

Groupes, anneaux et corps

I. Lois de composition interne

Vous manipulez depuis longtemps l'addition des entiers, la multiplication des complexes ou la composition des applications. Ces opérations ont des propriétés communes. Ce chapitre leur donne un vocabulaire unique. Ainsi, un même théorème s'appliquera d'un coup à tous les exemples.

1. Définitions

Définition :

Soit E un ensemble. Une **loi de composition interne** sur E est une application $- : E \times E \rightarrow E$, $(x, y) \rightarrow x - y$. On dit que $(E, -)$ est un magma.

La loi $-$ est **associative** si $\forall (x, y, z) \in E^3$,
 $(x - y) - z = x - (y - z)$.

Elle est **commutative** si $\forall (x, y) \in E^2$,
 $x - y = y - x$.

Un élément $e \in E$ est **neutre** si $\forall x \in E$,
 $x - e = e - x = x$.

Exemple :

L'addition et la multiplication sont associatives et commutatives sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, de neutres respectifs 0 et 1 . En revanche, la soustraction sur $\mathbb{Z}$ n'est ni associative ni commutative : $(1 - 1) - 1 = -1$ alors que $1 - (1 - 1) = 1$. Sur l'ensemble $\mathcal{F}(X, X)$ des applications de X dans X , la composition $\circ$ est associative, de neutre id_X . Cependant, elle n'est pas commutative dès que X possède au moins deux éléments.

Propriété :

Si une loi admet un élément neutre, celui-ci est unique.

Démonstration :

Soient e et e' deux neutres. D'une part, $e \cdot e' = e'$ car e est neutre. D'autre part, $e \cdot e' = e$ car e' est neutre. Donc $e = e'$.

Lorsque la loi est associative, les parenthèses deviennent inutiles. On note alors x^n le composé de n copies de x , avec $x^0 = e$. En notation additive, on écrit plutôt nx .

2. Éléments inversibles

Définition :

Soit $(E, \cdot)$ muni d'une loi associative de neutre e . Un élément $x \in E$ est **inversible** (ou symétrisable) s'il existe $y \in E$ tel que $x \cdot y = y \cdot x = e$. Cet élément y est alors unique : on l'appelle l'inverse de x et on le note x^{-1} , ou $-x$ en notation additive.

Proposition :

Si x et y sont inversibles, alors $x \cdot y$ est inversible et $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$. De plus, x^{-1} est inversible et $(x^{-1})^{-1} = x$.

Démonstration :

Par associativité, $(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = x \cdot (y \cdot y^{-1}) \cdot x^{-1} = x \cdot x^{-1} = e$. Le calcul dans l'autre sens est identique. L'unicité de l'inverse vient de l'associativité : si y et y' conviennent, alors $y = y \cdot (x \cdot y') = (y \cdot x) \cdot y' = y'$.

Attention :

L'ordre s'inverse. Pour des bijections, $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$: on défait d'abord ce qui a été fait en dernier.

3. Parties stables

Définition :

Une partie A de E est **stable** par $\cdot$ si $\forall (x, y) \in A^2, x \cdot y \in A$. La restriction de $\cdot$ à $A \times A$ définit alors une loi interne sur A , dite induite.

Exemple :

L'ensemble $\mathbb{U}$ des complexes de module 1 est stable par multiplication, car $|zz'| = |z||z'|$.
Par contre, $\mathbb{R}_+$ est stable par addition, mais pas par multiplication : $(-1) \times (-1) = 1$.

II. Groupes : définition et exemples usuels

1. Définition d'un groupe

Définition :

Un **groupe** est un couple $(G, \cdot)$ où $\cdot$ est une loi interne sur G qui est associative, qui possède un élément neutre e , et pour laquelle tout élément de G est inversible. Le groupe est dit **abélien** (ou commutatif) si la loi est commutative.

Dans un groupe, on peut simplifier. En effet, si $a \cdot x = a \cdot y$, on compose à gauche par a^{-1} et l'on obtient $x = y$. De même, l'équation $a \cdot x = b$ admet l'unique solution $x = a^{-1} \cdot b$. Par ailleurs, les règles de calcul $x^{m+n} = x^m \cdot x^n$ et $(x^m)^n = x^{mn}$ valent pour tous entiers relatifs m et n .

Attention :

Dans un groupe non abélien, $(xy)^2 = xyxy$ diffère en général de x^2y^2 . La formule $(xy)^n = x^n y^n$ n'est valable que si x et y commutent.

2. Les groupes usuels

Vous connaissez déjà de nombreux groupes. D'abord, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes abéliens. Ensuite, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{R}_+^*, \times)$ et $(\mathbb{C}^*, \times)$ le sont aussi. En revanche, $(\mathbb{N}, +)$ n'est pas un groupe, car 1 n'a pas d'opposé dans $\mathbb{N}$. De même, $(\mathbb{Z}^*, \times)$ n'est

pas un groupe, car 2 n'a pas d'inverse entier.

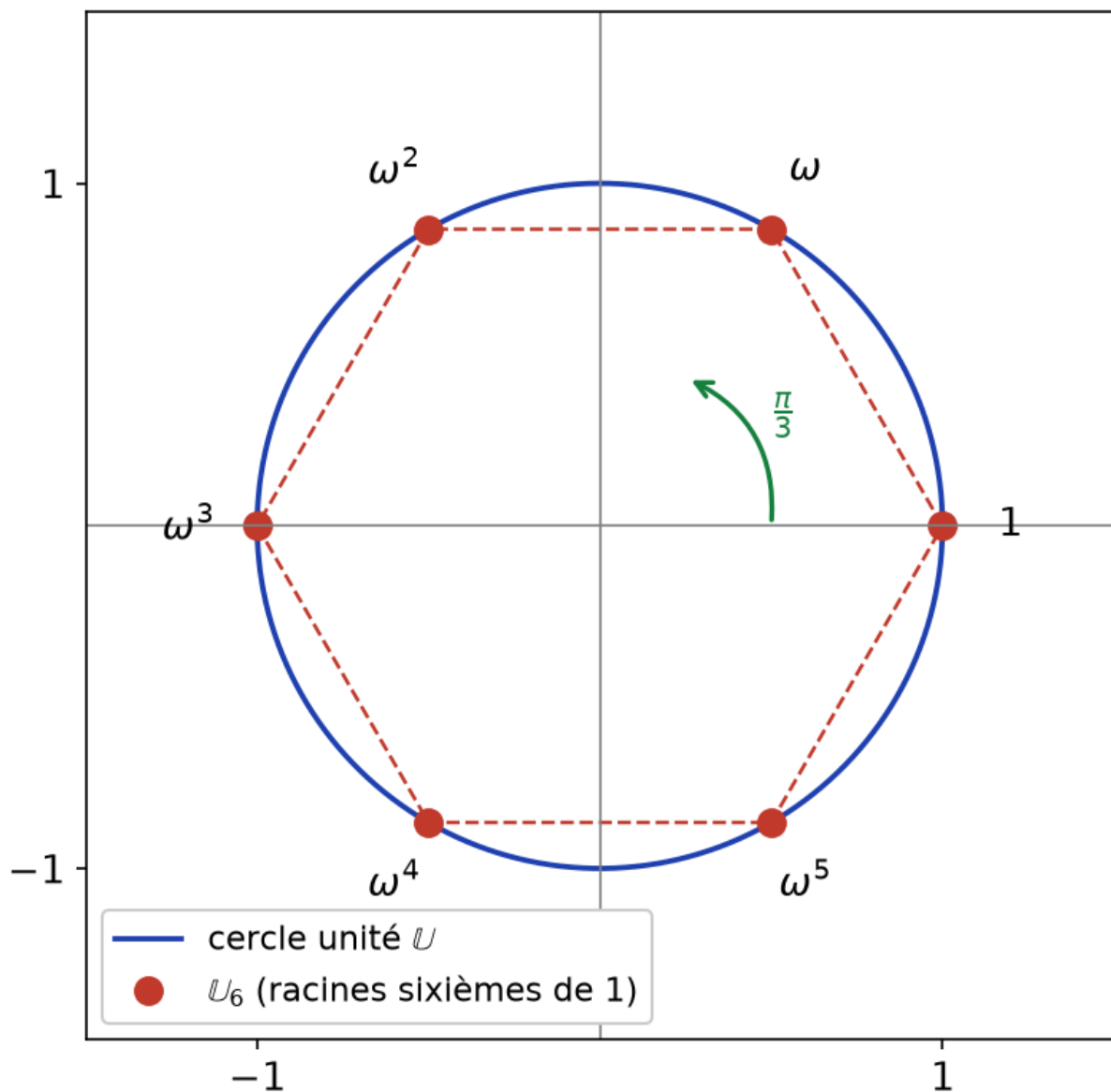
Exemple :

Le cercle unité $\mathbb{U} = \{z \in \mathbb{C}, |z| = 1\}$ est un groupe pour la multiplication. Pour $n \geq 1$, l'ensemble des racines n -ièmes de l'unité

$$\mathbb{U}_n = \left\{ z \in \mathbb{C}, z^n = 1 \right\} = \left\{ e^{2ik\pi/n}, 0 \leq k \leq n-1 \right\}$$

est aussi un groupe multiplicatif, à n éléments.

Géométriquement, les éléments de $\mathbb{U}_n$ sont les sommets d'un polygone régulier inscrit dans le cercle unité. La figure ci-dessous représente $\mathbb{U}_6$ avec $\omega = e^{i\pi/3}$. Multiplier par ω revient à tourner d'un angle $\pi/3$, ce qui permute les sommets.



3. Le groupe des permutations

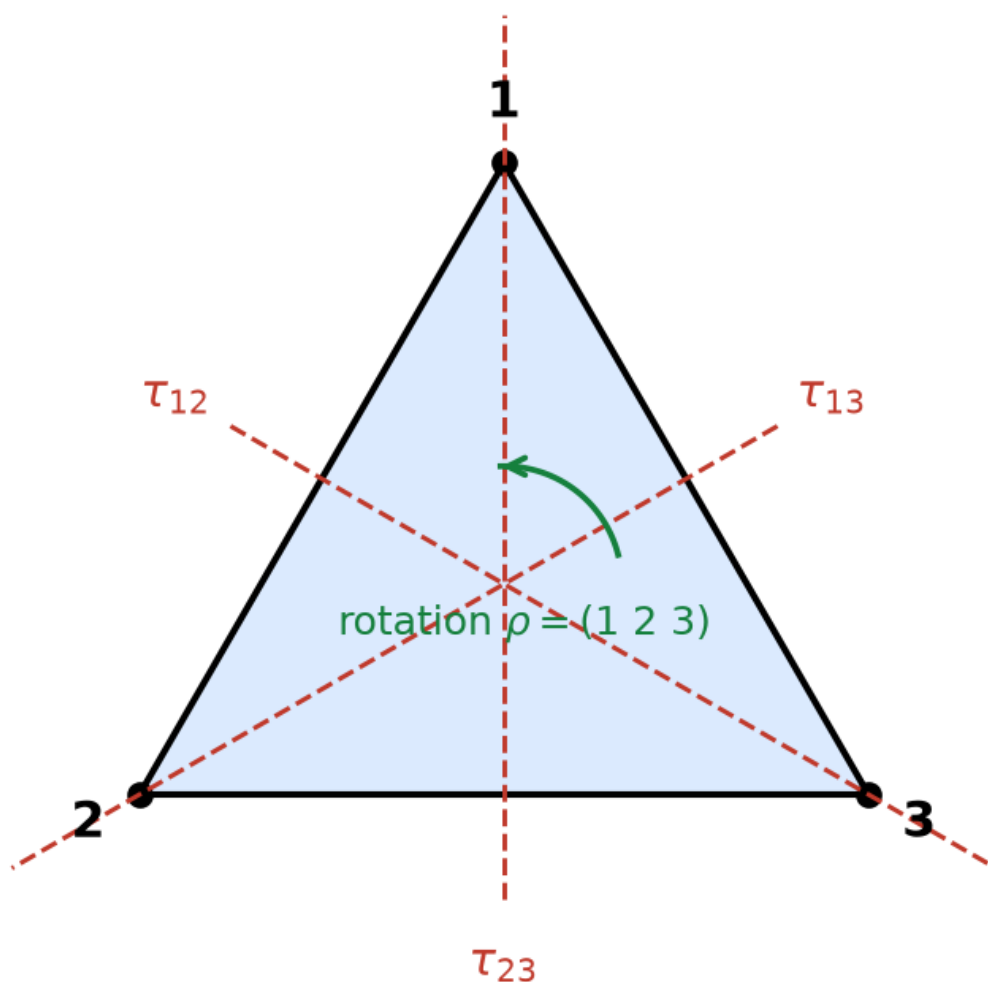
Théorème :

Soit X un ensemble non vide. L'ensemble S_X des bijections de X dans X , muni de la composition, est un groupe de neutre id_X . On l'appelle le **groupe des permutations** de X . Pour $X = \{1, \dots, n\}$, on le note S_n ; il possède $n!$ éléments.

Démonstration :

La composée de deux bijections est une bijection, donc $\circ$ est une loi interne sur S_X . Elle est associative, et id_X est une bijection neutre. Enfin, la réciproque f^{-1} d'une bijection est une bijection qui vérifie $f \circ f^{-1} = f^{-1} \circ f = \text{id}_X$.

Le groupe S_3 a six éléments : l'identité, deux rotations et trois transpositions. On peut le voir comme le groupe des symétries d'un triangle équilatéral dont les sommets sont numérotés, comme le montre la figure suivante. Ainsi, la transposition τ_{12} , qui échange 1 et 2, correspond à la réflexion d'axe passant par le sommet 3.



Exemple :

Dans S_3 , notons ρ la permutation $1 \rightarrow 2 \rightarrow 3 \rightarrow 1$. Alors $\tau_{12} \circ \rho$ envoie 1 sur $\tau_{12}(\rho(1)) = 2$, tandis que $\rho \circ \tau_{12}$ envoie 1 sur $\rho(1) = 2$. Par conséquent, $\tau_{12} \circ \rho \neq \rho \circ \tau_{12}$: le groupe S_3 n'est pas abélien.

4. Groupe produit

Proposition :

Soient $(G, \cdot)$ et $(H, \diamond)$ deux groupes de neutres e_G et e_H . Le produit cartésien $G \times H$, muni de la loi $(g, h) \cdot (g', h') = (g \cdot g', h \diamond h')$, est un groupe. Son neutre est (e_G, e_H) et l'inverse de (g, h) est (g^{-1}, h^{-1}) .

Toutes les vérifications se font composante par composante. Par exemple, $\mathbb{R}^2$ muni de l'addition des vecteurs est le groupe produit $(\mathbb{R}, +) \times (\mathbb{R}, +)$.

III. Sous-groupes

Définition :

Soit $(G, \cdot)$ un groupe. Une partie H de G est un **sous-groupe** de G si H est stable par $\cdot$ et si H , muni de la loi induite, est un groupe.

En pratique, on n'utilise jamais cette définition directement. On se sert plutôt de la caractérisation suivante, beaucoup plus rapide.

Théorème :

Une partie H d'un groupe $(G, -)$ est un sous-groupe si et seulement si :

$$(i) \quad e \in H ; (ii) \quad \forall (x, y) \in H^2, \\ x \cdot y^{-1} \in H.$$

Démonstration :

Si H est un sous-groupe, son neutre e_H vérifie $e_H \cdot e_H = e_H$. En simplifiant dans G , on obtient $e_H = e$, donc $e \in H$. De plus, l'inverse dans H d'un élément coïncide avec son inverse dans G , d'où (ii). Réciproquement, supposons (i) et (ii). Pour $y \in H$, on applique (ii) à $(e, y) : y^{-1} \in H$. Ensuite, pour $x, y \in H$, on applique (ii) à $(x, y^{-1}) : x \cdot y \in H$. La loi induite est associative, e est neutre et tout élément a son inverse dans H .

Méthode :

Pour montrer que H est un sous-groupe de G : vérifiez d'abord que $H \subset G$. Ensuite, vérifiez que le neutre appartient à H . Enfin, prenez x, y quelconques dans H et montrez que $x \cdot y^{-1} \in H$ (ou $x - y \in H$ en notation additive). Pour montrer qu'une partie n'est pas un sous-groupe, un seul contre-exemple suffit : le neutre absent, ou deux éléments dont le produit sort de H .

Exemple :

Montrons que $\mathbb{U}$ est un sous-groupe de $(\mathbb{C}^*, \times)$. D'abord, $\mathbb{U} \subset \mathbb{C}^*$ et $1 \in \mathbb{U}$. Ensuite, pour $z, z' \in \mathbb{U}$, on a $|z \cdot z'^{-1}| = |z| / |z'| = 1$. Donc $\mathbb{U}$ est un sous-groupe. De même, si $z^n = 1$ et $w^n = 1$, alors $(z \cdot w^{-1})^n = z^n (w^n)^{-1} = 1$ car $\mathbb{C}^*$ est abélien. Ainsi, $\mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$.

Pour tout entier n , l'ensemble $n\mathbb{Z}$ des multiples de n est un sous-groupe de $(\mathbb{Z}, +)$. En effet, $0 = n \times 0$ et $na - nb = n(a - b)$. De plus, $\mathbb{R}_+^*$ est un sous-groupe de $(\mathbb{R}^*, \times)$. Au contraire, $\mathbb{R}_-^*$ n'en est pas un, car il ne contient pas 1 .

Proposition :

Une intersection quelconque de sous-groupes de G est un sous-groupe de G . En revanche, la réunion de deux sous-groupes n'est en général pas un sous-groupe.

Par exemple, $2\mathbb{Z} \cup 3\mathbb{Z}$ contient 2 et 3 , mais pas $3 - 2 = 1$.

IV. Morphismes de groupes

1. Définition et premières propriétés

Définition :

Soient $(G, \star)$ et $(G', \diamond)$ deux groupes. Une application $f : G \rightarrow G'$ est un **morphisme de groupes** si

$$\forall (x, y) \in G^2, f(x \star y) = f(x) \diamond f(y).$$

Exemple :

L'exponentielle est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$, car $e^{x+y} = e^x e^y$. Le logarithme népérien est un morphisme de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$. Le module est un morphisme de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}_+^*, \times)$. Enfin, pour $n \in \mathbb{Z}$, l'application $z \rightarrow z^n$ est un morphisme

de $(\mathbb{C}^*, \times)$ dans lui-même.

Proposition :

Si $f : G \rightarrow G'$ est un morphisme de groupes, alors $f(e) = e'$ et, pour tout $x \in G$, $f(x^{-1}) = f(x)^{-1}$. De plus, pour tout $n \in \mathbb{Z}$, $f(x^n) = f(x)^n$.

Démonstration :

On a $f(e) = f(e \cdot e) = f(e) \diamond f(e)$. En simplifiant par $f(e)$ dans G' , on trouve $f(e) = e'$. Ensuite, $f(x) \diamond f(x^{-1}) = f(x \cdot x^{-1}) = f(e) = e'$. Donc $f(x^{-1})$ est l'inverse de $f(x)$. La dernière formule s'obtient par récurrence pour $n \geq 0$, puis par passage à l'inverse.

Proposition :

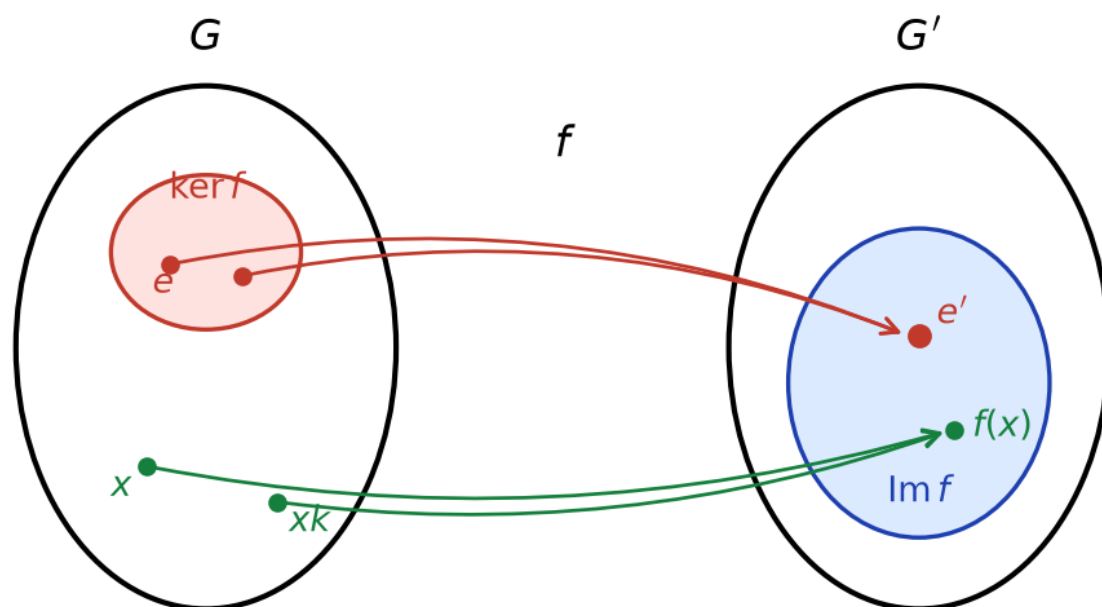
L'image directe d'un sous-groupe de G par un morphisme f est un sous-groupe de G' .
L'image réciproque d'un sous-groupe de G' est un sous-groupe de G . La composée de deux morphismes est un morphisme.

2. Noyau et image

Définition :

Soit $f : G \rightarrow G'$ un morphisme de groupes. Le **noyau** de f est $\ker f = f^{-1}(\{e'\}) = \left\{ x \in G, \begin{matrix} x \in G, \\ f(x) = e'e \end{matrix} \right\}$. L'**image** de f est $\operatorname{Im} f = f(G)$. D'après la proposition précédente, $\ker f$ est un sous-groupe de G et $\operatorname{Im} f$ est un sous-groupe de G' .

La figure ci-dessous résume la situation. Le noyau est la partie de G envoyée sur le neutre e' . Deux éléments x et xk , avec $k \in \ker f$, ont la même image, car $f(xk) = f(x)f(k) = f(x)$.



Théorème :

Un morphisme de groupes $f : G \rightarrow G'$ est injectif si et seulement si $\ker f = \{e\}$. Il est surjectif si et seulement si $\text{Im } f = G'$.

Démonstration :

Si f est injectif, alors $f(x) = e' = f(e)$ impose $x = e$, d'où $\ker f = \{e\}$.

Réciproquement, supposons $\ker f = \{e\}$ et $f(x) = f(y)$. Alors

$f(x \cdot y^{-1}) = f(x) \diamond f(y)^{-1} = e'$. Donc $x \cdot y^{-1} \in \ker f$, c'est-à-dire $x \cdot y^{-1} = e$, soit $x = y$. Le second point est la définition de la surjectivité.

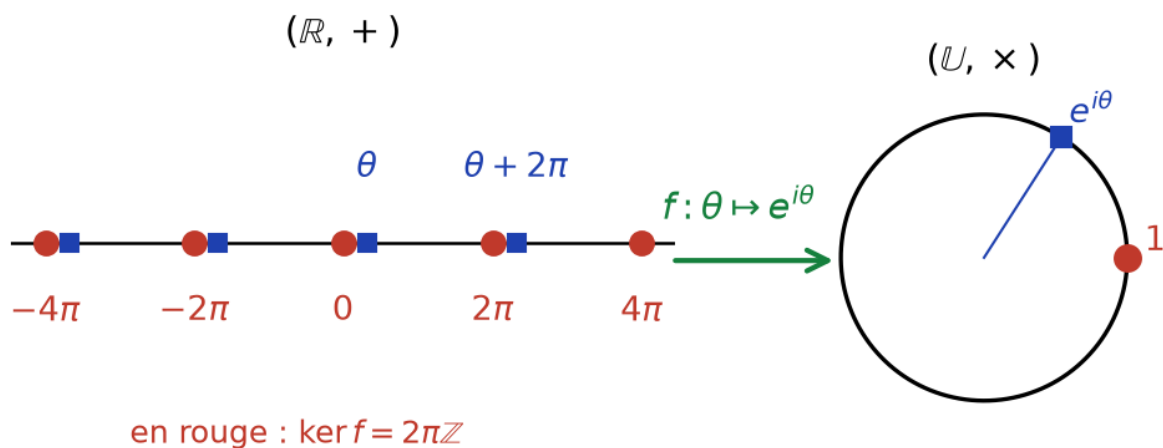
Méthode :

Pour étudier un morphisme : vérifiez d'abord la relation $f(x \cdot y) = f(x) \diamond f(y)$ pour x, y quelconques. Ensuite, résolvez l'équation $f(x) = e'$: c'est le noyau. Enfin, concluez à l'injectivité si le noyau se réduit au neutre. Cette méthode évite de résoudre l'équation plus générale $f(x) = f(y)$.

Exemple :

Considérons $f : (\mathbb{R}, +) \rightarrow (\mathbb{U}, \times)$, $\theta \mapsto e^{i\theta}$. C'est un morphisme, car $e^{i(\theta + \theta')} = e^{i\theta} e^{i\theta'}$. Il est surjectif, car tout complexe de module 1 s'écrit $e^{i\theta}$. Son noyau est $\left\{ \theta, e^{i\theta} = 1 \right\} = 2\pi\mathbb{Z}$. Par conséquent, f n'est pas injectif.

La figure suivante illustre cet exemple : la droite réelle s'enroule sur le cercle. Tous les multiples de 2π tombent sur 1, et deux réels qui diffèrent de 2π ont la même image.



De même, le morphisme $z \mapsto z^n$ de $\mathbb{C}^*$ dans $\mathbb{C}^*$ a pour noyau $\mathbb{U}_n$. Il n'est donc pas injectif pour $n \geq 2$. En revanche, il est surjectif, car tout complexe non nul possède des racines n -ièmes.

3. Isomorphismes de groupes

Définition :

Un **isomorphisme** de groupes est un morphisme bijectif. Deux groupes sont isomorphes s'il existe un isomorphisme de l'un sur l'autre. Un isomorphisme d'un groupe sur lui-même s'appelle un automorphisme.

Proposition :

La réciproque d'un isomorphisme de groupes est un morphisme de groupes, donc un isomorphisme.

Démonstration :

Soient $x', y' \in G'$, et posons $x = f^{-1}(x')$, $y = f^{-1}(y')$. Alors
 $f(x \cdot y) = x' \diamond y'$. En appliquant f^{-1} , on obtient
 $f^{-1}(x' \diamond y') = x \cdot y = f^{-1}(x') \cdot f^{-1}(y')$.

Deux groupes isomorphes ont exactement les mêmes propriétés algébriques. Par exemple, l'exponentielle réalise un isomorphisme de $(\mathbb{R}, +)$ sur $(\mathbb{R}_+^*, \times)$, de réciproque $\ln$. Autrement dit, additionner des réels revient à multiplier leurs exponentielles. Pour prouver que deux groupes ne sont pas isomorphes, on cherche une propriété conservée par isomorphisme qui les distingue : le nombre d'éléments, la commutativité, ou le nombre de solutions de $x^2 = e$.

V. Anneaux

1. Définition et règles de calcul dans un anneau

Définition :

Un **anneau** est un triplet $(A, +, \times)$ tel que :

- (i) $(A, +)$ est un groupe abélien, de neutre noté 0_A ;
- (ii) la loi $\times$ est associative et possède un neutre noté 1_A ;
- (iii) $\times$ est distributive sur $+$: $a(b + c) = ab + ac$ et $(b + c)a = ba + ca$.

L'anneau est dit commutatif si la loi $\times$ l'est.

Exemple :

Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, munis de l'addition et de la multiplication usuelles, sont des anneaux commutatifs. De même, l'ensemble $\mathcal{F}(X, \mathbb{R})$ des fonctions de X dans $\mathbb{R}$ est un anneau commutatif pour les opérations point par point, de neutres les fonctions constantes 0 et 1 . Plus tard, l'ensemble des matrices carrées $\mathcal{M}_n(\mathbb{R})$ fournira un anneau non commutatif pour $n \geq 2$.

Proposition :

Dans un anneau A , pour tous $a, b \in A$: $0_A \times a = a \times 0_A = 0_A$,
 $(-a)b = a(-b) = -(ab)$ et $(-a)(-b) = ab$.

Démonstration :

Par distributivité, $0_A a = (0_A + 0_A) a = 0_A a + 0_A a$. En simplifiant dans le groupe $(A, +)$, il vient $0_A a = 0_A$. Ensuite, $ab + (-a)b = (a + (-a))b = 0_A b = 0_A$, donc $(-a)b = -(ab)$. La dernière égalité s'en déduit en appliquant deux fois la précédente.

2. Formule du binôme dans un anneau

Théorème :

Soient a et b deux éléments d'un anneau A qui **commutent**, c'est-à-dire tels que $ab = ba$. Alors, pour tout $n \in \mathbb{N}$,

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}, \quad a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}.$$

La preuve est la même que dans $\mathbb{C}$, par récurrence sur n . L'hypothèse de commutation intervient pour regrouper les termes : on a besoin de $ba^k = a^k b$. Sans elle, la formule tombe en défaut. Par exemple, $(a + b)^2 = a^2 + ab + ba + b^2$, qui diffère de $a^2 + 2ab + b^2$ dès que $ab \neq ba$.

Méthode :

Pour calculer x^n dans un anneau, cherchez une décomposition $x = a + b$ où a et b commutent, et où les puissances de b s'annulent à partir d'un certain rang (on dit que b est nilpotent). Un choix fréquent est $a = \lambda \cdot 1_A$, qui commute avec tout élément. La somme du binôme devient alors finie et courte. N'oubliez pas de justifier explicitement que $ab = ba$.

3. Groupe des inversibles, anneau intègre

Proposition :

L'ensemble $A^\times$ des éléments inversibles pour la multiplication d'un anneau A est un groupe pour $\times$. On l'appelle le **groupe des inversibles** de A .

Exemple :

On a $\mathbb{Z}^\times = \{-1, 1\}$: si $ab = 1$ avec a, b entiers, alors $|a| |b| = 1$, donc $|a| = 1$. Par ailleurs, $\mathbb{R}^\times = \mathbb{R}^*$. Enfin, le groupe des inversibles de $\mathcal{F}(X, \mathbb{R})$ est formé des fonctions qui ne s'annulent jamais.

Définition :

Un anneau A est **intègre** s'il est commutatif, non réduit à $\{0_A\}$, et si
 $\forall (a, b) \in A^2$,
 $ab = 0_A \Rightarrow (a = 0_A \text{ ou } b = 0_A)$.

Dans un anneau intègre, on peut simplifier par un élément non nul : $ab = ac$ avec $a \neq 0$ entraîne $a(b - c) = 0$, donc $b = c$. L'anneau $\mathbb{Z}$ est intègre. En revanche, $\mathcal{F}(\mathbb{R}, \mathbb{R})$ ne l'est pas. En effet, deux fonctions non nulles peuvent avoir un produit nul si l'une s'annule là où l'autre ne s'annule pas.

4. Sous-anneaux et morphismes d'anneaux

Définition :

Une partie B d'un anneau A est un **sous-anneau** si $1_A \in B$ et si, pour tous $x, y \in B$, on a $x - y \in B$ et $xy \in B$. Muni des lois induites, B est alors un anneau de mêmes neutres.

Exemple :

L'ensemble $\mathbb{Z}[i] = \left\{ a + bi \mid (a, b) \in \mathbb{Z}^2 \right\}$ des entiers de Gauss est un sous-anneau de $\mathbb{C}$. En effet, $1 = 1 + 0i$ lui appartient, la différence de deux entiers de Gauss en est un, et $(a + bi)(c + id) = (ac - bd) + i(ad + bc)$ aussi. En revanche, $2\mathbb{Z}$ n'est pas un sous-anneau de $\mathbb{Z}$, car $1 \notin 2\mathbb{Z}$.

Définition :

Soient A et B deux anneaux. Une application $f : A \rightarrow B$ est un **morphisme d'anneaux** si, pour tous $x, y \in A$: $f(x + y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$ et $f(1_A) = 1_B$.

Un morphisme d'anneaux est en particulier un morphisme de groupes additifs. Il possède donc un noyau, et il est injectif si et seulement si ce noyau vaut $\{0_A\}$. Par exemple, la conjugaison $z \rightarrow \bar{z}$ est un morphisme d'anneaux de $\mathbb{C}$ dans $\mathbb{C}$, et même un automorphisme. Remarquez que la condition $f(1_A) = 1_B$ est indispensable : l'application nulle vérifie les deux premières relations, mais ce n'est pas un morphisme d'anneaux.

VI. Corps

Définition :

Un **corps** est un anneau commutatif K , non réduit à $\{0_K\}$, dans lequel tout élément non nul est inversible. Autrement dit, $K^\times = K \setminus \{0_K\}$.

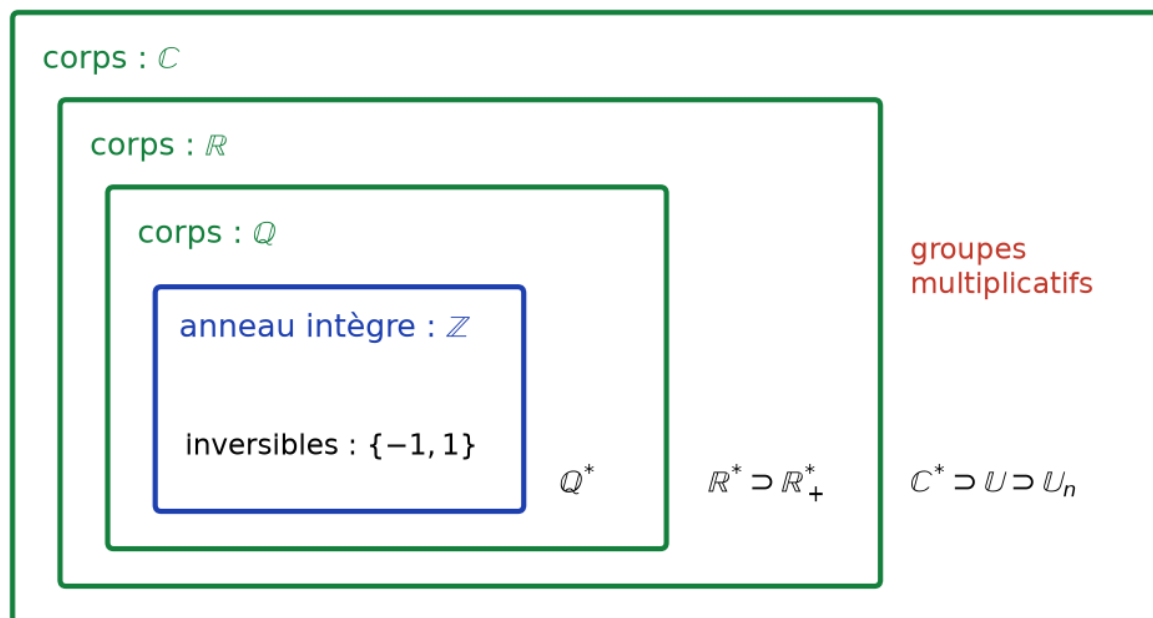
Propriété :

Tout corps est un anneau intègre.

Démonstration :

Soient $a, b \in K$ tels que $ab = 0$. Si $a \neq 0$, alors a est inversible et $b = a^{-1}(ab) = a^{-1} \times 0 = 0$. Donc $a = 0$ ou $b = 0$.

Les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps. En revanche, $\mathbb{Z}$ est intègre sans être un corps, puisque 2 n'y est pas inversible. La figure ci-dessous situe ces structures les unes par rapport aux autres. On y voit aussi les groupes multiplicatifs rencontrés dans ce chapitre.



Exemple :

L'ensemble $\mathbb{Q}[\sqrt{2}] = \left\{ a + b\sqrt{2} \mid (a, b) \in \nu \mathbb{Q}^2 \right\}$ est un corps. D'abord, c'est un sous-anneau de $\mathbb{R}$, par un calcul analogue à celui des entiers de Gauss. Ensuite, si $a + b\sqrt{2} \neq 0$, alors $a - b\sqrt{2} \neq 0$ par irrationalité de $\sqrt{2}$. On peut donc écrire

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2},$$

qui appartient encore à $\mathbb{Q}[\sqrt{2}]$.

Remarque :

La notion de sous-corps se définit comme celle de sous-anneau, en ajoutant la stabilité par passage à l'inverse des éléments non nuls. Ainsi, $\mathbb{Q}[\sqrt{2}]$ est un sous-corps de $\mathbb{R}$. Dans l'arithmétique de $\mathbb{Z}$, vous verrez aussi des corps finis, obtenus à partir des entiers modulo un nombre premier.

Ce qu'il faut retenir

- Une loi interne associative a au plus un neutre, et un élément a au plus un inverse ; de plus, $(xy)^{-1} = y^{-1}x^{-1}$.
- Un groupe est un ensemble muni d'une loi associative, avec neutre, où tout élément est inversible.
- Les groupes usuels sont $(\mathbb{Z}, +)$, $(\mathbb{C}^*, \times)$, $(\mathbb{R}_+^*, \times)$, $(\mathbb{U}, \times)$, $(\mathbb{U}_n, \times)$ et le groupe des permutations $(S_X, \circ)$.
- Pour montrer que H est un sous-groupe : $e \in H$ et $xy^{-1} \in H$ pour tous $x, y \in H$.
- Un morphisme de groupes envoie le neutre sur le neutre et l'inverse sur l'inverse ; son noyau et son image sont des sous-groupes.
- Un morphisme de groupes est injectif si et seulement si son noyau est réduit au neutre.
- Dans un anneau, la formule du binôme n'est valable que pour deux éléments qui commutent.

- Les inversibles d'un anneau forment un groupe ; un anneau intègre n'a pas de diviseur de zéro.
- Un sous-anneau contient 1 et est stable par différence et produit ; un morphisme d'anneaux vérifie $f(1) = 1$.
- Un corps est un anneau commutatif où tout élément non nul est inversible ; tout corps est intègre.

Questions fréquentes sur groupes, anneaux et corps

Quelle est la différence entre un anneau intègre et un corps ?

Un corps est un anneau commutatif non nul où tout élément non nul est inversible, alors qu'un anneau intègre demande seulement l'absence de diviseurs de zéro. Tout corps est intègre, mais la réciproque est fausse : $\mathbb{Z}$ est intègre sans être un corps, car 2 n'y a pas d'inverse. En revanche, un anneau intègre fini est toujours un corps.

Comment montrer rapidement qu'une partie est un sous-groupe ?

On vérifie que la partie est incluse dans le groupe, qu'elle contient le neutre, puis que xy^{-1} lui appartient pour tous x, y de la partie. En notation additive, on contrôle $x - y$. Une autre méthode très efficace consiste à reconnaître la partie comme le noyau ou l'image d'un morphisme.

Pourquoi le noyau suffit-il pour prouver l'injectivité d'un morphisme ?

Si $f(x) = f(y)$, alors $f(xy^{-1})$ est le neutre, donc xy^{-1} appartient au noyau. Lorsque le noyau est réduit au neutre, on obtient $x = y$. Cette propriété est propre aux morphismes et ne vaut pas pour une application quelconque.

Quand peut-on utiliser la formule du binôme dans un anneau ?

Uniquement lorsque les deux éléments commutent, c'est-à-dire lorsque $ab = ba$. C'est toujours le cas dans un anneau commutatif comme $\mathbb{Z}$ ou $\mathbb{C}$, ou si l'un des deux est un multiple de 1 . Pour des matrices qui ne commutent pas, $(A + B)^2$ vaut $A^2 + AB + BA + B^2$ et la formule tombe en défaut.

Pour aller plus loin en maths sup

- Les énoncés : [exercices de maths sup sur groupes, anneaux et corps](#)
- À maîtriser avant : [Logique, ensembles, applications et relations](#), [Nombres complexes et exponentielle complexe](#)
- Chapitre précédent : [Arithmétique dans l'ensemble des entiers relatifs](#)
- Chapitre suivant : [Calcul matriciel et systèmes linéaires](#)
- Tester vos connaissances : [QCM de maths sup par chapitre](#)
- Le sommaire : [tous les chapitres de maths sup](#) et les [chapitres de maths spé](#)