Chapitre VIII

Groupes, anneaux et corps

0.⁻ Lois de composition interne

a) C'est quoi ?

Définition VIII.1. Soit E un ensemble non vide. On appelle **loi de composition interne** (LCI) sur E toute application $\star : E \times E \to E$.

➠ **Exemple VIII.1.** Nous en avons déjà rencontré un certain nombre ; par exemple

$$\begin{aligned} + : \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (m, n) &\mapsto m + n \,, \end{aligned}$$

$$\begin{aligned} - : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (m, n) &\mapsto m - n \end{aligned}$$

ou

$$\begin{aligned} \circ : \mathbb{R}^{\mathbb{R}} \times \mathbb{R}^{\mathbb{R}} &\to \mathbb{R}^{\mathbb{R}} \\ (f, g) &\mapsto f \circ g \,. \end{aligned}$$

Il en existe d'autres, moins évidentes : l'intersection et la réunion d'ensembles, ainsi que la différence ensembliste, sont des LCI sur $\mathscr{P}(E)$.

Notation. Si $\star$ est une LCI sur E et $x, y \in E$, nous noterons $\star(x, y)$ "$x \star y$" ; cette convention s'appelle la **notation infixée** (par opposition à la notation préfixée $\star(x, y)$ et à la notation postfixée $(x, y)\star$).

✌ **Remarque VIII.1.** Dans le cas de certaines LCI (la multiplication vient à l'esprit), nous n'écrirons parfois même pas l'opérateur : $x \times y$ deviendra xy.

Définition VIII.2. Une partie A d'un ensemble E muni d'une LCI $\star$ est dite **stable par** $\star$ si :

$$\forall x, y \in A,\ x \star y \in A \,.$$

➠ **Exemple VIII.2.** $\mathbb{N}$ est une partie de $\mathbb{Z}$ stable par addition et multiplication.

b) Propriétés remarquables

Dans ce paragraphe, nous listons certaines propriétés intéressantes pouvant être possédées par une loi de composition interne $\star$ que nous supposerons fixée sur un ensemble arbitraire E.

◇ Associativité

Définition VIII.3. La LCI $\star$ est dite **associative** si :

$$\forall x, y, z \in E,\ (x \star y) \star z = x \star (y \star z)\ .$$

✌ **Remarque VIII.2.** Lorsque $\star$ est associative, on peut écrire des choses du style "$x \star y \star z$" sans ambiguïté.

➠ **Exemple VIII.3.**
- Nous avons vu que les opérations $+, \times, \circ$ étaient systématiquement associatives sur les ensembles *ad–hoc*.
- La soustration n'est pas associative : $(2-3)-1 = -2 \neq 2-(3-1) = 0$. Cela signifie qu'il est logiquement insensé d'écrire des choses comme "$-2-3-1$" sans avoir préalablement décidé d'un sens prioritaire dans les opérations.
- De même, la division n'est pas associative.
- La réunion et l'intersection ensemblistes sont associatives, mais pas la différence.

◇ Élément neutre

Définition VIII.4. On dit que $e \in E$ est un **élément neutre** pour $\star$ si :

$$\forall x \in E,\ x \star e = e \star x = x\ .$$

➠ **Exemple VIII.4.**
- Dans les sous–ensembles de $\mathbb{C}$ appropriés, 1 est le neutre pour la multiplication et 0 le neutre pour l'addition.
- Dans E^E, l'application id_E est un élément neutre pour la composition.
- Dans $\mathscr{P}(E)$, $\emptyset$ est neutre pour la réunion et E est neutre pour l'intersection.
- L'ensemble $2\mathbb{Z} = \{2k \,|\, k \in \mathbb{Z}\}$ n'admet pas d'élément neutre pour la multiplication.

Proposition VIII.1. Un élément neutre, si il existe, est unique.

Démonstration. Soient $e, e' \in E$ deux éléments neutres pour $\star$. Alors, comme e est neutre, $e \star e' = e'$, et comme e' est neutre, $e \star e' = e$, donc $e = e'$. □

✌ **Remarque VIII.3.** Un élément $\tau \in E$ tel que $\forall x \in E,\ \tau \star x = x \star \tau = \tau$ est appelé **élément absorbant**. Penser à 0 et à la multiplication.

◇ Inversibles

Supposons dans ce paragraphe que la loi de composition interne $\star$ soit **associative** et admette un élément neutre, que nous noterons e.

Définition VIII.5. Un élément $x \in E$ est dit **inversible** si :

$$\exists\, y \in E,\ x \star y = y \star x = e\ .$$

Proposition VIII.2. Il y a unicité de l'inverse lorsqu'il existe.

Démonstration. Soit $x \in E$ d'inverse(s) y et z. Alors, comme $x \star y = e$, $z \star (x \star y) = z$ *i.e* $(z \star x) \star y = z$. Or $z \star x = e$ donc *in fine* $y = z$. □

Corollaire VIII.2.a. Soit $x \in E$ un élément inversible. Alors $(x^{-1})^{-1} = x$.

Notation. y est appelé **inverse de** x et noté x^{-1}. De plus :
- si $\star$ est l'addition, y sera noté $-x$;
- si $\star$ est la multiplication sur un sous–ensemble de $\mathbb{C}$, y sera noté $\dfrac{1}{x}$.

➠ **Exemple VIII.5.**
- Pour l'addition sur $\mathbb{R}$, $2^{-1} = -2$.
- Pour la multiplication sur ce même ensemble, $2^{-1} = \dfrac{1}{2}$

✖ **Attention :** il convient d'être extrêmement vigilant quant à la LCI considérée, et à rendre cette dernière limpide pour le correcteur au concours ou en exercices.

Qui sont les inversibles des LCI classiques ?
- pour l'addition sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$: tout le monde ;
- pour la multiplication sur $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$: tout le monde sauf 0 ;
- pour la composition sur E^E : les bijections ;
- pour la réunion sur $\mathscr{P}(E)$: uniquement $\emptyset$;
- pour l'intersection sur $\mathscr{P}(E)$: uniquement E.

Proposition VIII.3 (Simplification)**.** Soit $x, y, z \in E$ tels que x soit inversible. Alors :

(i) $(x \star y = x \star z) \Rightarrow (y = z)$;

(ii) $(y \star x = z \star x) \Rightarrow (y = z)$.

Démonstration. Il suffit de faire le produit (du bon côté et au sens de $\star$) par x^{-1} et d'utiliser l'associativité pour simplifier les égalités. □

✖ **Attention :** on ne peut simplifier **que** par un élément inversible. En effet, $0 \times 2 = 0 \times 1$ et pourtant $1 \neq 2$. Plus subtil : si on pose $f : x \mapsto x^2$, $g : x \mapsto \sqrt{|x|}$ et $h : x \mapsto -\sqrt{|x|}$ sur $\mathbb{R}$, on a $f \circ g = f \circ h$ et $g \neq h$.

Proposition VIII.4. Soient $x, y \in E$ deux éléments inversibles. Alors $x \star y$ est inversible et :

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

Démonstration. Vérifier que cet inverse convient et conclure par unicité. □

◇ Distributivité

Définition VIII.6. Soit Δ une LCE sur E ; on dit que $\star$ **est distributive par rapport à** Δ si on a, pour tous $x, y, z \in E$:

$$x \star (y \Delta Z) = (x \star y) \Delta (x \star z)$$

et

$$(y \Delta z) \star x = (y \star x) \Delta (z \star x) .$$

Exemple VIII.6.

- La multiplication est distributive par rapport à l'addition sur les sous–ensembles de $\mathbb{C}$.
- L'intersection et la réunion sont mutuellement distributives sur $\mathscr{P}(E)$.

◇ Commutativité

Définition VIII.7. La LCE $\star$ est dite **commutative** si :

$$\forall x, y \in E,\ x \star y = y \star x .$$

✌ **Remarque VIII.4.** Certaines des propriétés précédentes sont plus simples à énoncer dans le cas commutatif.

Exemple VIII.7.

- La multiplication et l'addition le sont sur les sous–ensembles de $\mathbb{C}$, mais pas la soustraction ou la division.
- L'intersection et la réunion le sont sur $\mathscr{P}(E)$, mais pas la différence ensembliste.

1.⁻ Groupes

a) C'est quoi ?

Définition VIII.8. Soit G un ensemble muni d'une LCI $\star$. On dit que le couple $(G, \star)$ est un **groupe** si :

(A) la loi $\star$ est associative ;

(N) la loi $\star$ admet un élément neutre, noté e_G ;

(I) tous les éléments de G sont inversibles pour $\star$.

Si de plus la loi $\star$ est commutative, on parle de **groupe abélien** (du mathématicien norvégien Niels Henrik Abel, 1802—1829) ou commutatif.

Notation. Dans le cas général, nous utiliserons la notation multiplicative xy pour $x \star y$ afin d'alléger les énoncés des propositions lorsque cela sera pertinent. Nous réserverons la notation additive $x + y$ au cas des groupes abéliens.

✌ **Remarque VIII.5.** Un groupe est nécessairement non vide car il contient au moins son élément neutre.

➠ **Exemple VIII.8.**
- si e est neutre pour $\star$, $(\{e\}, \star)$ est un groupe, appelé **groupe trivial** ;
- $(\mathbb{Z}, +)$ est un groupe abélien, mais pas $(\mathbb{N}, +)$ (mise en défaut de la propriété (I)) ;
- $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes, abélien mais pas $(\mathbb{R}, \times)$ (même problème) ;
- $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes abéliens ;
- $(\mathbb{Q}_+^*, \times)$ et $(\mathbb{R}_+^*, \times)$ sont des groupes abéliens ;
- si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $(\mathbb{K}^{\mathbb{N}}, +)$ est un groupe abélien ;
- $(\mathfrak{S}_E, \circ)$ est un groupe, non abélien pour tout ensemble E ayant au moins 3 éléments (*cf. infra*).

La proposition suivante, dont la démonstration est laissée en exercice à notre lecteur favori (ainsi qu'aux autres, par souci d'équité) fournit pléthore de nouveaux exemples de groupes qui nous serons fort utiles dans le chapitre XVIII.

Proposition/définition VIII.9. Soit $(G, \star)$ et (H, Δ) deux groupes. Alors le produit cartésien $G \times H$ est un groupe, appelé **groupe produit**, pour la loi

$$((x, y), (x', y')) \mapsto (x \star x', y \Delta y') .$$

Ce groupe est abélien si et seulement si G et H le sont.

➠ **Exemple VIII.9.** Les ensembles $\mathbb{R}^n$ et $\mathbb{C}^n$ (pour $n \geq 1$) sont des groupes pour l'addition terme à terme.

✍ **Exercice VIII.1.** Soient $K = \{e, a, b, c\}$ un ensemble à quatre éléments ; démontrer que la LCI suivante définit une loi de groupe abélien sur K, que l'on appelle

alors **groupe de Klein** (Felix, 1849—1925, mathématicien allemand).

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

◇ **Un exemple fondamental : le groupe des permutations.**

Soit $n \geq 1$; on appelle **groupe des permutations de** $[\![1, n]\!]$ l'ensemble (aussi noté S_n)

$$\mathfrak{S}_n = \mathfrak{S}_{[\![1,n]\!]}$$

muni de la composition. Il s'agit d'un groupe non abélien dont les éléments sont les applications associant à chaque entier de $[\![1, n]\!]$ un autre tel nombre de façon bijective.

➠ **Exemple VIII.10.**
- $\mathfrak{S}_1 = \{\mathrm{id}_{[\![1,n]\!]}\}$ est le groupe trivial ;
- $\mathfrak{S}_2 = \{\mathrm{id}_{[\![1,n]\!]}, \sigma\}$, avec σ l'application permutant 1 et 2 ;
- $\mathfrak{S}_3$ possède 6 éléments : lesquels ?

Un élément $\sigma \in \mathfrak{S}_n$ peut être construit de la façon suivante : on dispose de n choix pour l'image de 1, puis (une fois celui–ci fixé), de $n-1$ choix pour l'image de 2, $n-2$ choix pour l'image de 3, etc. On en déduit que $\mathfrak{S}_n$ possède exactement $n!$ éléments.

✍ **Exercice VIII.2.** Déterminer $\mathfrak{S}_4$.

b) Puissances

Définition VIII.10. Soit G un groupe de neutre e. On définit, pour $x \in G$ et $n \in \mathbb{Z}$ l'élément **puissance** n**–ième de** x comme suit :
- $x^0 = e$;
- si $n \in \mathbb{N}$, $x^{n+1} = x^n x$;
- si $n < 0$, $x^n = (x^{-1})^{-n}$.

➠ **Exemple VIII.11.**
- sur $(\mathbb{C}^*, \times)$, cela correspond aux puissances usuelles ;
- sur $(\mathbb{C}, +)$, pour $x \in \mathbb{C}$ et $n \geq 1$, $x^n = \underbrace{x + \ldots + x}_{n \text{ fois}} = nx$. On en déduit aisément que **les puissances additives sont les multiples**. Attention ici aux notations et à leur potentiel de confusion.
- sur $\mathfrak{S}_n$, passer une permutation à la puissance $n \in \mathbb{N}^*$ revient à la composer n fois avec elle–même.

Proposition VIII.5. Soit G un groupe et soient $x \in G$ et $n, m \in \mathbb{Z}$. Alors :

(i) $x^{n+m} = x^n x^m = x^m x^n$;

(ii) $(x^n)^m) = x^{nm}$.

✌ **Remarque VIII.6.** Ce résultat, comme tous ceux de ce paragraphe, peut se reformuler en notation additive (traditionnellement utilisée dans le cas abélien uniquement) :

(i) $(n+m)x = nx + mx$;

(ii) $m(nx) = (mn)x$.

Proposition VIII.6. Soit G un groupe et soient $x, y \in G$ tels que $xy = yx$. Alors, pour tous $m, n \in \mathbb{Z}$:

$$x^n y^m = y^m x^n \ .$$

De plus :

$$(xy)^n = x^n y^n = y^n x^n \ .$$

Démonstration. Ce résultat et le précédent se démontrent par récurrence en distinguant les cas d'exposants positifs et négatifs. □

c) Sous–groupes

Définition VIII.11. Soit $(G, \star)$ un groupe. On appelle **sous–groupe** de G tout ensemble H tel que :

— $H \subset G$;

— $(H, \star)$ est un groupe.

➠ **Exemple VIII.12.**

— $(\mathbb{Q}, +)$ est un sous–groupe de $(\mathbb{R}, +)$;

— $\mathfrak{S}_3$ est un sous–groupe de $\mathfrak{S}_3$.

Proposition VIII.7. Soit $(G, \star)$ un groupe et H un sous–groupe de G. Alors :

(i) $e_H = e_G$;

(ii) si $x \in H$ alors son inverse est le même dans H et dans G.

Démonstration.

(i) Remarquons que $e_H \star e_H = e_H$ dans H donc dans G. Ainsi, toujours dans G, $e_H = e_H \star e_H^{-1}$ et donc $e_H = e_G$.

(ii) Notons y l'inverse de x dans G et z son inverse dans H. Alors, en posant $e = e_H = e_G$ (*cf.* (i)) on a :

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

et donc

$$y \star x \star z = z \star x \star z$$

ce qui entraîne que $y = z$ car $x \star z = e$.

□

Proposition VIII.8 (Caractérisation des sous–groupes)**.** Soit G un groupe de neutre e et soit $H \subset G$. Alors :

$$H \text{ est un sous–groupe de } G \iff \begin{cases} H \neq \emptyset \\ \forall x, y \in H,\ xy \in H \\ \forall x \in H,\ x^{-1} \in H \end{cases} .$$

✌ **Remarque VIII.7.** Les deux derniers points de la caractérisation peuvent être remplacés par :

$$\forall x, y \in H,\ xy^{-1} \in H .$$

➠ **Exemple VIII.13.** Cette caractérisation permet de démontrer, en utilisant des résultats vus dans le chapitre précédents, que :
- $\mathbb{U}$ est un sous–groupe de $(\mathbb{C}^*, \times)$;
- pour $n \in \mathbb{N}^*$, $\mathbb{U}_n$ est un sous–groupe de $\mathbb{U}$;
- pour $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nk \,|\, k \in \mathbb{Z}\}$ est un sous–groupe de $(\mathbb{Z}, +)$.
- $\mathbb{R}_+^*$ est un sous–groupe de $(\mathbb{R}^*, \times)$, qui est lui–même un sous–groupe de $\mathbb{C}^*$.

✍ **Exercice VIII.3.** Soit $n \geq 1$; on pose

$$H_n = \{\sigma \in \mathfrak{S}_n \,|\, \sigma(n) = n\} .$$

Démontrer que H_n est un sous–groupe de $(\mathfrak{S}_n, \circ)$.

➥ **Correction :** *H_n est non vide car il contient* $\mathrm{id}_{[\![1,n]\!]}$*. De même, il est clair que la composée et l'inverse de deux éléments de H_n sont dans H_n, d'où le résultat (composer par σ^{-1} dans $\sigma(n) = n$).*

Corollaire VIII.8.a. L'intersection de deux sous–groupes d'un même groupe en est un sous–groupe.

Démonstration. Soient H et K deux sous–groupes d'un groupe G de neutre e. Alors :
- $e \in H \cap K$ donc cet ensemble est non vide ;
- si $x, y \in H \cap K$, alors $xy^{-1} \in H$ et $xy^{-1} \in K$ car $x, y \in H$ et $x, y \in K$ respectivement.

D'où le résultat. □

✖ **Attention :** la réunion de deux sous–groupes n'est pas un sous groupe : en effet, $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ et pourtant $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

d) Morphismes de groupes

Définition VIII.12. Soit $(G, \star)$ et (H, Δ) deux groupes. On appelle **morphisme de groupes** de G vers H toute application $f : G \to H$ telle que :

$$\forall x, y \in G,\ f(x \star y) = f(x) \Delta f(y) .$$

➠ **Exemple VIII.14.** La encore nous en avons déjà croisés quelques–un :
— $\exp : (\mathbb{R}, +) \to (\mathbb{R}_+^*, \times)$;
— $\ln : (\mathbb{R}_+^*, \times) \to (\mathbb{R}, +)$;
—

$$\begin{aligned} \varphi : (\mathbb{R}, +) &\to (\mathbb{U}, \times) \\ \theta &\mapsto e^{i\theta} \quad . \end{aligned}$$

Proposition VIII.9. Soit G, H deux groupes et $f : G \to H$ un morphisme de groupes. Alors :
(i) $f(e_G) = e_H$;
(ii) si $x \in G$, $f(x^{-1}) = f(x)^{-1}$;
(iii) si $x \in G$ et $n \in \mathbb{Z}$, $f(x^n) = f(x)^n$.

Démonstration.
(i) Il suffit de remarquer que $f(e_G) = f(e_G \cdot e_G) = f(e_G)f(e_G)$ et de simplifier.
(ii) Soit $x \in G$; alors :

$$f(x)f(x^{-1}) = f(x \cdot x^{-1}) = f(e_G) = e_H$$

d'où le résultat.
(iii) À démontrer par récurrence en distinguant les cas d'exposants positifs et négatifs.

□

Vocabulaire. Soit G, H deux groupes. Un morphisme de groupes $f : G \to H$ est appelé...
— ...**isomorphisme** s'il est bijectif ;
— ...**endomorphisme** si $G = H$;
— ...**automorphisme** si il est bijectif et que $G = H$.

Proposition VIII.10. L'inverse d'un morphisme de groupes bijectif est un morphisme de groupes.

Démonstration. Soit $f : (G, \star) \to (H, \Delta)$ un tel morphisme et soient $h, h' \in H$. En posant $g = f^{-1}(h)$ et $g' = f^{-1}(h')$ on a :

$$\begin{aligned} f^{-1}(h \Delta h') &= f^{-1}(f(g) \Delta f(g')) \\ &= f^{-1}(f(g \star g') \\ &= g \star g' \\ &= f^{-1}(h) \star f^{-1}(h') \end{aligned}$$

d'où le résultat. □

Proposition VIII.11. Soient G, H deux groupes, G' (resp. H') un sous–groupe de G (resp. H) et $f : G \to H$ un morphisme de groupes. Alors :

(i) $f(G')$ est un sous–groupe de H ;

(ii) $f^{-1}(H')$ est un sous–groupe de G.

Démonstration. Notons $\star$ (resp. Δ) la LCI sur G (resp. H) associée à sa structure de groupe.

(i) Il est clair que $f(G') \subset H$; de plus $e_G \in G'$ (car G' est un sous–groupe de G) ce qui entraîne que $e_H = f(e_G) \in f(G')$. Soient ensuite $X, Y \in f(G')$; alors il existe $x, y \in G'$ tels que $X = f(x)$ et $Y = f(y)$ donc :

$$\begin{aligned} X\Delta Y &= f(x)\Delta f(y) \\ &= f(\underbrace{x \star y}_{\in G'}) \in f(G') \,. \end{aligned}$$

(ii) On sait que $f^{-1}(H') \subset G$; de plus $e_H \in F'$ ce qui entraîne que $e_G = f^{-1}(e_H) \in f^{-1}(H')$. Soient ensuite $x, y \in f^{-1}(H')$; alors :

$$f(x \star y) = f(x)\Delta f(y) \in H'$$

et donc $x \star y \in f^{-1}(H')$.

□

➠ **Exemple VIII.15.** L'ensemble $\ln^{-1}(\mathbb{Z})$ est un sous–groupe de $\mathbb{R}^*$ (égal à $\exp(\mathbb{Z})$ par ailleurs).

Ce résultat nous permet, outre les exemples de sous–groupes qu'il fournit, de définir deux ensembles essentiels à toute étude de morphisme qui se respecte, à savoir son image et son noyau.

Proposition/définition VIII.13. Soient G, H deux groupes et soit $f : G \to H$ un morphisme de groupes. On appelle :

— **noyau** de f l'ensemble

$$\mathrm{Ker}(f) = \{x \in G \,|\, f(x) = e_H\} \,;$$

— **image** de f l'ensemble

$$\mathrm{Im}(f) = \{f(x) \,|\, x \in G\} \,.$$

Ces deux ensembles sont de plus des sous–groupes de G et H respectivement.

Démonstration. Il suffit de remarquer que $\mathrm{Ker}(f) = f^{-1}(\{e_H\})$ et $\mathrm{Im}(f) = f(G)$.

□

➠ **Exemple VIII.16.**

— Le noyau de l'application ln est réduit à $\{1\}$;

— le noyau de l'application

$$\begin{aligned}\phi : (\mathbb{R}, +) &\to (\mathbb{C}^*, \times)\\ \theta &\mapsto e^{i\theta} \quad .\end{aligned}$$

est égal à $2\pi\mathbb{Z} = \{2k\pi \,|\, k \in \mathbb{Z}\}$ et son image est égale à $\mathbb{U}$.

L'utilité première de ces deux sous–groupe est, à notre niveau, de fournir une CNS d'injectivité et de surjectivité fort sympathique.

Proposition VIII.12. Soient G, H deux groupes et soit $f : G \to H$ un morphisme de groupes. Alors :

(i) f est injective $\Leftrightarrow \mathrm{Ker}(f) = \{e_G\}$;

(ii) f est surjective $\Leftrightarrow \mathrm{Im}(f) = H$.

Démonstration. Notons $\star$ (resp. Δ) la LCI sur G (resp. H) associée à sa structure de groupe.

(i) **(⇒)** Immédiat car $f(e_G) = e_H$.

(⇔) Supposons que $\mathrm{Ker}(f) = \{e_G\}$ et fixons $x, x' \in G$ tels que $f(x) = f(x')$. Alors, $f(x \star x'^{-1}) = f(x)\Delta f(x')^{-1} = e_H$ et donc $x \star x'^{-1} \in \mathrm{Ker}(f)$, ce qui entraîne que $x = x'$.

(ii) Il s'agit de la définition de surjectivité.

□

2.⁻ Anneaux, corps

a) Qu'est-ce ?

Définition VIII.14. Un ensemble $\mathbb{A}$ muni de **deux** LCI distinctes $+$ et $\times$ est appelé **anneau** (unitaire) si :

(G) $(\mathbb{A}, +)$ est un groupe **abélien** ;

(A) $\times$ est associative ;

(D) $\times$ est distributive par rapport à $+$;

(N) la loi $\times$ admet un élément neutre.

Si de plus la loi $\times$ est commutative, on parle d'**anneau commutatif**.

Notation. L'élément neutre pour $+$ est noté $0_{\mathbb{A}}$ (ou simplement 0), le neutre pour $\times$ est noté $1_{\mathbb{A}}$ (ou 1).

✌ **Remarque VIII.8.** Soit $(\mathbb{A}, +, \times)$ est un anneau.

— pour tout $x \in \mathbb{A}$,

$$0 \cdot x = (1 - 1)x = x - x = 0$$

; 0 est donc absorbant pour la loi $\times$.

— Si $a \in \mathbb{A}$ et $n \in \mathbb{A}$, on peut définir le **multiple** na comme sa puissance additive. On ne peut toute fois pas définir la puissance a^n pour $n < 0$ lorsque a n'est pas inversible.

➠ **Exemple VIII.17.**
— les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des anneaux pour l'addition et la multiplication standards ;
— si E est un ensemble et $\mathbb{A}$ un anneau, $\mathbb{A}^E$ est un anneau pour les opérations terme à terme (*cf.* chapitre II) ;
— le seul anneau dans lequel $0 = 1$ est l'**anneau nul** $\{0\}$. En effet, si x est un élément d'un tel anneau alors $0 \cdot x = 0 = 1 \cdot x = x$.

b) Identités remarquables

Soit $(\mathbb{A}, +, \times)$ un anneau ; alors la notation suivante a un sens, pour $a_1, \dots, a_h \in \mathbb{A}$:

$$\sum_{k=1}^{n} a_k = a_1 + \ldots + a_n \, .$$

De plus, si $\mathbb{A}$ est commutatif, on pose :

$$\prod_{k=1}^{n} a_k = a_1 \times \ldots \times a_n \, .$$

On généralise ces notations au cas de familles **finies** indexées par un ensemble quelconque. De plus, toutes les propriétés et techniques élémentaires (scission, linéarité de la somme, changement d'indice) vues dans le chapitre II se généralisent au cas d'un anneau.

Proposition VIII.13. Soit $\mathbb{A}$ un anneau et $a, b \in \mathbb{A}$ tels que $ab = ba$. Alors, pour tout $n \in \mathbb{N}$:

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

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

Démonstration. Comme a et b commutent, on peut recopier les démonstrations des propositions II.11 et II.10. □

Corollaire VIII.13.a. Soit $\mathbb{A}$ un anneau et $a \in \mathbb{A}$. Alors, pour tout $n \in \mathbb{N}^*$:

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

Démonstration. Appliquer le (ii) de la proposition VIII.13 à $b = 1$. □

✌ **Remarque VIII.9.** On peut voir dans cette formule un analogue de la somme des termes d'une suite géométrique vue dans le chapitre II.

c) Sous–anneaux, groupe des inversibles

Définition VIII.15. Soit $\mathbb{A}$ un anneau et soit $\mathbb{B} \subset \mathbb{A}$. On dit que $\mathbb{B}$ est un **sous–anneau** de $\mathbb{A}$ si :
— $\mathbb{B}$ est un anneau ;
— $1_{\mathbb{B}} = 1_{\mathbb{A}}$.

➠ **Exemple VIII.18.** $\mathbb{Z}$ est un sous–anneau de $\mathbb{R}$, qui est un sous–anneau de $\mathbb{C}$.

Comme dans le cas des sous–groupes, on dispose d'une caractérisation (analogue à a la proposition VIII.8) des sous–anneaux : si $\mathbb{A}$ est un anneau et $\mathbb{B} \subset \mathbb{A}$, alors

$$\mathbb{B} \text{ est un sous–anneau de } \mathbb{A} \iff \begin{cases} 1 \in \mathbb{B} \\ \forall x, y \in \mathbb{B},\ x - y \in \mathbb{B} \\ \forall x, y \in \mathbb{B},\ xy \in \mathbb{B} \end{cases}.$$

➠ **Exemple VIII.19.** À l'aide de cette caractérisation, il est aisé de montrer que l'ensemble des **entiers de Gauss**

$$\mathbb{Z}[i] = \{a + ib \,|\, a, b \in \mathbb{Z}\}$$

est un sous–anneau de $\mathbb{C}$.

Définition VIII.16. Soit $\mathbb{A}$ un anneau ; on dit que $x \in \mathbb{A}$ est **inversible** si il l'est pour la loi $\times$.

Notation. On note $\mathbb{A}^\times$ l'ensemble des inversibles de l'anneau $\mathbb{A}$.

✌ **Remarque VIII.10.** Remarquons que $(\mathbb{A}^\times, \times)$ est naturellement un groupe.

➠ **Exemple VIII.20.**
— $\mathbb{Z}^\times = \{-1, 1\}$;
— $\mathbb{C}^\times = \mathbb{C}^*$;
— $\{0\}^\times = \{0\}$ (et oui...).

d) Morphismes d'anneaux

Définition VIII.17. Soient $\mathbb{A}$ et $\mathbb{B}$ deux anneaux. On dit qu'une application $f : \mathbb{A} \to \mathbb{B}$ est un **morphisme d'anneaux** si :
— $f(1_{\mathbb{A}}) = 1_{\mathbb{B}}$;
—
$$\forall x, y \in \mathbb{A}, \quad f(x + y) = f(x) + f(y) \quad \text{et} \quad f(xy) = f(x)f(y).$$

✌ **Remarque VIII.11.** Un morphisme d'anneau est donc un morphisme de groupes entre $(\mathbb{A}, +)$ et $(\mathbb{B}, +)$ et hérite donc de toutes les propriétés **additives** que cela implique.

Vocabulaire. Soit $\mathbb{A}, \mathbb{B}$ deux anneaux. Un morphisme d'anneaux $f : \mathbb{A} \to \mathbb{B}$ est appelé...
- ...**isomorphisme** s'il est bijectif ;
- ...**endomorphisme** si $\mathbb{A} = \mathbb{B}$;
- ...**automorphisme** si il est bijectif et que $\mathbb{A} = \mathbb{B}$.

➠ **Exemple VIII.21.**
- $x \mapsto x$ est un morphisme d'anneaux de $\mathbb{Z}$ vers $\mathbb{Q}$;
- $z \mapsto \overline{z}$ est un endomorphisme de $(\mathbb{C}, +, \times)$;
- $k \mapsto 2k$ n'est **pas** un endomorphisme de $(\mathbb{Z}, +, \times)$ alors qu'il s'agit d'un endomorphisme du **groupe** $(\mathbb{Z}, +)$.

✌ **Remarque VIII.12.** De la même façon que pour les morphismes de groupes, on peut définir le noyau et l'image d'un morphisme d'anneaux (qui seront ceux du morphisme de groupes sous–jacent) et obtenir une CNS d'injectivité et de surjectivité.

e) Anneaux intègres, corps

Définition VIII.18. Un anneau $\mathbb{A}$ est dit **intègre** si
- il est commutatif ;
- il est différent de l'anneau nul ;
- pour tous $x, y, z \in \mathbb{A}$ tels que $z \neq 0$ on a :

$$(xz = yz) \Rightarrow (x = y)\,.$$

✌ **Remarque VIII.13.** Un anneau intègre est donc un anneau dans lequel on peut simplifier par un élément non nul dans un produit. Ceci signifie, par contraposée, qu'il existe dans tout anneau non intègre deux éléments a et b **non nuls** tels que $ab = 0$. De tels éléments sont appelés **diviseurs de zéro**.

➠ **Exemple VIII.22.**
- les anneaux $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont intègres ;
- l'anneau $\mathbb{R}^{\mathbb{R}}$ n'est pas intègre : penser au produit $\mathbb{1}_{\mathbb{R}_+^*} \times \mathbb{1}_{\mathbb{R}_-}$.

Définition VIII.19. Un anneau est appelé **corps** si :
- il est commutatif ;
- il est différent de l'anneau nul ;
- tous ses éléments non nuls sont inversibles pour la multiplication.

➠ **Exemple VIII.23.** $\mathbb{R}$ et $\mathbb{C}$ sont des corps, mais pas $\mathbb{Z}$, $\mathbb{D}$ ou $\mathbb{R}^{\mathbb{R}}$.

✌ **Remarque VIII.14.**

— un corps est automatiquement un anneau intègre ;
— si $\mathbb{K}$ est un corps, alors $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$.

Vocabulaire. Un sous–anneau d'un corps qui est lui–même un corps est appelé **sous–corps** du corps de base.

✌ **Remarque VIII.15.** On a naturellement la caractérisation suivante : si $\mathbb{K}$ est un corps et $\mathbb{L} \subset \mathbb{K}$, alors

$$\mathbb{L} \text{ est un sous–corps de } \mathbb{K} \iff \begin{cases} 1 \in \mathbb{L} \\ \forall x, y \in \mathbb{L},\ x - y \in \mathbb{L} \\ \forall (x, y) \in \mathbb{L} \times \mathbb{L}^*,\ xy^{-1} \in \mathbb{L} \end{cases}.$$

✍ **Exercice VIII.4.** Démontrer que $\mathbb{Q}[j] = \{a + bj + cj^2 \mid a, b, c \in \mathbb{Q}\}$ est un corps.