Groupes et anneaux

Table des matières

1 La structure de groupe

1.1 Définitions

Définition. Soit G un ensemble muni d'une loi interne notée "$\times$". On suppose que G est un monoïde dont l'élément neutre sera notée 1_G.
On dit que $(G, \times)$ est un groupe si et seulement si tout élément de G possède un symétrique pour la loi interne, c'est-à-dire si et seulement si, pour tout $x \in G$, il existe $y \in G$ tel que $x \times y = y \times x = 1_G$.
Dans ce cas, pour tout $x \in G$, le symétrique de x est unique, il est noté x^{-1}.

Démonstration.
Soit $x \in G$. Soit y et z deux symétriques de x. Alors
$y = y \times e = y \times (x \times z) = (y \times x) \times z = e \times z = z$. □

Remarque. On aurait très bien pu continuer à noter Δ la loi de G et e son élément neutre, avec Δ et e substituable par n'importe quel autre symbole, mais l'usage restreint la notation de la loi interne d'un groupe à seulement deux notations : la notation multiplicative, que l'on vient de voir, et la notation additive, réservée aux groupes commutatifs. Ainsi, $(G, +)$ est la notation générique d'un groupe commutatif. Son élément neutre est alors noté 0 ou 0_G et le symétrique de x est alors noté $-x$.

Remarque. En notation multiplicative, le produit de deux éléments x et y est souvent noté xy au lieu de $x.y$ ou $x \times y$, c'est-à-dire que la loi utilisée est notée par ... rien du tout.
En résumé, $(G, .)$ est un groupe si et seulement si G est un ensemble muni d'une loi interne "." vérifiant

- l'associativité : pour tout $x, y, z \in G$, $x(yz) = (xy)z$;
- l'existence d'un élément neutre 1_G : pour tout $x \in G$, $1_G.x = x.1_G = x$:
- l'existence, pour tout $x \in G$, d'un symétrique x^{-1} tel que : $xx^{-1} = x^{-1}x = 1_G$.

Exemple.

- $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ sont des groupes commutatifs.
- $(\mathbb{Q}^*, \times)$ est un groupe commutatif mais $(\mathbb{Z}^*, \times)$ n'est pas un groupe.
- $(\mathbb{R}^*, .)$ et $(\mathbb{C}^*, .)$ sont des groupes commutatifs.
- L'ensemble des matrices carrées de taille n à coefficients réels $\mathcal{M}_n(\mathbb{R})$ muni de son addition est un groupe commutatif.
- L'ensemble des matrices inversibles de $\mathcal{M}_n(\mathbb{R})$ muni de la multiplication matricielle est un groupe **non commutatif**.

Définition. Si $(G, .)$ est un groupe fini, le cardinal de G est appelé l'***ordre*** de G.

Définition. Pour un groupe, "commutatif" et "abélien" sont synonymes.

1.2 Calculs dans un groupe

Propriété. Soit $(G,.)$ un groupe et $a \in G$. Alors a est régulier (ou simplifiable) à gauche et à droite, c'est-à-dire que

$$\forall x, y \in G,\ \ [ax = ay \Longrightarrow x = y] \text{ et } [xa = ya \Longrightarrow x = y].$$

Notation.
◇ Dans un groupe $(G,.)$, en notation multiplicative donc, si $x_1, \ldots, x_n \in G$, on note $x_1 \times \cdots \times x_n = \prod_{i=1}^{n} x_i$, en convenant que ce produit vaut 1_G lorsque $n = 0$ (produit vide).
Il est préférable de limiter l'usage de cette notation au cas où les éléments $x_1, \ldots, x_n$ commutent deux à deux (c'est-à-dire lorsque, pour tout $i, j \in \{1, \ldots, n\}$, $x_i x_j = x_j x_i$).
◇ Dans un groupe abélien $(G,+)$, en notation additive donc, si $x_1, \ldots, x_n \in G$, on note $x_1 + \cdots + x_n = \sum_{i=1}^{n} x_i$, en convenant que cette somme vaut 0_G lorsque $n = 0$ (somme vide).

Propriété. Soit $(G,.)$ un groupe et $(x,y) \in G^2$. Alors

$$(x^{-1})^{-1} = x \quad \text{et } (xy)^{-1} = y^{-1}x^{-1}.$$

Démonstration.
$x \times x^{-1} = x^{-1} \times x = 1_G$, donc le symétrique de x^{-1} est bien x.
$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x.1_G.x^{-1} = 1_G$ et de même, $(y^{-1}x^{-1})xy = 1_G$, donc le symétrique de xy est $y^{-1}x^{-1}$. □

Remarque. Par récurrence, on en déduit que si $n \in \mathbb{N}$ et $x_1, \ldots, x_n \in G$, où $(G,.)$ est un groupe, alors $(x_1 \times \cdots \times x_n)^{-1} = x_n^{-1} \times \cdots \times x_1^{-1}$.

Définition et propriété : Soit $(G,+)$ un groupe abélien.
Alors, pour tout $x, y \in G$, on note (1) : $x - y \stackrel{\Delta}{=} x + (-y)$.
On dispose alors des règles suivantes :

$$\forall x, y, z \in G,\ \ x - (y + z) = x - y - z \quad \text{et} \quad x - (y - z) = x - y + z.$$

Démonstration.
Soit $x, y, z \in G$.

$$\begin{aligned} x - (y+z) &= x + [-(y+z)] \text{ (d'après (1))} \\ &= x + [(-y) + (-z)] \text{ (c'est la propriété précédente en notation additive)} \\ &= (x + (-y)) + (-z) \text{ (d'après l'associativité)} \\ &= (x - y) - z \text{ (en utilisant deux fois (1))} \\ &= x - y - z \text{ (car c'est bien ainsi qu'il faut lire } x - y - z). \end{aligned}$$

et

$$\begin{aligned} x-(y-z) &= x+[-(y+(-z))] \text{ (d'après (1) utilisée 2 fois)} \\ &= x+[(-y)+(-(-z))] \text{ (c'est la propriété prédente en notation additive)} \\ &= x+[(-y)+z] \text{ (c'est la propriété prédente en notation additive)} \\ &= (x+(-y))+z \text{ (d'après l'associativité)} \\ &= (x-y)+z \text{ (d'après (1)).} \end{aligned}$$

□

1.3 Construction de groupes

1.3.1 Groupe produit

Définition. Soient $n \in \mathbb{N}^*$ et $((G_i, ._i))_{i\in\{1,\dots,n\}}$ une famille de n groupes.
Le ***groupe produit*** de cette famille de groupes est le couple $(G, .)$, où $G = G_1 \times \cdots \times G_n$ et où la loi "." est définie par :

$$\forall x = (x_1, \dots, x_n) \in G \ \ \forall y = (y_1, \dots, y_n) \in G \ \ x.y = (x_1 ._1 y_1, \dots, x_n ._n y_n).$$

Démonstration.
Il faut montrer que $(G, .)$ est un groupe.
La loi "." définie ci-dessus est bien une application de G^2 dans G.
Associativité. Soient $x = (x_1, \dots, x_n) \in G$, $y = (y_1, \dots, y_n) \in G$
et $z = (z_1, \dots, z_n) \in G$.
$x.(y.z) = (x_1 ._1 (y_1 ._1 z_1), \dots, x_n ._n (y_n ._n z_n)) = ((x_1 ._1 y_1) ._1 z_1, \dots, (x_n ._n y_n) ._n z_n)$, car les lois $._i$ des groupes G_i sont associatives.
Ainsi $x.(y.z) = (x.y).z$.

Elément neutre. Notons 1_i l'élément neutre de G_i.
Pour tout $x = (x_1, \dots, x_n) \in G$,
$x.(1_1, \dots, 1_n) = (x_1 ._1 1_1, \dots, x_n ._n 1_n) = (x_1, \dots, x_n) = x$
et $(1_1, \dots, 1_n).x = (1_1 ._1 x_1, \dots, 1_n ._n x_n) = (x_1, \dots, x_n) = x$, donc l'élément $1 = (1_1, \dots, 1_n)$ de G est un élément neutre.

Elément symétrique. Soit $x = (x_1, \dots, x_n) \in G$. Notons $y = (x_1^{-1}, \dots, x_n^{-1})$.
$x.y = (x_1 ._1 x_1^{-1}, \dots, x_n ._n x_n^{-1}) = (1_1, \dots, 1_n) = 1$, et de même $y.x = 1$. □

Remarque. Avec les notations précédentes, G est abélien si et seulement si, pour tout $i \in \mathbb{N}_n$, G_i est abélien.

Démonstration.
Supposons que G est abélien. Soit $i \in \mathbb{N}_n$.
Soit $(x_i, y_i) \in G_i^2$. Pour tout $j \in \mathbb{N}_n$ avec $j \neq i$, posons $x_j = y_j = 1_j$.
Notons $x = (x_1, \dots, x_n)$ et $y = (y_1, \dots, y_n)$.
G est abélien, donc $x.y = y.x$. En prenant la $i^{\text{ème}}$ composante de cette égalité, on obtient : $x_i ._i y_i = y_i ._i x_i$.
Ainsi G_i est commutatif, pour tout $i \in \mathbb{N}_n$.
La réciproque est simple à établir. □

Exemple. En prenant, pour tout $i \in \mathbb{N}_n$, $(G_i, ._i) = (\mathbb{R}, +)$, on obtient $G = (\mathbb{R}^n, +)$. C'est la structure canonique de $\mathbb{R}^n$ en tant que groupe abélien.

Exemple. Le produit du groupe $(\mathbb{R}, +)$ avec le groupe $(\mathbb{R}_+^*, .)$ donne le groupe $\mathbb{R} \times \mathbb{R}_+^*$ muni de la loi Δ définie par :
pour tous $(x, y), (x', y') \in \mathbb{R} \times \mathbb{R}_+^*$, $(x, y)\Delta(x', y') = (x + x', yy')$.

1.3.2 Produit fonctionnel

Définition. Soit $(G, .)$ un groupe et A un ensemble quelconque. Pour tout $f, g \in G^A$, on convient que $f.g$ est l'application de A dans G définie par :

$$\forall a \in A, \ \ (f.g)(a) = f(a).g(a).$$

Alors G^A est un groupe, dont l'élément neutre est l'application constante $a \longmapsto 1_G$ et pour lequel le symétrique de $f \in G^A$ est $f^{-1} : \begin{array}{ccc} A & \longrightarrow & G \\ a & \longmapsto & [f(a)]^{-1} \end{array}$.

Démonstration.
Exercice. □

Remarque. La notation f^{-1} désigne ici le symétrique de f pour cette loi de groupe. Mais rien n'interdit de supposer que f est bijective. Dans ce cas, f^{-1} peut également désigner la bijection réciproque de f, ce qui n'est pas du tout le même objet, donc il y a un vrai conflit de notation. Dans ces conditions, ou bien le contexte permet de savoir de quoi on parle, ou bien il faut adopter localement d'autres notations.

Exemple. $\mathcal{F}(\mathbb{R}, \mathbb{R})$ est un groupe abélien en convenant que, pour tout $f, g \in \mathbb{R}^{\mathbb{R}}$, pour tout $x \in \mathbb{R}$, $(f + g)(x) = f(x) + g(x)$. L'élément neutre est l'application identiquement nulle.

1.3.3 Le groupe symétrique

Propriété. Si E est un ensemble, alors l'ensemble des bijections de E dans E est un groupe pour la loi de composition. On l'appelle le groupe symétrique de E et on le note $\mathcal{S}(E)$. Son élément neutre est l'application identité Id_E et, pour tout $f \in \mathcal{S}(E)$, le symétrique de f est la bijection réciproque de f, dont la notation f^{-1} est en cohérence avec cette propriété.

Démonstration.
On sait qu'une composée de bijections est une bijection, donc il s'agit d'une loi interne et on sait déjà qu'elle est associative. Id_E est neutre pour la composition et, pour tout $f \in \mathcal{S}(E)$, $f \circ f^{-1} = f^{-1} \circ f = Id_E$, donc f^{-1} est bien le symétrique de f. □

Remarque. Lorsque G est un groupe, on dispose donc du groupe G^G de toutes les applications de G dans G, muni de la loi $(f.g)(x) = f(x).g(x)$, et du groupe $\mathcal{S}(G)$ des bijections de G dans G, muni de la loi de composition. Il importe de ne pas les confondre.

Remarque. La notation x^{-1} pour désigner le symétrique d'un élément x dans un groupe en notation multiplicative est donc compabible avec la notation f^{-1} pour désigner la bijection réciproque d'une bijection f. Cette dernière est cependant parfois délicate à utiliser : l'expression $\exp^{-1}(x)$ représente a priori $\ln(x)$, puisque ln est la bijection réciproque de la fonction exponentielle (vue comme une fonction allant de $\mathbb{R}$ dans $\mathbb{R}_+^*$). Mais dans certains contextes, il n'est pas impossible que $\exp^{-1}(x)$ représente plutôt $(\exp(x))^{-1}$, c'est-à-dire l'inverse du réel e^x dans le groupe $(\mathbb{R}^*, \times)$, auquel cas il s'agirait de e^{-x}.

Exemple. Prenons $E = \{1, 2, 3\}$. Notons f la bijection sur E qui échange 1 et 2 et laisse 3 invariant. De même, notons g la bijection sur E qui échange 1 et 3 et laisse 2 invariant.
Alors $g \circ f$ envoie 1,2 et 3 respectivement sur 2,3, et 1 et $f \circ g$ envoie 1,2 et 3 respectivement sur 3,1 et 2, donc $g \circ f \neq f \circ g$.
Ceci prouve qu'en général $\mathcal{S}(E)$ n'est pas commutatif. En adaptant cet exemple, il est aisé de montrer que $\mathcal{S}(E)$ est commutatif si et seulement si E possède moins de 2 éléments.

1.4 Sous-groupes

1.4.1 Définition

Propriété et définition : Soit $(G, .)$ un groupe et H une partie de G.
H est un groupe pour la restriction de la loi "." à $H \times H$, avec le même élément neutre 1_G si et seulement si
- $H \neq \emptyset$;
- $\forall (x, y) \in H^2$, $xy \in H$ (stabilité du produit) ;
- $\forall x \in H$, $x^{-1} \in H$ (stabilité du symétrique).

Cet ensemble de conditions est équivalent à
- $H \neq \emptyset$;
- $\forall (x, y) \in H^2$, $xy^{-1} \in H$.

Dans ce cas, on dit que H est un ***sous-groupe*** de G.

Démonstration.
$\diamond$ Supposons que H est un groupe pour la restriction de la loi "." à $H \times H$, avec le même élément neutre 1_G.
Pour que la loi utilisée soit bien une loi interne, il est nécessaire que, pour tout $x, y \in H$, $xy \in H$.
Pour que H admette 1_G comme élément neutre, il est nécessaire que $1_G \in H$, donc que H soit non vide.
Soit $x \in H$. H étant un sous-groupe, x admet un symétrique y dans H :
$xy = yx = 1_G$. Ainsi, y est également symétrique de x dans G, donc par unicité du symétrique, $y = x^{-1}$. Ainsi, $x^{-1} \in H$.

On a montré que si H est un groupe pour la restriction de la loi "." à $H \times H$, avec le même élément neutre 1_G, alors H vérifie (C) : $\begin{cases} H \neq \emptyset \\ \forall x, y \in H,\ \ xy \in H \\ \forall x \in H,\ \ x^{-1} \in H \end{cases}$.

$\diamond$ Réciproquement, supposons que (C) est vérifiée et montrons que H est un groupe pour la restriction de la loi "." à $H \times H$, avec le même élément neutre 1_G.
D'après (C), la loi "." est bien une loi interne. De plus, G étant un groupe, pour tout $x, y, z \in G$, $x(yz) = (xy)z$, donc a fortiori, c'est vrai lorsque $x, y, z \in H$.
$H \neq \emptyset$, donc il existe $x_0 \in H$. D'après (C), $x_0^{-1} \in H$, puis $x_0.x_0^{-1} = 1_G \in H$.
De plus, pour tout $x \in H$, $x.1_G = 1_G.x = x$, donc 1_G est élément neutre de $(H, .)$.
Enfin, pour tout $x \in H$, $x^{-1} \in H$ et $xx^{-1} = x^{-1}x = 1_G$, donc x possède un symétrique dans $(H, .)$.

$\diamond$ Il reste à montrer que (C) est équivalente à (C') : $\begin{cases} H \neq \emptyset \\ \forall x, y \in H,\ \ xy^{-1} \in H \end{cases}$.
Supposons (C). Soit $x, y \in H$. Alors $y^{-1} \in H$, donc xy^{-1} est le produit de deux éléments de H, donc d'après (C), $xy^{-1} \in H$. Ainsi, $(C) \Longrightarrow (C')$.
Supposons (C'). Il existe $x_0 \in H$, donc d'après (C'), $1_G = x_0x_0^{-1} \in H$.
Soit $x \in H$. $x^{-1} = 1_G.x^{-1} \in H$ d'après (C').
Soit $x, y \in H$. $y^{-1} \in H$, donc d'après (C'), $xy = x.(y^{-1})^{-1} \in H$. Ainsi, $(C') \Longrightarrow (C)$.
□

Remarque. La démonstration précédente prouve en particulier que si H est un sous-groupe de $(G, .)$, alors $1_G \in H$.

En notation additive, cette propriété devient :
Propriété et définition : Soit $(G, +)$ un groupe abélien et H une partie de G.
H est un groupe pour la restriction de la loi "+" à $H \times H$, avec le même élément neutre 0_G si et seulement si
- $H \neq \emptyset$;
- $\forall (x, y) \in H^2\ ,\ \ x + y \in H$ (stabilité de la somme) ;
- $\forall x \in H\ ,\ \ -x \in H$ (stabilité du symétrique).

Cet ensemble de conditions est équivalent à
- $H \neq \emptyset$;
- $\forall (x, y) \in H^2\ ,\ \ x - y \in H$.

Dans ce cas, on dit que H est un ***sous-groupe*** de G.

Remarque. Pour montrer qu'un ensemble G muni d'une certaine loi est un groupe, il est pratique lorsque c'est possible, de trouver un ensemble G', que l'on sait déjà être un groupe, qui contient G. Il suffit alors de montrer que G est un sous-groupe de G', ce qui évite d'avoir à prouver l'associativité.

Exemple.
- $\mathbb{Z}$ est un sous-groupe additif de $\mathbb{R}$, lequel est un sous-groupe additif de $\mathbb{C}$.
- L'ensemble des matrices diagonales est un sous-groupe additif de $\mathcal{M}_n(\mathbb{R})$.
- L'ensemble des applications polynomiales de $\mathbb{R}$ dans $\mathbb{R}$ est un sous-groupe de $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

— $\mathbb{R}^*$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
— L'ensembles des matrices diagonales à coefficients diagonaux non nuls est un sous-groupe commutatif pour la multiplication de l'ensemble des matrices inversibles de $(\mathcal{M}_n(\mathbb{R}), \times)$.
— Soit $n \in \mathbb{N}^*$. Notons $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité dans $\mathbb{C}$: $\mathbb{U}_n = \{e^{2i\pi\frac{k}{n}}/k \in \{0, \dots, n-1\}\}$. C'est un sous-groupe de $(\mathbb{C}^*, \times)$.

Exemple. Si $(G, .)$ est un groupe, $\{1_G\}$ est le plus petit sous-groupe de G (au sens de l'inclusion) et G est le plus grand sous-groupe de G.

Propriété de transitivité : Un sous-groupe d'un sous-groupe d'un groupe G est un sous-groupe de G.

Démonstration.
Exercice. □

1.4.2 Groupe engendré par une partie

Propriété. Soit I un ensemble non vide, éventuellement infini. Soient G un groupe et $(H_i)_{i\in I}$ une famille de sous-groupes de G. Alors l'intersection $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

Démonstration.
Notons $H = \bigcap_{i\in I} H_i$. Pour tout $i \in I$, $1_G \in H_i$, donc $1_G \in H$.
Soit $x, y \in H$. Soit $i \in I$: $x, y \in H_i$ et H_i est un sous-groupe, donc $xy^{-1} \in H_i$. C'est vrai pour tout $i \in I$, donc $xy^{-1} \in H$.
Ceci démontre que H est bien un sous-groupe de G. □

Exercice. Qu'en est-t-il avec la réunion ?

Définition. Soit G un groupe et A une partie de G.
Notons $\mathcal{S}$ l'ensemble des sous-groupes de G contenant A. $\mathcal{S}$ est non vide car $G \in \mathcal{S}$.
Alors $\bigcap_{H\in\mathcal{S}} H$ est un sous-groupe de G contenant A et, par construction, c'est le plus petit sous-groupe contenant A. On le note $Gr(A)$.

Exemple. $Gr(\emptyset) = \{1\}$, puisque $\{1\}$ est le plus petit sous-groupe de G.
Si H est un sous-groupe d'un groupe G, $Gr(H) = H$.

Propriété. Soient $(G, .)$ un groupe et A et B deux parties de G.

$$\text{Si } A \subset B, \text{ alors } Gr(A) \subset Gr(B).$$

Démonstration.
$Gr(B)$ est un groupe contenant A, donc il est plus grand (au sens de l'inclusion) que $Gr(A)$. □

Propriété. Soit $(G,.)$ un groupe et A une partie de G. Notons $A^{-1} = \{a^{-1}/a \in A\}$.
Alors $Gr(A) = \left\{ \prod_{i=1}^{n} a_i / n \in \mathbb{N},\ \forall i \in \{1,\dots,n\},\ a_i \in A \cup A^{-1} \right\}$.

Démonstration.
Posons $H = \left\{ \prod_{i=1}^{n} a_i / n \in \mathbb{N},\ \forall i \in \{1,\dots,n\},\ a_i \in A \cup A^{-1} \right\}$. H est non vide car, avec $n = 0$, $\prod_{i=1}^{n} a_i$ désigne le produit vide, qui vaut 1_G.
H est de plus clairement stable pour le produit et le passage au symétrique, donc H est un sous-groupe de G qui contient clairement A.
Soit K un sous-groupe contenant A. Alors par stabilité par passage au symétrique, $A^{-1} \subset K$, puis par récurrence sur $n \in \mathbb{N}$, on montre que, pour tout $a_1,\dots,a_n \in A \cup A^{-1}$, $\prod_{i=1}^{n} a_i \in K$. Ainsi, $H \subset K$, ce qui montre que H est le plus petit sous-groupe de G contenant A. □

Définition. Si H et K sont deux sous-groupes d'un groupe abélien $(G,+)$, on note $H + K = \{h + k/(h,k) \in H \times K\}$. C'est le groupe engendré par $H \cup K$.

Définition. Soit G un groupe et A une partie de G.
A est une ***partie génératrice*** de G si et seulement si $Gr(A) = G$.

Exemple.
◇ $[0,1]$ engendre $(\mathbb{R},+)$. En effet, si G est un sous-groupe de $(\mathbb{R},+)$ contenant $[0,1]$, alors $1 \in G$, donc $\mathbb{Z} \subset G$. De plus, pour tout $x \in \mathbb{R}$, $x = \lfloor x \rfloor + f$ où $f \in [0,1[$, donc $x \in G$.
◇ Groupe des entiers de Gauss : $G = \{n + im/(n,m) \in \mathbb{Z}^2\}$ est un sous-groupe de $(\mathbb{C},+)$. Il est engendré par $\{1,i\}$.

1.4.3 Puissances d'un élément d'un groupe

Définition. Soit $(G,.)$ un groupe et $a \in G$. On définit la famille $(a^n)_{n\in\mathbb{Z}}$ par les relations suivantes :
- Initialisation : $a^0 = 1_G$ (encore le produit vide) ;
- Itération : pour tout $n \in \mathbb{N}$, $a^{n+1} = a.a^n$ (donc pour $n \in \mathbb{N}^*$, $a^n = \underbrace{a \times \cdots \times a}_{n fois}$) ;
- Symétrique : pour tout $n \in \mathbb{Z}$ avec $n < 0$, $a^n = (a^{-n})^{-1}$.

Propriété. Soit $(G,.)$ un groupe et a un élément de G. On dispose des formules suivantes :

$$\forall n,m \in \mathbb{Z},\ a^n a^m = a^{n+m},$$
$$\forall n,m \in \mathbb{Z},\ (a^n)^m = a^{nm}.$$

Démonstration.

1. On montre d'abord par récurrence que, pour tout $n \in \mathbb{N}$, $R(n)$: $a^n a = a^{n+1}$.
   En effet, pour $n = 0$, $a^0 a = a = a^{n+1}$.
   De plus, pour $n \geq 0$, si $R(n)$ est vrai, alors $a^{n+1}a = (aa^n)a$, d'après la partie "itération" de la définition de la famille $(a^m)_{m\in\mathbb{Z}}$, donc $a^{n+1}a = a(a^n a) = aa^{n+1}$ d'après $R(n)$, puis $a^{n+1}a = a^{n+2}$ grâce à nouveau à la partie "itération" de la définition. Ceci prouve $R(n+1)$.
   D'après le principe de récurrence, on a montré que, pour tout $n \in \mathbb{N}$, $a^n a = a^{n+1}$.
2. En remplaçant a par a^{-1} dans la définition précédente, on dispose également de la famille $((a^{-1})^n)_{n\in\mathbb{Z}}$.
   Toujours par récurrence, montrons que, pour tout $n \in \mathbb{N}$, $S(n)$: $a^{-n} = (a^{-1})^n$.
   Pour $n = 0$, $a^{-0} = a^0 = 1_G = (a^{-1})^0$.
   Pour $n \geq 0$, supposons que $S(n)$ est vrai et montrons $S(n+1)$.
   D'après la propriété 1, $a^{n+1} = a^n a$ et d'après la définition de la famille $((a^{-1})^n)_{n\in\mathbb{Z}}$, $(a^{-1})^{n+1} = a^{-1}(a^{-1})^n$, donc
   $a^{n+1}(a^{-1})^{n+1} = (a^n a)(a^{-1}(a^{-1})^n) = a^n(aa^{-1})(a^{-1})^n = a^n(a^{-1})^n = a^n a^{-n}$ d'après $S(n)$, or d'après la définition de la famille $(a_n)_{n\in\mathbb{Z}}$, a^{-n} est le symétrique de a^n, donc $a^{n+1}(a^{-1})^{n+1} = 1_G$. Ainsi, le symétrique de a^{n+1} est égal à $(a^{-1})^{n+1}$: on a prouvé $S(n+1)$.
3. On en déduit que, pour tout $n \in \mathbb{Z}$, $a^n a = a^{n+1}$.
   En effet, lorsque $n < 0$, en posant $m = -n \in \mathbb{N}^*$, d'après la propriété 2,
   $a^n a = (a^{-1})^m a$, donc d'après la propriété 1 appliquée à a^{-1},
   $a^n a = [(a^{-1})^{m-1}a^{-1}]a = (a^{-1})^{m-1}$. Alors, d'après la propriété 2,
   $a^n a = a^{-(m-1)} = a^{n+1}$.
4. On en déduit aussi que, pour tout $n \in \mathbb{Z}$, $a^{-n} = (a^{-1})^n$.
   En effet, lorsque $n < 0$, posons $m = -n \in \mathbb{N}$ et appliquons la propriété 2 à a^{-1}.
   Ainsi, $(a^{-1})^n = (a^{-1})^{-m} = ([a^{-1}]^{-1})^m = a^m = a^{-n}$.
5. Pour $m \in \mathbb{N}$, notons $T(m)$ l'assertion : $\forall n \in \mathbb{Z},\ a^n a^m = a^{n+m}$.
   Pour $m = 0$, on vérifie $T(0)$.
   Pour $m \geq 0$, supposons $T(m)$. Soit $n \in \mathbb{Z}$.
   $$\begin{aligned} a^n a^{m+1} &= a^n(aa^m) \text{ (d'après la définiton de } (a_k)_{k\in\mathbb{Z}}) \\ &= a^{n+1}a^m \text{ (d'après la propriété 3)} \\ &= a^{(n+1)+m} \text{ (d'après } T(m)). \end{aligned}$$
   Ceci prouve $T(m+1)$.
6. Soit maintenant $m, n \in \mathbb{Z}$. Nous avons montré que $a^n a^m = a^{n+m}$ lorsque $m \in \mathbb{N}$.
   Si $m < 0$, posons $k = -m$: d'après la propriété 4, $a^n a^m = (a^{-1})^{-n}(a^{-1})^k$, donc d'après la propriété 5 appliquée à a^{-1}, $a^n a^m = (a^{-1})^{-n+k}$, puis à nouveau d'après la propriété 4, $a^n a^m = a^{-(-n+k)} = a^{n+m}$.
   Ainsi, pour tout $m, n \in \mathbb{Z}$, on a $a^n a^m = a^{n+m}$.

7. Pour $m \in \mathbb{N}$, notons $U(m)$ l'assertion : $\forall n \in \mathbb{Z},\ (a^n)^m = a^{nm}$.
   Pour $m = 0$, on vérifie $U(0)$.
   Pour $m \geq 0$, supposons $U(m)$. Soit $n \in \mathbb{Z}$.
   $$\begin{aligned}(a^n)^{m+1} &= a^n(a^n)^m \text{ (d'après la définition de la famille } (a^n)_{k\in\mathbb{Z}})\\ &= a^n a^{nm} \text{ (d'après } U(m))\\ &= a^{n+nm} \text{ (d'après la propriété 6)}\\ &= a^{n(m+1)}.\end{aligned}$$
8. Il reste à montrer que $(a^n)^m = a^{nm}$ lorsque $n \in \mathbb{Z}$ et $m < 0$. Pour cela, posons $k = -m \in \mathbb{N}$. $(a^n)^m = (a^n)^{-k}$. D'après la propriété 4 utilisée en remplaçant a par a^n, on a $(a^n)^{-k} = [(a^n)^{-1}]^k$, puis toujours d'après la propriété 4, $(a^n)^{-k} = (a^{-n})^k$, mais $k \in \mathbb{N}$, donc on peut utiliser la propriété 7.
   Ainsi, $(a^n)^m = (a^{-n})^k = a^{(-n)k} = a^{nm}$.

□

Propriété. Soit $(G, .)$ un groupe et $a, b \in G$.

$$\forall a, b \in G,\ (ab = ba) \Longrightarrow [\forall n \in \mathbb{Z},\ (ab)^n = a^n b^n].$$

Lorsque $ab = ba$, on dit que a et b commutent.

Démonstration.
Soit $a, b \in G$ tels que $ab = ba$.
On peut montrer par récurrence sur n que, pour tout $n \in \mathbb{N}$, a^n commute avec b.
Alors, si l'on suppose que $(ab)^n = a^n b^n$,
$(ab)^{n+1} = ab(ab)^n = ab(a^n b^n) = a(ba^n)b^n = a(a^n b)b^n = a^{n+1}b^{n+1}$.
Ainsi, par récurrence, on a montré que, pour tout $n \in \mathbb{N}$, (1) : $(ab)^n = a^n b^n$.
Si maintenant $n < 0$, posons $k = -n \in \mathbb{N}$.
Alors $(ab)^n = (ba)^{-k} = ([ba]^{-1})^k = (a^{-1}b^{-1})^k$.
Or $ab = ba$, donc $(ab)^{-1} = (ba)^{-1}$, ce qui s'écrit aussi $b^{-1}a^{-1} = a^{-1}b^{-1}$. Ainsi, a^{-1} et b^{-1} commutent, donc on peut appliquer l'assertion (1) en remplaçant le couple (a, b) par (a^{-1}, b^{-1}). Ainsi, $(a^{-1}b^{-1})^k = (a^{-1})^k(b^{-1})^k = a^{-k}b^{-k}$. On a donc prouvé que $(ab)^n = a^n b^n$. □

Remarque. Il ressort de cette démonstration que lorsque a et b sont deux éléments d'un groupe $(G, .)$, si a et b commutent, alors pour tout $n, k \in \mathbb{Z}$, a^n et b^k commutent également entre eux.
En effet, on a vu que si a et b commutent, alors a^n et b commutent avec $n \in \mathbb{N}$, et que a^{-1} et b commutent, donc a^n et b commutent pour tout $n \in \mathbb{Z}$. Alors, en remplaçant dans cette dernière affirmation le couple (a, b) par le couple (b, a^k) (où $k \in \mathbb{Z}$), on en déduit que b^n et a^k commutent pour tout $n, k \in \mathbb{Z}$.

En notation additive, dans le cadre des groupes commutatifs, ce qui précède devient :

Définition. soit $(G, +)$ un groupe commutatif et a un élément de G. On **définit** la famille $(na)_{n\in\mathbb{Z}}$ par les relations suivantes :
— Initialisation : $0.a = 0_G$;

— Itération : pour tout $n \in \mathbb{N}$, $(n+1).a = a + (n.a)$
(donc pour $n \in \mathbb{N}^*$, $n.a = \underbrace{a + \cdots + a}_{n fois}$) ;
— Symétrique : pour tout $n \in \mathbb{Z}$ avec $n < 0$, $n.a = -((-n).a)$.

Remarque. Ces formules définissent en fait une nouvelle loi, mais ce n'est plus une loi interne, car elle associe un élément de G à un couple (n, a) de $\mathbb{Z} \times G$. C'est ce qu'on appelle une loi externe dont $\mathbb{Z}$ est le domaine des opérateurs.
En particulier, la dernière ligne, lorsque $n = -1$, définit $(-1).a$ en posant $(-1).a = -a$, c'est-à-dire que $(-1).a$ est le symétrique de a.
Il est important de comprendre que cette loi $\begin{array}{ccc} \mathbb{Z} \times G & \longrightarrow & G \\ (n, a) & \longmapsto & n.a \end{array}$ est définie à partir de la loi interne "+" du groupe G.

Propriété. Soit $(G, +)$ un groupe abélien et $a, b \in G$. On dispose des formules suivantes :

$$\begin{array}{l} \forall n, m \in \mathbb{Z},\ \ (n.a) + (m.a) = (n+m).a, \\ \forall n, m \in \mathbb{Z},\ \ m.(n.a) = (nm).a, \\ \forall n \in \mathbb{Z},\ \ n.(a+b) = (na) + (nb). \end{array}$$

Propriété. Soit $(G, +)$ un groupe abélien et A une partie de G.
Alors $Gr(A) = \left\{ \sum_{a \in A} n_a.a / (n_a)_{a \in A} \in \mathbb{Z}^{(A)} \right\}$.
On rappelle que $\mathbb{Z}^{(A)}$ désigne l'ensemble des familles presque nulles d'entiers relatifs, dont les éléments sont tous nuls sauf pour un nombre fini d'entre eux.

Démonstration.
◇ Soit $(n_a)_{a \in A}, (p_a)_{a \in A} \in \mathbb{Z}^{(A)}$. Alors, par définition, $\sum_{a \in A} n_a.a = \sum_{\substack{a \in A \\ n_a \neq 0_G}} n_a.a$, donc c'est une somme d'un nombre fini de termes. De plus, pour toute partie finie B contenant $\{a \in A / n_a \neq 0\}$, on a encore $\sum_{a \in A} n_a.a = \sum_{a \in B} n_a.a$. Aussi peut-on écrire

$$\begin{aligned} \sum_{a \in A} n_a.a + \sum_{a \in A} p_a a &= \sum_{\substack{a \in A \\ n_a \neq 0}} n_a.a + \sum_{\substack{a \in A \\ p_a \neq 0}} p_a.a \\ &= \sum_{\substack{a \in A \\ (n_a \neq 0) \vee (p_a \neq 0)}} n_a.a + \sum_{\substack{a \in A \\ (n_a \neq 0) \vee (p_a \neq 0)}} p_a.a \\ &= \sum_{\substack{a \in A \\ (n_a \neq 0) \vee (p_a \neq 0)}} (n_a.a + p_a.a) \\ &= \sum_{\substack{a \in A \\ (n_a \neq 0) \vee (p_a \neq 0)}} (n_a + p_a).a \\ &= \sum_{a \in A} (n_a + p_a).a. \end{aligned}$$

Ce calcul utilise la notion de somme finie qui est fondée sur un principe de commutativité généralisée. Ce dernier sera effectivement démontré page 20.
◇ On pose $H = \left\{\sum_{a\in A} n_a.a/(n_a)_{a\in A} \in \mathbb{Z}^{(A)}\right\}$. On vérifie que H est non vide (même lorsque $A = \emptyset$ car la somme vide vaut 0_G par convention), qu'il est stable pour l'addition (d'après le point précédent) et pour le passage à l'opposé, donc H est un sous-groupe de G. Il contient clairement A.
De plus, si K est un sous-groupe de G contenant A, pour tout $a \in A$, K étant stable pour l'addition, pour tout $n \in \mathbb{N}$, $na \in K$, puis K étant stable par passage à l'opposé, pour tout $n \in \mathbb{Z}$, $na \in K$. Enfin, K étant stable pour l'addition, tout élément de H appartient à K. Ainsi, $H \subset K$, ce qui prouve que H est bien le plus petit sous-groupe de G contenant A. □

Remarque. En particulier, lorsque $A = \{x_1, \ldots, x_p\}$ est une partie finie de G, $Gr(\{x_1, \ldots, x_p\}) = \left\{\sum_{i=1}^{p} n_i x_i/(n_i)_{1\leq i\leq p} \in \mathbb{Z}^p\right\}$.

1.4.4 Groupe monogène

Propriété. Soit $(G, .)$ un groupe et $a \in G$. Alors le groupe engendré par la partie $\{a\}$ est $Gr(\{a\}) = \{a^n/n \in \mathbb{Z}\}$. On le note plus simplement $Gr(a)$.

Propriété. Soit $(G, +)$ un groupe abélien et $a \in G$. Alors le groupe engendré par la partie $\{a\}$ est $Gr(\{a\}) = \{na/n \in \mathbb{Z}\}$. On le note $Gr(a)$. On peut donc écrire $Gr(a) = \mathbb{Z}.a$.

Propriété. Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, où $n \in \mathbb{N}$.

Démonstration.
◇ Soit $n \in \mathbb{N}$. $n\mathbb{Z}$ est non vide, stable pour l'addition et le passage à l'opposé, donc $n\mathbb{Z}$ est bien un sous-groupe de $\mathbb{Z}$.
◇ Soit G un sous-groupe de $(\mathbb{Z}, +)$. Si $G = \{0\}$, alors $G = 0.\mathbb{Z}$.
On peut donc supposer que $G \neq \{0\}$. Ainsi, il existe $x \in G$ avec $x \neq 0$. Alors x et $-x$ sont tous deux dans G, donc $G \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}$. Elle possède donc un minimum noté a.
$a \in G$, donc $a\mathbb{Z} = Gr(a) \subset G$.
Réciproquement, soit $k \in G$. Écrivons la division euclidienne de k par a : il existe $q, r \in \mathbb{Z}$ tels que $k = qa + r$ avec $0 \leq r < a$.
$r = k - qa \in G$, mais $0 \leq r < a = \min(G \cap \mathbb{N}^*)$, donc $r = 0$, puis $k = qa \in a\mathbb{Z}$.
Ainsi, $G = a\mathbb{Z}$. □

Définition. Soit a un élément d'un groupe G. Lorsque $Gr(a)$ est de cardinal fini, ce cardinal est appelé l'ordre de a.

Définition. On dit qu'un groupe $(G, .)$ est ***monogène*** si et seulement si il existe $a \in G$ tel que $G = Gr(a)$.

On dit alors que a est un ***générateur*** de G.

Remarque. Tout groupe monogène est abélien.

Définition. Un groupe G est dit ***cyclique*** si et seulement si G est monogène et fini.

Exemple. Soit $n \in \mathbb{N}^*$. $\mathbb{U}_n = \{e^{2i\pi\frac{k}{n}}/k \in \{0,\dots,n-1\}\} = \{(e^{\frac{2i\pi}{n}})^k/k \in \mathbb{Z}\}$ est un groupe cyclique.

Propriété. Soit $(G,.)$ un groupe, $a \in G$ et $n \in \mathbb{N}^*$.
Les propriétés suivantes sont équivalentes :
- i) $Gr(a)$ est cyclique de cardinal n.
- ii) $\{k \in \mathbb{N}^*/a^k = 1\}$ est non vide et son minimum est égal à n.
- iii) Pour tout $k \in \mathbb{Z}$, $[a^k = 1 \iff k \in n\mathbb{Z}]$.
- iv) Les éléments de $Gr(a)$ sont exactement $1, a, \dots, a^{n-1}$ et ils sont deux à deux distincts.

Dans ce cas, n est l'ordre de a et de $Gr(a)$.

Remarque. Ainsi, lorsque $Gr(a)$ est cyclique d'ordre n, les puissances de a sont $1_G, a, \dots, a^{n-1}$, puis $a^n = 1_G$, ce qui ferme le "cycle".

Démonstration.
ii)$\Longrightarrow$ iii) : On suppose ii).
Si $k \in n\mathbb{Z}$, il existe $h \in \mathbb{Z}$ tel que $k = nh$, donc $a^k = (a^n)^h = 1^h = 1$.
Réciproquement, soit $k \in \mathbb{Z}$ tel que $a^k = 1$.
Ecrivons la division euclidienne de k par n : $k = qn + r$ avec $0 \leq r < n$.
On a $a^r = a^{qn}a^r = a^k = 1$, mais $0 \leq r < n$ et $n = \min\{k \in \mathbb{N}^*/a^k = 1\}$, donc $r = 0$, puis $k = qn \in n\mathbb{Z}$.

iii)$\Longrightarrow$ iv) : On suppose iii).
Posons $H = \{1_G, a, a^2, \dots, a^{n-1}\}$. Ainsi, $H \subset Gr(a)$.
Soit $x \in Gr(a)$. Il existe $k \in \mathbb{Z}$ tel que $x = a^k$. Par division euclidienne, $k = qn + r$, où $0 \leq r < n$. Ainsi, $x = (a^n)^q.a^r = a^r \in H$.
On a donc prouvé que $Gr(a) = \{1_G, a, a^2, \dots, a^{n-1}\}$.
Soit $(h,k) \in \{0,\dots,n-1\}$ avec $h \geq k$ tel que $a^h = a^k$.
Ainsi, $a^{h-k} = 1$, donc $h - k \in n\mathbb{Z}$, mais $0 \leq h - k < n$, donc $h = k$.

iv)$\Longrightarrow$ i) : évident.

i)$\Longrightarrow$ ii) : On suppose i).
Supposons que l'application $\varphi : \begin{array}{ccc} \mathbb{N} & \longrightarrow & Gr(a) \\ k & \longmapsto & a^k \end{array}$ est injective. Alors $\varphi|^{\varphi(\mathbb{N})}$ réalise une bijection de $\mathbb{N}$ dans une partie de G. D'après le cours sur les ensembles finis, toute partie d'un ensemble fini est finie, et tout ensemble en bijection avec un ensemble fini est également fini. On en déduit ainsi, que $\mathbb{N}$ est fini, ce qui est faux. En conséquence, φ n'est pas injective.
Ainsi, il existe $(h,k) \in \mathbb{N}^2$ tel que $h < k$ et $a^h = a^k$. Alors $a^{k-h} = 1_G$ et $k - h \in \mathbb{N}^*$, donc $\{k \in \mathbb{N}^*/a^k = 1\}$ est un ensemble non vide d'entiers : il possède un minimum que l'on note p.

On sait que ii)$\Longrightarrow$ iii)$\Longrightarrow$ iv)$\Longrightarrow$ i), en remplaçant n par p, donc $Gr(a)$ est cyclique de cardinal p, ce qui montre que $p = n$. □

1.5 Morphisme de groupes

Définition. Soient (G, Δ) et (H, ∇) deux groupes.
Une application f de G dans H est un ***morphisme*** (on dit aussi un ***homomorphisme***) de groupes si et seulement si

$$\forall (x, y) \in G^2 \quad f(x \Delta y) = f(x) \nabla f(y).$$

Un ***isomorphisme*** est un morphisme bijectif.
Un ***endomorphisme*** est un morphisme de G dans lui-même.
Un ***automorphisme*** est un endomorphisme bijectif.

Exemple.

- L'application constante $x \longmapsto 1_G$ d'un groupe $(G, .)$ dans lui-même est un endomorphisme.
- Id_G est un automorphisme du groupe G.
- $\begin{array}{rccc} \ln : & (\mathbb{R}_+^*, \times) & \longrightarrow & (\mathbb{R}, +) \\ & x & \longmapsto & \ln x \end{array}$ est un isomorphisme.
- L'application $z \longmapsto |z|$ est un morphisme de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}_+^*, \times)$. Cependant ce n'est pas un morphisme de $(\mathbb{C}, +)$ dans $(\mathbb{R}, +)$.
- L'application $z \longmapsto \overline{z}$ est un automorphisme involutif sur $(\mathbb{C}, +)$ ainsi que sur $(\mathbb{C}^*, \times)$.

Définition. Soient $n \in \mathbb{N}^*$ et $((G_i, ._i))_{i \in \{1,\dots,n\}}$ une famille de n groupes. On note $(G, .)$ leur groupe produit. Soit $i \in \mathbb{N}_n$, on note $\begin{array}{rccc} p_i : & G & \longrightarrow & G_i \\ & (g_1, \dots, g_n) & \longmapsto & g_i \end{array}$.
p_i s'appelle la $i^{\text{ème}}$ ***projection***. C'est un morphisme surjectif de groupes.

Démonstration.
Soit $i \in \mathbb{N}_n$. Pour tout $x \in G_i$, $x = p_i(1_{G_1}, \dots, 1_{G_{i-1}}, x, 1_{G_{i+1}}, \dots, 1_{G_n})$, donc p_i est surjective.
Soient $x = (x_1, \dots, x_n)$ et $y = (y_1, \dots, y_n)$ deux éléments de G.
$p_i(x.y) = p_i(x_1 ._1 y_1, \dots, x_i ._i y_i, \dots, x_n ._n y_n)) = x_i ._i y_i = p_i(x) ._i p_i(y)$, donc p_i est un morphisme de groupes. □

Propriété. Si a est un élément d'un groupe $(G, .)$, alors $\begin{array}{rccc} (\mathbb{Z}, +) & \longrightarrow & (G, .) \\ n & \longmapsto & a^n \end{array}$ est un morphisme de groupes.

Propriété. Soient $(G, .)$ et $(H, .)$ deux groupes et f un morphisme de G dans H.

$$f(1_G) = 1_H$$
$$\text{et, pour tout } x \in G, \quad f(x)^{-1} = f(x^{-1}).$$

Démonstration.
$f(1_G) = f(1_G * 1_G) = f(1_G) * f(1_G)$,
donc $1_H = [f(1_G)]^{-1} f(1_G) = [f(1_G)]^{-1}.(f(1_G) * f(1_G)) = f(1_G)$.
Soit $x \in G$. $f(x).f(x^{-1}) = f(x.x^{-1}) = f(1_G) = 1_H$, donc $f(x)^{-1} = f(x^{-1})$. □

Propriété. En notation additive, si f est un morphisme entre deux groupes abéliens $(G, +)$ et $(H, +)$, alors $f(0_G) = 0_H$ et, pour tout $x \in G$, $-f(x) = f(-x)$.

Propriété. Soit φ un morphisme du groupe $(G, .)$ vers le groupe $(G', .)$.
Alors, pour tout $n \in \mathbb{N}$ et $x_1, \ldots, x_n \in G$, $\varphi\Big(\prod_{i=1}^{n} x_i\Big) = \prod_{i=1}^{n} \varphi(x_i)$.
De plus, pour tout $n \in \mathbb{Z}$ et $a \in G$, $\varphi(a^n) = \varphi(a)^n$.

Démonstration.
La première propriété se démontre par récurrence sur n.
Soit $a \in G$. En appliquant cette première propriété lorsque tous les x_i sont égaux à a, on obtient que pour tout $n \in \mathbb{N}$, $\varphi(a^n) = \varphi(a)^n$.
De plus, si $n \in \mathbb{N}$, $\varphi(a^{-n}) = \varphi((a^n)^{-1}) = \varphi(a^n)^{-1} = (\varphi(a)^n)^{-1} = \varphi(a)^{-n}$.
Ainsi, pour tout $n \in \mathbb{Z}$, $\varphi(a^n) = \varphi(a)^n$. □

Propriété. Soit φ un morphisme du groupe abélien $(G, +)$ vers le groupe abélien $(G', +)$. Alors, pour tout $n \in \mathbb{N}$ et $x_1, \ldots, x_n \in G$, $\varphi\Big(\sum_{i=1}^{n} x_i\Big) = \sum_{i=1}^{n} \varphi(x_i)$.
De plus, pour tout $n \in \mathbb{Z}$ et $a \in G$, $\varphi(na) = n\varphi(a)$.

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

Propriété. Si $f : G \longrightarrow H$ est un isomorphisme de groupes, f^{-1} est encore un isomorphisme de groupes, de H dans G.

Démonstration.
Soit $(x', y') \in H^2$. Notons $x = f^{-1}(x')$ et $y = f^{-1}(y')$.
$f(xy) = f(x)f(y) = x'.y'$, donc $f^{-1}(x').f^{-1}(y') = xy = f^{-1}(f(xy)) = f^{-1}(x'y')$. □

Propriété. Soit $(G, .)$ un groupe. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G. C'est un sous-groupe de $\mathcal{S}(G)$.

Démonstration.
$Id_G \in \mathrm{Aut}(G)$, la composée de deux automorphismes est un automorphisme et la bijection réciproque d'un automorphisme est un automorphisme, donc $\mathrm{Aut}(G)$ est bien un sous-groupe du groupe $\mathcal{S}(G)$. □

Exemple. Soit $(G, .)$ et $(H, .)$ deux groupes. On note $Hom(G, H)$ l'ensemble des homomorphismes du groupe G vers le groupe H. Lorsque H est abélien, $Hom(G, H)$ est un sous-groupe de H^G.
En effet, L'application constante $x \longmapsto 1_H$ de G dans H est un élément de $Hom(G, H)$, donc ce dernier est non vide. De plus, si $f, g \in Hom(G, H)$, pour tout $x, y \in G$, $(fg^{-1})(xy) = f(xy)[g(xy)]^{-1} = f(x)f(y)g(y)^{-1}g(x)^{-1}$

et $(fg^{-1})(x).(fg^{-1})(y) = f(x)g(x)^{-1}f(y)g(y)^{-1}$, donc lorsque H est commutatif, $fg^{-1} \in Hom(G,H)$, ce qui prouve que $Hom(G,H)$ est un sous-groupe de H^G.

Propriété. Soit φ un morphisme de groupes. Alors φ reste un morphisme si on le restreint ou si on le corestreint à des sous-groupes. Plus précisément, en supposant que φ est un morphisme du groupe G vers le groupe G', alors
pour tout sous-groupe H de G, $\varphi|_H$ est un morphisme de H vers G' et
pour tout sous-groupe H' de G', si $\forall x \in G,\ \varphi(x) \in H'$, alors $\varphi|^{H'}$ est un morphisme de G vers H'.

Définition. Soit $\varphi : G \longrightarrow G$ un endomorphisme et H un sous-groupe de G. On peut définir $\varphi|_H^H$ si et seulement si H est stable par φ, c'est-à-dire si et seulement si $[\forall x \in H,\ \varphi(x) \in H]$. Dans ce cas, $\varphi|_H^H$ est aussi un **endo**morphisme, appelé l'endomorphisme induit par φ sur H, ou plus simplement la restriction de φ à H (il y a bien sûr ambiguïté).

Propriété. Soient G et H deux groupes, G' un sous-groupe de G et H' un sous-groupe de H. Soit f un morphisme de G dans H.
Alors $f(G')$ est un sous-groupe de H et $f^{-1}(H')$ est un sous-groupe de G.

Démonstration.
$\diamond$ $G' \neq \emptyset$, donc $f(G') \neq \emptyset$.
Soit $(x',y') \in f(G')^2$. Il existe $(x,y) \in {G'}^2$ tel que $x' = f(x)$ et $y' = f(y)$.
$x'y'^{-1} = f(xy^{-1}) \in f(G')$, car, G' étant un sous-groupe, $xy^{-1} \in G'$.
$\diamond$ $f(1_G) = 1_H \in H'$, car H' est un sous-groupe, donc $1_G \in f^{-1}(H')$. Ainsi, $f^{-1}(H') \neq \emptyset$.
Soit $(x,y) \in [f^{-1}(H')]^2$. $f(xy^{-1}) = f(x)f(y)^{-1} \in H'$, car $f(x) \in H'$, $f(y) \in H'$ et H' est un sous-groupe. Ainsi, $xy^{-1} \in f^{-1}(H')$. $\square$

Définition. Soient $(G,.)$ et $(H,.)$ deux groupes, et f un morphisme de G dans H.
On appelle ***noyau*** de f le sous-groupe de G suivant :

$$\boxed{Ker(f) = f^{-1}(\{1_H\}) = \{x \in G / f(x) = 1_H\}.}$$

On appelle ***image*** de f le sous-groupe de H suivant :

$$\boxed{Im(f) = f(G) = \{f(x) / x \in G\}.}$$

Remarque. En notation additive, Si f est un morphisme dont le groupe d'arrivée $(H,+)$ est abélien, alors $Ker(f) = f^{-1}(\{0_H\}) = \{x \in G / f(x) = 0_H\}$.

Propriété. Soient $(G,.)$ et $(H,.)$ deux groupes, et f un morphisme de G dans H.

$$\begin{array}{rl} f \text{ est injective si et seulement si} & Ker(f) = \{1_G\}, \\ f \text{ est surjective si et seulement si} & Im(f) = H. \end{array}$$

Démonstration.
Supposons que f est injective. Soit $x \in Ker(f)$. Alors $f(x) = 1_H = f(1_G)$, donc $x = 1_G$. Ainsi, $Ker(f) \subset \{1_G\}$ et l'inclusion réciproque est évidente.
Réciproquement, supposons que $Ker(f) = \{1_G\}$. Soit $x, y \in G$ tels que $f(x) = f(y)$. Alors $f(xy^{-1}) = f(x)f(y)^{-1} = 1_H$, donc $xy^{-1} \in Ker(f)$, puis $xy^{-1} = 1_G$. Ainsi, $x = y$, ce qui prouve que f est injective. □

Exemple.
- Avec $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^*, \times)$, $Ker(\exp) = \{0\}$ et $Im(\exp) = \mathbb{R}_+^*$.
- Avec $\ln : (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}, +)$, $Ker(\ln) = \{1\}$ et $Im(\ln) = \mathbb{R}$.
- Avec $|.| : (\mathbb{C}^*, \times) \longrightarrow (\mathbb{C}^*, \times)$, $Ker(|.|) = \mathbb{U}$ et $Im(|.|) = \mathbb{R}_+^*$.
- Avec $\begin{array}{rccc} \varphi : & (\mathbb{R}, +) & \longrightarrow & (\mathbb{C}^*, \times) \\ & x & \longmapsto & e^{ix} \end{array}$, $Ker(\varphi) = 2\pi\mathbb{Z}$ et $Im(\varphi) = \mathbb{U}$.

Propriété. Un groupe est monogène non cyclique si et seulement si il est isomorphe à $(\mathbb{Z}, +)$.

Démonstration.
◇ Soit $(G, .)$ un groupe monogène non cyclique. Il existe $a \in G$ tel que $G = Gr(a) = \{a^n / n \in \mathbb{Z}\}$.
Notons $\begin{array}{rccc} \varphi : & \mathbb{Z} & \longrightarrow & G \\ & n & \longmapsto & a^n \end{array}$. On sait que φ est un morphisme de groupes. Il est surjectif car $G = \{a^n / n \in \mathbb{Z}\}$. S'il existait $k \in \mathbb{N}^*$ tel que $a^k = 1_G$, on a vu que G serait cyclique, donc $Ker(\varphi) = \{0\}$ et φ est injectif. Ainsi, φ réalise un isomorphisme de $\mathbb{Z}$ dans G.
◇ Réciproquement, supposons qu'il existe un isomorphisme φ de $\mathbb{Z}$ dans G. Posons $a = \varphi(1)$. Alors, pour tout $n \in \mathbb{Z}$, $\varphi(n) = \varphi(n.1) = \varphi(1)^n = a^n$, donc $G = \varphi(\mathbb{Z}) = \{a^n / n \in \mathbb{Z}\}$, ce qui prouve que G est monogène. De plus G est en bijection avec $\mathbb{Z}$, donc il est de cardinal infini. Ainsi G est bien monogène et non cyclique. □

1.6 Le groupe symétrique de degré n

Notation. Pour tout $n \in \mathbb{N}$, on pose $\mathbb{N}_n = \{k \in \mathbb{N} / 1 \leq k \leq n\}$. En particulier $\mathbb{N}_0 = \emptyset$.

Définition. Soit $n \in \mathbb{N}$. $\mathcal{S}(\mathbb{N}_n)$ s'appelle le groupe symétrique de degré n. Il est plus simplement noté $\mathcal{S}_n$. Ses éléments sont les bijections sur $\mathbb{N}_n$, que l'on appelle aussi des permutations.

Notation. Si $f \in \mathcal{S}_n$, on note $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$.

Définition. Soient $k \in \mathbb{N}_n$ et a_1, a_2 $\ldots a_k$ k éléments distincts de $\mathbb{N}_n$.
On note $(a_1\ a_2\ \ldots\ a_k)$ la permutation f telle que : $\forall i \in \{1, \ldots, k-1\}\ f(a_i) = a_{i+1}$, $f(a_k) = a_1$, les autres éléments de $\mathbb{N}_n$ étant invariants par f.
On dit que $(a_1\ \ldots\ a_k)$ est un ***cycle*** de longueur k dont le ***support*** est $\{a_1, \ldots, a_k\}$.

Démonstration.
On vérifie que le cycle $(a_k\ a_{k-1}\ \ldots\ a_1)$ est sa bijection réciproque. □

Exemple. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 4 & 2 & 5 \end{pmatrix}$ désigne la permutation σ de $\mathcal{S}_6$ telle que : $\sigma(1) = 3$, $\sigma(2) = 6$, $\sigma(3) = 1$, $\sigma(4) = 4$, $\sigma(5) = 2$ et $\sigma(6) = 5$.
1 est transformé en 3 qui est transformé en 1,
2 est transformé en 6 qui est transformé en 5, puis en 2
et 4 est transformé en lui-même,
donc $\sigma = (1\ 3) \circ (2\ 6\ 5)$.

Propriété. Soit c et c' deux cycles de $\mathcal{S}_n$ dont les supports sont disjoints.
Alors c et c' commutent.

Démonstration.
Notons $c = (a_1\ a_2\ \dots\ a_p)$ et $c' = (b_1\ b_2\ \dots\ b_q)$. En convenant de noter $a_{p+1} = a_1$ et $b_{q+1} = b_1$, on vérifie que, pour tout $\alpha \in \mathbb{N}_n$, $cc'(\alpha) = c'c(\alpha) = \begin{cases} a_{i+1} & \text{si } \alpha = a_i \\ b_{i+1} & \text{si } \alpha = b_i \\ \alpha & \text{sinon} \end{cases}$. □

Théorème. Toute permutation de $\mathcal{S}_n$ se décompose de manière unique en un produit (commutatif) de cycles dont les supports sont deux à deux disjoints.

Démonstration.
Cf DM. □

Définition. On appelle ***transposition*** tout cycle de longueur 2.
Si $a, b \in \mathbb{N}_n$ avec $a \neq b$, la transposition $(a\ b)$ échange a et b sans modifier les autres éléments de $\mathbb{N}_n$.

Propriété. Pour tout $n \in \mathbb{N}^*$, pour toute permutation σ de $\mathcal{S}_n$, il existe $k \in \mathbb{N}$ et k transpositions $\tau_1, \dots, \tau_k$ telles que $\sigma = \tau_1 \circ \dots \circ \tau_k$. Cependant une telle décomposition n'est pas unique.

Démonstration.
Notons $R(n)$ cette propriété.
Pour $n = 1$, $\mathcal{S}_1$ est le singleton contenant l'identité, qui est aussi l'élément neutre de ce groupe. Avec la convention du paragraphe précédent, l'identité s'écrit comme un produit de 0 transposition.
Pour $n \geq 1$, supposons $R(n)$. Soit $\sigma \in \mathcal{S}_{n+1}$.
Si $\sigma(n+1) \neq n+1$, on pose $s = (n+1\ \sigma(n+1)) \circ \sigma$. Ainsi, $\sigma = (n+1\ \sigma(n+1)) \circ s$.
Si $\sigma(n+1) = n+1$, on pose $s = \sigma$.
Dans tous les cas, $s(n+1) = n+1$, donc l'application r déduite de s par restriction au départ et à l'arrivée à $\mathbb{N}_n$ est un élément de $\mathcal{S}_n$. D'après l'hypothèse de récurrence, il existe $k \in \mathbb{N}$ et k transpositions $\tau_1, \dots, \tau_k$ telles que $r = \tau_1 \circ \dots \circ \tau_k$.
Pour tout $h \in \{1, \dots, k\}$, notons t_h l'unique transposition de $\mathbb{N}_{n+1}$ dont la restriction à $\mathbb{N}_n$ est égale à τ_h.
Alors $s = t_1 \circ \dots \circ t_k$, ce qui prouve $R(n+1)$. □

Remarque. La formule $(a_1\ a_2\ \dots\ a_k) = (a_1\ a_2) \circ (a_2\ a_3) \circ \dots \circ (a_{k-1}\ a_k)$ décompose explicitement tout cycle en un produit de transpositions. Elle permet donc de montrer la propriété précédente à partir du théorème de décomposition en produit de cycles.

Exercice. Soit $n \in \mathbb{N}$ avec $n \geq 2$. Montrer que toute permutation de $\mathcal{S}_n$ est un produit de transpositions de la forme $(i \;\; i+1)$ où $i \in \{1, \ldots, n-1\}$.

Solution : Pour tout i, j tels que $1 \leq i < j < n$,
on vérifie que $(j \;\; j+1) \circ (i \;\; j) \circ (j \;\; j+1) = (i \;\; j+1)$.
Pour tout $k \in \{1, \ldots, n-1\}$, on peut alors montrer par récurrence la propriété $T(k)$ suivante : Pour tout $i \in \mathbb{N}^*$ tel que $i + k \leq n$, $(i \;\; i+k)$ est un produit de transpositions de la forme $(j \;\; j+1)$.

On peut maintenant démontrer un résultat que l'on avait admis lors du cours portant sur les sommes finies :

Commutativité généralisée : On suppose que $(G, +)$ est un monoïde commutatif. Soit $n \in \mathbb{N}$ et $x_1, \ldots, x_n \in G$. Alors, pour toute bijection σ de $\mathbb{N}_n$ dans lui-même, $\sum_{i=1}^{n} x_i = \sum_{j=1}^{n} x_{\sigma(j)}$.

Démonstration.

Notons $P(\sigma)$ la propriété $\sum_{i=1}^{n} x_i = \sum_{j=1}^{n} x_{\sigma(j)}$.

$\diamond$ Supposons d'abord qu'il existe $k \in \{1, \ldots, n-1\}$ tel que $\sigma = (k \;\; k+1)$.
Alors, par associativité, et en convenant que les sommes vides sont nulles,
$\sum_{j=1}^{n} x_{\sigma(j)} = (x_1 + \cdots + x_{k-1}) + (x_{k+1} + x_k) + (x_{k+2} + \cdots + x_n)$, or $(G, +)$ est commutatif,
donc $\sum_{j=1}^{n} x_{\sigma(j)} = (x_1 + \cdots + x_{k-1}) + (x_k + x_{k+1}) + (x_{k+2} + \cdots + x_n) = \sum_{i=1}^{n} x_i$.

$\diamond$ Soit $\ell \in \mathbb{N}$. Notons $R(\ell)$ l'assertion : $P(\sigma)$ est vraie lorsque σ est le produit de ℓ transpositions de la forme $(k \;\; k+1)$.
$R(0)$ est évidente car dans ce cas $\sigma = Id_{\mathbb{N}_n}$.
Soit $\ell \geq 1$. On suppose $R(\ell - 1)$.
Soit σ un produit de ℓ transpositions de la forme $(k \;\; k+1)$.
On peut écrire $\sigma = s \circ \tau$ où $\tau = (a \;\; a+1)$ avec $a \in \{1, \ldots, n-1\}$ et où s est le produit de $\ell - 1$ transpositions de la forme $(k \;\; k+1)$.
Pour tout $j \in \mathbb{N}_n$, posons $y_j = x_{s(j)}$. Alors
$\sum_{j=1}^{n} x_{\sigma(j)} = \sum_{j=1}^{n} x_{s(\tau(j))} = \sum_{j=1}^{n} y_{\tau(j)}$, mais d'après le premier point de la démonstration,
$\sum_{j=1}^{n} y_{\tau(j)} = \sum_{j=1}^{n} y_j$, donc $\sum_{j=1}^{n} x_{\sigma(j)} = \sum_{j=1}^{n} x_{s(j)}$ et on conclut grâce à l'hypothèse de récurrence.

$\diamond$ Selon l'exercice précédent, toute permutation de $\mathcal{S}_n$ est le produit d'un nombre fini de transpositions de la forme $(k \; k+1)$, donc la propriété est démontrée. $\square$

Définition. Soit $n \in \mathbb{N}^*$ et soit $\sigma \in \mathcal{S}_n$. La décomposition de σ en un produit de transpositions $\tau_1 \circ \cdots \circ \tau_k$ n'est pas unique, mais le nombre k de transpositions utilisées

a toujours la même parité. Ainsi $(-1)^k$ ne dépend que de σ. On l'appelle la signature de σ et on le note $\varepsilon(\sigma)$.
Les permutations de signature 1 s'appellent les permutations paires,
Les permutations de signature -1 s'appellent les permutations impaires.

Démonstration.
Cf DM. □

Propriété. L'application signature est l'unique morphisme de $\mathcal{S}_n$ dans $(\{-1,1\},\times)$ qui envoie toute transposition sur -1.

Démonstration.
Soit $\sigma,\sigma' \in \mathcal{S}_n$. Il existe des transpositions $\tau_1,\dots,\tau_k$ et $\tau_{k+1},\cdots,\tau_{k+h}$ telles que $\sigma = \tau_1 \circ \cdots \circ \tau_k$ et $\sigma' = \tau_{k+1} \circ \cdots \circ \tau_{k+h}$. Alors $\sigma\sigma' = \tau_1 \circ \cdots \circ \tau_{k+h}$,
donc $\varepsilon(\sigma\sigma') = (-1)^{k+h} = (-1)^k(-1)^h = \varepsilon(\sigma)\varepsilon(\sigma')$. □

Exemple. Reprenons l'exemple précédent. $\sigma = (1\ 3)\circ(2\ 6\ 5) = (1\ 3)(2\ 6)(6\ 5)$, donc σ est une permutation impaire.

Remarque. Plus généralement, tout cycle $(a_1\ \cdots\ a_k)$ de $\mathcal{S}_n$ se décompose en le produit suivant de transpositions : $(a_1\ \cdots\ a_k) = (a_1\ a_2)(a_2\ a_3)\cdots(a_{k-1}a_k)$.
En particulier, la signature d'un cycle de longueur k est $(-1)^{k+1}$.

Propriété. Soit $n \in \mathbb{N}^*$. On note $\mathcal{A}_n$ l'ensemble des permutations paires de $\mathcal{S}_n$.
C'est un sous-groupe de $\mathcal{S}_n$, appelé le groupe alterné de degré n.

Démonstration.
$\mathcal{A}_n$ est le noyau du morphisme ε. □

Propriété. Si $n \geq 2$, alors $|\mathcal{A}_n| = \dfrac{n!}{2}$.

Démonstration.
Soit τ une transposition de $\mathcal{S}_n$. Alors $\mathcal{S}_n = \mathcal{A}_n \sqcup [\tau\mathcal{A}_n]$. En effet, pour tout $\sigma \in \mathcal{S}_n$, ou bien $\sigma \in \mathcal{A}_n$, ou bien σ est une permutation impaire, auquel cas $\sigma = \tau(\tau\sigma)$ et $\tau\sigma \in \mathcal{A}_n$, donc $\sigma \in \tau\mathcal{A}_n$. De plus, une permutation de $\mathcal{A}_n \cap [\tau\mathcal{A}_n]$ serait paire et impaire, ce qui est impossible, donc $\mathcal{A}_n \cap [\tau\mathcal{A}_n] = \emptyset$. On en déduit que $n! = |\mathcal{S}_n| = |\mathcal{A}_n| + |\tau\mathcal{A}_n|$.
D'autre part, l'application $\sigma \longmapsto \tau\sigma$ est une bijection de $\mathcal{A}_n$ dans $\tau\mathcal{A}_n$, dont la bijection réciproque est $\begin{array}{ccc} \tau\mathcal{A}_n & \longrightarrow & \mathcal{A}_n \\ \sigma & \longmapsto & \tau\sigma \end{array}$. Ainsi, $|\mathcal{A}_n| = |\tau\mathcal{A}_n|$, ce qui permet de conclure. □

2 La structure d'anneau

2.1 Définition

Définition. Soit A un ensemble muni de deux lois internes notées "+" et ".". On dit que $(A,+,.)$ est un anneau si et seulement si $(A,+)$ est un groupe commutatif et si
- le produit est associatif ;
- le produit admet un élément neutre ;

— le produit est distributif par rapport à l'addition :
pour tout $x, y, z \in A$, $x(y+z) = xy + xz$ et $(y+z)x = yx + zx$.

On dit que l'anneau $(A, +, .)$ est commutatif (ou abélien) si et seulement si son produit est commutatif.

Exemple.
— $(\mathbb{Z}, +, .)$ et $(\mathbb{Q}, +, .)$ sont des anneaux commutatifs. Idem avec $\mathbb{R}$ et $\mathbb{C}$.
— $(\mathcal{M}_n(\mathbb{R}), +, \times)$ est un anneau non commutatif.
— Soit I un intervalle. Alors l'ensemble $\mathbb{R}^I$ des applications de I dans $\mathbb{R}$ est un anneau commutatif.
— Nous verrons plus tard que l'ensemble des applications polynomiales de $\mathbb{R}$ dans $\mathbb{R}$ est un anneau commutatif. Il s'agit des applications de la forme $\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \displaystyle\sum_{n\in\mathbb{N}} a_n x^n \end{array}$ où $(a_n) \in \mathbb{R}^{(\mathbb{N})}$, c'est-à-dire que (a_n) est une suite de réels, tous nuls saufs pour un nombre fini d'entre eux.
— Anneau de Boole : $(\mathcal{P}(E), \Delta, \cap)$ est un anneau.

2.2 Calculs dans un anneau

Propriété. Soit A un anneau. Alors

$$\forall x \in A \;\; 0.x = x.0 = 0, \text{ et}$$

$$\forall (n, x, y) \in \mathbb{Z} \times A \times A \;\; (nx).y = x.(ny) = n(x.y).$$

En particulier,

$$\forall x \in A \;\; -x = (-1_A).x = x.(-1_A).$$

Démonstration.
Soit $x \in A$. L'application $\varphi : \begin{array}{ccc} (A,+) & \longrightarrow & (A,+) \\ y & \longmapsto & x.y \end{array}$ est un morphisme de groupes, d'après la distributivité de "." par rapport à "+". Ainsi, $\varphi(0) = 0$ et, pour tout $n \in \mathbb{Z}$, pour tout $y \in A$, $\varphi(ny) = n\varphi(y)$. Ceci montre que $x.0 = 0$ et $x.(ny) = n(x.y)$.
En utilisant le morphisme $y \longmapsto y.x$, on montre de même que
$0.x = 0$ et $(ny).x = n(y.x)$.
Cette dernière relation, avec $n = -1$ et $y = 1_A$ donne : $(-1_A).x = -x$. De même, la relation $x.(ny) = n(x.y)$ donne, lorsque $n = -1$ et $y = 1_A$: $x.(-1_A) = -x$. □

Exemple. $\{0\}$ est un anneau en posant $0 + 0 = 0$ et $0.0 = 0$.

Propriété. Si A est un anneau contenant au moins deux éléments,

$$1_A \neq 0_A.$$

Démonstration.
Soit A un anneau tel que $1_A = 0_A$.
Soit $x \in A$. $x = x.1_A = x.0_A = 0_A$. Ainsi $A = \{0_A\}$.
On a montré que si $1_A = 0_A$, A est réduit à un singleton. La contraposée de cette implication est la propriété qu'il fallait démontrer. □

Propriété. *Généralisation de la distributivité.*
Soient A un anneau, $(a_1, \ldots, a_n) \in A^n$ et $(b_1, \ldots, b_p) \in A^p$.

$$\left(\sum_{i=1}^{n} a_i\right).\left(\sum_{i=1}^{p} b_i\right) = \sum_{\substack{1\leq i\leq n\\ 1\leq j\leq p}} a_i.b_j.$$

2.3 Puissances d'un élément

Notation. Dans ce paragraphe on fixe un anneau A.

Définition. Un élément $a \in A$ est dit ***inversible*** si et seulement s'il admet un symétrique (alors appelé inverse) pour la loi ".".

Définition. Si $a \in A$. On définit la famille (a^n) par les relations suivantes :
- Initialisation : $a^0 = 1_A$ (encore le produit vide) ;
- Itération : pour tout $n \in \mathbb{N}$, $a^{n+1} = a.a^n$ (donc pour $n \in \mathbb{N}^*$, $a^n = \underbrace{a \times \cdots \times a}_{n fois}$) ;
- Lorsque a est inversible, pour tout $n \in \mathbb{Z}$ avec $n < 0$, on note $a^n = (a^{-n})^{-1}$.

Définition. On dit que $a \in A \setminus \{0\}$ est nilpotent si et seulement si il existe $n \in \mathbb{N}$ avec $n \geq 2$ tel que $a^n = 0$.

Propriété. On dispose des formules suivantes :

$$\forall n, m,\ \ a^n a^m = a^{n+m},$$
$$\forall n, m,\ \ (a^n)^m = a^{nm},$$

valables pour tout $n, m \in \mathbb{N}$ lorsque a est quelconque dans A
et valables pour tout $n, m \in \mathbb{Z}$ lorsque a est un élément inversible de A.

Démonstration.
Adapter ce que l'on a fait dans le cours sur les groupes. □

Propriété. Soit $a, b \in A$ tels que $ab = ba$ (on dit que a et b commutent).
Alors $(ab)^n = a^n b^n$, pour tout $n, m \in \mathbb{N}$ lorsque a et b sont quelconques dans A
et pour tout $n, m \in \mathbb{Z}$ lorsque a et b sont des éléments inversibles de A.

Démonstration.
Adapter ce que l'on a fait dans le cours sur les groupes. □

2.4 Les sous-anneaux

Définition. Soit $(A, +, .)$ un anneau et $B \subset A$. B est un sous-anneau de A si et seulement si, en le munissant des restrictions sur B^2 des lois "+" et ".", B est un anneau possédant les mêmes éléments neutres que ceux de A.

Propriété. Soit A un anneau et B une partie de A.

$$B \text{ est un } \textbf{\textit{sous-anneau}} \text{ de } A \text{ si et seulement si } \begin{cases} 1_A & \in B, \\ \forall (x,y) \in B^2 \;\; x-y & \in B, \\ \forall (x,y) \in B^2 \;\; xy & \in B. \end{cases}$$

Remarque. $\{0_A\}$ est un anneau mais ce n'est pas un sous-anneau de A lorsque $A \neq \{0_A\}$.

Exemple. L'ensemble $\mathcal{C}^\infty([0,1], \mathbb{C})$ des applications de classe C^∞ de $[0,1]$ dans $\mathbb{C}$ est un sous-anneau de $\mathcal{F}([0,1], \mathbb{C})$.
L'ensemble des suites convergentes est un sous-anneau de $\mathbb{R}^{\mathbb{N}}$.

Exemple. $\mathbb{Z}$ n'admet qu'un seul sous-anneau : lui-même.
En effet, si A est un sous-anneau de $\mathbb{Z}$, c'est un sous-groupe, donc il existe $n \in \mathbb{N}$ tel que $A = n\mathbb{Z}$, et $1 \in A$, donc $n = 1$ et $A = \mathbb{Z}$.

Propriété. Si A est un anneau, son plus petit sous-anneau est $\mathbb{Z}.1_A = \{n.1_A / n \in \mathbb{Z}\}$.

Démonstration.
Si B est un sous-anneau de A, il contient 1_A, donc il contient le groupe engendré par 1_A, égal à $\mathbb{Z}.1_A$, or ce dernier est un sous-anneau. □

2.5 Les corps

Propriété. Soit A un anneau. l'ensemble des éléments inversibles de A muni de la loi "." est un groupe, appelé ***groupe des inversibles*** et noté A^* ou $U(A)$.

Exemples. Le groupe des inversibles de l'anneau $\mathbb{Z}$ est réduit à $\{-1, 1\}$.
Le groupe des inversibles de l'anneau $\mathbb{R}$ est égal à $(\mathbb{R}^*, \times)$.
Quel est le groupe des inversibles de $\mathcal{F}([0,1], \mathbb{C})$?

Définition. Un anneau A est un ***corps*** si et seulement si
- A n'est pas réduit à $\{0_A\}$,
- A est commutatif,
- et tout élément de A différent de 0_A est inversible.

Remarque. Dans certains ouvrages, un corps n'est pas forcément commutatif, c'est seulement un anneau non nul dans lequel tout élément non nul est inversible. Dans ce cas, nous dirons qu'il s'agit d'un *corps gauche*.

On peut montrer (théorème de Wedderburn) que tout corps gauche fini est commutatif. Cependant il existe des corps gauches infinis non commutatifs, dont le corps des quaternions.

Définition. Soit $(\mathbb{K}, +, .)$ un corps et $\mathbb{L} \subset \mathbb{K}$. $\mathbb{L}$ est un sous-corps de $\mathbb{K}$ si et seulement si, en le munissant des restrictions sur $\mathbb{L}^2$ des lois "+" et ".", $\mathbb{L}$ est un corps possédant les mêmes éléments neutres que ceux de $\mathbb{K}$.

Propriété. Si K est un corps, B est un sous-corps de K si et seulement si B est un sous-anneau de K vérifiant la propriété suivante : $\forall x \in B \setminus \{0\}\ \ x^{-1} \in B$.

Exemple. $(\mathbb{Q} + \sqrt{2}\mathbb{Q}, +, .)$ est un sous-corps de $\mathbb{R}$.
En effet, 1 appartient à $\mathbb{Q} + \sqrt{2}\mathbb{Q} = \{\alpha + \sqrt{2}\beta / (\alpha, \beta) \in \mathbb{Q}^2\}$ et cet ensemble est clairement stable pour le produit et la différence. Il reste donc à montrer que tout élément non nul de $\mathbb{Q} + \sqrt{2}\mathbb{Q}$ a son inverse dans $\mathbb{Q} + \sqrt{2}\mathbb{Q}$.
Soit $(\alpha, \beta) \in \mathbb{Q}^2$ tel que $\alpha + \sqrt{2}\beta \neq 0$. $\alpha - \sqrt{2}\beta \neq 0$, car $\sqrt{2}$ est irrationnel, donc
$$\frac{1}{\alpha + \sqrt{2}\beta} = \frac{\alpha - \sqrt{2}\beta}{\alpha^2 - 2\beta^2} = \frac{\alpha}{\alpha^2 - 2\beta^2} + \sqrt{2}\frac{-\beta}{\alpha^2 - 2\beta^2} \in \mathbb{Q} + \sqrt{2}\mathbb{Q}.$$

2.6 Formules

Formule du *binôme de Newton*.
Soient A un anneau et a et b deux éléments de A **qui commutent entre eux**. Alors, pour tout $n \in \mathbb{N}$,
$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

Démonstration.
Déjà fait. □

Formule du *multinôme* (hors programme) :
Soient A un anneau et $(b_1, \ldots, b_p)$ un p-uplet d'éléments de A qui commutent deux à deux. Alors, pour tout $n \in \mathbb{N}$,
$$(b_1 + \cdots + b_p)^n = \sum_{\alpha_1 + \cdots + \alpha_p = n} \frac{n!}{\alpha_1! \cdots \alpha_p!} b_1^{\alpha_1} \cdots b_p^{\alpha_p}.$$

Démonstration.
Déjà fait. □
Formule de Bernoulli : Soit $(A, +, \times)$ un anneau. Soit a et b deux éléments de A qui commutent (i.e $ab = ba$). Alors, pour tout $n \in \mathbb{N}$,
$$a^{n+1} - b^{n+1} = (a-b) \sum_{k=0}^{n} a^k b^{n-k}.$$

Démonstration.
$(a-b)\sum_{k=0}^{n} a^k b^{n-k} = \sum_{k=0}^{n}(a^{k+1}b^{(n+1)-(k+1)} - a^k b^{(n+1)-k})$. Il s'agit d'une somme télescopique, ce qui permet de conclure. □

Remarque. Lorque $n+1$ est impair,
$a^{n+1} + b^{n+1} = a^{n+1} - (-b)^{n+1} = (a+b)\sum_{k=0}^{n} a^k(-1)^{n-k}b^{n-k}$.

Exemple. $a^3 - b^3 = (a-b)(a^2+ab+b^2)$.

Sommes partielles d'une série géométrique.
Soient A un anneau et $x \in A$. Alors, pour tout $(m,n) \in \mathbb{N}^2$ avec $m \leq n$,

$$\boxed{(1_A - x).\sum_{i=m}^{n} x^i = x^m - x^{n+1}.}$$

2.7 Anneaux intègres

Définition. Soit A un anneau. Si $a \in A \setminus \{0\}$, on dit que a est un ***diviseur*** à gauche de 0 si et seulement s'il existe $b \in A \setminus \{0\}$ tel que $ab = 0$.
On dit que a est un diviseur à droite de 0 si et seulement s'il existe $b \in A \setminus \{0\}$ tel que $ba = 0$.

Propriété. Un élément non nul d'un anneau est régulier à gauche si et seulement si ce n'est pas un diviseur à gauche de 0. Idem à droite.

Démonstration.
Soit $a \in A \setminus \{0\}$. On suppose que a n'est pas un diviseur de 0 à gauche.
Soit $b, c \in A$ tels que $ab = ac$. Alors $a(b-c) = 0$, mais a n'est pas un diviseur de 0 et $a \neq 0$, donc $b - c = 0$, puis $b = c$.
La réciproque est simple. □

Définition. On dit qu'un anneau A est ***intègre*** si et seulement si
- il n'est pas réduit à $\{0_A\}$;
- il est commutatif ;
- il n'admet aucun diviseur de 0.

Propriété. Un corps est en particulier un anneau intègre.

Exemple. $\mathcal{F}(\mathbb{R},\mathbb{R})$ est un anneau non intègre.

2.8 Morphismes d'anneaux

Définition. Soient $(A, +_A, \cdot_A)$ et $(B, +_B, \cdot_B)$ deux anneaux.
Une application $f : A \longrightarrow B$ est un ***morphisme d'anneaux*** si et seulement si

- $f(1_A) = 1_B$,
- $\forall (x,y) \in A^2 \;\; f(x +_A y) = f(x) +_B f(y)$,
- $\forall (x,y) \in A^2 \;\; f(x._A y) = f(x)._B f(y)$.

Un ***isomorphisme*** est un morphisme bijectif.
Un ***endomorphisme*** est un morphisme de A dans lui-même.
Un ***automorphisme*** est un endomorphisme bijectif.

Remarque. Un morphisme d'anneaux est en particulier un morphisme de groupes. Ainsi, lorsque f est un morphisme d'anneaux, on dispose de son image $Im(f)$ et de son noyau $Ker(f) = f^{-1}(\{0\})$.

Exemple.
- Id_A est un automorphisme de l'anneau A.
- L'application $z \longmapsto \overline{z}$ est un automorphisme involutif de l'anneau $(\mathbb{C}, +, .)$.
- L'application $(x_n) \longmapsto \lim_{n\to+\infty}(x_n)$ est un morphisme d'anneaux, de $\mathcal{C}$ dans $\mathbb{R}$, où $\mathcal{C}$ désigne le sous-anneau des suites convergentes de réels.

Propriété. Soient A et B deux anneaux et f un morphisme d'anneaux de A dans B. Pour tout $a \in A$, $p \in \mathbb{N}$ et $n \in \mathbb{Z}$,
- $f(na) = nf(a)$,
- $f(a^p) = f(a)^p$,
- Si a est inversible, alors $f(a)$ est inversible et $f(a^n) = f(a)^n$. En particulier, $f(a^{-1}) = f(a)^{-1}$.

Démonstration.
Le second point se démontre par récurrence sur $p \in \mathbb{N}$.
Le premier point est connu, car f est un morphisme entre les groupes $(A, +)$ et $(B, +)$.
Pour le dernier point, si a est inversible alors $f(a)f(a^{-1}) = f(aa^{-1}) = f(1_A) = 1_B$, donc $f(a)$ est inversible. Ainsi $f|_{U(A)}^{U(B)}$ est bien défini. Il est clair que c'est un morphisme de groupes multiplicatifs, ce qui permet de conclure. □

Propriété. La composée de deux morphismes d'anneaux est un morphisme d'anneaux.

Propriété. Si f est un isomorphisme d'anneaux, f^{-1} est encore un isomorphisme d'anneaux.

Propriété. Soient $(A, +_A, ._A)$ et $(B, +_B, ._B)$ deux anneaux et $f : A \longrightarrow B$ un morphisme d'anneaux.
L'image directe par f de tout sous-anneau de A est un sous-anneau de B.
L'image réciproque selon f de tout sous-anneau de B est un sous-anneau de A.

Définition. Soit $\mathbb{K}$ et $\mathbb{L}$ deux corps et f une application de $\mathbb{K}$ dans $\mathbb{L}$. On dit que f est un morphisme de corps si et seulement si c'est un morphisme d'anneaux.

Propriété. (hors programme) Un morphisme de corps est toujours injectif.

Démonstration.
Soit $f : \mathbb{K} \longrightarrow \mathbb{L}$ un morphisme de corps. Soit $x \in \mathbb{K}$ avec $x \neq 0$. Alors x est inversible, donc il existe $y \in \mathbb{K}$ tel que $xy = 1$. Ainsi, $1 = f(1) = f(xy) = f(x)f(y)$, donc $f(x) \neq 0$.

Ainsi, $Ker(f) = \{0\}$ et f est injectif. □

Propriété. Soit $f : \mathbb{K} \longrightarrow \mathbb{L}$ un morphisme de corps.
Si $\mathbb{K}'$ est un sous-corps de $\mathbb{K}$, alors $f(\mathbb{K}')$ est un sous-corps de $\mathbb{L}$.
Si $\mathbb{L}'$ est un sous-corps de $\mathbb{L}$, alors $f^{-1}(\mathbb{L}')$ est un sous-corps de $\mathbb{K}$.

2.9 Les anneaux produits

Définition. Soient $n \in \mathbb{N}^*$ et $((A_i, +, .))_{i\in\{1,\dots,n\}}$ une famille de n anneaux.
L'anneau produit de cette famille est $(A, +, .)$, où $A = A_1 \times \cdots \times A_n$ et où les lois "+" et "." sont définies par : pour tout $x = (x_1, \dots, x_n) \in A$ et $y = (y_1, \dots, y_n) \in A$,
$x + y = (x_1 + y_1, \dots, x_n + y_n)$ et $x.y = (x_1.y_1, \dots, x_n.y_n)$.

Démonstration.
On vérifie que A est bien un anneau. □

Exemple. $(\mathbb{C}^n, +, \times)$ est un anneau.
$(\mathbb{R}^2, +, \times)$ est un anneau, qu'il convient de distinguer de l'anneau $\mathbb{C}$. En effet, dans le premier anneau, $(a, b) \times (c, d) = (ac, bd)$ alors que dans le second,
$(a, b) \times (c, d) = (ac - db, ad + bc)$.

Remarque. Comme pour les groupes produits, on montre que, avec les notations précédentes, A est abélien si et seulement si, pour tout $i \in \mathbb{N}_n$, A_i est abélien.

Définition. Reprenons les notations de la définition précédente.
Pour tout $i \in \mathbb{N}_n$, la $i^{\text{ème}}$ projection, $p_i : \begin{array}{ccc} A & \longrightarrow & A_i \\ (a_1, \dots, a_n) & \longmapsto & a_i \end{array}$ est un morphisme surjectif d'anneaux.

2.10 Les idéaux

Définition. Une partie I d'un anneau A est un ***idéal*** de A à gauche (resp : à droite) si et seulement s'il vérifie les propriétés suivantes :

$$\begin{array}{l} I \neq \emptyset, \\ \forall (x, y) \in I^2,\ \ x + y \in I, \text{ et} \\ \forall (x, y) \in A \times I,\ \ x.y \in I \text{ (resp : } y.x \in I). \end{array}$$

Ainsi un idéal est stable pour l'addition et "superstable" pour le produit. On dit aussi qu'un idéal est absorbant pour le produit.
Lorsque I est un idéal à gauche et à droite, on dit que c'est un idéal bilatère.

Notation. Pour la suite, on fixe un anneau $(A, +, .)$ **que l'on suppose commutatif**.

Propriété. Tout idéal est un groupe pour la loi "+".

Démonstration.
Soit I un idéal d'un anneau commutatif A. I est non vide et stable pour l'addition, donc il reste à montrer qu'il est stable par passage au symétrique. Mais $-1_A \in A$, donc, si $x \in I$, $-x = (-1_A).x \in I$. □

Exemples. A et $\{0\}$ sont des idéaux de A.

Propriété. Soit A un anneau commutatif et I un idéal de A. Alors $1 \in I \iff I = A$. Ainsi les idéaux de A différents de A ne sont pas des sous-anneaux de A.

Démonstration.
Supposons que $1 \in I$. Soit $a \in A$. $a = a.1 \in I$ d'après la superstabilité de I pour le produit.
La réciproque est claire. □

Propriété. Une intersection d'idéaux de A est un idéal de A.

Démonstration.
Soit $(I_k)_{k\in K}$ une famille d'idéaux (K peut être de cardinal infini). Notons $I = \bigcap_{k\in K} I_k$.
On sait déjà que I est un sous-groupe de A, en tant qu'intersection de sous-groupes.
Soit $(a, x) \in A \times I$. Soit $k \in K$.
$a \in A$ et $x \in I_k$, mais I_k est superstable pour le produit, donc $a.x \in I_k$. Ainsi $a.x \in I$, ce qui prouve que I est un idéal. □

Définition. Soit B une partie de A. L'idéal engendré par B est l'intersection des idéaux de A contenant B. C'est le plus petit idéal (au sens de l'inclusion) contenant B. On le note $Id(B)$.

Propriété. Soient B et C deux parties de A telles que $C \subset B$. Alors $Id(C) \subset Id(B)$.

Propriété. Si B est une partie de A,
$Id(B) = \{\sum_{i=1}^{n} a_i b_i / n \in \mathbb{N}, (a_1, \ldots, a_n) \in A^n, (b_1, \ldots, b_n) \in B^n\}$.

Démonstration.
Notons temporairement $B' = \{\sum_{i=1}^{n} a_i b_i / n \in \mathbb{N}, (a_1, \ldots, a_n) \in A^n, (b_1, \ldots, b_n) \in B^n\}$.
Avec $n = 0$, par convention, $\sum_{i=1}^{n} a_i b_i = 0$, donc $B' \neq \emptyset$. De plus, on vérifie que B' est stable pour l'addition et superstable pour le produit, donc B' est un idéal de A, qui contient clairement B.
Enfin, si I est un idéal de A contenant B, il contient B' car I est stable pour l'addition et superstable pour le produit. □

Exemples. $Id(\emptyset) = \{0\}$.
Pour tout $b \in A$, $Id(b) = \{ab / a \in A\} = Ab$: c'est l'ensemble des multiples de b.

Exemple. Si $A = \mathbb{Z}$, pour tout $n \in \mathbb{N}$, $Id(n) = n\mathbb{Z}$.

Définition. Un idéal I de A est principal si et seulement si il existe $b \in A$ tel que $I = Id(b)$.

Définition. Un anneau est principal si et seulement si c'est un anneau intègre dont tous les idéaux sont principaux.

Remarque. $A = Id(1)$, donc A est un idéal principal de A, mais ce n'est pas toujours un anneau principal.

Théorème. $\mathbb{Z}$ est un anneau principal.

Démonstration.
Soit I un idéal de $\mathbb{Z}$: c'est un sous-groupe de $\mathbb{Z}$ et on sait alors qu'il existe $n \in \mathbb{N}$ tel que $I = n\mathbb{Z}$, donc I est un idéal principal de $\mathbb{Z}$. □

Propriété. Soit I et J deux idéaux d'un anneau commutatif A.
Alors $I + J$ est un idéal de A. C'est l'idéal engendré par $I \cup J$.

Propriété. Soient A et B deux anneaux commutatifs et $f : A \longrightarrow B$ un morphisme d'anneaux.

$$Ker(f) \text{ est un idéal de } A.$$

De plus,

$$\text{si } I \text{ est un idéal de } B,\ f^{-1}(I) \text{ est un idéal de } A \text{ contenant } Ker(f).$$

Démonstration.
• Soit I un idéal de B. $f^{-1}(I)$ est un sous-groupe de A, en tant qu'image réciproque d'un sous-groupe par un morphisme de groupes.
Soit $(a, i) \in A \times f^{-1}(I)$. $f(ai) = f(a)f(i) \in I$ car $f(i) \in I$ et I est un idéal de B, donc $ai \in f^{-1}(I)$. Ainsi $f^{-1}(I)$ est un idéal de A.
• $\{0\} \subseteq I$, donc $Ker(f) = f^{-1}(\{0\}) \subseteq f^{-1}(I)$.
• $\{0\}$ est un idéal de B, donc $Ker(f) = f^{-1}(\{0\})$ est un idéal de A. □

Exercice. Que peut-on dire de l'image directe d'un idéal par un morphisme d'anneaux ?

Résolution. Soient A et B deux anneaux commutatifs, $f : A \longrightarrow B$ un morphisme d'anneaux, et I un idéal de A. Montrons que $f(I)$ est un idéal de l'anneau $Im(f)$.
En effet, $f(I)$ est un sous-groupe de B, en tant qu'image d'un groupe par un morphisme et $f(I)$ est inclus dans le sous-anneau $Im(f)$ de B, donc $f(I)$ est un sous-groupe de $Im(f)$.
Soit $(a', i') \in Im(f) \times f(I)$. Il existe $(a, i) \in A \times I$ tel que $a' = f(a)$ et $i' = f(i)$. $a'.i' = f(a).f(i) = f(a.i)$, or $a.i \in I$, donc $a'.i' \in f(I)$. Ceci achève la preuve.

Exemple. Notons E l'ensemble des applications de classe C^∞ de $[0, 1]$ dans $\mathbb{C}$. C'est un anneau commutatif.
l'application $\begin{array}{ccc} E & \longrightarrow & \mathbb{C} \\ f & \longmapsto & f(\frac{1}{2}) \end{array}$ est un morphisme d'anneaux, donc son noyau, constitué des éléments de E qui s'annulent en $\frac{1}{2}$, est un idéal de E.

3 $\mathbb{Z}/n\mathbb{Z}$

3.1 Groupes quotients

Notation. On fixe un groupe $(G, .)$ et un sous-groupe H de G.
On note R_H la relation binaire définie sur G par :

$$\forall (x, y) \in G^2, \ [xR_H y \iff x^{-1}y \in H].$$

Propriété. R_H est une relation d'équivalence et, pour tout $x \in G$, la classe d'équivalence de x pour R_H est $\overline{x} = \{xh/h \in H\} \stackrel{\Delta}{=} xH$.

On note G/H l'ensemble des classes d'équivalence : $G/H = \{\overline{x}/x \in G\}$.

Démonstration.
$\diamond$ Pour tout $x \in G$, $x^{-1}x = 1_G \in H$, donc R_H est réflexive.
$\diamond$ Soit $x, y \in G$ tels que $xR_H y$. Alors $x^{-1}y \in H$, mais H est stable par passage à l'inverse, donc $y^{-1}x \in H$, ce qui montre que $yR_H x$. Ainsi R_H est symétrique.
$\diamond$ Soit $x, y, z \in G$ tels que $xR_H y$ et $yR_H z$. Ainsi $x^{-1}y \in H$ et $y^{-1}z \in H$. Alors, H étant un sous-groupe, $x^{-1}z = (x^{-1}y).(y^{-1}z) \in H$, donc $xR_H z$. Ainsi, R_H est transitive.
$\diamond$ Soit $x, y \in G$.
$y \in \overline{x} \iff [\exists h \in H \ \ x^{-1}y = h] \iff [\exists h \in H \ \ y = xh]$, donc $\overline{x} = xH$. $\square$

Exemple. Lorsque $G = (\mathbb{Z}, +)$ et $H = n\mathbb{Z}$, où $n \in \mathbb{N}$,
$\mathbb{Z}/n\mathbb{Z} = \{\overline{k}/k \in \mathbb{Z}\}$, où $\overline{k} = \{k + na/a \in \mathbb{Z}\}$.

Théorème de Lagrange (Hors programme) : Si G est de cardinal fini, alors le cardinal de H divise celui de G.

Démonstration.
R_H étant une relation d'équivalence, ses classes d'équivalence forment une partition de G, donc $\#G = \sum_{C \in G/H} \#C$.
Soit $C \in G/H$. Il existe $x \in G$ tel que $C = \overline{x} = xH$.
L'application $\begin{array}{rccc} \varphi : & H & \longrightarrow & xH \\ & h & \longmapsto & xh \end{array}$ est surjective par définition de xH. De plus, pour $h, h' \in H$, si $\varphi(h) = \varphi(h')$, alors $xh = xh'$, donc en composant par x^{-1}, on obtient $h = h'$. Ainsi φ est une bijection, ce qui montre que $\#C = \#(xH) = \#H$.
Ainsi $\#G = \sum_{C \in G/H} \#C = [\#H].[\#(G/H)]$, ce qu'il fallait démontrer. $\square$

Corollaire. (Hors programme) Si p est un nombre premier, tout groupe de cardinal p est cyclique.

Démonstration.
On suppose que $\#G = p \in \mathbb{P}$.
$p \geq 2$, donc il existe $x \in G$ avec $x \neq 1_G$. Ainsi $Gr(x)$ est de cardinal supérieur à 2 et il divise p. p étant premier, $\#[Gr(x)] = p$, donc $G = Gr(x)$ et G est cyclique. $\square$

Théorème. (au programme) : Si $(G,.)$ est un groupe d'ordre fini, alors l'ordre de chacun de ses éléments divise l'ordre de G.
Cela signifie que, $\forall a \in G,\ a^{|G|} = 1_G$.

Démonstration.
C'est évident en utilisant le théorème de Lagrange, mais il est hors programme. Lorsque $(G,.)$ est commutatif, la preuve suivante est à connaître :
Soit $a \in G$. Alors $G = aG$: en effet, l'application $\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & ax \end{array}$ est une bijection, d'application réciproque $x \longmapsto a^{-1}x$.
Ainsi, $\displaystyle\prod_{\alpha\in G}\alpha = \prod_{\beta\in aG}\beta = \prod_{\alpha\in G} a.\alpha = a^{\#G}\prod_{\alpha\in G}\alpha$,
or $\displaystyle\prod_{\alpha\in G}\alpha$ est inversible, donc $a^{\#G} = 1_G$. □

Notation. Pour la suite, on suppose que $(G,+)$ est un groupe **commutatif**. Ainsi, pour tout $x, y \in G$, $xR_Hy \iff y - x \in H$.

Théorème. En posant, pour tout $x, y \in G$, $\overline{x} + \overline{y} \stackrel{\Delta}{=} \overline{x+y}$, on définit une loi "+" sur G/H **pour laquelle** G/H **est un groupe commutatif.**

Démonstration.
◇ la relation $\overline{x} + \overline{y} \stackrel{\Delta}{=} \overline{x+y}$ a un sens seulement si la quantité $\overline{x+y}$ est bien une fonction de $(\overline{x}, \overline{y})$. Il faut donc montrer que si $(\overline{x}, \overline{y}) = (\overline{a}, \overline{b})$, alors $\overline{x+y} = \overline{a+b}$.
Supposons donc que $\overline{x} = \overline{a}$ et $\overline{y} = \overline{b}$, où $x, y, a, b \in G$.
Alors $(x+y) - (a+b) = (x-a) + (y-b)$, or $x - a \in H$ car xR_Ha et $y - b \in H$.
H étant un sous-groupe, $(x+y) - (a+b) \in H$, donc $\overline{x+y} = \overline{a+b}$.
◇ On montre facilement que la loi "+" ainsi définie sur G/H est commutative et associative.
Il est clair également que $\overline{0_G}$ est l'élément neutre et que, pour tout $x \in H$, $-\overline{x} = \overline{(-x)}$.
□

Définition. L'application $\begin{array}{ccc} G & \longrightarrow & G/H \\ x & \longmapsto & \overline{x} \end{array}$ est un morphisme surjectif de groupes, que l'on appelle la surjection canonique.

Exemple. (seul cet exemple est au programme) : Soit $n \in \mathbb{N}$. Dans le groupe abélien $(\mathbb{Z}/n\mathbb{Z}, +)$, on dispose des règles de calcul suivantes :
- Pour tout $a, b \in \mathbb{Z}$, $\overline{a} = \overline{b} \iff a \equiv b\ [n]$,
- Pour $a, b \in \mathbb{Z}$, $\overline{a + nb} = \overline{a}$,
- $\overline{0} = 0_{\mathbb{Z}/n\mathbb{Z}}$,
- pour tout $k \in \mathbb{Z}$, $-\overline{k} = \overline{-k}$,
- pour tout $h, k \in \mathbb{Z}$, $\overline{h+k} = \overline{h} + \overline{k}$,
- pour tout $h, k \in \mathbb{Z}$, $h\overline{k} = \overline{hk}$.

La dernière règle provient du fait que si l'on note φ la surjection canonique, alors $h\overline{k} = h\varphi(k) = \varphi(hk) = \overline{hk}$.

Propriété. Si $n = 0$, $\mathbb{Z}/n\mathbb{Z}$ est monogène non cyclique. Il est isomorphe à $\mathbb{Z}$.

Tout groupe monogène non cyclique est isomorphe à $\mathbb{Z}$.

Démonstration.

$\diamond$ Soit $n \in \mathbb{N}$: $\mathbb{Z}/n\mathbb{Z} = \{\overline{k}/k \in \mathbb{Z}\} = \{k\overline{1}/k \in \mathbb{Z}\} = Gr(\overline{1})$, donc $\mathbb{Z}/n\mathbb{Z}$ est toujours monogène.

$\diamond$ Dans $\mathbb{Z}/0\mathbb{Z}$, pour tout $k \in \mathbb{Z}$, $\overline{k} = \{k\}$, car la relation d'équivalence $R_{0\mathbb{Z}} = R_{\{0\}}$ est la relation d'égalité sur $\mathbb{Z}$. Ainsi, l'application $\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/0\mathbb{Z} \\ k & \longmapsto & \overline{k} = \{k\} \end{array}$ est un isomorphisme de groupes.

$\diamond$ Soit $G = Gr(a)$ un groupe monogène non cyclique. Alors l'application $\begin{array}{ccc} \mathbb{Z} & \longrightarrow & (G,.) \\ n & \longmapsto & a^n \end{array}$ est un isomorphisme de groupes. $\square$

Propriété. Si $n \geq 1$, $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique de cardinal n.
En particulier $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$.
Si $G = Gr(a)$ est un autre groupe cyclique de cardinal n, il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
En particulier, $\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & (G,.) \\ \overline{k} & \longmapsto & a^k \end{array}$ est un isomorphisme de groupes.

Démonstration.

On a déjà vu que $\mathbb{Z}/n\mathbb{Z}$ est monogène, engendré par $\overline{1}$.

$\diamond$ $k\overline{1} = \overline{0} \iff \overline{k} = \overline{0} \iff k \in n\mathbb{Z}$, donc d'après la propriété décrivant les groupes cycliques (cf page 14), $\mathbb{Z}/n\mathbb{Z}$ est cyclique de cardinal n.

$\diamond$ Supposons que $(G,.)$ est cyclique de cardinal n et que a engendre G.

Notons $f : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & (G,.) \\ k & \longmapsto & a^k \end{array}$. f est surjective. Soit $h, k \in \mathbb{Z}$ avec $h < k$.

Alors $f(h) = f(k) \iff a^{k-h} = 1 \iff k - h \in n\mathbb{Z} \iff \overline{k} = \overline{h}$, donc d'après le cours "Applications et dénombrement" page 8, $\overline{f} : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & (G,.) \\ \overline{k} & \longmapsto & a^k \end{array}$ est une bijection. C'est clairement un morphisme de groupes. $\square$

Remarque. Tous les groupes cycliques de cardinal n étant isomorphes entre eux, il suffit d'étudier l'un d'entre eux. Mais pourquoi privilégier $\mathbb{Z}/n\mathbb{Z}$, alors que l'on en connaît déjà au moins 1, à savoir $\mathbb{U}_n = \{z \in \mathbb{C}/z^n = 1\}$?

3.2 Anneaux quotients

Notation. On fixe un anneau commutatif $(A, +, .)$ et un idéal I de A.

Remarque. $(A, +)$ est un groupe commutatif et I est un sous-groupe de A, donc on dispose déjà du groupe commutatif $(A/I, +)$.

Propriété. $(A/I, +, .)$ est un anneau commutatif en posant, pour tout $x, y \in A$ $\overline{x.y} = \overline{x}.\overline{y}$.

Démonstration.

$\diamond$ Il faut à nouveau vérifier que si $x, x', y, y' \in A$ avec $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, alors $\overline{xy} = \overline{x'y'}$: en effet, $xy - x'y' = xy - x'y + x'y - x'y' = y(x - x') + x'(y - y')$, or $\overline{x} = \overline{x'}$, donc

$x - x' \in I$. De même $y - y' \in I$, or I est un idéal, donc $xy - x'y' \in I$, ce qu'il fallait démontrer.
◇ On vérifie facilement que le produit ainsi défini sur A/I est associatif et distributif par rapport à l'addition, puis que $\overline{1}$ est l'élément neutre. Ainsi $\overline{1} = 1_{A/I}$. □

Exemple. (seul cet exemple est au programme) : Avec $A = \mathbb{Z}$ et $I = n\mathbb{Z}$, où $n \in \mathbb{N}$, on dispose des régles supplémentaires de calculs suivantes :
— Pour tout $h, k \in \mathbb{Z}$, $\overline{hk} = \overline{h}.\overline{k}$.
— $\overline{1} = 1_{\mathbb{Z}/n\mathbb{Z}}$.

Exemple. Calcul de $\overline{2}^{2019}$ dans $\mathbb{Z}/17\mathbb{Z}$:
$\overline{2}^4 = \overline{16} = \overline{-1}$, donc $\overline{2}^8 = \overline{1}$. On en déduit que, pour tout $k \in \mathbb{N}$, $\overline{2}^{8k} = \overline{1}$. Or $2019 = 8 * 252 + 3$, donc $\overline{2}^{2019} = \overline{8}$.

Propriété (Hors programme) : Soit $n \in \mathbb{N}^*$.
Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $\overline{k}(\mathbb{Z}/n\mathbb{Z})$ où $k \mid n$.
En particulier, $\mathbb{Z}/n\mathbb{Z}$ est un anneau dont tous les idéaux sont principaux. En général il n'est pas intègre, donc on ne peut pas dire que $\mathbb{Z}/n\mathbb{Z}$ est un anneau principal.

Démonstration.
Soit I un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.
L'application $\begin{array}{rccc}\varphi : & \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & k & \longmapsto & \overline{k}\end{array}$ est un morphisme d'anneaux (c'est la surjection canonique de $\mathbb{Z}/n\mathbb{Z}$), donc $\varphi^{-1}(I)$ est un sous-groupe de $\mathbb{Z}$, donc il est de la forme $k\mathbb{Z}$ avec $k \in \mathbb{N}$, et $\varphi^{-1}(I)$ contient $\varphi^{-1}(\{0\}) = \text{Ker}\varphi = n\mathbb{Z}$, donc $k \mid n$.
φ étant surjective, on a $I = \varphi(\varphi^{-1}(I)) = \varphi(k\mathbb{Z}) = \overline{k}(\mathbb{Z}/n\mathbb{Z})$.
Réciproquement si $k \in \mathbb{Z}$ avec $k \mid n$, on vérifie que $\overline{k}(\mathbb{Z}/n\mathbb{Z})$ est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Il s'agit de l'idéal principal engendré par $\overline{k}$, donc cette étude montre également que les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont principaux ; □

3.3 Propriétés spécifiques de $\mathbb{Z}/n\mathbb{Z}$

Notation. On fixe $n \in \mathbb{N}$ avec $n \geq 2$.

Théorème. Soit $k \in \mathbb{Z}$.
◇ $\overline{k}$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si k et n sont premiers entre eux.
◇ $\overline{k}$ est un élément inversible de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$ si et seulement si k et n sont premiers entre eux.
Ainsi les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont exactement les inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$.

Démonstration.
◇ $\overline{k}$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si $Gr(\overline{k}) \supset \mathbb{Z}/n\mathbb{Z} = Gr(\overline{1})$, donc si et seulement si $\overline{1} \in Gr(\overline{k})$ ou encore si et seulement si il existe $h \in \mathbb{Z}$ tel que $\overline{1} = h\overline{k} = \overline{hk}$, ce qui montre que $\overline{k}$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si $\overline{k}$ est un élément inversible de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$.
◇ De plus cette dernière condition s'écrit :

$(C) \iff \exists h \in \mathbb{Z}\ \ hk \equiv 1\ [n] \iff \exists h, h' \in \mathbb{Z}\ \ hk + h'n = 1$. D'après l'identité de Bezout, (C) est équivalente à $k \wedge n = 1$. □

Exemple. Dans $\mathbb{Z}/14\mathbb{Z}$, $\overline{3}$ est inversible car 3 et 14 sont premiers entre eux. Recherchons l'inverse de $\overline{3}$.
◇ Une première méthode consiste à calculer les $\overline{3}.\overline{h}$, où $\overline{h}$ décrit $\{\overline{2}, \overline{3}, \ldots, \overline{n-1}\}$: $\overline{3}.\overline{2} = \overline{6}$, puis $\overline{3}.\overline{3} = \overline{6} + \overline{3} = \overline{9}$, puis en ajoutant successivement $\overline{3}$, $\overline{3}.\overline{4} = \overline{12}$ et enfin $\overline{3}.\overline{5} = \overline{15} = \overline{1}$, donc $\overline{3}^{\,-1} = \overline{5}$.
Cependant cette méthode n'est pas adaptée lorsque n est grand.
◇ Une seconde méthode, plus efficace, consiste à s'inspirer de la démonstration précédente : pour calculer l'inverse de $\overline{3}$, il suffit de calculer des coefficients de Bezout de 3 et 14, ce que l'on sait faire grâce à l'algorithme d'Euclide :
$14 = 3.4 + 2$ puis $3 = 2 + 1$, donc $1 = 3 - 2 = 3 - (14 - 3.4) = -14 + 5.3$, donc dans $\mathbb{Z}/14\mathbb{Z}$, $\overline{1} = \overline{5}.\overline{3}$.
◇ Ainsi, pour chercher l'inverse de $\overline{78}$ dans $\mathbb{Z}/829\mathbb{Z}$, l'algorithme d'Euclide montre que $829u + 78v = 1$ avec $u = -35$ et $v = 372$. On en déduit que $\overline{78}$ est bien inversible dans $\mathbb{Z}/829\mathbb{Z}$ et que $\overline{78}^{-1} = \overline{372}$.

Théorème. n est toujours un entier tel que $n \geq 2$.
Les propriétés suivantes sont équivalentes :
- (i) : $\mathbb{Z}/n\mathbb{Z}$ est un corps.
- (ii) : $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.
- (iii) : n est un nombre premier.

Démonstration.
◇ Si $(A, +, .)$ est un corps, c'est un anneau non nul et commutatif. De plus, si $a, b \in A$ vérifie $ab = 0$ et $a \neq 0$, alors a est inversible donc $b = a^{-1}(ab) = 0$, ce qui montre que A est intègre. Ainsi tout corps est un anneau intègre. En particulier $(i) \Rightarrow (ii)$.
Cependant il existe des anneaux intègres qui ne sont pas des corps : $\mathbb{Z}$ et $\mathbb{R}[X]$ en sont des exemples.
◇ Si n n'est pas premier, il existe $a, b \in \mathbb{N}$ tels que $2 \leq a \leq b \leq n-1$ et $n = ab$. Alors, dans $\mathbb{Z}/n\mathbb{Z}$, $\overline{a}.\overline{b} = \overline{n} = \overline{0} = 0$ et $\overline{a} \neq 0$, $\overline{b} \neq 0$, donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. On a prouvé $(ii) \Rightarrow (iii)$.
◇ Supposons enfin que n est un nombre premier. Soit $x \in \mathbb{Z}/n\mathbb{Z}$ tel que $x \neq 0$. Il existe $k \in \{0, \ldots, n-1\}$ tel que $x = \overline{k}$.
$x \neq 0$, donc $k \in \{1, \ldots, n-1\}$, or n est premier, donc k et n sont premiers entre eux. Alors d'après le théorème précédent, $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. De plus $\mathbb{Z}/n\mathbb{Z}$ est un anneau non nul et commutatif, donc c'est un corps. □

Remarque. Lorsque p est premier, le corps $\mathbb{Z}/p\mathbb{Z}$ est souvent noté $\mathbb{F}_p$ ($\mathbb{F}$ pour *field*, qui signifie *corps* en anglais).

Remarque. Soit $p \in \mathbb{P}$ avec $p \geq 3$. Soit $a, b \in \mathbb{Z}/p\mathbb{Z}$. Notons (E) : $x^2 + ax + b = 0$. C'est une équation de degré 2 dont l'inconnue x est dans $\mathbb{Z}/p\mathbb{Z}$.
$\overline{2}$ et $\overline{4}$ sont inversibles dans $\mathbb{Z}/p\mathbb{Z}$, donc on peut écrire $(E) \iff (x + \overline{2}^{-1}a)^2 = -b + \overline{4}^{-1}a^2$.
S'il existe $\delta \in \mathbb{Z}/p\mathbb{Z}$ tel que $\delta^2 = -b + \overline{4}^{-1}a^2$, alors $(E) \iff x = -\overline{2}^{-1}a \pm \delta$.

3.4 Théorème chinois

Théorème des restes chinois : Si a et b sont deux entiers supérieurs à 2 et **premiers entre eux**, alors l'application $\begin{array}{rccc} f: & \mathbb{Z}/ab\mathbb{Z} & \longrightarrow & (\mathbb{Z}/a\mathbb{Z})\times(\mathbb{Z}/b\mathbb{Z}) \\ & \overline{k} & \longmapsto & (\overline{k},\overline{k}) \end{array}$ est un isomorphisme d'anneaux.

Remarque. Le nom de *théorème des restes chinois* provient du fait que le mathématicien chinois Sun Zi du III-ième siècle a su répondre à la question suivante : "Soit une armée. Si on range les soldats par 3 il en reste 2, si on les range par 5, il en reste 3 et si on les range par 7 il en reste 2. Combien y a-t-il de soldats ?"

Démonstration.
$\diamond$ Soit $k,h\in\mathbb{Z}$ tels que ${}^{ab}\overline{k}={}^{ab}\overline{h}$. Alors $h-k\in ab\mathbb{Z}$, donc $h-k\in a\mathbb{Z}$ et $h-k\in b\mathbb{Z}$. On en déduit que $({}^{a}\overline{k},{}^{b}\overline{k})=({}^{a}\overline{h},{}^{b}\overline{h})$, ce qui prouve que f est correctement définie.
$\diamond$ On a clairement, pour tout $k,h\in\mathbb{Z}$, $f(\overline{k}+\overline{h})=(\overline{k}+\overline{h},\overline{k}+\overline{h})=f(\overline{k})+f(\overline{h})$ et $f(\overline{k}.\overline{h})=f(\overline{k}).f(\overline{h})$ (d'après la définition d'un anneau produit).
De plus $f(\overline{1})=(\overline{1},\overline{1})=1_{(\mathbb{Z}/a\mathbb{Z})\times(\mathbb{Z}/b\mathbb{Z})}$, donc f est un morphisme d'anneaux.
$\diamond$ Supposons que $\overline{k}\in Ker(f)$: ainsi $0=f(\overline{k})=(\overline{k},\overline{k})$, donc k est congru à 0 modulo a et modulo b. Ainsi k est un multiple de a et de b, donc de ab, car a et b sont premiers entre eux. On en déduit que, dans $\mathbb{Z}/ab\mathbb{Z}$, $\overline{k}=0$, donc $Ker(f)=\{0\}$ et f est injective. Enfin, $\mathbb{Z}/ab\mathbb{Z}$ et $(\mathbb{Z}/a\mathbb{Z})\times(\mathbb{Z}/b\mathbb{Z})$ ont le même cardinal, donc f est bijective. □

Remarque. La démonstration précédente prouve notamment la surjectivité de f, ce qui signifie que, pour tout $h,k\in\mathbb{Z}$, il existe $\ell\in\mathbb{Z}$ tel que $\ell\equiv h\ [a]$ et $\ell\equiv k\ [b]$. Cependant la démonstration précédente n'est pas constructive, en ce sens qu'elle ne fournit pas un algorithme permettant de calculer un tel ℓ en fonction de h et k.
Ainsi, cette preuve ne permet pas de répondre au problème de Sun Zi simplifié : "si on range les soldats par 5, il en reste 3 et si on les range par 7, il en reste 2. Combien l'armée compte-t-elle de soldats ?".
On peut fournir une preuve constructive (ce qui redémontre la surjectivité de f) :
a et b étant premiers entre eux, d'après l'identité de Bezout, il existe $u,v\in\mathbb{Z}$ tels que $ua+vb=1$. Alors $\ell=kua+hvb$ convient. En effet, $kua+hvb\equiv hua+hvb\equiv h\ [a]$ et $kua+hvb\equiv kua+kvb\equiv k\ [b]$.
En particulier, pour le problème simplifié de Sun Zi, comme $3\times5-2\times7=1$, on peut affirmer que l'armée est constituée de n soldats tel que
$n\equiv 2\times3\times5-3\times2\times7=30-42\equiv 23\ [35]$, donc il existe $k\in\mathbb{N}$ tel que $n=23+k35$.

Remarque. Lorsque a et b ne sont pas premiers entre eux, $\mathbb{Z}/ab\mathbb{Z}$ et $(\mathbb{Z}/a\mathbb{Z})\times(\mathbb{Z}/b\mathbb{Z})$ sont des groupes additifs non isomorphes.
En effet, en notant p le PPCM de a et b, pour tout $(x,y)\in(\mathbb{Z}/a\mathbb{Z})\times(\mathbb{Z}/b\mathbb{Z})$, $p.(x,y)=0$, or dans $\mathbb{Z}/ab\mathbb{Z}$, $p.\overline{1}\neq 0$ car $p<ab$ ...

Théorème chinois (généralisation) : Soit $n\geq 2$ et $a_1,\ldots,a_n$ n entiers supérieurs à 2 et **deux à deux premiers entre eux**.

Alors l'application $\begin{array}{ccc} \mathbb{Z}/(a_1 \times \cdots \times a_n)\mathbb{Z} & \longrightarrow & (\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_n\mathbb{Z}) \\ \overline{k} & \longmapsto & (\overline{k}, \ldots, \overline{k}) \end{array}$ est un isomorphisme d'anneaux.

Démonstration.
Adapter la démonstration du premier théorème. □

Remarque. Pour une preuve constructive de la surjectivité, on peut procéder par récurrence : notons $R(n)$ la propriété suivante, correspondant à la surjectivité : pour tout $h_1, \ldots, h_n \in \mathbb{Z}$, il existe $\ell \in \mathbb{Z}$ tel que, pour tout $i \in \{1, \ldots, n\}$, $\ell \equiv h_i\ [a_i]$.
On a déjà démontré $R(2)$ (et $R(1)$ est évidente).
Supposons que $n \geq 3$ et que $R(n-1)$ est vraie.
Soit $h_1, \ldots, h_n \in \mathbb{Z}$. D'après $R(n-1)$, il existe $k \in \mathbb{Z}$ tel que, pour tout $i \in \{1, \ldots, n-1\}$, $k \equiv h_i\ [a_i]$.
Posons $a = a_1 \times \cdots \times a_{n-1}$: a est premier avec a_n, donc d'après $R(2)$, il existe $\ell \in \mathbb{Z}$ tel que $\ell \equiv k\ [a]$ et $\ell \equiv h_n\ [a_n]$. Alors ℓ convient.
On peut alors résoudre le problème de Sun Zi : il suffit de chercher n tel que $n \equiv 23\ [35]$ et $n \equiv 2\ [3]$. Or $12 \times 3 - 35 = 1$, donc $n \equiv 23 \times 12 \times 3 - 2 \times 35 = 758 \equiv 23\ [105]$, ce que l'on aurait pu deviner. Si l'on sait par exemple que l'armée comprend entre 100 et 200 soldats, le nombre de soldats est égal à 128.

Exercice. Résoudre les deux systèmes $\begin{cases} x \equiv 3\ [42] \\ x \equiv 9\ [49] \end{cases}$ et $\begin{cases} x \equiv 3\ [42] \\ x \equiv 10\ [49] \end{cases}$ en l'inconnue $x \in \mathbb{N}$.

Solution : On ne peut pas appliquer directement le théorème chinois car 42 et 49 ne sont pas premiers entre eux.
$\begin{cases} x \equiv 3\ [42] \\ x \equiv 9\ [49] \end{cases} \iff \begin{cases} x \equiv 3\ [6] \\ x \equiv 3\ [7] \\ x \equiv 9\ [49] \end{cases}$, or si $x \equiv 9\ [49]$, alors $x \equiv 9 \equiv 2\ [7]$, donc ce premier système ne possède aucune solution.
$(S)\ :\ \begin{cases} x \equiv 3\ [42] \\ x \equiv 10\ [49] \end{cases} \iff \begin{cases} x \equiv 3\ [6] \\ x \equiv 3\ [7] \\ x \equiv 10\ [49] \end{cases}$, or $x \equiv 10\ [49] \implies x \equiv 3\ [7]$, donc $(S) \iff \begin{cases} x \equiv 3\ [6] \\ x \equiv 10\ [49] \end{cases}$. Or 49 et 6 sont premiers entre eux, donc on peut utiliser ce qui précède : on remarque que $49 - 6 \times 8 = 1$ donc
$(S) \iff x \equiv 3 \times 49 - 10 \times 6 \times 8 = 147 - 480\ [6 \times 49]$, ainsi l'ensemble des solutions est $255 + 294\mathbb{N}$.

Remarque. Plus généralement, pour résoudre un système de la forme
$\forall i \in \{1, \ldots, n\},\ x \equiv k_i\ [a_i]$, en l'inconnue $x \in \mathbb{Z}$, lorsque les a_i ne sont pas deux à deux premiers entre eux, on décompose chaque a_i en produit de nombres premiers afin de se ramener au cas où chaque a_i est une puissance d'un nombre premier. Lorsque le système présente plusieurs équations modulo des puissances d'un même nombre premier, on regarde si elles sont compatibles entre elles et dans ce cas on ne conserve que l'équation relative à la plus grande puissance.

3.5 L'indicatrice d'Euler

Définition. L'indicatrice d'Euler est l'application de $\mathbb{N}^*$ dans $\mathbb{N}^*$, qui à tout $n \in \mathbb{N}^*$ associe le nombre d'éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
Pour la suite, l'indicatrice d'Euler sera notée φ.

Remarque. $\varphi(1) = 1$, car $\mathbb{Z}/1.\mathbb{Z}$ est l'anneau nul, pour lequel 0 est inversible.
Pour $n \geq 2$, $\varphi(n) = \#\{k \in \{1, \dots, n-1\}/k \wedge n = 1\}$.

Propriété. Si p est un nombre premier, alors $\varphi(p) = p - 1$.

Démonstration.
Dans ce cas, $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc l'ensemble des inversibles de $\mathbb{Z}/p\mathbb{Z}$ est $\{\overline{1}, \overline{2}, \dots, \overline{p-1}\}$.
□

Propriété. Si p est premier et si $k \in \mathbb{N}^*$, alors $\varphi(p^k) = p^k - p^{k-1}$.

Démonstration.
Soit $h \in \{1, \dots, p^k - 1\}$. p étant premier,
$h \wedge p^k = 1$ si et seulement si p n'intervient pas dans la décomposition de h en produit de nombres premiers, donc si et seulement si $h \notin p\mathbb{Z}$. Ainsi,
$\varphi(p^k) = \#\Big(\{0, \dots, p^k - 1\} \setminus p\mathbb{Z}\Big) = p^k - \#\Big(\{0, \dots, p^k - 1\} \cap p\mathbb{Z}\Big)$,
puis $\varphi(p^k) = p^k - \#\{ph / 0 \leq h < \frac{p^k}{p} = p^{k-1}\} = p^k - p^{k-1}$. □

Propriété. Soit a et b sont deux entiers supérieurs à 2.
Si $a \wedge b = 1$, alors $\varphi(ab) = \varphi(a)\varphi(b)$.

Démonstration.
◇ $\varphi(ab) = \#(U(\mathbb{Z}/ab\mathbb{Z})) = \#[f(U(\mathbb{Z}/ab\mathbb{Z}))]$, où f est l'isomorphisme
$\begin{array}{ccc} \mathbb{Z}/ab\mathbb{Z} & \longrightarrow & (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z}) \\ \overline{k} & \longmapsto & (\overline{k}, \overline{k}) \end{array}$ du théorème chinois.
Mais si g est un isomorphisme d'un anneau A dans un anneau A',
alors $g(U(A)) = U(A')$: en effet, si $a' \in g(U(A))$, il existe $a \in U(A)$ tel que $a' = g(a)$.
Il existe $b \in A$ tel que $ab = ba = 1_A$,
donc $a'g(b) = g(a)g(b) = g(ab) = g(1_A) = 1_{A'}$ et $g(b)a' = 1_{A'}$, donc $a' \in U(A')$.
Réciproquement, si $a' \in U(A')$, en posant $a = g^{-1}(a')$, on vérifie que a est inversible dans A (d'inverse $g^{-1}(a'^{-1})$), donc $a' = g(a)$ avec $a \in U(A)$, ce qui montre que $a' \in g(U(A))$.
◇ On a donc $\varphi(ab) = \#[U((\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z}))]$. Mais si A et B sont deux anneaux, alors $U(A \times B) = U(A) \times U(B)$: en effet,
$\begin{aligned} (a,b) \in U(A \times B) &\iff \exists (a',b') \in A \times B \ \ (a,b).(a',b') = (a',b').(a,b) = 1_{A\times B} = (1_A, 1_B) \\ &\iff \exists (a',b') \in A \times B \ \ [aa' = a'a = 1_A \text{ et } bb' = b'b = 1_B] \\ &\iff [a \in U(A) \text{ et } b \in U(B)]. \end{aligned}$
◇ On a donc $\varphi(ab) = \#[U(\mathbb{Z}/a\mathbb{Z}) \times U(\mathbb{Z}/b\mathbb{Z})] = \varphi(a).\varphi(b)$. □

Corollaire. Soit n un entier supérieur à 2, dont la décomposition en produit de nombres premiers s'écrit $n = \prod_{i=1}^{k} p_i^{m_i}$ (où $k \geq 1$, pour tout i, $p_i \in \mathbb{P}$ et $m_i \in \mathbb{N}^*$). Alors

$$\varphi(n) = n\prod_{i=1}^{k}\Big(1-\frac{1}{p_i}\Big).$$

Démonstration.
Les $p_i^{m_i}$ étant deux à deux premiers entre eux, par récurrence sur k, on montre que $\varphi(n) = \prod_{i=1}^{k}\varphi(p_i^{m_i})$, donc $\varphi(n) = \prod_{i=1}^{k}(p_i^{m_i} - p_i^{m_i-1})$. □

Exercice. Montrer que, pour tout $n \in \mathbb{N}^*$, $n = \sum_{d\in\mathbb{N},d|n}\varphi(d)$.

Solution : C'est clair pour $n = 1$. On suppose maintenant que $n \geq 2$.
Pour tout $k \in \{1,\dots,n\}$, on sait que le rationnel $\frac{k}{n}$ admet une unique écriture irréductible $\frac{k}{n} = \frac{h}{d}$, où $d|n$ et $h \wedge d = 1$. De plus $\frac{k}{n} \in]0,1]$, donc $h \in \{1,\dots,d\}$.
Ainsi, si l'on pose pour tout entier naturel d diviseur de n,
$C_d = \{\frac{h}{d}/h \in \{1,\dots,d\}$ avec $h \wedge d = 1\}$, la famille $(C_d)_{d\in\mathbb{N},d|n}$ est une partition de $\{\frac{k}{n}/k \in \{1,\dots,n\}\}$.
Ainsi, $n = \#\Big(\{\frac{k}{n}/k \in \{1,\dots,n\}\}\Big) = \sum_{d\in\mathbb{N},d|n}\#(C_d) = \sum_{d\in\mathbb{N},d|n}\varphi(d)$.

3.6 RSA

Propriété d'Euler-Fermat : Soit $n \in \mathbb{N}$ avec $n \geq 2$ et soit $k \in \mathbb{Z}$.
Si $k \wedge n = 1$, alors $k^{\varphi(n)} \equiv 1\ [n]$.

Démonstration.
Dans $\mathbb{Z}/n\mathbb{Z}$, $\overline{k}$ est inversible, donc $\overline{k}$ est un élément du groupe multiplicatif $U(\mathbb{Z}/n\mathbb{Z})$, qui est de cardinal $\varphi(n)$. On sait alors que $\overline{k}^{\varphi(n)} = 1$. □

Corollaire. (petit théorème de Fermat) :
Si p est un nombre premier, alors pour tout $k \in \mathbb{Z}$, $k^p \equiv k\ [p]$.

Démonstration.
Si k et p sont premiers entre eux, sachant que $\varphi(p) = p-1$, d'après le théorème précédent, $k^{p-1} \equiv 1\ [p]$ et l'on conclut en multipliant par k.
Sinon, p étant premier, $k \in p\mathbb{Z}$, donc $k \equiv 0\ [p]$, puis $k^p \equiv 0 \equiv k\ [p]$. □

Exercice. Soit p un nombre premier impair tel que $-\overline{1}$ est un carré dans $\mathbb{F}_p$. Montrer que $p \equiv 1\ [4]$.

Solution :
Première solution : Par hypothèse, il existe $a \in \mathbb{F}_p$ tel que $a^2 = -\overline{1}$. Alors $a \neq 0$, donc $a^{p-1} = \overline{1}$, mais on a aussi $a^{p-1} = (a^2)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}\overline{1}$, or $\overline{1} \neq -\overline{1}$ car $p \geq 3$, donc $(-1)^{\frac{p-1}{2}} = 1$ puis $\frac{p-1}{2}$ est pair, donc $p-1 \equiv 0\ [4]$.

Seconde solution : Par hypothèse, il existe $a \in \mathbb{F}_p$ tel que $a^2 = -\overline{1}$. Notons ω l'ordre de a. $a^4 = 1$ et $a^2 \neq 1$, car $p \geq 3$, donc $\overline{1} \neq -\overline{1}$. Ainsi ω divise 4 mais ne divise pas 2. Ainsi $\omega = 4$. Or d'après le théorème de Lagrange, ω divise $|\mathbb{F}_p \setminus \{0\}| = p - 1$, donc $p \equiv 1[4]$.

Théorème RSA : On fixe deux nombres premiers p et q distincts et on pose $n = pq$. On choisit $e \in \mathbb{N}^*$ tel que $e \wedge \varphi(n) = 1$. On calcule (par exemple via l'algorithme d'Euclide) $d \in \mathbb{N}^*$ tel que dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$, $\overline{e}.\overline{d} = \overline{1}$.
Alors, pour tout $M \in \mathbb{Z}$, $M^{ed} \equiv M\ [n]$.

Démonstration.
Soit $M \in \mathbb{Z}$: $M^{ed} \equiv M\ [n] \iff M^{ed} - M \in n\mathbb{Z} = p\mathbb{Z} \cap q\mathbb{Z}$, car $p \wedge q = 1$, donc il suffit de montrer que $M^{ed} \equiv M\ [p]$ et $M^{ed} \equiv M\ [q]$.
Si $M \in p\mathbb{Z}$, alors $M^{ed} \equiv 0 \equiv M\ [p]$, car $ed \geq 1$.
Si $M \notin p\mathbb{Z}$, alors $M \wedge p = 1$ car p est premier donc d'après le théorème d'Euler-Fermat avec $\varphi(p) = p - 1$, $M^{p-1} \equiv 1\ [p]$.
D'autre part, $ed \equiv 1\ [\varphi(n)]$ et $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$, donc il existe $k \in \mathbb{Z}$ tel que $ed = 1 + k(p-1)(q-1)$. Alors $M^{ed} = M.(M^{p-1})^{k(q-1)} \equiv M\ [p]$. □

Algorithme de cryptographie RSA : R,S et A sont les initiales des trois inventeurs de cet algorithme en 1977 : Rivest, Shamir et Adleman.
Supposons que Alice souhaite transmettre à Bob un message M via un canal de communication espionné par Oscar. Comment transmettre ce message à Bob sans que Oscar n'en ait la moindre bribe ?
L'algorithme RSA préconise que Bob (ou plutôt un logiciel installé sur son ordinateur) construise p, q, n, e et d comme dans le théorème précédent mais en imposant à p et q d'être de très grands nombres premiers, de l'ordre de 2^{2000}. Même avec une telle contrainte, on sait construire de telles quantités selon des algorithmes polynomiaux efficaces : construction probabiliste de grands nombres premiers, produit pour calculer $pq = n$ et $(p-1)(q-1) = \varphi(n)$, construction de e, calcul de d par l'algorithme d'Euclide.
Bob publie au monde entier ses "clés publiques" : n et e. Oscar en a donc connaissance, ainsi qu'Alice.
Alice découpe son message en sous-messages qui, codés en bits, sont de longueurs inférieures à $\ln_2(n)$ (ici $\ln_2(n)$ est de l'ordre de 2000). Notons encore M un sous-message à transmettre. C'est une suite de moins de 2000 bits, que l'on peut donc identifier à un entier toujours noté M, avec $M < n$.
Alice calcule alors le reste de la division euclidienne de M^e par n, ce qui constitue le message codé M', qu'elle envoie à Bob.
Bob récupère le message M' et calcule le reste de la division euclidienne de M'^d par n. Il obtient ainsi $M'' \in [0, n[\cap\mathbb{N}$ tel que, modulo n, $M'' \equiv M'^d \equiv M^{ed} \equiv M$ d'après le théorème RSA. Mais $M, M' \in [0, n[$, donc $M'' = M$ et Bob a ainsi décodé le message d'Alice.
De son côté, Oscar a récupéré n, e et M^e. On conjecture que Oscar n'a pas d'autre moyen pour retrouver M, de calculer d puis M^{ed} modulo n (il existe de nombreux moyens de casser RSA par d'autres procédés, mais seulement si RSA est mal utilisé).

Calculer d connaissant e et $n = pq$ peut sembler facile : il suffit de factoriser n pour récupérer p et q, ce qui permet de calculer $\varphi(n) = (p-1)(q-1)$ puis un d tel que $ed \equiv 1\ [\varphi(n)]$.
Là encore, on conjecture (mais ce n'est pas démontré) qu'il n'y a pas d'autres moyens de récupérer d.
Ce qui est en fait difficile dans cette récupération de d, c'est la factorisation de $n = pq$ permettant de récupérer p et q. Autant le produit de p par q pour obtenir n est réalisable selon des algorithmes polynomiaux efficaces, autant l'opération inverse de factorisation de n est d'une grande complexité : actuellement les meilleurs algorithmes connus de factorisation de n sont sous-exponentiels en fonction du nombre de bits de n, ce qui signifie qu'ils ne sont pas utilisables dès que $\ln_2(n)$ est suffisamment grand même si l'on dispose d'un supercalculateur pendant quelques années.
Mais on ne sait pas démontrer qu'il n'existe pas un algorithme polynomial de factorisation, pour des ordinateur classiques. On espère donc que c'est faux, ou bien qu'Oscar n'en dispose pas.
On dispose en fait d'un algorithme polynomial, mais il ne peut fonctionner que sur un ordinateur quantique.

3.7 Caractéristique d'un anneau (hors programme)

Notation. On fixe un anneau commutatif noté A.
Notons $\varphi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & A \\ m & \longmapsto & m.1_A \end{array}$. φ est un morphisme d'anneaux dont le noyau est $Ker(\varphi) = \{m \in \mathbb{Z} / m.1_A = 0_A\}$, or $Ker(\varphi)$ est un idéal de $\mathbb{Z}$, qui est principal, donc il existe $n \in \mathbb{N}$ tel que $Ker(\varphi) = n\mathbb{Z}$.
Si $n = 0$, alors φ est injectif et pour tout $m \in \mathbb{N}^*$, $m.1_A \neq 0_A$.
Si $n \geq 1$, alors $\{m \in \mathbb{N}^* \ / \ m.1_A = 0_A\}$ est non vide et n est son minimum. Cela justifie la définition suivante et cela prouve la propriété qui suit.

Définition. S'il existe $n \in \mathbb{N}^*$ tel que $n.1_A = 0_A$, la caractéristique de A est

$$\text{car}(A) \triangleq \min\{n \in \mathbb{N}^* \ / \ n.1_A = 0_A\}.$$

Sinon, on convient que $\text{car}(A) = 0$.

Remarque. $\varphi(\mathbb{Z}) = \mathbb{Z}.1_A$ est le groupe engendré par 1_A. Il est monogène.
Il est cyclique si et seulement si $\text{car}(A) \neq 0$.

Propriété. Soit A un anneau de caractéristique n.
Alors, pour tout $m \in \mathbb{Z}$, $m.1_A = 0_A \iff n|m$.

Exemples. L'anneau nul est l'unique anneau de caractéristique 1.
Pour tout $n \in \mathbb{N}$, $\text{car}(\mathbb{Z}/n\mathbb{Z}) = n$.
$\text{car}(\mathbb{R}) = 0$.

Propriété. Deux anneaux isomorphes ont la même caractéristique.

Démonstration.
Soit f un isomorphisme entre deux anneaux A et B.
Pour tout $k \in \mathbb{N}^*$, $k.1_B = 0 \iff f(k.1_A) = 0 \iff k.1_A = 0$. □

Reprenons les notations du début de ce paragraphe.
Pour tout $h, k \in \mathbb{Z}$, $\varphi(h) = \varphi(k) \iff h - k \in n\mathbb{Z} \iff h \equiv k\ [n]$, donc l'application $\begin{array}{rccc} \overline{\varphi} : & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \varphi(\mathbb{Z}) = \mathbb{Z}.1_A \\ & \overline{m} & \longmapsto & m.1_A \end{array}$ est bien définie et elle est bijective. Or c'est un morphisme d'anneaux, donc $\mathbb{Z}.1_A$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, où $n = \text{car}(A)$. Ainsi,

Propriété. Si $\text{car}(A) = 0$, alors le plus petit sous-anneau de A est isomorphe à $\mathbb{Z}$. Sinon, il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, où $n = \text{car}(A)$.

Corollaire. Un anneau de caractéristique nulle est de cardinal infini.

Remarque. La réciproque est fausse, car pour tout $n \in \mathbb{N}^*$, l'anneau $(\mathbb{Z}/n\mathbb{Z})[X]$ est infini mais de caractéristique n non nulle.

Propriété. Si A est intègre et $\text{car}(A) \neq 0$, alors $\text{car}(A) \in \mathbb{P}$.

Démonstration.
Posons $n = \text{car}(A)$ et supposons que $n = pq$.
Alors $(p.1_A)(q.1_A) = n.1_A = 0_A$, or A est intègre, donc $p.1_A = 0$ ou bien $q.1_A = 0$. Or $n \in \mathbb{N}^*$, donc $1 \leq p, q \leq n$. Alors, d'après la définition de $\text{car}(A)$, $p = n$ ou $q = n$. Ceci démontre que n est premier. □

Propriété. On suppose que A est un anneau commutatif de caractéristique $p \in \mathbb{P}$. Alors l'application $x \longmapsto x^p$ est un endomorphisme sur A, appelé l'endomorphisme de Frobenius.

Démonstration.
Posons $\begin{array}{rccc} f : & A & \longrightarrow & A \\ & x & \longmapsto & x^p \end{array}$. $f(1_A) = 1_A$.
Soit $x, y \in A$. $f(xy) = f(x)f(y)$ car A est commutatif.
D'après la formule du binôme de Newton, $f(x+y) = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$.
Soit $k \in \{1, \ldots, p-1\}$: $k \geq 1$, donc $p \mid p(p-1)\cdots(p-k+1) = \binom{p}{k} k!$, or $k < p$, donc $p \wedge (k!) = 1$. Alors d'après le théorème de Gauss, $p \mid \binom{p}{k}$, donc $\binom{p}{k}.1_A = 0$.
On en déduit que $(x+y)^p = x^p + y^p$. □

Notation. Pour toute la suite de ce paragraphe, $\mathbb{K}$ désigne un corps quelconque.

Propriété. La caractéristique d'un corps est ou bien nulle, ou bien un nombre premier.

Démonstration.
Tout corps est intègre. □

Propriété. On appelle sous-corps premier de $\mathbb{K}$ le plus petit sous-corps de $\mathbb{K}$.
— Si $p = \text{car}(\mathbb{K}) \in \mathbb{P}$, le sous-corps premier de $\mathbb{K}$ est $\mathbb{Z}.1_{\mathbb{K}}$, il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

— Si $\text{car}(\mathbb{K}) = 0$, le sous-corps premier de $\mathbb{K}$ est $\{(p.1_\mathbb{K})(q.1_\mathbb{K})^{-1} \ / \ p \in \mathbb{Z}, q \in \mathbb{N}^*\}$. Il est isomorphe à $\mathbb{Q}$. En particulier, $\mathbb{K}$ est de cardinal infini.

Démonstration.
Lorsque $\text{car}(\mathbb{K}) \in \mathbb{P}$, on sait déjà que $\mathbb{Z}.1_\mathbb{K}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, lequel est un corps car $p \in \mathbb{P}$, donc $\mathbb{Z}.1_\mathbb{K}$ est un corps. C'est bien le plus petit sous-corps de $\mathbb{Z}$.
Supposons maintenant que $\text{car}(\mathbb{K}) = 0$.
Pour tout $q \in \mathbb{N}^*$, $q.1_\mathbb{K} \neq 0_\mathbb{K}$, donc on peut définir $\begin{array}{rccc} \varphi : & \mathbb{Q} & \longrightarrow & \mathbb{K} \\ & \frac{p}{q} & \longmapsto & (p.1_\mathbb{K})(q.1_\mathbb{K})^{-1} \end{array}$.
φ est bien définie car pour tout $r \in \mathbb{Z}^*$, $(rp.1_\mathbb{K})(rq.1_\mathbb{K})^{-1} = (p.1_\mathbb{K})(q.1_\mathbb{K})^{-1}$.
Si $\frac{p}{q}, \frac{r}{s} \in \mathbb{Q}$, avec $p, r \in \mathbb{Z}$ et $q, s \in \mathbb{N}^*$, alors

$$\begin{aligned} \varphi\Big(\frac{p}{q} + \frac{r}{s}\Big) &= \varphi\Big(\frac{ps + rq}{qs}\Big) = ((ps + rq).1_\mathbb{K})(qs.1_\mathbb{K})^{-1} \\ &= (ps.1_\mathbb{K})(qs.1_\mathbb{K})^{-1} + (rq.1_\mathbb{K})(qs.1_\mathbb{K})^{-1} = \varphi\Big(\frac{p}{q}\Big) + \varphi\Big(\frac{r}{s}\Big). \end{aligned}$$

On vérifie également que $\varphi(1) = 1$ et que $\varphi(\frac{p}{q} \times \frac{r}{s}) = \varphi(\frac{p}{q}) \times \varphi(\frac{r}{s})$, donc φ est un morphisme de corps. À ce titre, il est injectif,
donc $\varphi(\mathbb{Q}) = \{(p.1_\mathbb{K})(q.1_\mathbb{K})^{-1} \ / \ p \in \mathbb{Z}, q \in \mathbb{N}^*\}$ est un sous-corps de $\mathbb{K}$, isomorphe à $\mathbb{Q}$.
C'est clairement le plus petit sous-corps de $\mathbb{K}$. □

Remarque. On admettra que pour tout $p \in \mathbb{P}$ et $n \in \mathbb{N}^*$, il existe un corps fini de cardinal p^n, unique à un isomorphisme près de corps. Il est noté $\mathbb{F}_{p^n}$. On a $\text{car}(\mathbb{F}_{p^n}) = p$.
Attention : lorsque $n \geq 2$, $\mathbb{F}_{p^n} \neq \mathbb{Z}/p^n\mathbb{Z}$.

Propriété. On suppose que $\text{car}(\mathbb{K}) = p \neq 0$.
On désigne par f l'endomorphisme de Frobenius de $\mathbb{K}$.
f est injectif, comme tout morphisme de corps.
Si $\mathbb{K}$ est fini, f est un automorphisme de corps.
Lorsque $\mathbb{K} = \mathbb{F}_p$, $f = Id_{\mathbb{F}_p}$ d'après le petit théorème de Fermat.