Structures algébriques

Emmanuel Vieillard-Baron[1], Alain Soyeur[2], and François Capaces[3]

[1]Enseignant en CPGE, Lycée Kléber, Strasbourg
[2]Enseignant en CPGE, Lycée Pierre de Fermat, Toulouse
[3], ,

1er octobre 2022

1 Structures algébriques

Structures algébriques de base.

Pour bien aborder ce chapitre

La notion de groupe est apparue dès la fin du 18 e de manière parallèle dans différents domaines des mathématiques.

En 1798, Karl Friedrich Gauss, dans ses « Disquisitiones Arithmeticae », utilise implicitement la notion de groupe abélien. Plus tard, au milieu du 19 e, Ernst Kummer établie des résultats de factorisation sur les groupes dans une tentative de prouver le grand théorème de Fermat.

Dans la première moitié du 19 e siècle, le jeune mathématicien prodige Évariste Galois cherche à prouver que les équations polynomiales de degré $\geqslant 5$ à coefficients complexes ne peuvent être résolues par radicaux, ce qui signifie que leurs racines ne peuvent être écrites au moyen des opérations usuelles. Pour ce faire, il s'intéresse à un groupe relié aux racines de l'équation considérée. Son génie consiste alors à comprendre que les difficultés pour résoudre l'équation ne proviennent pas de son degré mais des propriétés mathématiques de ce groupe.

À la fin du 19 e, Félix Klein utilise les groupes pour classifier les nouvelles géométries tout juste découvertes.

Les mathématiciens savent depuis que les groupes interviennent dans de très nombreux domaines. L'ensemble des isométries de l'espace ou du plan est un groupe appelé groupe orthogonal, voir le chapitre **??**. L'ensemble des isométries préservant un objet donné (un polygone régulier, un solide platonicien, etc...) a une structure de groupe. L'ensemble des permutations $\mathfrak{S}_n$ d'un ensemble fini est un groupe qui fut étudié par Cauchy et Cayley à la fin du 19 e siècle. Le chapitre **??** lui est consacré. Le groupe découvert par Galois est d'ailleurs un sous-groupe de ce groupe. L'ensemble

des transformations qui, en relativité restreinte, permettent de changer de référentiel galiléen tout en préservant les lois de la physique et la vitesse de la lumière, forment un groupe appelé groupe de Lorenz. En chimie, les symétries des molécules permettent de leur associer des groupes qui aident à comprendre mieux leurs propriétés. Plus concrètement encore, l'ensemble des manipulations qu'on peut effectuer sur un Rubik's cube a lui aussi une structure de groupe. L'étude de ce groupe permet de mettre en place des stratégies gagnantes pour le reconstituer.

L'objet de ce chapitre, peu ambitieux, est d'introduire la notion de groupe ainsi que le vocabulaire attenant. Nous le terminerons par l'étude de deux autres structures, celles d'anneaux et de corps, qui sont elles aussi omniprésentes en mathématiques.

1.1 Groupe

1.1.1 Loi de composition interne

DÉFINITION 0.1 **Loi de composition interne**
Soit E un ensemble. On appelle *loi de composition interne* une application de $E \times E$ dans E :

$$\varphi : \left\{ \begin{array}{ccc} E \times E & \longrightarrow & E(a,b) \\ \longmapsto & & \varphi(a,b) \end{array} \right.$$

Exemple 0.1

— Si $E = \mathbb{N}$, la multiplication ou l'addition des entiers forme une loi de composition interne.

— Si E est un ensemble, la composition des applications est une loi de composition interne sur l'ensemble des fonctions de E dans E : $\mathcal{F}(E,E)$

— Si E est un ensemble, l'intersection ou la réunion sont des lois de composition interne sur l'ensemble des parties de E : $\mathcal{P}(E)$

✎ *Notation 0.2*

— Pour alléger les notations, on écrit plus simplement $\varphi(a,b) = a \,{}_{\varphi}\, b$ ou $\varphi(a,b) = a \star b$ par exemple, ou encore $\varphi(a,b) = a.b$, et pour les moins courageux $\varphi(a,b) = ab$ etc.

— On note alors $(E, \star)$ un ensemble E muni d'une loi de composition interne $\star$.

Remarque 0.1

— Ce qui est important, bien entendu, c'est que $\varphi(a,b)$ reste dans E.

— Il n'y a aucune raison à priori pour que $a \star b = b \star a$.

— On peut itérer une loi de composition interne : si $(a,b,c) \in E^3$, on notera

$$(a \star b) \star c = \varphi\big(\varphi(a,b), c\big)$$

$$a \star (b \star c) = \varphi\big(a, \varphi(b,c)\big)$$

Il n'y a aucune raison à priori pour que ces deux éléments soient égaux.

✎ *Notation 0.3* Pour simplifier les notations, on utilisera, suivant le contexte, pour la loi de composition interne $\star$:

— une *notation additive* : $a + b = a \star b = \varphi(a, b)$.

— ou une *notation multiplicative* : $ab = a \star b = \varphi(a, b)$.

DÉFINITION 0.2 **Loi associative, commutative**
Soit $\star$ une loi de composition interne sur un ensemble E. On dit que $\star$ est :

— *commutative* si et seulement si $\forall (a, b) \in E^2$, $a \star b = b \star a$,

— *associative* si et seulement si $\forall (a, b, c) \in E^3$, $a \star (b \star c) = (a \star b) \star c$.

On dit que plus que $\star$ admet $e \in E$ comme *élément neutre* si et seulement si $\forall x \in E$, $e \star x = x \star e = x$

PLAN 0.1 : Pour montrer que...

... $\star$ est commutative :

1. Soit $(x, y) \in E^2$
2. $x \star y = y \star x$
3. *Donc $\star$ est commutative*

... $\star$ est associative :

1. soit $(x, y, z) \in E^3$
2. $x \star (y \star z) = (x \star y) \star z$
3. *Donc $\star$ est associative*

... $e \in E$ est neutre :

1. Soit $x \in E$
2. $e \star x = x$, $x \star e = x$
3. *Donc e est neutre.*

PROPOSITION 0.1 **Unicité de l'élément neutre**
Si $(E, \star)$ possède un élément neutre, il est unique.

Démonstration *Supposons que e' soit un autre élément neutre pour $\star$. Alors $e = e \star e' = e'$ et donc $e = e'$.*

Exemple 0.4

— Pour le couple $(\mathbb{N}, +)$, $+$ est commutative et associative, l'élément neutre est 0.

— Pour le couple $(\mathbb{N}, \times)$, $\times$ est commutative et associative, 1 est l'unique élément neutre .

— Pour le couple $(\mathcal{P}(G), \cup)$, la loi est commutative, associative, la partie $\varnothing$ est neutre pour cette loi.

— Soit E un ensemble. On considère l'ensemble des applications de E dans E muni de la composition : $(\mathcal{F}(E, E), \circ)$. La loi de composition interne $\circ$ est associative mais pas commutative. Id_E est l'élément neutre de cette loi.

Remarque 0.2 Si une loi de composition interne est *commutative* et *associative*, on définit les notations suivantes pour $(x_1, \ldots, x_n) \in E^n$:

— Lorsque la loi est notée additivement, on définit

$$\sum_{i=1}^{n} x_i = x_1 + \cdots + x_n,$$

— et lorsque la loi est notée multiplicativement,

$$\prod_{i=1}^{n} x_i = x_1 \star \cdots \star x_n.$$

Exemple 0.5 Soit E un ensemble. On considère l'ensemble des applications de E dans E muni de la composition : $(\mathcal{F}(E,E), \circ)$. La loi de composition interne $\circ$ est associative mais pas commutative. Id_E est l'élément neutre de cette loi.

Dans la suite, on suppose que $\star$ est associative et admet un élément neutre.

DÉFINITION 0.3 **Symétrique**
On suppose que $(E, \star)$ possède un élément neutre e. Soit un élément $x \in E$. On dit qu'un élément $y \in E$ est un *symétrique* (ou un *inverse*) de l'élément x si et seulement si :

$$x \star y = y \star x = e$$

Si tel est le cas, y est unique et est appelé le *symétrique de* x.

Démonstration *Supposons que x possède deux symétriques $y_1 \in E$ et $y_2 \in E$, alors, par application de la définition et par associativité de $\star$, il vient :*

$$y_2 = (x \star y_1) \star y_2 = (y_1 \star x) \star y_2 = y_1 \star (x \star y_2) = y_1 \star e = y_2.$$

PLAN 0.2 : Pour montrer que $y \in E$ est le symétrique de $x \in E$

1. *On montre que $x \star y = e$;*
2. *On montre que $y \star x = e$;*
3. *Donc y est le symétrique de x.*

Remarque 0.3 L'élément neutre est toujours son propre symétrique : $e^{-1} = e$.

✎ *Notation 0.6* Si un élément x de $(E, \star)$ admet un symétrique :

— on l'appelle *inverse* de x et on le note x^{-1} lorsque la loi est notée multiplicativement

— on l'appelle *opposé* de x et on le note de x et on le note $-x$ lorsque la loi est notée additivement.

Exemple 0.7

— Le seul élément de $(\mathbb{N}, +)$ qui admet un opposé est 0.

— Tout élément $n \in \mathbb{Z}$ muni de l'addition admet un opposé.

— Les deux seuls éléments de $\mathbb{Z}^*$ muni de la multiplication qui admettent un inverse sont 1 et -1.

— Tout élément p/q de $\mathbb{Q}^*$ admet un inverse donné par q/p.

— Si $f \in \mathcal{F}(E,E)$ muni de la loi de composition, f est inversible si et seulement si elle est bijective.

PROPOSITION 0.2 **Règles de calcul avec les inverses**

— Si x est symétrisable alors x^{-1} est aussi symétrisable et : $\boxed{\left(x^{-1}\right)^{-1} = x}$.

— Si x et y sont symétrisables, $x \star y$ est aussi symétrisable et : $\boxed{(x \star y)^{-1} = y^{-1} \star x^{-1}}$.

Démonstration

— *Soit x un élément symétrisable de E et soit $y = x^{-1}$. Comme $y \star x = x \star y = e$, y est symétrisable et $x = y^{-1} = \left(x^{-1}\right)^{-1}$.*

— *Supposons que x et y sont symétrisables, alors, par associativité de $\star$, on a :*

$$(x \star y) \star \left(y^{-1} \star x^{-1}\right) = x \star \left(y \star y^{-1}\right) \star x^{-1} = x \star e \star x^{-1} = x \star x^{-1} = e.$$

On montre de même que $\left(y^{-1} \star x^{-1}\right) \star (x \star y) = e$, ce qui prouve bien que $x \star y$ est symétrisable et que $(x \star y)^{-1} = y^{-1} \star x^{-1}$.

Remarque 0.4 La propriété $(x \star y)^{-1} = y^{-1} \star x^{-1}$ dit simplement que l'on se déshabille dans l'ordre inverse de l'habillage. Si x désigne l'opération « je mets ma chaussette droite » et y l'opération « je mets ma chaussure droite », les opérations inverses sont x^{-1}, « j'ôte ma chaussette droite » et y^{-1} l'opération « j'ôte ma chaussure droite ». L'opération « je mets ma chaussette droite, puis ma chaussure droite » est désignée par $x \star y$. Son opération inverse est bien $(x \star y)^{-1} = y^{-1} \star x^{-1}$ c'est-à-dire « j'ôte ma chaussure droite, puis ma chaussette droite ».

L'opération z « je mets ma chaussette gauche » commute avec x et y, (donc avec x^{-1} et y^{-1}). De ce fait $(x \star z)^{-1} = z^{-1} \star x^{-1}$, ce qui peut être facilement vérifié expérimentalement.

1.1.2 Groupe

DÉFINITION 0.4 **Groupe**
Soit G un ensemble. On dit que $(G, \star)$ est un *groupe* si $\star$ est une loi de composition interne sur G vérifiant :

1. la loi $\star$ est associative ;
2. G possède un élément neutre ;
3. tout élément x de G admet un symétrique.

Si de plus la loi $\star$ est commutative, on dit que le groupe est *abélien* (ou *commutatif*).

Exemple 0.8

— Les couples $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes.

— Les couples $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ sont des groupes.

— Rappelons que $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\} = \{z \in \mathbb{C} \mid \exists \theta \in \mathbb{R} \ : z = e^{i\theta}\}$. On a montré dans la proposition **??** page **??** que $(\mathbb{U}, \times)$ est un groupe.

— Les couples $(\mathbb{N}, +)$, $(\mathbb{Z} \setminus \{0\}, \times)$ ne sont pas des groupes. Pourquoi ?

Présentons maintenant un autre exemple essentiel.

PROPOSITION 0.3 **Groupes des bijections d'un ensemble**
Soit E un ensemble. On note $\mathfrak{S}(E)$ l'ensemble des bijections de E dans E. Alors $(\mathfrak{S}(E), \circ)$ est un groupe (en général non abélien).

Démonstration

- *On a déjà prouvé que $\circ$ est une loi de composition interne : si $(f, g) \in (\mathfrak{S}(E))^2$ alors $f \circ g$ et $g \circ f$ sont encore des bijections sur E.*
- *On a aussi déjà prouvé que $\circ$ est associative.*
- *$\mathfrak{S}(E)$ possède un élément neutre Id_E.*
- *Toute application f de E possède une application symétrique : son application réciproque f^{-1}.*

Évariste Galois né à Bourg-la-Reine le 25 octobre 1811, mort à Paris le 31 mai 1832.

Malgré une scolarité en dents de scie, Galois montre des capacités extraordinaires en mathématiques. Il a un tel goût pour cette matière qu'un de ses professeurs dira « C'est la fureur des mathématiques qui le domine ; aussi je pense qu'il vaudrait mieux pour lui que ses parents consentent à ce qu'il ne s'occupe que de cette étude ». En 1826, il obtient un prix en mathématiques au concours général. En 1828, il essaie d'intégrer l'école Polytechnique alors qu'il n'est pas élève, comme c'est normalement l'usage, en mathématiques spéciales. Il est recalé. Il entre alors en mathématiques spéciales à Louis-le-Grand dans la classe de Louis-Paul-Émile Richard. Ce dernier prend vite conscience du génie de son élève. Il conservera d'ailleurs ses copies. Le père de Galois se suicide pour des raisons politiques quelques jours avant que Galois ne se présente à nouveau à Polytechnique. Il est une seconde fois recalé, à la stupéfaction de son maître. La légende veut qu'il ait jeté le chiffon servant à effacer le tableau à la tête de son examinateur devant la stupidité des questions posées ... Il intègre cependant l'École préparatoire (appelée maintenant l'École Normale Supérieure, rue d'Ulm). Il publie cette même année son premier article de mathématiques dans les Annales de mathématiques pures et appliquées de Gergonne.
Il soumet dans les mois qui suivent plusieurs autres articles sur la résolubilité des équations algébriques. La légende veut que Cauchy, qui en était le rapporteur, les aurait égarés. Il est plus probable en fait qu'il les ait conservés pour que Galois puisse concourir au grand prix de mathématiques de l'Académie des sciences en 1830. Galois candidate à ce concours et Fourier qui est chargé de rapporter son manuscrit meurt peu après ... Le grand prix échoit à Abel et Jacobi.
Suite à la révolution de juillet 1830, Galois s'engage en politique au côté des républicains. Fin décembre 1830, il est expulsé de l'école préparatoire suite à la rédaction d'un texte critique à l'égard de son directeur. En 1831, lors d'un banquet, Galois porte maladroitement un toast à Louis-Philippe avec un couteau à la main ... Il est arrêté et passe un mois en prison. Quelques mois après, il est à nouveau arrêté et passe six mois en prison pour port illégal de l'uniforme de l'artillerie. Cette même année, il soumet un nouveau manuscrit à l'Académie des sciences, toujours sur la résolubilité des équations polynomiales. Poisson, qui le rapporte est rebuté par sa difficulté et le refuse. En prison, Galois poursuit ses recherches mathématiques et s'intéresse aux fonctions elliptiques.
Le 30 mai 1832, Galois se bat en duel au pistolet suite, semble-t-il, à une bête querelle amoureuse. Il décède le lendemain de ses blessures. La nuit précédant le duel, il rédige une lettre[1] *à son ami Auguste Chevalier lui enjoignant de faire connaître ses travaux à Jacobi et Gauss. Elle se termine par cette phrase très émouvante qui permet de mesurer l'optimisme de Galois quant à l'issue du duel : « Après cela, il y aura, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis ».*
Liouville, dix ans plus tard, re-découvrira les travaux de Galois et qui les popularisera.

THÉORÈME 0.4 **Règles de calcul dans un groupe**
Soit $(G, \star)$ un groupe.

1. L'élément neutre est unique .
2. Tout élément possède un *unique* symétrique ;
3. Pour tout élément x d'un groupe, on a $\left(x^{-1}\right)^{-1} = x$.
4. Règle de *simplification* : $\forall (a, x, y) \in G^3$;

$$\begin{cases} a \star x = a \star y & \Rightarrow x = yx \star a = y \star a \\ & \Rightarrow x = y \end{cases}.$$

1. On peut consulter cette lettre à l'adresse http ://www.imnc.univ-paris7.fr/oliver/galois/LettreGaloisA4.ps

5. Soit $(a, b) \in G^2$. L'équation $a \star x = b$ possède une unique solution :

$$x = a^{-1} \star b.$$

6. $\forall (x, y) \in G^2$, $(x \star y)^{-1} = y^{-1} \star x^{-1}$.

PROPOSITION 0.5 **Groupe produit**
On considère deux groupes $(G, \star)$ et $(H, \bullet)$ et sur l'ensemble $G \times H$, on définit la loi $\bigstar$ par :

$$\forall ((x, y), (x', y')) \in (G \times H)^2, \quad (x, y) \bigstar (x', y') = (x \star x', y \bullet y')$$

Alors $(G \times H, \bigstar)$ est un groupe appelé *groupe produit*.

Démonstration *La preuve est laissée en exercice. Il suffit de vérifier chacun des axiomes définissant un groupe.*

DÉFINITION 0.5 **Sous-groupe**
Soit $(G, \star)$ un groupe. On dit qu'une partie $H \subset G$ est un *sous-groupe* de G si et seulement si :

1. $e \in H$.
2. la partie H est *stable* par la loi : $\forall (x, y) \in H^2,\ x \star y \in H$.
3. $\forall x \in H$, $x^{-1} \in H$.

Exemple 0.9

— $\mathbb{Z}$ est un sous-groupe de $\mathbb{R}$ pour l'addition.

— $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ pour l'addition.

— L'ensemble des bijections croissantes est un sous-groupe du groupe des bijections de $\mathbb{R}$ dans $\mathbb{R}$.

— L'ensemble des isométries du plan est un sous-groupe du groupe des bijections du plan. (Rappelons qu'une isométrie est une bijection conservant les distances).

PROPOSITION 0.6 **Caractérisation des sous-groupes**
Soient $(G, \star)$ un groupe et H une partie **non vide** de G. H est un sous-groupe de G si et seulement si

1. $e \in H$;
2. $\forall (x, y) \in H^2$, $\boxed{x \star y^{-1} \in H}$.

Démonstration

— *Soit H un sous-groupe non vide de G et soit $(x, y) \in H^2$. y^{-1} est élément de H et il en est de même du produit $x \star y^{-1}$.*

— *Soit H une partie non vide de G vérifiant : $\forall (x,y) \in H^2, \quad x \star y^{-1} \in H$. Soit $x \in H$. On a : $e = x \star x^{-1} \in H$ donc l'élément neutre de G est élément de H. Pour tout $(e,x) \in H^2$, $e \star x^{-1} \in H$ donc $x^{-1} \in H$. Enfin, pour tout $(x,y) \in H^2$, on a $(x,y^{-1}) \in H^2$ et donc $x \star \left(y^{-1}\right)^{-1} \in H$, soit $x \star y \in H$.*

PLAN 0.3 : Pour montrer que $H \subset G$ est un sous-groupe du groupe $(G, \star)$

1. *$e \in H$;*
2. Soit $(x,y) \in H^2$;
3. *Vérifions que $x \star y^{-1} \in H$ ...*
4. *Donc H est un sous-groupe de G.*

THÉORÈME 0.7 Un sous-groupe a une structure de groupe
Si la partie H est un sous-groupe de $(G, \star)$, alors puisque cette partie est stable pour la loi de composition interne, on peut définir la restriction de la loi $\star$ à H qui est une loi de composition interne sur H. Muni de cette loi restreinte, $(H, \star)$ est un groupe.

Ce théorème est d'une grande utilité pour prouver rapidement que des ensembles sont des groupes.

PLAN 0.4 : Pour montrer qu'un ensemble a une structure de groupe...

...il suffit de montrer que c'est un sous-groupe d'un groupe connu.

Exemple 0.10 Montrons que $(\mathbb{U}, \times)$ est un groupe avec : $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$. Il suffit de prouver que c'est un sous-groupe de $(\mathbb{C}^*, \times)$.

1. Comme $|1| = 1$, il est clair que $1 \in \mathbb{U}$.
2. Soient $x, y \in \mathbb{U}$.
3. On a $\left|xy^{-1}\right| = |x| \left|y\right|^{-1} = 1$ donc $xy^{-1} \in \mathbb{U}$.
4. Donc $\mathbb{U}$ est un sous-groupe de $(\mathbb{C}^*, \times)$ et $(\mathbb{U}, \times)$ admet par conséquent une structure de groupe.

THÉORÈME 0.8 L'intersection de deux sous-groupes est un sous-groupe
Si H_1 et H_2 sont deux sous-groupes d'un groupe G, alors $H_1 \cap H_2$ est un sous-groupe de G

Démonstration *Notons $H = H_1 \cap H_2$ et montrons que H est un sous-groupe de G. Utilisons la caractérisation précédente. Soit $(x,y) \in H^2$. On a alors $(x,y) \in H_1^2$ ce qui amène que $x \star y^{-1} \in H_1$ car H_1 est un sous-groupe de G et $(x,y) \in H_2^2$ ce qui amène aussi que $x \star y^{-1} \in H_2$. Donc $x \star y^{-1} \in H_1 \cap H_2 = H$ et H est bien un sous-groupe de G.*

⚠ *Attention 0.11* $H_1 \cup H_2$ n'est pas un sous-groupe de G, sauf si $G_1 \subset G_2$ ou $G_2 \subset G_1$. Voir exercice **??** p. **??**.

1.1.3 Morphisme de groupes

DÉFINITION 0.6 **Morphisme**
Soient deux groupes $(G_1, \star)$ et $(G_2, \bullet)$. Une application $f : G_1 \longrightarrow G_2$ est un *morphisme* de groupes ou *homomorphisme* si et seulement si :

$$\forall (x, y) \in G_1^2, \quad f(x \star y) = f(x) \bullet f(y)$$

On dit de plus que φ est un :

— **endomorphisme** lorsque $G_1 = G_2$

— **isomorphisme** lorsque f est bijective

— **automorphisme** lorsque f est un endomorphisme et un isomorphisme.

PLAN 0.5 : Pour montrer que $f : G_1 \longrightarrow G_2$ est un morphisme

1. Soit $(x, y) \in G_1^2$;
2. On a bien $f(x \star y) = f(x) \bullet f(y)$.

Remarque 0.5

— Un morphisme entre un groupe $(G_1, \star_1)$ et un groupe $(G_2, \star_2)$ permet de transformer des produits pour la loi $\star_1$ dans le groupe de départ en des produits pour la loi $\star_2$ dans le groupe d'arrivée.

— La notion d'isomorphisme est fondamentale en mathématiques. Le mot isomorphisme provient du grec et peut se traduire en « même forme ». Deux groupes isomorphes ont non seulement le même nombre d'éléments mais aussi des tables de multiplication identiques. Du coup toute propriété algébrique vraie pour un des deux groupes est vraie pour l'autre. Si un de ces deux groupes est plus simple à étudier que l'autre, on préférera travailler avec celui-ci et on en tirera les propriétés de l'autre. Cette idée est à la base de la théorie des représentations. Par ailleurs, il est intéressant pour un groupe donné, de chercher s'il est isomorphe à un groupe connu. C'est ce qu'on appelle un problème de classification. La classification des groupes finis, terminée au 20 e siècle pour ceux qu'on dit simples, occupe à l'heure actuelle encore de nombreux mathématiciens.

PROPOSITION 0.9 **Propriétés des morphismes de groupes**
Si $(G_1, \star)$ est un groupe d'élément neutre e_1, si $(G_2, \bullet)$ est un groupe d'élément neutre e_2 et si $f : G_1 \longrightarrow G_2$ est un morphisme de groupes, alors

1. $\boxed{f(e_1) = e_2}$;
2. $\forall x \in G_1$, $\boxed{[f(x)]^{-1} = f(x^{-1})}$.

Démonstration

1. *Remarquons que* $f(e_1) = f(e_1 \star e_1) = f(e_1) \bullet f(e_1) = (f(e_1))^2$. *On a par ailleurs l'égalité* $f(e_1) \bullet e_2 = (f(e_1))^2$. *En multipliant cette égalité des deux côtés à gauche par* $(f(e_1))^{-1}$, *on obtient* $e_2 = f(e_1)$.

2. *Soit $x \in G$. Comme f est un morphisme de groupes, $f\left(x \star x^{-1}\right) = f(x) \bullet f\left(x^{-1}\right)$. D'autre part, $f\left(x \star x^{-1}\right) = f(e_1) = e_2$. Donc $f(x) \bullet f\left(x^{-1}\right) = e_2$. On montrerait de même que $f\left(x^{-1}\right) \bullet f(x) = e_2$. Ce qui prouve que $f\left(x^{-1}\right) = [f(x)]^{-1}$.*

THÉORÈME 0.10 **Image directe et réciproque de sous-groupes par un morphisme**
Soient $(G_1, \star)$ et $(G_2, \bullet)$ deux groupes et soit $f : G_1 \mapsto G_2$ un morphisme de groupes.

1. Si H_1 est un sous-groupe de G_1, alors $f(H_1)$ est un sous-groupe de G_2 ;
2. Si H_2 est un sous-groupe de G_2, alors $f^{-1}(H_2)$ est un sous-groupe de G_1.

Démonstration

1. *Comme $e_2 = f(e_1)$ et que $e_1 \in H_1$ alors $e_2 \in f(H_1)$. Soient $y, y' \in f(H_1)$. Montrons que $y \bullet y'^{-1} \in f(H_1)$. Il existe $x, x' \in H_1$ tels que $f(x) = y$ et $f(x') = y'$. Comme $f\left(x'^{-1}\right) = (f(x'))^{-1} = y'^{-1}$, il vient $y \bullet y'^{-1} = f(x) \bullet f\left(x'^{-1}\right) = f\left(x \star x'^{-1}\right)$. Mais H_1 est un sous-groupe de G_1 donc $x \star x'^{-1} \in H_1$. On prouve ainsi que $y \bullet y'^{-1}$ est l'image d'un élément de H_1 par f et donc que $y \bullet y'^{-1} \in f(H_1)$.*
2. *Comme $e_2 = f(e_1)$ et que $e_2 \in H_2$, $e_1 \in f^{-1}(H_2)$. Soient $x, x' \in f^{-1}(H_2)$. Montrons que $x \star x'^{-1} \in f^{-1}(H_2)$. Pour ce faire, il suffit de montrer que $f\left(x \star x'^{-1}\right) \in H_2$. Mais $f\left(x \star x'^{-1}\right) = f(x) \bullet (f(x'))^{-1} \in H_2$ car H_2 est un sous-groupe de G_2. On montre ainsi que $f^{-1}(H_2)$ est un sous-groupe de G_1.*

DÉFINITION 0.7 **Noyau, image d'un morphisme de groupes**
On considère un morphisme de groupes $f : G_1 \mapsto G_2$. On note e_1 l'élément neutre du groupe G_1 et e_2 l'élément neutre du groupe G_2. On définit

— le *noyau* du morphisme f :

$$\operatorname{Ker} f = \{x \in G_1 \mid f(x) = e_2\} = f^{-1}\big(\{e_2\}\big)$$

— l'*image* du morphisme f :

$$\operatorname{Im} f = f(G_1) = \{y \in G_2 \mid \exists x \in G_1 \ f(x) = y\}$$

PROPOSITION 0.11 **Le noyau et l'image d'un morphisme de groupes sont des sous-groupes**
On considère un morphisme de groupes $f : G_1 \mapsto G_2$. Alors

— $\operatorname{Ker} f$ est un sous-groupe de G_1

— $\operatorname{Im} f$ est un sous-groupe de G_2.

Démonstration

— *Comme $f(e_1) = e_2$, $\operatorname{Ker} f$ est un sous-ensemble non vide de G_1. De plus, $\{e_2\}$ est un sous-groupe de G_2 et $\operatorname{Ker} f = f^{-1}(\{e_2\})$ donc $\operatorname{Ker} f$ est un sous-groupe de G_1 d'après la proposition précédente.*

— *Comme* $\operatorname{Im} f = f(G_1)$*, on sait que* $\operatorname{Im} f$ *est un sous-groupe de* G_2 *d'après la proposition précédente.*

Théorème 0.12 Caractérisation des morphismes injectifs
Un morphisme f de $(G_1, \star)$ dans $(G_2, \bullet)$ est injectif si et seulement si $\boxed{\operatorname{Ker} f = \{e_1\}}$.

Démonstration

— *Supposons que* f *est injectif. Comme* f *est un morphisme, on a* $e_1 \in \operatorname{Ker} f$*. Comme* f *est injectif,* e_1 *est le seul élément de* $f^{-1}(e_2)$ *dans* G_1*, ce qui prouve que* $\operatorname{Ker} f = \{e_1\}$*.*

— *Réciproquement, supposons que* $\operatorname{Ker} f = \{e_1\}$*. Soient* $(x, y) \in (G_1)^2$ *tel que* $f(x) = f(y)$*. Montrons que* $x = y$*. On multiplie à droite l'égalité* $f(x) = f(y)$ *par* $(f(y))^{-1}$*. On obtient* $f(x) \bullet (f(y))^{-1} = f(y) \bullet (f(y))^{-1} = e_2$*. D'après les propriétés des morphismes de groupe* $f\left(x \star y^{-1}\right) = e_2$*. Donc* $x \star y^{-1} \in \operatorname{Ker} f$ *et nécéssairement* $x \star y^{-1} = e_1$*. On multiplie à droite par* y *les deux membres de cette égalité et on obtient* $x = y$*, ce qui prouve que* f *est injectif.*

Plan 0.6 : $\boxed{\text{Pour montrer qu'un morphisme } f \ : \ (G_1, \star) \mapsto (G_2, \bullet) \text{ est injectif}}$

1. Soit $x \in G_1$ *tel que* $f(x) = e_2$
2. *Alors* $x = e_1$ *;*
3. *Donc* $\operatorname{Ker} f = \{e_1\}$*, et puisque* f *est un morphisme,* f *est injectif.*

Théorème 0.13 Caractérisation des morphismes surjectifs
Un morphisme f de $(G_1, \star)$ dans $(G_2, \bullet)$ est surjectif si et seulement si $\boxed{\operatorname{Im} f = G_2}$.

Démonstration *Par définition de la surjectivité !*
Ajoutons, à titre indicatif, les deux propositions suivantes. Leur preuves forment un exercice instructif laissé au lecteur.

Proposition 0.14 Composition de morphismes de groupes

— La composée de deux morphismes de groupes est un morphisme de groupes.

— La bijection réciproque d'un isomorphisme de groupes est un isomorphisme de groupes.

Proposition 0.15 L'ensemble des automorphismes d'un groupe est un groupe pour la composition
Si $(G, \star)$ est un groupe, on note $\operatorname{Aut}(G)$ l'ensemble des automorphismes de G. $(\operatorname{Aut}(G), \circ)$ est un groupe.

1.2 Anneau, corps

1.2.1 Structure d'anneau

Définition 0.8 **Anneau**
Soit A un ensemble muni de deux loi de composition interne notées $+$ et $\times$. On dit que $(A,+,\times)$ est un *anneau* si et seulement si :

1. Le couple $(A,+)$ est un groupe commutatif ;
2. la loi $\times$ est associative ;
3. la loi $\times$ est *distributive* par rapport à la loi $+$:

$$\forall (x,y,z)\in A^3,\quad x\times(y+z)=x\times y+x\times z\quad (x+y)\times z=x\times z+y\times z;$$

4. il existe un élément neutre pour $\times$, noté 1.

Si en plus la loi $\times$ est commutative, on dit que $(A,+,\times)$ est un anneau commutatif.

Exemple 0.12

— Les triplets $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$,$(\mathbb{R},+,\times)$,$(\mathbb{C},+,\times)$ sont des anneaux commutatifs. Ce n'est pas le cas de $(\mathbb{N},+,\times)$.

— Si E est un ensemble, l'ensemble $\mathscr{F}(E,\mathbb{R})$ des applications définies sur E et à valeurs dans $\mathbb{R}$ muni de l'addition et du produit des fonctions est un anneau commutatif.

— L'ensemble des fonctions polynômes de $\mathbb{R}$ dans $\mathbb{R}$ muni de l'addition et du produit des fonctions est un anneau commutatif.

— L'ensemble des suites réelles (ou complexes) $\mathscr{S}(\mathbb{R})$ (ou $\mathscr{S}(\mathbb{C})$) muni de l'addition et de la multiplication des suites est un anneau commutatif.

— On verra au chapitre **??** que l'ensemble des matrices carrées à coefficients réels (ou complexes) muni de l'addition et du produit des matrices est un anneau en général non commutatif.

✎ *Notation 0.13* Dans un anneau $(A,+,\times)$, on note $-x$ le symétrique de l'élément x pour la loi $+$ et 0 l'élément neutre de la loi $+$. Attention, un élément $x\in A$ n'a pas forcément de symétrique pour la loi $\times$, la notation x^{-1} n'a pas de sens en général.

Théorème 0.16 **Règles de calcul dans un anneau**
On considère un anneau $(A,+,\times)$. On a les règles de calcul suivantes :

1. $\forall a\in A,\ a\times 0=0\times a=0$;
2. $\forall a\in A,\ (-1)\times a=-a$;
3. $\forall (a,b)\in A^2,\ (-a)\times b=-(a\times b)$.

Démonstration *Soit* $(a,b)\in A^2$

1. *La distributivité de la loi* $\times$ *par rapport à la loi* $+$ *permet d'écrire :* $0\times a+0\times a=(0+0)\,a=0\times a$. *Par soustraction de* $0\times a$ *des deux côtés de cette égalité, on obtient :* $0\times a=0$. *On prouve de même que* $a\times 0=0$.
2. *Toujours par distributivité de la la loi* $\times$ *par rapport à la loi* $+$, *on a :* $a+(-1)\times a=1\times a+(-1)\times a=(1-1)\times a=0\times a=0$. *De même, on montrerait que* $(-1)\times a+a=0$. *Donc* $(-1)\times a$ *est l'opposé de* a *et* $(-1)\times a=-a$.

3. La dernière relation se prouve de la même façon.

Remarque 0.6 Si $(A,+,\times)$ est un anneau, $(A,\times)$ n'est pas un groupe . Sauf dans le cas où $1=0$ et $A=\{0\}$.

⚠ *Attention 0.14* En général,

$$\boxed{a\times b=0 \not\Rightarrow a=0 \text{ ou } b=0}.$$

On dit que de tels éléments a et b sont des *diviseurs de zéro*. Par exemple, dans l'anneau $\mathcal{F}(\mathbb{R},\mathbb{R})$, considérer les fonctions $\delta_a : \mathbb{R}\to\mathbb{R}, x\mapsto \begin{cases} 0 & \text{si } x\neq a1 \\ \text{si } x=a \end{cases}$ pour $a\in\mathbb{R}$. Il est clair que $\delta_2\delta_0=0$ et pourtant δ_2 et δ_0 ne sont pas identiquement nulles.

DÉFINITION 0.9 **Anneau intègre**
Soit un anneau $(A,+,\times)$. On dit que cet anneau est *intègre* si et seulement si :

1. $A\neq\{0\}$;
2. la loi $\times$ est commutative ;
3. $\forall (x,y)\in A^2,\ x\times y=0\Rightarrow x=0$ ou $y=0$.

Remarque 0.7 Dans un anneau *intègre*, on peut « simplifier » à gauche et à droite : Si $(a,y,z)\in A^3$, avec $ax=ay$, et si $a\neq 0$, alors $x=y$, que a soit inversible ou non. Cette propriété est fausse dans un anneau général.

DÉFINITION 0.10 **Notations**
On considère un anneau $(A,+,\times)$. Soit un élément $a\in A$ et un entier $n\in\mathbb{N}$. On note

- $na=\begin{cases}\underbrace{a+\cdots+a}_{n \text{ fois}} & \text{si } n\neq 0\\ 0 & \text{si } n=0\end{cases}$
- $(-n)a=n(-a)=\underbrace{(-a)+\cdots+(-a)}_{n \text{ fois}}$
- $a^n=\begin{cases}\underbrace{a\times\cdots\times a}_{n \text{ fois}} & \text{si } n\neq 01\\ \text{si } n=0\end{cases}$
- a^{-n} n'a de sens que si a est inversible pour $\times$. On a alors $a^{-n}=\left(a^{-1}\right)^n$.

DÉFINITION 0.11 **Élément nilpotent**
Soit un anneau $(A,+,\times)$. On dit qu'un élément $a\in A$ $(a\neq 0)$ est *nilpotent* s'il existe un entier $n\in\mathbb{N}^*$ tel que $a^n=0$.

Le plus petit entier n vérifiant $a^n=0$ s'appelle l'indice de nilpotence de l'élément a.

Remarque 0.8 Si l'anneau A est intègre, il n'y a pas d'élément nilpotent dans cet anneau.

THÉORÈME 0.17 **Formule du binôme de Newton et formule de factorisation**
Dans un anneau $(A,+,\times)$, si $(a,b)\in A^2$ vérifient

$$\boxed{a\times b = b\times a}$$

Alors pour tout $n\in\mathbb{N}$, on a la formule du *binôme de Newton*

$$\boxed{(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}}$$

et pour tout $n\geqslant 1$, la formule de factorisation suivante

$$\boxed{a^n - b^n = (a-b)(a^{n-1}+a^{n-2}b+\cdots+ab^{n-2}+b^{n-1}) = (a-b)\sum_{k=0}^{n-1}a^{n-1-k}b^k}.$$

Démonstration *La démonstration de la formule du binôme dans le cas où a et b sont des éléments d'un anneau A tels que $ab=ba$ se fait comme dans le cas où a et b sont des complexes. On consultera alors la démonstration* **??** *page* **??**

Prouvons la seconde formule :

$$\begin{aligned}
&(a-b)(a^{n-1}+a^{n-2}b+\cdots+ab^{n-2}+b^{n-1})\\
=\ &\left(a^n+a^{n-1}b+\cdots+a^2b^{n-2}+ab^{n-1}\right)-\left(a^{n-1}b+a^{n-2}b^2+\cdots+ab^{n-1}+b^n\right)\\
=\ &a^n+\left(a^{n-1}b-a^{n-1}b\right)+\cdots+\left(a^2b^{n-2}-a^2b^{n-2}\right)+\left(ab^{n-1}-ab^{n-1}\right)-b^n = a^n-b^n.
\end{aligned}$$

THÉORÈME 0.18 **Calcul d'une progression géométrique**
Soit un anneau $(A,+,\times)$ et un élément $a\in A$. On considère un entier $n\in\mathbb{N}$, $n\geqslant 1$. De la formule de factorisation, on tire :

$$\boxed{1-a^n = (1-a)(1+a+a^2+\cdots+a^{n-1})}$$

En particulier, si l'élément a est *nilpotent* d'indice n : $a^n=0$, alors l'élément $(1-a)$ est inversible pour la loi $\times$ et on sait calculer son inverse :

$$(1-a)^{-1} = 1+a+a^2+\cdots+a^{n-1}$$

DÉFINITION 0.12 **Sous-anneau**
On considère un anneau $(A,+,\times)$ et une partie $A'\subset A$ de cet anneau. On dit que la partie A' est un sous-anneau de A si et seulement si :

1. $(A',+)$ est un sous-groupe du groupe $(A,+)$;

2. la partie A' est *stable* pour la loi$\times$: $\forall (a,b) \in {A'}^2$, $a \times b \in A'$;
3. l'élément neutre de l'anneau A est dans A' : $1 \in A'$.

1.2.2 Structure de corps

DÉFINITION 0.13 **Corps**
On considère un ensemble K muni de deux lois de composition interne, notées $+$ et $\times$. On dit que $(K,+,\times)$ est un *corps* si et seulement si :

1. $(K,+,\times)$ est un anneau intègre ;
2. $(K \setminus \{0\},\times)$ est un groupe commutatif.

Remarque 0.9 Comme $(K,+,\times)$ est intègre, la loi $\times$ (ou plutôt sa restriction à $K \setminus \{0\} \times K \setminus \{0\}$) est interne, ce qui permet d'envisager que $(K \setminus \{0\},\times)$ soit un groupe (commutatif).

Exemple 0.15 $(\mathbb{Q}, +,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$ sont des corps, mais $(\mathbb{Z},+,\times)$ n'en est pas un car ses seuls éléments inversibles sont 1 et -1.

DÉFINITION 0.14 **Sous-corps**
Soit $K' \setminus K$ un sous-ensemble d'un corps $(K,+,\times)$. On dit que la partie K' est un *sous-corps* du corps K si et seulement si :

1. K' est un sous-anneau de l'anneau $(K,+,\times)$;
2. l'inverse de tout élément non-nul de K' est dans K'.

THÉORÈME 0.19 **Calcul d'une somme géométrique dans un corps**
Soit un élément $k \in K$ du corps $(K,+,\times)$. Alors la formule suivante permet de calculer une progression géométrique de raison k :

$$\sum_{i=0}^{n} k^i = 1 + k + k^2 + \cdots + k^n = \begin{cases} (1-k)^{-1}\left(1-k^{n+1}\right) & \text{si } k \neq 1 (n+1)1_K \\ \text{si } k = 1 \end{cases}$$

Démonstration *Laissée en exercice.*

Références