Chapitre II - Des groupes

Le problème originel : **résolution des équations algébriques par radicaux**

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0$$

- $n = 2$: connue des Babyloniens
- XII^e : résolution littérale
- 1545 : *Ars magna* de Cardan $n = 3$ et $n = 4$ (del Ferro, Tartaglia, Viète, . . . ?)
- $\sim$1770 : résolvante (Lagrange, Vandermonde, Waring)
- "permutations" (ou "arrangements") de n objets et "substitutions" (Ruffini, Vandermonde, Cauchy, . . . ?)
- 1830 : Evariste Galois (1811-1832) : Groupe de Galois de P

Groupe de Galois (d'un polynôme, d'une extension de corps ...)

Soient $P \in K[X]$ et $z_1, \ldots, z_n$ ses $n \leq \deg(P)$ racines distinctes dans un corps de décomposition de P.

Définition (groupe de Galois d'un polynôme)

C'est le sous-groupe de $\mathfrak{S}_n$ qui préserve les relations algébriques entre les racines.

$$\begin{aligned}\mathrm{Gal}_K(P) \overset{\text{déf}}{=} \{\sigma \in \mathfrak{S}_n : \quad & (\forall R \in K[X_1, \ldots, X_n]) \\ & R(z_1, \ldots, z_n) = 0 \Longrightarrow R(z_{\sigma^{-1}(1)}, \ldots, z_{\sigma^{-1}(n)}) = 0\}\end{aligned}$$

Soit L/K une extension de corps.

Définition (groupe de Galois de L/K)

C'est le sous-groupe des automorphismes de L qui laisse K invariant :

$$\mathrm{Gal}(L/K) \overset{\text{déf}}{=} \mathrm{Aut}_K(L)$$

Soient $P \in K[X]$, $z_1, \ldots, z_n$ ses $n \leq \deg(P)$ racines distinctes, et $L = K(z_1, \ldots, z_n)$ son corps de décomposition.

$$\boxed{\mathrm{Gal}_K(P) \cong \mathrm{Gal}(L/K)}$$

Théorème (Galois)

$$P = 0 \text{ } \textit{résoluble par radicaux} \iff \textit{Gal}_K(P) \text{ } \textit{résoluble}$$

Symétrie, invariance et groupe

Exemples :

1. sous-groupe de $\mathrm{Isom}(\mathbb{R}^2)$ qui laisse invariant un triangle équilatéral, isocèle, quelconque.
2. groupe de symétrie de H_2O, CH_4, ...
3. 1872 : Le programme d'Erlangen, Félix Klein (1849-1925) : groupes et géométries.
4. Henri Poincaré (1854-1912) : groupes et équations différentielles, groupes et sciences physiques.
5. 1918 : Problèmes variationnels invariants, Emmy Noether (1882-1935) : groupes et lois de conservation.

(et depuis 1905 : relativité, mécanique quantique)

Sur l'ubiquité des groupes ...

dixit Hermann Weyl :

"Un principe directeur des mathématiques modernes tient en cette leçon : lorsque vous avez affaire à une entité S munie d'une certaine structure, essayez de déterminer son groupe d'automorphismes, *i.e.* le groupe des transformations de ses éléments qui préservent les relations structurales. Vous pouvez espérer gagner une profonde compréhension de la constitution de S de cette manière."

La structure de groupe est présente dans deux "grandes familles" :

1. les nombres : $(\mathbb{Z}, +, 0)$, ...
2. les transformations d'ensembles : $(\mathrm{Bij}(E), \circ, \mathrm{Id}_E)$, ...

On peut construire des groupes "à la main", mais le plus souvent, on obtient des groupes intéressants à partir d'autres groupes déjà construits : sous-groupe, groupe produit, noyau ou image de morphisme, groupe quotient, ...

Questions de groupes . . .

Quelques questions à propos d'un groupe :

- son ordre ? ses sous-groupes ?
- Est-il isomorphe à un groupe déjà connu ?
- Est-il simple ? résoluble ?
- Comment agit-il sur un ensemble ?
- Comment est-il engendré ?

Objectifs de ce chapitre :

1. donner un sens à ces questions ;
2. proposer des éléments de réponses . . .

. . . et faire des liens avec l'arithmétique.

1. Quelques exemples de groupe

1. groupes à (très) peu d'éléments, table de Pythagore d'un groupe fini
2. $(\mathrm{Bij}(E), \circ, \mathrm{Id}_E)$, $\mathrm{Aut}(G)$, $\mathrm{GL}(E)$, ...
3. groupe symétrique $\mathfrak{S}_n$

Comment les visualiser ?

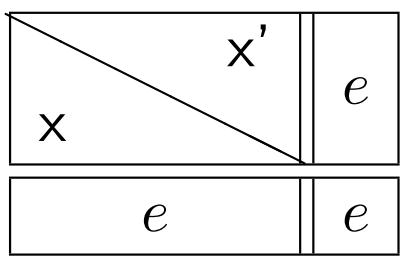
1. Groupes à (très) peu d'éléments

Premières questions :

- Soit $n \in \mathbb{N}$; existe-t-il des groupes à n éléments ?
- Les groupes à n éléments sont-ils isomorphes ?

• L'ensemble vide $\emptyset$ n'a pas de structure de groupe (élément neutre ?).

• **Le groupe à un élément :**
Un ensemble à un élément $E = \{e\}$ ne peut avoir qu'une seule structure de groupe $(E, *, e)$ puisque la loi $*$ se résume à $e * e = e$. Sa table (de Pythagore) est :



(chaque case contient $x * x'$)

Exercice : (de compréhension)
Tous les groupes à un élément sont isomorphes (de manière unique).

"le" groupe à 2 éléments

Soit un ensemble à 2 éléments : $E = \{a_0; a_1\}$ (avec $a_0 \neq a_1$).
On veut en faire un groupe $(E, *, e)$.

- Si on choisit $e = a_0$, la table de $(E, *, a_0)$ doit être (exercice) :

x \ x'	a_0	a_1
a_0	a_0	a_1
a_1	a_1	a_0

- Si on choisit $e = a_1$, la table de $(E, *', a_1)$ doit être (exercice) :

x \ x'	a_0	a_1
a_0	a_1	a_0
a_1	a_0	a_1

Table d'un groupe et exercices . . .

Lemme (la table d'un groupe est un carré latin)

Chaque colonne et chaque ligne de la table d'un groupe contient exactement une fois chaque élément du groupe.

Démonstration : sur la ligne a_i : $a_i * a_j = a_i * a_{j'} \Longrightarrow a_j = a_{j'}$. □

Exercices :

1. Permuter 2 lignes (resp. colonnes) d'une table ne change pas la loi.
2. L'associativité ne se lit pas directement sur la table ; vérifier-la pour les tables précédentes.
3. Montrer que les deux structures de groupes proposées pour $E = \{a_0; a_1\}$ sont isomorphes (de manière unique) : unicité, à isomorphisme (unique) près de la structure de groupe à 2 éléments.
4. Comment la table traduit-elle l'éventuelle commutativité de la loi ?

Table d'un groupe : effet d'un changement de nom

Lemme (bijection et structure de groupe)

Soient un groupe $(G, *, e)$, un ensemble G', et une bijection $\varphi : G \to G'$. Alors il existe une unique structure de groupe $(G', *', e')$ telle que φ soit un morphisme de groupe (et donc un isomorphisme) :

$$\forall a, b \in G, \qquad \varphi(a) *' \varphi(b) = \varphi(a * b), \qquad et \;\; e' = \varphi(e)$$

Démonstration : vérifier que $(G', *', e')$ est bien un groupe (exercice). □

Définition (changement de nom)

Soit une table d'opération sur G. La transformation de chaque élément de cette table par une bijection $\varphi : G \to G'$ s'appelle un changement de nom.

Par le lemme, un changement de nom sur une table d'un groupe $(G, *, e)$ est une table d'un groupe $(G', *', e')$ isomorphe.

Exemple d'effet d'un changement de nom

x \ x'	a_0	a_1	a_2
a_0	a_0	a_1	a_2
a_1	a_1	a_2	$a_1 * a_2$
a_2	a_2	a_0	a_1

$\xrightarrow{\varphi}$

x \ x'	$\varphi(a_0)$	$\varphi(a_1)$	$\varphi(a_2)$
$\varphi(a_0)$	$\varphi(a_0)$	$\varphi(a_1)$	$\varphi(a_2)$
$\varphi(a_1)$	$\varphi(a_1)$	$\varphi(a_2)$	$\varphi(a_1 * a_2)$
$\varphi(a_2)$	$\varphi(a_2)$	$\varphi(a_0)$	$\varphi(a_1)$

Lemme (automorphisme et changement de nom)

Soit un groupe $(G, *, e)$. Une bijection $\varphi : G \to G$ est un automorphisme de G si et seulement si le changement de nom associé à φ laisse la table de $*$ invariante.

Démonstration : automorphisme $\iff$ $*' = *$ (comprendre cela !). $\square$

"le" groupe à 3 éléments

Soit un ensemble à 3 éléments : $E = \{a_0; a_1; a_2\}$.
On veut en faire un groupe $(E, *, e)$.
Exercices :

1. Si on choisit $e = a_0$, la table de $(E, *, a_0)$ doit être :

x \ x'	a_0	a_1	a_2
a_0	a_0	a_1	a_2
a_1	a_1	a_2	a_0
a_2	a_2	a_0	a_1

2. Montrer que le changement de nom associé à une bijection $\varphi : E \to E$ telle que $\varphi(a_0) = a_0$ laisse cette table invariante ; il s'agit donc d'un automorphisme.
3. Ecrire les 2 autres tables possibles. En déduire que deux groupes à 3 éléments sont nécessairement isomorphes.

“les deux” groupes à 4 éléments

Soit un ensemble à 4 éléments : $E = \{a_0; a_1; a_2; a_3\}$.
Si on choisit $e = a_0$, la table de $(E, *, a_0)$ doit être l'une de celles-ci (exercice) :

(I)

x \ x'	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_0	a_3	a_2
a_2	a_2	a_3	a_1	a_0
a_3	a_3	a_2	a_0	a_1

(II)

x \ x'	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_0	a_3	a_2
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_2	a_1	a_0

(III)

x \ x'	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_2	a_3	a_0
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_0	a_1	a_2

(IV)

x \ x'	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_3	a_0	a_2
a_2	a_2	a_0	a_3	a_1
a_3	a_3	a_2	a_1	a_0

“les deux” groupes à 4 éléments (2)

Exercices :

1. Vérifier que les 4 tables sont bien des tables de groupe. Programme MuPAD pour tester l'associativité ?
2. Montrer que les tables (I), (III) et (IV) sont isomorphes, *i.e.* se déduisent l'une de l'autre par un changement de nom (à préciser).
3. Montrer que la table (II) n'est pas isomorphe aux autres.

(voir TP ?)

2. $(\mathrm{Bij}(E), \circ, \mathrm{Id}_E)$, $\mathrm{Aut}(G)$, $\mathrm{GL}(E)$, ...

Soit E un ensemble non vide.

$$\mathrm{Bij}(E) \overset{\text{déf}}{=} \{f : E \to E \ \text{ bijective}\}$$

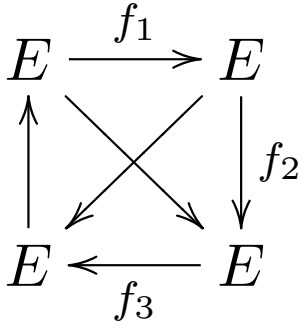
Lemme (groupe des bijections d'un ensemble)

$(Bij(E), \circ, Id_E)$ est un groupe.

Démonstration : découle de la définition de $\circ$. □

L'associativité équivaut à la commutativité des diagrammes :

$$\begin{aligned} & f_3 \circ (f_2 \circ f_1) \\ = \ & (f_3 \circ f_2) \circ f_1 \end{aligned}$$



groupe des automorphismes $\mathrm{Aut}(G)$

Si l'ensemble E possède une structure (de groupe par exemple), il est légitime de considérer les permutations de E qui respectent cette structure.

Définition (groupe des automorphismes)

Soit un groupe $(G, *, e)$. On appelle groupe des automorphismes de G

$$\mathrm{Aut}(G) \overset{\text{déf}}{=} \left\{\varphi : G \to G \ \text{ automorphisme (de groupe)}\right\}$$

(muni de la composée $\circ$).

Remarques :

1. Cette définition est générique : remplacer "groupe" par anneau, ...
2. $\mathrm{Aut}(G)$ est un sous-groupe de $(\mathrm{Bij}(G), \circ, \mathrm{Id}_G)$.
3. automorphisme intérieur associé à $g \in G$:

$$\begin{array}{rcl} i_g : G & \longrightarrow & G \\ x & \longmapsto & g * x * g^{-1} \end{array}$$

groupe linéaire $\mathrm{GL}(E)$

Si l'ensemble E possède une structure de $\mathbb{K}$-espace vectoriel, le groupe des automorphismes correspondant s'appelle le groupe linéaire de E.

Définition (groupe linéaire)

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

$$\mathrm{GL}_{\mathbb{K}}(E) \overset{\text{déf}}{=} \{\varphi : E \to E \quad \mathbb{K}-\text{linéaire et bijective}\}$$

(muni de la composée $\circ$).

$\mathrm{GL}_{\mathbb{K}}(E)$ est un sous-groupe de $(\mathrm{Bij}(E), \circ, \mathrm{Id}_E)$.

Exercice : rappeler la structure d'espace vectoriel.

3. Groupe symétrique $\mathfrak{S}_n$

Soit $n \in \mathbb{N}, \quad n \geq 1$

Définition (groupe symétrique)

$\mathfrak{S}_n$ est "le" groupe des permutations d'un ensemble à n éléments, soit (pour fixer les idées),

$$\mathfrak{S}_n \overset{\text{déf}}{=} \left(\mathrm{Bij}(\llbracket 1, n \rrbracket), \circ, \mathrm{Id}_{\llbracket 1,n \rrbracket}\right)$$

Exercice : Montrer que si $\mathrm{card}(E) = n$ alors le groupe $(\mathrm{Bij}(E), \circ, \mathrm{Id}_E)$ est isomorphe à $\mathfrak{S}_n$. L'isomorphisme est-il unique ?

Notation pour $\sigma \in \mathfrak{S}_n$:

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

... qui s'abrège pour les éléments remarquables : transpositions, cycles

$$\tau = \begin{pmatrix} 1 & 2 \end{pmatrix} \quad , \qquad c = \begin{pmatrix} i_1 & i_2 & \cdots & i_k \end{pmatrix}$$