Chapitre 8 : structures algébriques

MPSI Lycée Camille Jullian

8 décembre 2022

L'algèbre est généreuse : elle donne souvent plus qu'on ne lui demande.

Desmond MacHale

Il vaut mieux viser la perfection et la manquer
que viser l'imperfection et l'atteindre.

Bertrand Russell

Dans ce premier chapitre consacré à des notions d'algèbre générale, nous allons aborder ensemble un domaine des mathématiques tout nouveau pour vous mais qui va revêtir une importance essentielle pour la suite de votre formation (notamment quand nous aborderons au second semestre la théorie des espaces vectoriels). Le principe en est très simple : regrouper au sein de structures abstraites des ensembles mathématiques très divers munis d'opérations élémentaires (essentiellement addition, multiplication ou composition pour nous cette année), et définir sur ces structures un vocabulaire commun, puis prouver des résultats qui pourront s'adapter uniformément à des domaines a priori très éloignés des mathématiques (un même théorème pourra très bien s'appliquer de la même façon à l'ensemble géométrique des rotations du plan qu'à celui beaucoup plus « analytique » des suites géométriques, par exemple). Cette conception des choses nécessite une bonne capacité d'abstraction (même si nous essaierons d'illustrer le plus possible ce cours pas des exemples concrets), mais permet vraiment de gagner un recul extrêmement appréciable sur le fonctionnement même des opérations couramment utilisées en mathématiques.

Objectifs du chapitre :

- connaissance précise du vocabulaire de l'algèbre générale.
- capacité à prouver rigoureusement qu'un ensemble muni d'une ou deux opérations est ou non un groupe, un anneau, un corps.

1 Structure de groupe.

1.1 Lois de composition interne.

Définition 1. Une **loi de composition interne** (lci) sur un ensemble E est une application $\star : E \times E \to E$.

En fait, une loi de composition interne n'est rien d'autre qu'une opération s'appliquant à deux éléments d'un ensemble, et renvoyant un résultat appartenant au même ensemble. En général, on notera le résultat d'une telle opération sous la forme $x \star y$ plutôt que $\star(x, y)$, comme on a l'habitude de le faire pour les opérations classiques que sont les quatre opérations usuelles.

Exemple : vous connaissez déjà énormément d'opérations qui sont des lois de composition internes, matérialisées habituellement par un symbole d'opération. Attention tout de même au fait qu'une même opération peut être une lci sur un ensemble, mais ne pas l'être sur un de ses sous-ensembles si le caractère « interne » n'est plus vérifié.

- l'opération d'addition $+$ est une lci sur les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, mais aussi sur l'ensemble des suites réelles ou l'ensemble de tous les polynômes par exemple. Par contre, il ne s'agit par exemple pas d'une lci dans l'ensemble des polynômes de degré exactement égal à 2 (si le coefficient de degré 2 de deux tels polynômes est opposé, leur somme n'est plus un polynôme de degré 2).
- l'opération de multiplication $\times$ est une lci sur tous les ensembles de nombres cités ci-dessus, mais pas par exemple sur l'ensemble $\mathbb{Z}^- = \{n \in \mathbb{Z} \mid z \leqslant 0\}$ puisque le produit de deux entiers négatifs est rarement un entier négatif (l'addition serait une lci sur ce même ensemble).
- l'opération de soustraction est une lci sur $\mathbb{Z}$ ou sur $\mathbb{R}$, mais pas sur $\mathbb{N}$.
- l'opération de composition $\circ$ est une lci sur l'ensemble des applications $f : E \to E$, quel que soit l'ensemble E. Elle l'est aussi sur le sous-ensemble constitué de toutes les applications bijectives de E dans E.
- les opérations d'union et d'intersection constituent deux lci sur l'ensemble $\mathcal{P}(E)$ des sous-ensembles d'un ensemble donné E.
- on peut aussi définir des lci nettement moins naturelles : par exemple, la loi $\star$ définie sur l'ensemble $]-1, 1[$ par $x \star y = \dfrac{x+y}{1+xy}$ est une lci (preuve laissée en exercice !).

Définition 2. Si $\star$ est une lci sur un ensemble E, un sous-ensemble F de l'ensemble E est **stable** par la loi $\star$ si $\forall (x, y) \in F^2$, $x \star y \in F$.

Définition 3. Soit $\star$ une lci sur un ensemble E. La loi $\star$ est :

- **associative** si $\forall (x, y, z) \in E^3$, $x \star (y \star z) = (x \star y) \star z$.
- **commutative** si $\forall (x, y) \in E^2$, $x \star y = y \star x$

Remarque 1. Même si la lci n'est pas commutative, on dira que les deux éléments **commutent** s'ils vérifient la propriété $x \star y = y \star x$. Une lci est donc commutative si tous les couples d'éléments de E commutent.

Exemples : la plupart des opérations usuelles que nous connaissons sont associatives et commutatives, mais leurs « opérations réciproques » ne le sont pas en général !

- l'addition ou la multiplication sont ainsi des lci associatives et commutatives sur tous les ensembles que nous avions évoquées plus haut, mais la soustraction est une lci qui n'est ni associative ni commutative sur $\mathbb{R}$ (ou sur $\mathbb{Z}$), et la division n'est pas non plus associative ni commutative sur $\mathbb{R}^*$.
- la composition des applications est un bon exemple de lci qui est associative mais pas du tout commutative. On dira donc que deux applications f et g commutent si elles vérifient $g \circ f = f \circ g$.
- l'union et l'intersection sont des lci associatives et commutatives sur $\mathcal{P}(E)$.
- la lci définie par $x \star y = \dfrac{x+y}{1+xy}$ est associative et commutative sur $]-1, 1[$ (la commutativité est évidente, l'associativité nécessite de calculer $(x \star y) \star z = \dfrac{\frac{x+y}{1+xy} + z}{1 + \frac{(x+y)z}{1+xy}} = \dfrac{x+y+z+xyz}{1+xy+xz+yz}$, expression qui n'est pas modifiée si on échange le rôle des variables x, y et z, et donc égale à $x \star (y \star z)$).

Remarque 2. Les lci définies sur des ensembles finis peuvent facilement être représentées par des tableaux à double entrée donnant le résultat de l'opération pour tous les choix possibles de couples d'éléments de l'ensemble. Par exemple, dans un ensemble à quatre éléments notés e, a, b et c, on peut définir une lci $\star$ pour laquelle le résultat de l'opération $\star$ serait donné par le tableau suivant :

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Ainsi, on aurait $a \star b = c$ ou $e \star e = e$. On peut aisément constater ici que l'opération $\star$ est une lci associative et commutative. Une question intéressante serait de savoir combien de lci associatives et commutatives différentes on peut créer sur un ensemble à quatre éléments. On ne répondra pas tout de suite à ce genre de question, car on va encore ajouter quelques propriétés à vérifier par notre lci pour qu'elle devienne vraiment « intéressante » d'un point de vue mathématique.

Définition 4. Soit E un ensemble muni d'une lci $\star$. Un élément $e \in E$ est **élément neutre** pour la loi $\star$ si $\forall x \in E$, $e \star x = x \star e = x$. Si un tel élément neutre existe, un élément $x \in E$ est **symétrisable** pour la loi $\star$ si $\exists y \in E$, $x \star y = y \star x = e$.

Remarque 3. Le symétrique d'un élément x sera appelé **opposé** et noté $-x$ dans le cas où la lci étudiée est une addition, il sera appelé **inverse** et noté x^{-1} dans le cas où la lci est une multiplication.

Exemples : Par analogie avec ce qui se passe dans les ensembles de nombres usuels, l'élément neutre d'une loi additive sera très souvent noté 0 (ou 0_E pour être certain que la notation ne soit pas ambiguë), et celui d'une loi multiplicative sera noté 1. On verra une exception notable à ce principe dans les ensembles de matrices, où l'élément neutre multiplicatif est noté I. Quelques exemples un peu moins évidents :

- la lci $\circ$ sur l'ensembles des applications de E dans E admet id_E comme élément neutre. Les éléments symétrisables sont les applications bijectives, et leur symétrique est alors noté f^{-1} même s'il ne s'agit ici pas d'une lci multiplicative à proprement parler.
- sur l'ensemble $\mathcal{P}(E)$, la lci d'union admet pour élément neutre l'ensemble vide, et la lci d'intersection admet pour élément neutre l'ensemble E tout entier. Aucun élément autre que ces éléments neutres n'est symétrisable pour l'opération correspondante.
- l'opération $x \star y = \dfrac{x+y}{1+xy}$ sur l'ensemble $]-1,1[$ admet 0 pour élément neutre et tout élément est symétrisable ($-x$ étant simplement le symétrique de x). Peut-on dire pour autant que les lci $\star$ et $+$ sont « identiques » ou « semblables » ? Identiques, non, car le résultat des deux opérations n'est pas toujours le même, semblables oui mais il faudra une définition précise pour pouvoir l'affirmer.
- la lci $\star$ définie un peu plus haut sur l'ensemble à quatre éléments (e, a, b, c) admet pour élément neutre e (qui n'avait pas été nommé ainsi par hasard), et tout élément est symétrisable, et égal à son propre symétrique.

Proposition 1. S'il existe un élément neutre pour une lci, celui-ci est unique.

Si la lci est associative et admet un élément neutre, le symétrique éventuel d'un élément x est également unique.

Démonstration. En effet, en notant $\star$ notre lci, on peut supposer qu'elle a deux éléments neutres e et e'. Mais on aura alors par définition $e \star e' = e$ (car e est neutre) et en même temps $e \star e' = e'$ (car e' est neutre), ce qui impose $e = e'$.

Supposons de même que x admette deux symétriques y et z. On peut alors calculer $z \star (x \star y) = z \star e = z$, et $(z \star x) \star y = e \star y = y$, ce qui impose $z = y$. On notera qu'il est en effet indispensable que la lci soit associative pour pouvoir effectuer ce petit calcul. □

Proposition 2. Si x est un élément symétrisable pour une lci $\star$, alors son symétrique x^{-1} est aussi symétrisable, et $(x^{-1})^{-1} = x$.

Si deux éléments x et y sont symétrisables pour une lci associative $\star$ alors $x \star y$ est aussi symétrisable, et $(x \star y)^{-1} = y^{-1} \star x^{-1}$.

Démonstration. La première affirmation découle de façon évidente de la définition du symétrique d'un élément. Pour la deuxième, on effectue simplement le petit calcul $(y^{-1} \star x^{-1}) \star (x \star y) = y^{-1} \star e \star y = e$, et de même $(x \star y) \star (y^{-1} \star x^{-1}) = e$. □

1.2 Groupes et sous-groupes.

Définition 5. Un **groupe** $(G, \star)$ est un ensemble G muni d'une lci $\star$ associative, pour laquelle G possède un élément neutre et tout élément de G est symétrisable.

Le groupe $(G, \star)$ est un groupe **commutatif** (ou groupe **abélien**) si de plus la loi $\star$ est commutative.

Exemples : $(\mathbb{R}, +)$ ou $(\mathbb{Z}, +)$ sont des groupes commutatifs. Par contre, $(\mathbb{N}, +)$ n'est pas un groupe. De même, $(\mathbb{R}, \times)$ n'est pas un groupe (car 0 n'est pas inversible), mais $(\mathbb{R}^*, \times)$ en est un. Parmi les exemples déjà étudiés précédemment, $(\{f : E \to E\}, \circ)$ est un groupe, $(\mathcal{P}(E), \cap)$ n'est pas un groupe, $(]-1, 1[, \star)$ est un groupe.

Un dernier exemple un peu plus tordu que les précédents, puisqu'il s'agit d'une structure de groupe non commutatif, qui a pourtant une origine simple et géométrique. Prenez un beau triangle équilatéral (dessinez-le sur votre feuille si vous voulez) ABC. On s'intéresse aux isométries du plan laissant stable le triangle équilatéral (autrement dit, on va déplacer ou symétriser notre triangle, mais à la fin on doit toujours avoir un triangle équilatéral à la même place). Avec un peu de motivation, on peut prouver qu'il n'existe que six transformations géométriques convenables :

- l'application identité, notée i, qui ne fait rien bouger.
- la rotation par rapport au centre O du triangle d'angle $\frac{2\pi}{3}$ (qui permute les trois sommets, et donc les trois côtés, du triangle), qu'on notera r_1.
- la rotation par rapport au centre O du triangle d'angle $\frac{4\pi}{3}$, qu'on notera r_2.
- la réflexion par rapport à la droite (AI), où I est le milieu du côté $[BC]$ opposé à A. On notera cete réflexion s_1.
- de même, la réflexion par rapport à la droite (BJ), où J est le milieu du côté $[AC]$. On notera cette réflexion s_2.
- la réflexion par rapport à la droite (CK), où K est le milieu du côté $[AB]$. On notera cette réflexion s_3.

On dispose donc d'un ensemble à six éléments, sur lequel une opération très naturelle va créer une structure de groupe : l'opération de composition. Et c'est logique : la composée de deux applications laissant stable notre triangle continuera à le laisser stable, on a un élément neutre évident qui est l'identité i, et chaque application a une réciproque qui est dans la liste puisqu'elle va elle-même laisser le triangle stable. Si on écrit la table complète de l'opération $\circ$ sur cet ensemble, on obtient :

	i	r_1	r_2	s_1	s_2	s_3
i	i	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	i	s_2	s_3	s_1
r_2	r_2	i	r_1	s_3	s_1	s_2
s_1	s_1	s_3	s_2	i	r_2	r_1
s_2	s_2	s_1	s_3	r_1	i	r_2
s_3	s_3	s_2	s_1	r_2	r_1	i

Attention, la lecture de ce tableau est plus compliquée que pour les précédents puisque l'opération n'est pas commutative : le résultat donné est celui obtenu en composant l'élément de la ligne (à gauche) par l'élément de la colonne (à droite). Ainsi, on a par exemple $r_2 \circ s_1 = s_3$ mais $s_1 \circ r_2 = s_2$. Cette structure est en fait la structure de groupe non commutatif la plus simple qu'on puisse créer sur un ensemble fini (on ne peut pas en créer sur des ensembles à moins de six éléments). Les mathématiciens qui font de l'algébre tous les jours et qui aiment le vocabulaire compliqué l'appellent **groupe diédral** d'ordre 6, les autres l'appellent plus simplement groupe des symétries du triangle. On pourrait bien sûr faire de même avec un carré, un hexagone ou même n'importe quel polygone régulier à n cotés. On obtient toujours un groupe non commutatif à $2n$ éléments (il n'y que des rotations et des réflexions, comme pour le triangle).

Remarque 4. Les propriétés imposées sur la lci pour considérer que $(G, \star)$ est un groupe sont certes restrictives mais permettent de simplifier grandement les calculs. En particulier, dans un groupe, on peut toujours :

- simplifier des égalités à gauche comme à droite : si $x \star y = x \star z$, alors $y = z$, et de même, si $y \star x = z \star x$, alors $y = z$
- résoudre des équations du type $x \star y = z$ (où l'inconnue est ici x) en écrivant $x = z \star y^{-1}$

Définition 6. Si E est un ensemble quelconque, on note $\mathfrak{S}(E)$ l'ensemble des bijections $f : E \to E$ (aussi appelées **permutations** de l'ensemble E). On notera plus précisément $\mathfrak{S}_n$ l'ensemble des permutations de l'ensemble $\{1, 2, \ldots, n\}$.

Proposition 3. Quel que soit l'ensemble E, $(\mathfrak{S}(E), \circ)$ est un groupe, appelé **groupe des permutations** de l'ensemble E.

Remarque 5. Le groupe $\mathfrak{S}_n$ est un groupe fini contenant $n!$ éléments (on parle de groupe fini d'**ordre** $n!$). C'est en étudiant de tels ensembles qu'Évariste Galois a conçu la notion de groupe.

Proposition 4. Si $(G, \star)$ et $(G', *)$ sont deux groupes, on peut définir une loi de groupe $\otimes$ sur $G \times G'$ en posant, $\forall (x, y, x', y') \in G^2 \times G'^2$, $(x, y) \otimes (x', y') = (x \star x', y * y')$. Le groupe ainsi obtenu est appelé **groupe produit** des groupes G et G'.

Définition 7. Si $(G, \star)$ est un groupe, un sous-ensemble $H \subset G$ est un **sous-groupe** de G s'il est lui-même un groupe pour la loi $\star$.

Proposition 5. Un sous-ensemle H du groupe $(G, \star)$ est un sous-groupe de G si et seulement s'il vérifie les propriétés suivantes :

- $H \neq \emptyset$
- H est stable pour la loi $\star$: $\forall (x, y) \in H^2$, $x \star y \in H$
- H est stable par symétrisation : $\forall x \in H$, $x^{-1} \in H$

Remarque 6. Un sous-groupe contient nécessairement l'élément neutre e, qui sera également élément neutre dans H (c'est la même démonstration que celle qui permet de prouver qu'un élément neutre est unique dans un groupe). Les stabilités sont évidentes pour que H puisse être un groupe (la loi $\star$ doit être une lci pour H, ce qui impose la première stabilité, et le symétrique d'un élément de H est nécessairement son symétrique dans G, d'où la deuxième stabilité).

Exemples : On a déjà vu, sans le dire explicitement, des dizaines d'exemples de sous-groupes.

- $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$, qui est un sous-groupe de $(\mathbb{R}, +)$, qui est lui-même un sous-groupe de $(\mathbb{C}, +)$.
- l'ensemble des entiers pairs, noté $2\mathbb{Z}$, est un sous-groupe de $(\mathbb{Z}, +)$.
- $\mathbb{R}^{+*}$ est un sous-groupe du groupe multiplicatif $\mathbb{R}^*$.
- $\mathbb{U}$ est un sous-groupe du groupe multiplicatif $\mathbb{C}^*$, et $\mathbb{U}_n$ en est un sous-groupe pour tout entier naturel n (d'ailleurs, certins groupes $\mathbb{U}_n$ sont des sous-groupes d'autres du même type, par exemple $\mathbb{U}_4$ est un sous-groupe de $\mathbb{U}_8$).
- les ensembles $\{e\}$ et G tout entier sont toujours des sous-groupes de G, appelés sous-groupes triviaux.

Proposition 6. Un sous-ensemble $H \subset G$ est un sous-groupe de G si et seulement si :

- $e \in H$
- $\forall (x, x') \in H$, $x \star (x')^{-1} \in H$

Démonstration. Il est évident que ces conditions sont vérifiées par tout sous-groupe de G. Réciproquement, supposons ces deux conditions vérifiées. Alors, $\forall x \in H$, $e \star x^{-1} \in H$, donc $x^{-1} \in H$, ce qui prouve la stabilité de H par symétrisation. Ensuite, on peut écrire, $\forall (x, x') \in H^2$, $x \star x' = (x^{-1})^{-1} \star x'$ qui appartient aussi à H, donc H est également stable par l'opération $\star$, c'est bien un sous-groupe de G. □

1.3 Morphismes de groupes

Définition 8. Soient $(G, \star)$ et $(G', *)$ deux groupes, une application $f : G \to G'$ est un **morphisme de groupes** si $\forall (x, y) \in G^2$, $f(x \star y) = f(x) * f(y)$. Si $G = G'$, on parle d'**endomorphisme de groupe**. Si de plus f est bijectif, on parle d'**isomorphisme** de groupe, et même d'**automorphisme de groupe** quand de plus $G = G'$.

Exemples : L'idée derrière la définition d'un morphisme est simple, c'est une application qui respecte la structure imposée par les lci définissant les groupes. Dans le cas d'un isomorphisme, c'est encore mieux : l'isomorphisme « transporte » la structure imposée par la lci $\star$ sur l'ensemble G dans l'ensemble G'. On peut alors considérer que les deux groupes sont « les mêmes », au sens où ils peuvent être munis d'une structure de groupe qui aura exactement les mêmes propriétés. On dit que deux groupes sont **isomorphes** s'il existe (au moins) un isomorphisme de groupes entre eux.

- l'application $f : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z} \\ x & \mapsto & 5x \end{array} \right.$ est un endomorphisme de groupes de $(\mathbb{Z}, +)$ (il suffit pour cela d'écrire que $5(x + y) = 5x + 5y$).
- la fonction exponentielle effectue un isomorphisme du groupe $(\mathbb{R}, +)$ vers le groupe $(\mathbb{R}^{+*}, \times)$. C'est même l'une de ses propriétés fondamentales ! Sa réciproque ln effectue un isomorphisme dans l'autre sens.
- la fonction $f : z \mapsto |z|$ est un morphisme de groupes de $\mathbb{C}^*$ vers $\mathbb{R}^{+*}$ puisque $|zz'| = |z| \times |z'|$.
- en notant $G = \{f \text{ continues sur } [0, 1]\}$, l'application $\varphi : \left\{ \begin{array}{ccc} G & \to & \mathbb{R} \\ f & \mapsto & \displaystyle\int_0^1 f(t)\, dt \end{array} \right.$ est un morphisme de groupes de G vers $(\mathbb{R}, +)$.

Proposition 7. Si $f : G \to G'$ est un morphisme de groupe, alors :

- $f(e) = e'$ (en notant e et e' les éléments neutres respectifs des deux groupes)
- $\forall x \in G$, $f(x^{-1}) = (f(x))^{-1}$
- si H est un sous-groupe de G, alors $f(H)$ est un sous-groupe de G'
- si K est un sous-groupe de G', alors $f^{-1}(K)$ est un sous-groupe de G

Démonstration. Toutes ces propriétés sont faciles à prouver :

- avec les notations habituelles, $f(e \star e) = f(e) * f(e)$, donc $f(e) = f(e) * f(e)$. On peut simplifier par $f(e)$ pour obtenir $e' = f(e)$.
- $f(x) * f(x^{-1}) = f(x \star x^{-1}) = f(e) = e'$, donc $f(x^{-1}) = (f(x))^{-1}$
- si H est un sous-groupe de G, $e \in H$, donc $f(e) = e' \in f(H)$. De plus, si $(y, y') \in f(H)^2$, $\exists (x, x') \in H^2$ tels que $f(x) = y$ et $f(x') = y'$, et on peut simplement écrire $y * (y')^{-1} = f(x) * (f(x'))^{-1} = f(x) * f((x')^{-1}) = f(x \star (x')^{-1})$. Or, $x \star (x')^{-1} \in H$ (caractérisation des sous-groupes), donc $f(H)$ est lui aussi un sous-groupe.
- c'est encore plus simple dans l'autre sens : $f^{-1}(e') = e \in f^{-1}(K)$, et si x, x' sont deux éléments de $f^{-1}(K)$, $f(x \star (x')^{-1}) = f(x) * (f(x'))^{-1} \in K$, donc $f^{-1}(K)$ est bien un sous-groupe de G.

□

Définition 9. Soit $f : G \to G'$ un morphisme de groupes. Le **noyau** de f est l'ensemble $\ker(f) = \{x \in G \mid f(x) = e'\}$. L'**image** de f est l'ensemble $\mathrm{Im}(f) = f(G)$.

Proposition 8. Le morphisme f est surjectif si et seulement si $\mathrm{Im}(f) = G'$. Il est injectif si et seulement si $\ker(f) = \{e\}$.

Démonstration. La caractérisation de la sujectivité est évidente puisque c'est la définition d'une application surjective. Pour l'injectivité, il faut prouver les deux implications. Si f est injective, l'élément neutre e' de G' admet au maximum un antécédent par f. Or, il en a toujours au moins un : l'élément neutre e du groupe G. C'est donc nécessairement le seul, et $\ker(G) = \{e\}$. Réciproquement, supposons $\ker(G) = \{e\}$, et prenons deux éléments x et x' de G vérifiant $f(x) = f(x')$. On a alors $f(x) * f((x')^{-1}) = e'$, donc $f(x \star (x')^{-1}) = e'$, ce qui implique $x \star (x')^{-1} = e$ à cause de l'hypothèse faite sur le noyau. On a donc $x = x'$, et l'application est bien injective. □

Exemples : L'application $f : z \mapsto |z|$ a pour image $\mathbb{R}^{+*}$ (elle est surjective) et pour noyau $\mathbb{U}$. La fonction exponentielle, définie sur $\mathbb{C}$ et à valeurs dans $\mathbb{C}^*$, est un morphisme de groupes (groupe additif au départ, multiplicatif à l'arrivée) surjectif, dont le noyau est $\{z \in \mathbb{C} \mid e^z = 1\} = 2i\pi\mathbb{Z}$.

Proposition 9. Si $f : G \to H$ et $h : H \to K$ sont deux morphismes de groupe, leur composée $g \circ f$ est aussi un morphisme de groupe. De plus, si f et g sont deux isomorphismes, $g \circ f$ est aussi un isomorphisme.

Démonstration. C'est complètement trivial, il suffit d'appliquer deux fois de suite la définition. Bien entendu, on sait déjà que la composée de deux bijections est une bijection, donc la deuxième partie de la proposition est encore plus triviale. □

Proposition 10. La relation « être isomorphe à » est une relation d'équivalence sur l'ensemble de tous les groupes.

Démonstration. Cette relation est réflexive car tout groupe G est isomorphe à lui-même via l'isomorphisme trivial id_G. Supposons maintenant qu'il existe un isomorphisme $f : G \to G'$. Pour prouver la symétrie de la relation, il faut montrer qu'il existe un isomorphisme $g : G' \to G$. Il suffit tout simplement de prendre $g = f^{-1}$. En effet, f est une bijection, et c'est bien un morphisme : $f^{-1}(yy') = f^{-1}(f(f^{-1}(y))f(f^{-1}(y'))) = f^{-1}(f(f^{-1}(y)f^{-1}(y'))) = f^{-1} \circ f(f^{-1}(y)f^{-1}(y')) = f^{-1}(y)f^{-1}(y')$. Enfin, la transivité a été énoncée dans la propriété précédente. □

Revenons quelques instants sur l'étrange question posée un peu plus haut dans ce cours : combien existe-t-il de structures de groupes différentes sur un ensemble à quatre éléments ? On peut désormais donner un sens à cette question en rajoutant la précision « à isomorphisme près » (en considérant donc que deux groupes isomorphes correspondent en fait à la « même » structure de groupe), ce qui revient en fait à chercher le nombre de classes d'équivalence de la relation d'isomorphisme qui sont constituées de groupes à quatre éléments. En fait il existe une deuxième structure de groupe sur l'ensemble $\{e, a, b, c\}$ qui **ne peut pas** être obtenue à partir de la première définie plus haut par un isomorphisme :

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Il ne peut pas y avoir d'isomorphisme avec l'autre structure car ici il existe des éléments qui ne sont pas leur propre inverse (a et c sont inverses l'un de l'autre, e et b sont leur propre inverse), alors qu'un isomorphisme conserve nécessairement la propriété « être son propre inverse ». On peut en fait prouver (mais ce n'est pas évident !) qu'il n'y que deux structures de groupes différentes sur un ensemble contenant quatre éléments (les deux que nous venons de citer). Si notre ensemble contient un nombre d'éléments qui est un nombre **premier**, c'est encore pire, il n'y a qu'une seule façon de structurer l'ensemble pour en faire un groupe ! D'ailleurs, vous la connaissez déjà, cette structure : c'est la structure de l'ensemble $\mathbb{U}_n$ des racines n-èmes de l'unité, muni de l'opération de multiplication (**tout** groupe à n éléments est donc isomorphe à $\mathbb{U}_n$ si n est un entier premier). Pour un nombre d'éléments non premier, il existe en général plusieurs structures possibles, et bien sûr il peut y en avoir beaucoup si le nombre d'éléments est élevé, et encore plus si on accepte les lci non commutatives. On connait de toute façon très bien les structures de groupes sur tous les ensembles finis mais les démonstrations de ces résultats sont assez monstrueuses (elles prennent plusieurs **milliers** de pages, les plus curieux iront par exemple consulter la page Wikipédia « Liste des groupes finis simples », mais n'y comprendront probablement pas grand chose). Plus accessible, la « Liste des petits groupes » toujours disponible sur Wikipédia vous donne le nombre de structures possibles pour des nombres d'éléments inférieurs ou égaux à 20. On a par exemple pas moins de 14 lois de groupes différentes (dont neuf ne sont pas commutatives) si notre ensemble contient 16 éléments.

Proposition 11. Si G est un groupe, l'ensemble $Aut(G)$ des automorphismes de G est un groupe pour la composition.

Démonstration. C'est en fait un sous-groupe de $\mathfrak{S}(G)$. En effet, id_G est certainement un automorphisme donc appartient à $Aut(G)$, et la stabilité par composition et passage à la réciproque découle des propriétés démontrées précédemment. □

2 Anneaux et corps.

Définition 10. Un **anneau** est un triplet $(A, +, \times)$ constitué d'un ensemble muni de deux lci vérifiant les conditions suivantes :

- $(A, +)$ est un groupe commutatif
- $\times$ est une lci associative
- $\times$ admet un élément neutre
- $\times$ est distributive par rapport à $+$: $\forall (x, y, z) \in A^3$, $x \times (y+z) = x \times y + x \times z$ et $(y+z) \times x = y \times x + z \times x$

Si de plus la lci $\times$ est commutative, on dit que l'anneau A est commutatif.

Remarque 7. Les lois d'un anneau sont traditionnellement toujours notées comme une addition et une multiplication. De façon cohérente, les deux éléments neutres seront notés 0 et 1.

Remarque 8. Dans un anneau, on peut définir les **puissances** entières d'un élément quelconque par récurrence (comme dans $\mathbb{R}$) : $x^0 = 1$ et $\forall n \in \mathbb{N}$, $x^{n+1} = x^n \times x$. On peut également définir les **multiples** entiers d'un élément quelconque (c'est en fait le cas dans tout groupe additif) : $0x = 0$ et $\forall n \in \mathbb{N}$, $(n+1)x = nx + x$. On peut même étendre aux multiples négatifs : $(-n)x = -(nx)$.

Exemples : $(\mathbb{R}, +, \times)$ est un anneau commutatif. C'est également le cas de $\mathbb{C}$ ou $\mathbb{Z}$ pour les mêmes opérations. Il est plus difficile de construire des exemples intéressants d'anneaux avec des opérations « exotiques » que pour les groupes.

Proposition 12. Régles de calcul dans les anneaux :

- $\forall x \in A$, $0 \times x = x \times 0 = 0$ (l'élément 0 est **absorbant** pour la multiplication)
- $\forall n \in \mathbb{Z}$, $\forall (x, y) \in A^2$, $(nx) \times y = x \times (ny) = n(x \times y)$
- Formule du binôme de Newton : si x et y sont deux éléments de A qui commutent, alors
  $\forall n \in \mathbb{N}$, $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \times y^{n-k}$
- Si x et y sont deux éléments de A qui commutent, alors
  $\forall n \in \mathbb{N}$, $x^n - y^n = (x-y) \times \sum_{k=0}^{n-1} x^k \times y^{n-k-1}$

Démonstration. À chaque fois, il s'agit de calculs sans grand intérêt :

- $x \times 0 + x \times 0 = x \times (0+0) = x \times 0$, donc $x \times 0 = 0$ (distributivité puis simplication par $x \times 0$)
- $(nx) \times y = (x + x + \cdots + x) \times y = x \times y + x \times y + \cdots + x \times y = n(x \times y)$, et de même pour l'autre égalité
- pour le binôme et la dernière identité remarquable, on peut reprendre telles quelles les démonstrations déjà vues dans des cas particuliers. Bien sûr, le fait que les éléments commutent est ici essentielle.

□

Définition 11. Un élément $x \in A$ dans un anneau est une **unité** de A (ou simplement un **élément inversible** de A) s'il est inversible pour la multiplication de A.

Exemple : dans $\mathbb{R}$, tous les éléments sauf 0 sont des unités. Dans $\mathbb{Z}$, seuls 1 et -1 sont des unités.

Proposition 13. L'ensemble des unités d'un anneau A est un groupe multiplicatif, souvent noté A^*.

Démonstration. C'est évident : la loi $\times$ est bien interne dans l'ensemble des unités (si x et y sont inversibles, alors $x \times y$ aussi), elle reste bien sûr associative, 1 est toujours une unité et continuera à jouer le rôle d'élément neutre, et l'inverse d'un élément inversible est toujours inversible. □

Définition 12. Un anneau A est **intègre** s'il n'est pas réduit à un seul élément et si $\forall (x, y) \in A^2$, $x \times y = 0 \Rightarrow x = 0$ ou $y = 0$.

Exemples : Tous les anneaux constitués des ensembles de nombres classiques sont intègres. On ne connait en fait pas d'exemple évident à ce stade d'anneau qui ne soit pas intègre. On en croisera très fréquemment un peu plus tard dans l'année (les anneaux de matrices), mais un premier exemple sera donné un peu plus bas, après la définition des corps.

Définition 13. Soit A un anneau et $B \subset A$, B est un **sous-anneau** de A si $1 \in B$, B est un sous-groupe additif de A, et B est stable par produit.

Remarque 9. Dans ce cas, sans surprise, B sera lui-même un anneau. La condition d'appartenance de 1 au sous-ensemble B est indispensable, car il est en fait assez simple de créer des sous-groupes stables par multiplication qui ne sont pas des sous-anneaux. Par exemple, dans $\mathbb{Z}$, le sous-ensemble $5\mathbb{Z}$ des multiples de 5 est un sous-groupe et il est stable par produit.

Définition 14. Soient A et B deux anneaux, une application $f : A \to B$ est un **morphisme d'anneaux** si :

- $f(1_A) = 1_B$ (où 1_A et 1_B désignent les éléments neutres multiplicatifs des deux anneaux)
- $\forall (x, y) \in A^2$, $f(x + y) = f(x) + f(y)$
- $\forall (x, y) \in A^2$, $f(x \times y) = f(x) \times f(y)$

Exemple : les morphismes d'anneaux sont en fait rares. On peut citer par exemple $f : z \mapsto \overline{z}$ qui est un automorphisme d'anneaux dans $\mathbb{C}$.

Définition 15. Un anneau commutatif $(A, +, \times)$ est un **corps** si tout élément non nul de A est inversible.

Autrement dit, $(A, +, \times)$ est un corps si $(A, +)$ et $(A^*, \times)$ sont deux groupes commutatifs.

Exemple : Les ensembles $\mathbb{R}$, $\mathbb{Q}$ et $\mathbb{C}$ sont tous les trois des corps.

Définition 16. Un sous-ensemble K' d'un corps K est un **sous-corps** de K s'il est un sous-groupe additif de K et que K'^* est un sous-groupe multiplicatif de K^*.

Bien entendu, un sous-corps est lui-même muni d'une structure de corps. Ainsi, $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, qui est lui-même un sous-corps de $\mathbb{C}$.

Exemple : Il existe relativement peu d'ensembles munis d'une structure de corps, mais on peut en créer une assez facilement sur certains ensembles finis. Considérons par exemple l'ensemble $K = \{0, 1, 2, 3, 4\}$ muni des deux opérations d'addition et de multiplication. Bien entendu, ces opérations ne sont pas des lci, mais on peut s'en sortir en considérant le résultat, non pas dans $\mathbb{N}$, mais modulo 5 (en se ramenant toujours à une valeur comprise entre 0 et 4). En fait, si on veut être tout à fait rigoureux, les éléments du corps K ne sont pas des entiers, mais les classes d'équivalence de la relation d'équivalence de congruence module 5 dans $\mathbb{Z}$, qu'on note d'ailleurs $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$ et $\overline{4}$ si on veut les distinguer des « vrais » entiers. Par exemple, $\overline{1}$ contient les entiers positifs $1, 6, 11, 16, \ldots$ mais

aussi les négatifs $-4, -9, -14, \ldots$. Quand on écrit dans notre tableau que $\overline{3} \times \overline{2} = \overline{1}$, cela signifie que le produit d'un entier appartenant à la classe $\overline{3}$ par un entier appartenant à la classe $\overline{2}$ donne toujours un entier appartenant à la classe $\overline{1}$ (ce qui est vrai : $(5k+3) \times (5k'+2) = 25kk' + 15k' + 10k + 6 = 5(5kk' + 3k' + 2k + 1) + 1$). L'ensemble K est en fait noté en mathématiques $\mathbb{Z}/5\mathbb{Z}$ pour des raisons sur lesquelles nous ne nous étendrons pas. Donnons plutôt les tables des deux lois de groupes du corps K :

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\times$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

On vérifie aisément que les deux lois font bien de K un corps commutatif (pour le produit, $\overline{1}$ est bien sûr son propre inverse en tant qu'élément neutre, $\overline{4}$ est également son propre inverse, et $\overline{2}$ et $\overline{3}$ sont inverses l'un de l'autre). On peut en fait étendre le résultat à tous les ensembles du même type lorsque le nombre d'éléments est un nombre premier. En effet, si on tente la même chose par exemple sur $\{0, 1, 2, 3, 4, 5\}$ avec des opérations définies modulo 6, la loi multiplicative ne sera pas une loi de groupe, car les éléments 2 et 3 ne seront pas inversibles (c'est une conséquence du théorème de Bezout dont nous reparlerons en arithmétique). Plus généralement, tous les diviseurs de n (autres que 1) donneront des éléments non inversibles quand n n'est pas premier.