et $\phi : X \to X'$ une bijection. À toute application $f : X \to X$, on peut associer une application $g : X' \to X'$ qui est en quelque sorte égale à f « transformée » par ϕ, selon le diagramme :

$$\begin{array}{ccc} X & \xrightarrow{f} & X \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi} \\ X' & \xrightarrow[g=\phi f \phi^{-1}]{} & X' \end{array}$$

L'application $g = \phi f \phi^{-1}$ s'appelle la conjuguée de f par ϕ. Si X et X' sont munis d'une structure algébrique (telle que groupe, espace vectoriel, ...), si ϕ est un isomorphisme pour cette structure et si f est un morphisme, alors g sera aussi un morphisme qui possédera exactement les mêmes propriétés "géométriques" que f (en qualifiant de géométrique une propriété qui s'exprime à l'aide de la structure de X).

Si par exemple X et X' sont deux plans euclidiens orientés, $f \in L(X)$ et ϕ isométrie bijective directe de X dans X' (=isomorphisme d'espace vectoriel euclidien orienté) alors
f symétrie orthogonale par rapport à $F \implies g$ symétrie orthogonale par rapport à $\phi(F)$
f rotation d'angle $\theta \implies g$ rotation d'angle θ
Si ϕ est indirecte au lieu de directe, f rotation d'angle $\theta \implies g$ rotation d'angle $-\theta$.

Si on note $\mathrm{Iso}(X)$ le groupe des isomorphismes de X (pour la structure envisagée), et si ϕ est un isomorphisme de X dans X', alors la conjugaison par ϕ

$$\begin{array}{ccc} \mathrm{Iso}(X) & \to & \mathrm{Iso}(X') \\ f & \mapsto & \phi \circ f \circ \phi^{-1} \end{array}$$

est un isomorphisme de groupe. En particulier si $X = X'$, c'est un automorphisme de $\mathrm{Iso}(X)$

Il est remarquable qu'on puisse ensuite « abstraire » cette dernière situation à un groupe quelconque au lieu d'un groupe d'application $\mathrm{Iso}(X)$. Soit en effet un groupe quelconque G, et $a \in G$. L'application

$$\begin{array}{rccc} t_a & : & G & \to & G \\ & & g & \mapsto & aga^{-1} \end{array}$$

est un automorphisme de G, appelé automorphisme intérieur de G. Deux éléments (ou deux sous-groupes de G) images l'un de l'autre par un automorphisme intérieur sont dit conjugués.

1.2 Sous-groupes distingués, groupe quotient

Soit $f : G \to G'$ un morphisme de groupe. Le noyau $H = \mathrm{Ker}(f)$ de f est un sous-groupe de G, on le sait, mais ne peut pas être n'importe quel sous-groupe. On a en effet la propriété :

$$x^{-1}y \in H \iff f(x^{-1}y) = e \iff f(x) = f(y) \iff f(yx^{-1}) = e \iff yx^{-1} \in H$$

C'est-à-dire que les congruences à gauche et à droite modulo H sont les mêmes relations d'équivalence. Ce qui s'écrit aussi :

$$(*) \quad \forall x \in G,\ xH = Hx$$

Un sous-groupe H de G qui possède cette propriété est dit distingué dans G (ou normal, ou encore invariant[1]), ce que l'on note

$$H \lhd G$$

On vérifie aisément que $(*)$ équivaut à

$$\forall x \in G,\ xH \subset Hx$$

ou bien

$$\forall x \in G,\ xHx^{-1} \subset H \quad \text{ ou encore } \quad \forall x \in G,\ xHx^{-1} = H$$

Le noyau d'un morphisme est, comme on vient de le voir, un sous-groupe distingué. Ce qui suit montrera que, réciproquement, tout sous-groupe distingué est le noyau d'un certain morphisme.

Soient maintenant G un groupe et $\mathcal{R}$ une relation d'équivalence sur G. On dit que $\mathcal{R}$ est compatible avec la loi de G si $[xy]_\mathcal{R}$ ne dépend pas du choix de x et de y dans leur classe d'équivalence respectives. En d'autres termes :

$$\forall x, x', y, y' \in G,\ x\mathcal{R}x' \text{ et } y\mathcal{R}y' \implies xy\mathcal{R}x'y'$$

Lorsque c'est le cas (et seulement lorsque c'est le cas), on peut munir $G/\mathcal{R}$ d'une loi de composition interne en posant

$$[x]_\mathcal{R}[y]_\mathcal{R} = [xy]_\mathcal{R}$$

Il est alors immédiat qu'il s'agit d'une loi de groupe et que $x \mapsto [x]_\mathcal{R}$ est un morphisme de groupe. Notons H son noyau. C'est un sous-groupe distingué de G et l'on a

$$x\mathcal{R}y \iff [x]_\mathcal{R} = [y]_\mathcal{R} \iff [xy^{-1}]_\mathcal{R} \iff x^{-1}y \in H$$

On voit ainsi que $\mathcal{R}$ est la congruence modulo le sous-groupe distingué H.

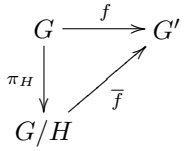
[1] Parce qu'il est invariant par les automorphismes intérieurs de G. Un automorphisme intérieur de G induit donc sur H distingué un automorphisme qu'on pourrait être tenté de qualifier « d'extérieur » !

Réciproquement, si H est un sous-groupe distingué, la congruence modulo H (à gauche ou à droite : ce sont les mêmes relations) est compatible avec la loi de G. L'ensemble $G/\mathcal{R}$ est ainsi muni d'une structure de groupe. Ce groupe est noté G/H. L'application

$$\begin{array}{rccc} \pi_H & : & G & \to & G/H \\ & & x & \mapsto & [x]_H = xH = Hx \end{array}$$

est un morphisme de G dans G/H dont le noyau est H.

Soient maintenant G, G' des groupes, $f : G \to G'$ un morphisme et $H \lhd G$. Comme dans le cas des groupes abéliens, l'application f est compatible avec la congruence modulo H si et seulement si $H \subset \mathrm{Ker}(f)$. Dans ce cas, f induit un morphisme $g : G/H \to G'$ (qui vérifie donc $g([x]_H) = f(x)$).



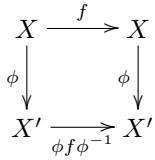
$f = \overline{f} \circ \pi_H$

1.3 Groupe symétrique

Soit X un ensemble. On appelle groupe symétrique de X le groupe $S(X)$ des permutations de X (= bijections de X dans lui-même). Pour un élément σ de $S(X)$, il faut savoir faire la différence entre une propriété « purement algébrique » et une propriété « géométrique » de σ. Les premières s'expriment uniquement à l'aide de la loi du groupe, tandis que les formulations des secondes utilise les propriétés de σ en tant qu'application. Par exemple le fait que σ vérifie $\sigma^2 = \mathrm{Id}_X$ est une propriété algébrique. Que σ soit une transposition est une propriété géométrique.

Ainsi qu'on l'a vu, si X et X' sont deux ensembles et $\phi : X \to X'$ est une bijection, alors la conjugaison par ϕ :

$$\begin{array}{ccc} S(X) & \to & S(X') \\ f & \mapsto & \phi \circ f \circ \phi^{-1} \end{array}$$



est un isomorphisme de groupe. En particulier, si $X = \{x_1, x_2, \ldots, x_n\}$ est fini, $S(X)$ est isomorphe à $S_n = S(\llbracket 1, n \rrbracket)$ (mieux : S_n opère sur $\llbracket 1, n \rrbracket$ exactement comme $S(X)$ opère sur X).

Un élément σ de S_n peut être indiqué par un tableau qui indique explicitement pour chaque $k \in \llbracket 1, n \rrbracket$ son image :

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

Si $\sigma \in S(X)$, on appelle support de σ l'ensemble des points de X qui sont affectés par σ : $\mathrm{Supp}(\sigma) = \{x \in X;\ \sigma(x) \neq x\}$. Un instant de réflexion convainc que deux permutations à supports disjoints commutent.

Si $a_1, a_2, \ldots, a_p$ sont des éléments distincts de X, on note $c = (a_1, a_2, \ldots, a_p)$ la permutation $c \in S(X)$ qui envoie a_k sur a_{k+1} pour $k \in \llbracket 1, p-1 \rrbracket$, a_p sur a_1 et fixe tout autre élément de X. Cette permutation

est qualifiée de cycle de longueur p. L'ensemble $\{a_1, a_2, \ldots, a_p\}$ est le support du cycle. Un cycle de longueur 2 est appelé transposition.

Si $a_1, a_2, \ldots, a_p, a_{p+1}, \ldots, a_q$ sont des éléments deux à deux distincts de X, on a la formule suivante utile, qui signifie que le produit de deux cycles dont les supports se rencontrent en un point unique est un cycle :

$$(a_1, a_2, \ldots, a_p)(a_p, a_{p+1}, \ldots, a_q) = (a_1, a_2, \ldots, a_q)$$

Une autre formule d'usage fréquent est la suivante. Soient un cycle $c = (a_1, a_2, \ldots, a_p)$ et $\sigma \in S(X)$:

$$\begin{array}{ccc} X & \xrightarrow{c} & X \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ X & \xrightarrow[\sigma c \sigma^{-1}]{} & X \end{array}$$

Alors le conjugué $c' = \sigma c \sigma^{-1}$ de c par σ est un cycle similaire à c, mais qui opère sur les images des a_i par σ :

$$\sigma(a_1, a_2, \ldots, a_p)\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_p))$$

(cette formule est une évidence dès lors qu'on a compris ce qu'est une conjugaison)

Soit X un ensemble fini et $\sigma \in S(X)$. La relation sur $x \mathcal{R} y \iff \exists n \in \mathbb{Z};\ y = \sigma^n(x)$ est une relation d'équivalence. Les classes d'équivalence sont appelées orbites de σ. Les classes d'équivalence réduite à un point sont constituées d'un point fixe. Soient $C_1, C_2, \ldots, C_q$ les classes d'équivalences non réduites à un point. Chaque classe C_k est stable par σ qui induit une permutation de C_k, laquelle, on le voit aisément, est un cycle dont le support est C_k. Si on note $c_k \in S(X)$ le cycle qui coïncident avec σ sur C_k et laisse fixe tout autre élément de X, on a

$$\sigma = c_1 c_2 \ldots c_q$$

Ainsi toute permutation se décompose en produit de cycles à supports disjoints. On vérifie que cette décomposition est unique à l'ordre des facteurs près.

Soient $\eta \in S(X)$, $\sigma \in S(X)$. Si on décompose η en produit de cycles disjoints : $\eta = c_1 c_2 \ldots c_q$, alors la décomposition en produit de cycles disjoints est

$$\sigma \eta \sigma^{-1} = (\sigma c_1 \sigma^{-1})(\sigma c_2 \sigma^{-1}) \ldots (\sigma c_q \sigma^{-1})$$

On voit ainsi que deux éléments conjugués ont, pour tout entier ℓ, le même nombre de cycles de longueur ℓ et on vérifie aisément que cette condition est aussi suffisante.

Soit X un ensemble fini. Les transpositions forment une famille génératrice de $S(X)$. En effet, si σ est une permutation distincte de l'identité et si l'on choisit $x \in X$ tel que $\sigma(x) \neq x$, alors $(x, \sigma(x)) \circ \sigma$ possède au moins un point fixe de plus que σ. Une récurrence descendante sur le nombre de points fixes atteste alors de l'existence de transpositions $\tau_1, \ldots, \tau_q$ telles que $\tau_q \tau_{q-1} \ldots \tau_1 \sigma = \mathrm{Id}$, d'où $\sigma = \tau_1 \tau_2 \ldots \tau_q$.

Étant donné $\sigma \in S_n$, on dit qu'une paire $P = \{i, j\} \subset [\![1, n]\!]$ $(i \neq j)$ est une inversion pour σ si $(\sigma(j) - \sigma(i))(j - i) < 0$. On désigne par signature de σ la valeur $\varepsilon(\sigma) = +1$ ou -1 selon que le nombre

d'inversions de σ est pair ou impair. Si on pose, pour une paire donnée, $s_\sigma(P) = 1$ ou -1 selon que P est ou non une inversion, on a $\varepsilon(\sigma) = \prod_P s_\sigma(P)$, d'où (en notant $\sigma(\{i,j\}) = \{\sigma(i), \sigma(j)\}$)

$$\varepsilon(\sigma' \circ \sigma) = \prod_P s_{\sigma' \circ \sigma}(P) = \prod_P s_{\sigma'}(\sigma(P)) s_\sigma(P) = \prod_P s_{\sigma'}(\sigma(P)) \prod_P s_\sigma(P) = \varepsilon(\sigma)\varepsilon(\sigma')$$

Ainsi, ε est un morphisme de S_n dans $\{-1, 1\}$. Son noyau, $A_n = \mathrm{Ker}(\varepsilon)$ est appelé le groupe alterné de degré n. Une permutation de signature 1 est dite paire. Une permutation de signature -1 est dite impaire.
On note que si c est un cycle de longueur ℓ, alors $\varepsilon(\ell) = (-1)^{\ell+1}$ (donc c et ℓ sont de « parités opposées » !). On en déduit :
Si σ est le produit de q transpositions, alors $\varepsilon(\sigma) = (-1)^q$
Si σ possède s orbites, alors $\varepsilon(\sigma) = (-1)^{n-s}$.

1.4 Action d'un groupe sur un ensemble

Soit G un groupe. Si on veut avoir une image « géométrique » de G, on peut tenter de « réaliser » G comme sous-groupe du groupe des permutation d'un ensemble X, c'est-à-dire de trouver un morphisme injectif de G dans $S(X)$. Une représentation moins « fidèle » est fournie par un morphisme quelconque de G dans $S(X)$. D'où les définitions :
Soit G un groupe et X un ensemble. Une opération (ou action) de G sur X est la donnée d'un morphisme $\rho : G \to S(X)$. On convient de noter, pour $g \in G$ et $x \in X$: $g.x = \rho(g)(x)$. On note que :

$$\forall g, g' \in G,\ \forall x \in X,\ g.(g'.x) = (gg').x \qquad \forall x \in X,\ e_G.x = x$$

Réciproquement, toute application $. : G \times X \to X$ vérifiant ces deux points définit une opération de G sur X (en posant $\rho(g)(x) = g.x$; attention, le premier point ne suffit pas). L'action est dite fidèle si ρ est injective.

Voici quelques exemples classiques d'actions de groupe :
• $S(X)$ opère fidèlement sur X (en posant $\sigma.x = \sigma(x)$).
• Si E est un K-espace vectoriel, $\mathrm{GL}(E)$ opère fidèlement sur E ($\rho : GL(E) \to S(E)$ est l'injection canonique et $g.x = g(x)$).
• Plus généralement, si X est un ensemble muni d'une structure donnée, $\mathrm{Iso}(X)$ opère fidèlement sur X.
• Si G est un groupe, E un $\mathbb{C}$-espace vectoriel, et $\rho : G \to GL(E)$ un morphisme, G opère "linéairement" sur E. On dit que ρ est une représentation linéaire de G (la théorie des représentations linéaires est passionnante !).
• Si X est une partie d'un espace affine euclidien $\mathcal{E}$, l'ensemble G des isométries de $\mathcal{E}$ qui laissent X globalement invariant est un sous-groupe de G de $Is(\mathcal{E})$ qui opère naturellement sur X (par $g.x = g(x)$). L'opération est fidèle si et seulement si X "engendre" $\mathcal{E}$, c'est-à-dire n'est contenu dans aucun sous-espace affine strict. On définit ainsi le groupe du cube, le groupe du tétraèdre, etc.
• Si G est un groupe, alors G opère sur lui-même par translation à gauche, c'est-à-dire en posant : $\forall g \in G, \forall x \in X,\ g.x = gx$
• Une autre action usuelle de G sur lui-même est l'action par conjugaison : $g.x = gxg^{-1}$.
• G opère par translation à gauche sur l'ensemble des classes à gauche modulo H (où H est un sous-groupe) : $g.(xH) = gxH$.
• G opère par conjugaison sur l'ensemble de ses sous-groupes : $x.H = xHx^{-1}$.
Ces quatre actions sont fort utiles pour obtenir des résultats théoriques sur les groupes finis.

Soit G un groupe opérant sur un ensemble X. On définit :

- L'orbite de $x \in X$, qu'on notera : $\omega_x = \{g.x,\ g \in G\}$
- Le stabilisateur de $x \in X$, qu'on notera : $G_x = \{g \in G;\ g.x = x\}$.
- L'ensemble des points fixes de $g \in G$, qu'on notera $X^g = \{x \in X;\ g.x = x\}$

Il faut avoir à l'esprit que deux points x et $y \in X$ d'une même orbite ont des rôles similaires relativement à G. Par exemple, si $y = h.x$ alors $g \in G_y \iff g.y = y \iff gh.x = h.x \iff h^{-1}gh \in G_x \iff g \in hG_xh^{-1}$, d'où

$$G_y = hG_xh^{-1}$$

Quelques relations fructueuses relient les cardinaux de ces parties :

• En premier lieu, il est naturel de penser que plus nombreux sont les éléments de G qui fixent x, moins l'orbite de x est vaste. Plus précisément :

$$\forall x \in X,\ [G : G_x] = |\omega_x| \qquad (\text{si } |G| \text{ est fini, } \frac{|G|}{|G_x|} = |\omega_x|)$$

En effet, l'application surjective $x \mapsto g.x$ de G dans ω_x définit une relation d'équivalence sur G (avoir même image) qui n'est autre que la congruence à gauche modulo G_x ($g.x = h.x \iff g^{-1}h.x = x \iff g^{-1}h \in G_x$).

• Les orbites constituent une partition de X. Si X est fini, on a, en notant Ω l'ensemble des orbites, la relation évidente

$$|X| = \sum_{\omega \in \Omega} |\omega|$$

Lorsque $|G|$ est fini, on peut l'écrire, C désignant une partie de X contenant un et un seul élément de chaque orbite :

$$|X| = \sum_{a \in C} \frac{|G|}{|G_a|}$$

C'est ce qu'on appelle « l'équation aux classes ».
Il est fréquent qu'on l'utilise en isolant les orbites réduites à un point. En notant $X^G = \{x \in X;\ \forall g \in G, g.x = x\}$ et C' une partie contenant un et un seul représentant de chaque orbite non réduite à un point (par exemple $C' = C \setminus X^G$) :

$$|X| = |X^G| + \sum_{a \in C'} \frac{|G|}{|G_a|}$$

En particulier, lorsque G est un p-groupe (groupe d'ordre p^n, p premier), il vient

$$|X| \equiv |X^G| \quad [p]$$

• Si G et X sont finis, on peut envisager le nombre moyen de points fixes des éléments de G et constater que

Le nombre d'orbites est égal au nombre moyen de points fixes des éléments de G.

C'est la formule de Burnside. On l'obtient facilement en dénombrant « horizontalement » et « verticalement » les éléments de $\{(g, x) \in G \times X;\ g.x = x\}$. C'est en effet d'une part $\sum_{g \in G} |X^g|$ et, d'autre part,

$$\sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|\omega_x|} = \sum_{\omega \in \Omega} |\omega| \times \frac{|G|}{|\omega|} = |G||\Omega|$$

D'où

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