Table des matières

Chapitre 1

Groupes

1.1 Définitions, exemples

1.1.1 Rappels

Définition 1.1.1. On appelle *groupe* tout ensemble muni d'une loi de composition interne, associative, possédant un élément neutre, et dans lequel tout élément est symétrisable. Le groupe est dit *commutatif ou abélien* lorsque sa loi est commutative.

Remarque 1.1.2.
- Un groupe n'est jamais vide : il a au moins un élément neutre. Un gropue est dit *multiplicatif* (resp. additif) si sa loi est + (resp. $\times$).
- Si l'ensemble G est fini, on dit que G est un groupe fini, et le cardinal de G est appelé *ordre* de G.
- Par abus de langage et lorsqu'il n'y a aucune ambiguïté, on dit souvent " soit G un groupe ... " sans préciser la loi.
- Dans un groupe, tout élément est régulier, puisqu'inversible.

Exemple 1.1.3. Chacun des ensembles $\mathbb{Z}$, $\mathbb{Q}$ est un groupe additif abélien et $\mathbb{Q}^*$ est un groupe multiplicatif abélien.

Définition 1.1.4. Soit $(G, \star)$ un groupe d'élément neutre e. Pour $x \in G$ et $n \in \mathbb{N}^*$, l'élément :

$$x^n = \underbrace{x \star x \star \cdots \star x}_{\text{n fois}}$$

appelé *itéré* $n^{ème}$ de x est défini par récurrence :

$$x^0 = e \text{ et } x^{n+1} = x \star (x^n) \text{ si } n \geq 0.$$

Proposition 1.1.5. *Soient $(G, \star)$ un groupe et $x \in G$.*
1. *Pour tous $m, n \in \mathbb{Z}$, on a :*

$$x^m \star x^n = x^{m+n},\ (x^n)^{-1} = x^{-n} \text{ et } (x^m)^n = x^{mn}. \tag{1.1}$$

2. *Soit $y \in G$ un élément commutant avec x. Pour tout $n \in \mathbb{Z}$, on a :*

$$(x \star y)^n = x^n \star y^n. \tag{1.2}$$

Démonstration. Ces propriétés se démontrent aisement par récurrence si m et n sont des entiers naturels. Par passage à l'inverse, on en déduit les résultats pour m et n entiers relatifs quelconques. □

1.1.2 Sous groupe

Définition 1.1.6. Soit $(G, \star)$ un groupe. Une partie H de G est appelée *sous-groupe* de G, si elle vérifie les conditions suivantes :
1. La partie H n'est pas vide.
2. La partie H est stable pour la loi $\star$.
3. Pour tout $x \in H$, le symétrique de x appartient aussi à H.

Les conditions 1, 2 et 3 sont équivalentes aux conditions *i* et *ii* ci-après :

Proposition 1.1.7. *Soit $(G, \star)$ un groupe d'élément neutre e. Une partie H de G est un sous-groupe de G si, et seulement si, elle vérifie les conditions suivantes :*
i. L'élément neutre e de G appartient à H.
ii. Pour tous $x, y \in H$, $x \star y^{-1}$ appartient aussi à H.

Démonstration. Supposons que H est un sous groupe de G. Soit $a \in H$ (condition 1). Puisque $a^{-1} \in H$ (condition 3), alors $e = a \star a^{-1} \in H$ (condition 2). Ensuite, si $x, y \in H$, alors $y^{-1} \in H$ (condition 3), puis $x \star y^{-1} \in H$ (condition 2).

Supposons que H vérifie i et ii. Puisque $e \in H$, alors H n'est pas vide ; donc 1 est vérifié. Si $x \in H$, $x^{-1} = e \star x^{-1} \in H$ et 3 est vérifiée. Si $x, y \in H$, on a $y^{-1} \in H$, donc $x \star (y^{-1})^{-1} = x \star y \in H$ et ainsi H est stable pour $\star$. □

Exemple 1.1.8.
1. Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$.
2. Noter que $\mathbb{Z}$ est un sous-groupe de $(\mathbb{Q}, +)$.
3. Les ensembles $\mathbb{Q}_+^*$ et $\{-1, 1\}$ sont des sous-groupes de $(\mathbb{Q}^*, \times)$.
4. Dans un groupe G d'élément neutre e, G et $\{e\}$ sont des sous-groupes de G et $\{e\}$ est appelé *sous-groupe trivial* de G.

Définition 1.1.9. Soient G un groupe et S une partie de G. On appelle *sous-groupe de G engendré par S* l'intersection de tous les sous-groupes de G contenant S, et ce groupe est noté $\langle S \rangle$.
Si $\langle S \rangle = G$, on dit que *S engendre G ou est une partie génératrice de G.*

Notation 1.1.10. Si $S := \{a_1, a_2, \ldots, a_n\}$ est fini, alors on écrit simplement $\langle a_1, a_2, \ldots, a_n \rangle$ au lieu de $\langle \{a_1, a_2, \ldots, a_n\} \rangle$.

Remarque 1.1.11. Soit S une partie d'un groupe G. Le sous-groupe $\langle S \rangle$ est, pour l'inclusion, le plus petit sous-groupe de G contenant S.

Proposition 1.1.12. *Soient G un groupe et $x \in G$. Alors $\langle x \rangle$ est formé des puissances x^n de x, n décrivant $\mathbb{Z}$.*

Démonstration. Posons $A := \{x^n \mid n \in \mathbb{Z}\}$. A est un sous-groupe de G contenant x, donc $A \supset \langle x \rangle$. Or $\langle x \rangle$ est un sous-groupe de G contenant x, il contient x^n pour tout entier $n \geq 0$. Si $n < 0$, $\langle x \rangle$ contient x^{-n}, donc son inverse x^n. Ainsi $\langle x \rangle \supset A$. □

Définition 1.1.13. Un groupe G est dit *monogène* s'il existe $x \in G$ tel que $\langle x \rangle = G$. Un tel x est dit *générateur* de G. Un groupe monogène fini est dit *cyclique*.

Remarque 1.1.14. La réunion de deux sous-groupes d'un groupe G n'est pas, en général, un sous-groupe de G. En effet, la réunion $F = 2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas additivement stable car $2 \in F$ et $3 \in F$ mais $5 \notin F$.

1.1.3 Morphismes de groupes

Définitions et premières propriétés

Définition 1.1.15. Soient $(G_1, \star_1)$ et $(G_2, \star_2)$ deux groupes. On dit qu'une application f de G_1 dans G_2 est un *morphisme de groupe* de $(G_1, \star_1)$ dans $(G_2, \star_2)$ si :

$$\forall (x, y) \in G_1^2,\ f(x \star_1 y) = f(x) \star_2 f(y). \tag{1.3}$$

- Un morphisme bijectif est appelé *isomorphisme*.
- Un morphisme de $(G, \star)$ dans lui-même est appelé endomorphisme de G.
- Un endomorphisme bijectif est appelé *automorphisme*.

Exemple 1.1.16.
1. La fonction logarithme est un isomorphisme de $(\mathbb{R}_+^*, \times)$ sur $(\mathbb{R}, +)$.
   Sa réciproque, l'exponentielle, est un isomorphisme de $(\mathbb{R}, +)$ sur $(\mathbb{R}_+^*, \times)$.
2. L'identité est un automorphisme de $(G, \star)$.
3. Soit $x \in \mathbb{Z}$.
   - L'application $\mathbb{Z} \longrightarrow \mathbb{Z}$, $n \longmapsto nx$ est un endomorphisme de $(\mathbb{Z}, +)$.
   - L'application $\mathbb{Z} \longrightarrow \mathbb{Z}$, $n \longmapsto x^n$ est un morphisme de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}, \times)$.
4. Soit $(G, \star)$ un groupe. La régle $x^m \star x^n = x^{m+n}$ de calcul sur les itérés peut s'énoncer en disant que l'application : $\mathbb{Z} \longrightarrow G$, $n \longmapsto x^n$ est un morphisme de $(\mathbb{Z}, +)$ dans $(G, \star)$.

Proposition 1.1.17. *La composée de deux morphismes de groupes est un morphisme de groupes.*

Démonstration. Soient $f : (G_1, \star_1) \longrightarrow (G_2, \star_2)$ et $g : (G_2, \star_2) \longrightarrow (G_3, \star_3)$ deux morphismes de groupes. Pour $(x, y) \in G_1^2$, on a :

$$\begin{aligned} g \circ f(x \star_1 y) &= g(f(x \star_1 y)) \\ &= g(f(x) \star_2 f(y)) \\ &= g(f(x)) \star_3 g(f(y)) \\ &= (g \circ f)(x) \star_3 (g \circ f)(y) \end{aligned}$$

□

Proposition 1.1.18. *La réciproque d'un isomorphisme de groupes est un isomorphisme de groupes.*

Démonstration. Soient f un isomorphisme de groupes de $(G_1, \star_1)$ dans $(G_2, \star_2)$ et $(x, y) \in G_1^2$. On a $f(f^{-1}(x) \star_1 f^{-1}(y)) = f(f^{-1}(x)) \star_2 f(f^{-1}(y)) = x \star_2 y = f(f^{-1}(x \star_2 y))$, et puisque f est injective, on en déduit que $f^{-1}(x) \star_1 f^{-1}(y) = f^{-1}(x \star_2 y)$. □

Proposition 1.1.19. *Soient $(G_1, \star_1)$ et $(G_2, \star_2)$ deux groupes d'éléments neutres respectifs e_1 et e_2, ainsi que f un morphisme de groupes de G_1 dans G_2. On a :*
1. $f(e_1) = e_2$.
2. $\forall x \in G_1$, $(f(x))^{-1} = f(x^{-1})$.
3. $\forall x \in G_1$, $\forall n \in \mathbb{Z}$, $(f(x))^n = f(x^n)$.

Démonstration.

- On a
$$e_2 \star_2 f(e_1) = f(e_1) = f(e_1 \star_1 e_1) = f(e_1) \star_2 f(e_1).$$
En simplifiant par $f(e_1)$ qui est régulier dans le groupe G_2, on en déduit que $f(e_1) = e_2$.
- D'autre part
$$f(x) \star_2 f(x^{-1}) = f(x \star_1 x^{-1}) = f(e_1) = e_2$$
et de même
$$f(x^{-1}) \star_2 f(x) = e_2$$
ce qui prouve que le symétrique de $f(x)$ est $f(x^{-1})$.
- Une récurrence permet de prouver la dernière formule pour $n \in \mathbb{N}$. Pour $n \in \mathbb{Z}$, on écrit alors
$$f(x)^n = (f(x)^{-n})^{-1} = f((x^{-n})^{-1}) = f(x^n).$$

□

Exemple 1.1.20. Dans le cas particulier de la fonction logarithme, on obtient :

$$\ln 1 = 0 \text{ et } \forall x > 0,\ \ln\left(\frac{1}{x}\right) = -\ln x.$$

Noyau, image

Soient G et G' deux groupes d'éléments neutres respectifs e et e', ainsi que f un morphisme de groupes de G dans G'.

Proposition 1.1.21.
1. *Si H est un sous-groupe de G, alors $f(H)$ est un sous-groupe de G'.*
2. *Si H' est un sous-groupe de G', alors $f^{-1}(H')$ est un sous-groupe de G.*

Démonstration. Soit H un sous-groupe de $(G, \star)$ et $H'_0 = f(H)$. Comme H contient l'élément neutre e de G, H'_0 contient $e' = f(e)$ qui est l'élément neutre de $(G', \diamond)$. Soit $(y, y') \in H'^2_0$. Prenons $(x, x') \in H^2$ tel que $y = f(x)$ et $y' = f(x')$. Alors $y \diamond y' = f(x) \diamond f(x') = f(x \star x') \in H'_0$ puisque $x \star x' \in H$. Aussi $y^{-1} = (f(x))^{-1} = f(x^{-1}) \in H'_0$ puisque $x^{-1} \in H$. Donc H'_0 est un sous-groupe de G'.

Soit H' un sous-groupe de G' et $H_0 = f^{-1}(H')$. Comme $f(e) = e' \in H'$, on a $e \in H_0$. Soit $(x, x') \in H_0^2$. Alors $f(x) \in H'$ et $f(x') \in H'$ et puisque H' est un sous-groupe, on a : $f(x \star x') = f(x) \diamond f(x') \in H'$ et $f(x^{-1}) = f(x)^{-1} \in H'$. Par suite $x \star x'$ et x^{-1} appartiennent à H_0. Donc H_0 est un sous-groupe de G. □

Corollaire 1.1.22. *Soit f un morphisme de groupes de $(G, \star)$ dans $(G', \diamond)$*
1. *$f(G)$, l'image de f, est un sous-groupe de G'. On le note $Im(f)$.*
2. *L'ensemble $f^{-1}(\{e'\})$, appelé noyau de f est un sous-groupe de G. On le note* $\ker(f)$.

Théorème 1.1.23. *Soit f un morphisme de groupes de $(G, \star)$ dans $(G', \diamond)$. Le morphisme f est injective si, et seulement si,* $\ker(f) = \{e\}$, *i.e.*

$$\forall x \in G,\ f(x) = e' \Longrightarrow x = e. \tag{1.4}$$

Démonstration.
- La relation (1.4) signifie $\ker(f) \subset \{e\}$, ce qui est bien équivalent à $\ker(f) = \{e\}$ puisque $\ker(f)$ étant un sous-groupe de G, il contient l'élément e.

- Supposons f est injective. Si $x \in \ker(f)$, alors $f(x) = e' = f(e)$ entraîne $x = e$ puisque f est injective.
- Supposons que $\ker(f) = \{e\}$. Soit $(x, y) \in G^2$ tels que $f(x) = f(y)$. On a $f(x \star y^{-1}) = f(x) \diamond f(y^{-1}) = f(x) \diamond f(y)^{-1} = e'$, i.e. $x \star y^{-1} \in \ker(f)$. Donc $x \star y^{-1} = e$, ce qui donne $x = y$. On en déduit que f est injective.

□

1.2 Groupe symétrique

1.2.1 Définitions

Notation 1.2.1. Soit $n \in \mathbb{N}^*$. On note S_n l'ensemble des permutations de l'ensemble $\{1, \ldots, n\}$, i.e. des bijections de $\{1, \ldots, n\}$ dans lui-même. Si $n = 1$, on a $S_n = \{Id\}$. Dans la suite, sauf mention contraire, nous supposerons $n \geq 2$.

Proposition 1.2.2. *Muni de la composition des applications, S_n est un groupe de cardinal $n!$ et l'on appelle groupe symétrique.*

Si $(\sigma, \tau) \in S_n^2$, le composé $\sigma \circ \tau$ est noté $\sigma\tau$ et appelé *produit des éléments* σ et τ.

Exemple 1.2.3.

1. Étant donnés deux éléments distincts i et j de $\{1, \ldots, n\}$, l'application τ définie par :

$$\tau(i) = j,\ \tau(j) = i \text{ et } \forall k \notin \{i, j\},\ \tau(k) = k$$

   est une *involution* donc une permutation de $\{1, \ldots, n\}$; on la note (i, j) ou $\tau_{i,j}$ ou $\tau_{j,i}$. Une telle permutation est appelée *transposition*.
2. $(S_2, \circ)$ est constitué de deux éléments : 'identité et la transposition $\tau_{1,2}$. Sa *table de Pythagore* est définie par :

$\circ$	Id	$\tau_{1,2}$
Id	Id	$\tau_{1,2}$
$\tau_{1,2}$	$\tau_{1,2}$	Id

3. Étant donné un entier $p \geq 2$, ainsi que des éléments distincts $a_1, a_2, \ldots, a_p$ de $\{1, \ldots, n\}$, l'application σ définie par :

$$\begin{aligned} \forall x \notin \{a_1, a_2, \ldots, a_p\},\ \sigma(x) &= x \\ \forall i \in \{1, 2, \ldots, p-1\},\ \sigma(a_i) &= a_{i+1} \\ \sigma(a_p) &= a_1 \end{aligned}$$

   est une permutation de $\{1, \ldots, n\}$ que l'on note $(a_1, a_2, \ldots, a_p)$. Une telle permutation est appelée *p-cycle ou cycle d'ordre p*. L'inverse du p-cycle $(a_1, a_2, \ldots, a_p)$ est le p-cycle $(a_p, \ldots, a_2, a_1)$.

Proposition 1.2.4. *Si $n \geq 3$, le groupe S_n n'est pas commutatif.*

Démonstration. Il suffit de vérifier par exemple

$$(1, 2)(1, 3) = (3, 2, 1) \text{ et } (1, 3)(1, 2) = (1, 2, 3)$$

□

1.2.2 Décomposition d'une permutation en produit de transpositions

Proposition 1.2.5. *Toute permutation de* $\{1, 2, \ldots, n\}$ *est un produit de transpositions.*

Démonstration. On montre le résultat par récurrence
1. $S_2 = \{Id, \tau_{1,2}\}$. On a $Id = \tau_{1,2} \circ \tau_{1,2}$ et $\tau_{1,2}$ est une transposition et donc un produit de une transposition.
2. Supposons le résultat pour n. Soit $\sigma \in S_{n+1}$.
   - Si $\sigma(n+1) = n+1$, la restriction de σ à $\{1, 2, \ldots, n\}$ réalise une permutation de $\{1, 2, \ldots, n\}$ que l'on note $\widetilde{\sigma}$. Vérifions le.
     L'image par $\widetilde{\sigma}$ d'un élément de $\{1, 2, \ldots, n\}$ est un élément de $\{1, 2, \ldots, n+1\}$ qui n'est pas $n+1$. Donc $\widetilde{\sigma}$ est bien une application de $\{1, 2, \ldots, n\}$ dans lui-même. L'application $\widetilde{\sigma}$ est injective car σ l'est. Enfin, tout élément de $\{1, 2, \ldots, n\}$ a un antécédent par σ dans $\{1, 2, \ldots, n+1\}$ qui n'est pas $n+1$ ou encore tout élément de $\{1, 2, \ldots, n\}$ à un antécédent par $\widetilde{\sigma}$ dans $\{1, 2, \ldots, n\}$ et $\widetilde{\sigma}$ est surjective. Finalement, $\widetilde{\sigma}$ est une permutation de $\{1, 2, \ldots, n\}$.
     Par hypothèse de récurrence, $\widetilde{\sigma}$ est un produit de transpositions $\widetilde{\tau_1}, \ldots, \widetilde{\tau_k}$ de $\{1, 2, \ldots, n\}$. On prolonge ces transpositions à $\{1, 2, \ldots, n+1\}$ en posant pour tout $i \in \{1, \ldots, k\}$, $\tau_i(n+1) = n+1$ et on obtient des transpositions de $\tau_1, \ldots, \tau_k$ de $\{1, 2, \ldots, n+1\}$ telles que $\sigma = \tau_1 \circ \cdots \circ \tau_k$.
   - Si $\sigma(n+1) \neq n+1$, soit $i = \sigma(n+1)$ puis $\sigma' = \tau_{i,n+1} \circ \sigma$. L'application σ' est une permutation de $\{1, 2, \ldots, n+1\}$ qui fixe $n+1$. D'après le cas précédent, il existe des transpositions $\tau_1, \ldots, \tau_k$ telles que $\tau_{i,n+1} \circ \sigma = \sigma' = \tau_1 \circ \cdots \circ \tau_k$. Mais alors, $\sigma = \tau_{i,n+1} \circ \tau_1 \cdots \circ \tau_k$.

□

La démonstration précédente fournit une demarche pratique pour décomposer une permutation en produit de transpositions. On fixe petit à petit les éléments de $\{1, \ldots, n\}$, en commençant par n puis en descendant, en composant à gauche par des transpositions.

Exemple 1.2.6. Décomposons en produit de transposition la permutaion $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 7 & 6 & 3 & 4 \end{pmatrix}$. Nous avons

$$\tau_{4,7} \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 4 & 6 & 3 & 7 \end{pmatrix}.$$

$$\tau_{3,6} \circ \tau_{4,7} \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 4 & 3 & 6 & 7 \end{pmatrix}.$$

$$\tau_{3,5} \circ \tau_{3,6} \circ \tau_{4,7} \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 4 & 5 & 6 & 7 \end{pmatrix}.$$

Ainsi $\tau_{3,5} \circ \tau_{3,6} \circ \tau_{4,7} \circ \sigma = \tau_{1,3}$. On en déduit que $\sigma = \tau_{4,7} \circ \tau_{3,6} \circ \tau_{3,5} \circ \tau_{1,3}$.

1.2.3 Signature

Définition 1.2.7. Soient $n \geq 2$ puis $\sigma \in S_n$. La *signature* de σ est $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$.

Remarque 1.2.8. Par convention, on pose $\varepsilon(Id) = 1$.

Exemple 1.2.9. On cpnsidère la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$. On a

$$\begin{aligned} \varepsilon(\sigma) &= \frac{2-4}{1-2} \times \frac{2-3}{1-3} \times \frac{2-1}{1-4} \times \frac{4-3}{2-3} \times \frac{4-1}{2-4} \times \frac{3-1}{3-4} \\ &= (-1)^4 \\ \varepsilon(\sigma) &= 1 \end{aligned}$$

Définition 1.2.10. Soit $\sigma \in S_n$. On dit qu'un couple (i, j) d'élément de $\{1, \ldots, n\}$ est une *inversion* de σ si $i < j$ et $\sigma(i) > \sigma(j)$. On note $I(\sigma)$ le nombre d'inversion de σ.

Théorème 1.2.11. *Soient $n \geq 2$ un entier et $\sigma \in S_n$. La signature de σ est $\varepsilon(\sigma) = (-1)^N$ où N est le nombre d'inversion de σ.*

Démonstration. Soient $n \geq 2$ puis $\sigma \in S_n$. Soit N le nonbre d'inversion de σ.

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} = \frac{\prod_{1 \leq i < j \leq n} \sigma(i) - \sigma(j)}{\prod_{1 \leq i < j \leq n} i - j}.$$

□

Définitions 1.2.12.
- Une *permutation paire* est une permutation de signature 1.
- Une *permutation impaire* est une permutation de signature -1.

Proposition 1.2.13. *La signature d'une transposition est égale à -1.*

Démonstration. il s'agit de compter le nombre d'inversion d'une transposition. Soient $i, j \in \{1, 2, \ldots, n\}$ tels que $i < j$ et $\tau = \tau_{i,j}$.

1. Une paire $\{k, l\}$ telle que $1 \leq k < l \leq n$ et $\{k, l\} \cap \{i, j\} = \emptyset$ n'est pas une inversion de τ car $\tau(k) = k < l \leq \tau(l)$.
2. La paire (i, j) est une inversion de σ car $\tau(i) = j > i = \tau(j)$.
3. Il reste à analyser les paires $\{i, k\}$ où $k \notin \{i, j\}$ et les paires $\{j, k\}$ où $k \notin \{i, j\}$.
   - Si $k < i$, alors $\tau(k) = k < i < j = \tau(i)$. Une paire $\{i, k\}$ telle que $k < i$ n'est pas une inversion de τ.
   - Si $k > j$, alors $\tau(k) = k > j = \tau(i)$. Une paire $\{k, i\}$ telle que $k > j$ n'est pas une inversion de τ.
   - Si $i < k < j$, alors $\tau(i) = j > k = \tau(k)$. Une paire $\{k, i\}$ telle que $i < k < j$ est une inversion de τ.

     Au total, il y a $j - 1 - i$ paires $\{i, k\}$ telles que $k \notin \{i, j\}$ qui sont des permutations de τ (y compris si $j = i + 1$).

   De même, il y a $j - 1 - i$ paires $\{j, k\}$ telles que $k \notin \{i, j\}$ qui sont des permutations de τ.

Au total, le nombre d'inversions de τ est $N = 2(j - 1 - i) + 1$. En particulier, τ admet un nombre impair d'inversions et donc $\epsilon(\tau) = (-1)^N = -1$. □

Théorème 1.2.14. *Si σ et τ sont deux permutations de $\{1, \ldots, n\}$, on a :*

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau).$$

L'application ε est donc un morphisme de groupe de S_n dans $(\{-1, 1\}, \times)$.

Corollaire 1.2.15. *Si $\sigma = \tau_1\tau_2\cdots\tau_p$ est une décomposition en produit de transpositions de la permutation σ, alors $\varepsilon(\sigma) = (-1)^p$.*

Remarque 1.2.16. Pour une permutation σ, il n'y a pas d'unicité de la décomposition en produit de transpositions. En revanche, la parité du nombre de transpositions intervenant dans un tel produit est constante.

1.2.4 Groupe alterné

Définition 1.2.17. On appelle *groupe alterné* $\mathcal{A}_n$, l'ensemble des permutations paires.

Remarque 1.2.18. Le groupe alterné $\mathcal{A}_n$ est un sous-groupe de S_n.

Exemple 1.2.19.
1. On a $S_2 = \{Id, (1,2)\}$, donc $\mathcal{A}_2 = \{Id\}$.
2. Le groupe S_3 est composé :
   - de l'identité, qui est paire,
   - des transpositions $(1,2)$, $(1,3)$ et $(2,3)$ qui sont impaires
   - des 3-cycles $(1,2,3)$ et $(3,2,1)$ qui sont pairs.

   Donc $\mathcal{A}_3 = \{Id, (1,2,3), (3,2,1)\}$

Proposition 1.2.20. *Si $\tau \in S_n$ est une permutation impaire, alors l'ensemble des permutations impaires est :*

$$\mathcal{A}_n\tau = \{\sigma\tau \ \mid \ \sigma \in \mathcal{A}_n\}.$$

Démonstration. Si $\sigma \in \mathcal{A}_n$, alors $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau) = -1$, ce qui prouve que $\sigma\tau$ est impaire. Réciproquement si σ est impaire, alors $\sigma\tau^{-1}$ est paire et donc $\sigma = (\sigma\tau^{-1})\tau \in \mathcal{A}_n\tau$. □

Il y a donc autant que de permutations paires que d'impaires, ce qui prouve :

Corollaire 1.2.21. *Le groupe $\mathcal{A}_n$ est de cardinal $\frac{n!}{2}$.*

1.2.5 Décomposition d'une permutation en produit de cycles à support disjoints

Définition 1.2.22. Soient $n \in \mathbb{N}^*$ et $\sigma \in S_n$. Pour $k \in \{1,\dots,n\}$, *l'orbite* de k sous σ est $\mathcal{O}(k) = \{\sigma^j(k), \ j \in \mathbb{Z}\}$

Théorème 1.2.23. *Soient $n \in \mathbb{N}^*$ et $\sigma \in S_n$. Tout k de $\{1,\dots,n\}$ appartient à une orbite et une seule, Les orbites sous σ forment une partition de $\{1,\dots,n\}$.*

Exemple 1.2.24. Reprenons la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 7 & 6 & 3 & 4 \end{pmatrix}$.
Dans l'orbite de l'élément 1, on trouve $\sigma(1) = 5$, $\sigma^2(1) = \sigma(5) = 6$, $\sigma^3(1) = \sigma(6) = 3$ et $\sigma^4(1) = \sigma(3) = 1$. On en déduit que $\mathcal{O}(1) = \{1,5,6,3\} = \mathcal{O}(3) = \mathcal{O}(5) = \mathcal{O}(6)$.
Ensuite, $\sigma(2) = 2$ et donc pour tout $k \in \mathbb{Z}$, $\sigma^k(2) = 2$. L'orbite de 2 est le singleton $\mathcal{O}(2) = \{2\}$.
Enfin, $\sigma(4) = 7$ et $\sigma^2(4) = \sigma(7) = 2$. Donc $\mathcal{O}(4) = \{4,7\}$.

Définitions 1.2.25. Soit $n \geq 2$.
Un *cycle* de $\{1,\dots,n\}$ est une permutation de $\{1,\dots,n\}$ qui admet une orbite et une seule non reduit à un singleton. Le *support* de ce cycle est son orbite et la *longueur* de ce cycle est le cardinal de son support.

Remarque 1.2.26. Les transpositions sont les cycles de longueurs 2.

Théorème 1.2.27. *Deux cycles à support disjoints commutent*

Théorème 1.2.28. *Toute permututation distincte de l'identité se décompose de manière unique, à l'ordre près en un produit de cycles à supports deux à deux disjoints.*

Remarque 1.2.29. La décomposition s'obtient en déterminant les orbites

.

Exemple 1.2.30. Reprenons la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 7 & 6 & 3 & 4 \end{pmatrix}$. et posons $c_1 = (1\ 5\ 6\ 3)$ et $c_2 = (4\ 7)$. On en déduit que $\sigma = c_1 \circ c_2 = c_2 \circ c_1$.

Théorème 1.2.31. *La signature d'un cycle de longeur $l \geq 2$ est $(-1)^{l-1}$.*

Théorème 1.2.32. *Soinet $n \geq 1$ puis $\sigma \in S_n$. Alors, $\epsilon(\sigma) = (-1)^{n-k}$ où k est le nombre d'orbites de σ.*

1.3 Sous-groupes distingués, Groupes quotients

1.3.1 Classes à gauches

On se donne un groupe multiplicatif $(G, \cdot)$. Si S est une partie non vide de G, on note, pour tout $g \in G$:

$$gS = \{gs \mid s \in S\} \text{ et } Sg = \{sg \mid s \in S\}.$$

Dans le cas où G est commutatif, on a $gS = Sg$.

Théorème 1.3.1. *Pour tout sous-groupe H de G, la relation $\mathcal{R}_g$ définie sur G par :*

$$g_1 \mathcal{R}_g g_2 \Longleftrightarrow g_1^{-1} g_2 \in H$$

est une relation d'équivalence.

Démonstration. Pour $g \in G$, on a $g^{-1}g = 1 \in H$, donc $\mathcal{R}_g$ est reflexive.
Si $g_1, g_2 \in G$ sont tels que $g_1^{-1}g_2 \in H$, on a alors $(g_1^{-1}g_2)^{-1} = g_2^{-1}g_1 \in H$, ce qui signifie que $g_2 \mathcal{R}_g g_1$. Cette relation est donc symétrique.
Si $g_1, g_2, g_3 \in G$ sont tels que $g_1^{-1}g_2 \in H$ et $g_2^{-1}g_3 \in H$, on a alors $g_1^{-1}g_3 = (g_1^{-1}g_2)(g_2^{-2}g_3) \in H$, ce qui signifie que $g_1 \mathcal{R}_g g_3$. Cette relation est donc transitive. □

Pour tout $g \in G$, on note $\bar{g}$ la classe d'équivalence de g modulo $\mathcal{R}_g$ et on dit que $\bar{g}$ est la *classe à gauche modulo H* de g.

On a donc, pour tout $g \in G$:

$$h \in \bar{g} \Leftrightarrow g \mathcal{R}_g h \Leftrightarrow g^{-1}h \in H \Leftrightarrow \exists k \in H \mid h = gk \Leftrightarrow h \in gH$$

C'est-à-dire $\bar{g} = gH$.

En particulier, $\bar{1} = H$ et $\bar{g} = H$ si, et seulement si, $g \in H$.

L'ensemble de toutes ces classes d'équivalences est noté G/H et on l'appelle *l'ensemble des classes à gauche modulo H*. On a donc :

$$G/H = \{\bar{g} \mid g \in G\} = \{gH \mid g \in G\}.$$

Remarque 1.3.2. On peut définir, de manière analogue l'ensemble

$$G\backslash H = \{Hg \mid g \in G\}.$$

des *classes à droites modulo* H à partir de la relation d'équivalence :

$$g_1 \mathcal{R}_g g_2 \Leftrightarrow g_1 g_2^{-1} \in H$$

Théorème 1.3.3. *Si H est un sous-groupe de G, alors l'ensemble des classes à gauche (resp. à droite) modulo H deux à deux distinctes forme une partition de G.*

Définition 1.3.4. Si H est un sous-groupe de G, le cardinal de l'ensemble G/H est noté $[G : H]$ et on l'appelle *l'indice* de H dans G.

Exercice 1.3.5. Soit H un sous-groupe du groupe G. On considère l'application $\varphi : G/H \longrightarrow G\backslash H$, $gH \longmapsto Hg^{-1}$.
1. Montrer que φ est bien définie.
2. Montrer que φ est isomorphisme.

On déduit de ce qui précède, $card(G/H) = card(G\backslash H)$.

Théorème 1.3.6 (Lagrange)**.** *Soient G un groupe fini d'ordre $n \geq 2$ et H un sous-groupe de G. Pour tout $g \in G$, on a $card(gH) = card(H)$ et :*

$$card(G) = [G : H]card(H)$$

donc l'ordre de H divise celui de G.

Démonstration. Pour g fixe dans le groupe G, la "la translation à gauche" $h \longmapsto gh$ est une bijection de G sur G et sa restriction à H réalise une bijection de H sur gH. Il en résulte que gH et H on même cardinal.

L'ensemble des classes à gauche suivant H réalise une partition de G et ces classes sont en nombre fini de même cardinal égal à celui de H, il en résulte que :

$$card(G) = [G : H]card(H)$$

et $card(H)$ divise $card(G)$. □

1.3.2 Sous-groupe distingués

Définition 1.3.7. On dit qu'une relation d'équivalence $\mathcal{R}$ sur G est compatible avec la loi de G si, pour tous g, g', h dans G, on a :

$$g\mathcal{R}g' \Rightarrow gh\mathcal{R}g'h \text{ et } hg\mathcal{R}hg'$$

Théorème 1.3.8. *Si H est un sous-groupe de G, alors la relation d'équivalence $\mathcal{R}_g$ associée à H est compatible avec la loi de G si, et seulement si, $gH = Hg$ pour tout $g \in G$.*

Démonstration. Supposons que $\mathbb{R}_g$ compatible avec la loi de G. Pour tout $k \in gH$, on a $g^{-1}k\mathcal{R}_g 1$ et avec la compatibilité à gauche et à droite, on en déduit que $g(g^{-1}k)\mathcal{R}_g g$ et $g(g^{-1}k)g^{-1}\mathcal{R}_g gg^{-1}$, soit $kg^{-1}\mathcal{R}_g 1$, ce qui revient à dire que $k \in Hg$. On a donc $gH \subset Hg$. De manière analogue, on montre que $Hg \subset gH$ et donc $gH = Hg$.

Réciproquement, supposons que $gH = Hg$, pour tout $g \in G$. Si $g\mathcal{R}_g g'$ et $h \in G$, on a alors $(gh)^{-1}g'h = h^{-1}g^{-1}g'h$ avec $g^{-1}g' \in H$, donc $g^{-1}g'h \in Hh = hH$ et $(gh)^{-1}g'h = h^{-1}hk = k \in H$, c'est-à-dire $gh\mathcal{R}_g g'h$. Puis avec $(hg)^{-1}hg' = g^{-1}h^{-1}hg' = g^{-1}g' \in H$, on en déduit que $hg\mathcal{R}_g g'h$. Donc $\mathcal{R}_g$ est compatible avec la loi de G. □

Définition 1.3.9. On dit qu'un sous-groupe H de G est *distingué ou normal* si on a $gH = Hg$ pour tout $g \in G$. On note $H \triangleleft G$ pour signifier que H est un sous-groupe distingué de G.

Exemple 1.3.10.
- $\{1\}$ et G sont toujours distingués dans G.
- Si le groupe G est commutatif, alors tous ses sous-groupes sont distingués.

Remarque 1.3.11. Un sous-groupe H de G est distingué si, et seulement si, on a $gHg^{-1} = H$ ou $H = g^{-1}Hg$ ce qui équivaut à dire que $ghg^{-1} \in H$ ou $g^{-1}hg \in H$ pour tout $(h, g) \in H \times G$.

Théorème 1.3.12. *Si G et G' sont deux groupes et φ un morphisme de groupes de G dans G'. Alors* $\ker(\varphi)$ *est un sous-groupe distingué de G.*

Démonstration. Pour $(g, h) \in \ker(\varphi)$, on a $\varphi(g^{-1}hg) = \varphi(g^{-1})\varphi(h)\varphi(g) = \varphi(g)^{-1} \cdot 1_{G'}\varphi(g) = 1_{G'}$, i.e. $g^{-1}hg \in \ker(\varphi)$. Le sous-groupe $\ker(\varphi)$ de G est donc distingué. □

Exemple 1.3.13. Le groupe alterné $\mathcal{A}_n$ est distingué dans le groupe symétrique S_n comme noyau de la signature.

Théorème 1.3.14. *Un sous-groupe H d'un groupe G est distingué si, et seulement si, il existe un unique structure de groupe sur l'ensemble quotient G/H des classes modulo H telle que la surjection canonique $\pi : G \longrightarrow G/H$, définie par $\pi(g) = \overline{g} = g\ker(\varphi)$ pour tout $g \in G$, soit un morphisme de groupes.*

Démonstration. Si G/H est muni d'une structure de groupe telle que π soit un morphisme de groupes, on a alors nécessairement pour tous g, g' dans G, $\overline{g}\overline{g'} = \pi(g)\pi(g') = \pi(gg') = \overline{gg'}$.
Pour $(g, h) \in G \times H$, on a alors $\overline{g^{-1}hg} = \overline{g^{-1}h}\overline{g} = \overline{g^{-1}}\overline{g} = \overline{g^{-1}g} = \overline{1} = H$, ce qui signifie que $g^{-1}hg \in H$ (on rappelle que $\overline{g} = gH = \overline{1} = H$ si, et seulement si, $g \in H$).

Supposons H distingué. L'analyse que l'on vient de faire nous montre que la seule loi possible sur G/H est définie par $\overline{g}\overline{g'} = \overline{gg'}$. Pour montrer qu'une telle définition est permise, il s'agit de montrer qu'elle ne dépend pas des choix des représentants de $\overline{g}$ et $\overline{g'}$, ce qui résulte du fait $\mathcal{R}_g$ est compatible avec la loi de G. En effet, si $g\mathcal{R}_g g_1$ et $g'\mathcal{R}_g g_1'$, on a alors $gg'\mathcal{R}_g g_1 g'$ et $g_1 g'\mathcal{R}_g g_1 g_1'$, donc $gg'\mathcal{R}_g g_1 g_1'$ et $\overline{gg'} = \overline{g_1 g_1'}$.

Il reste à vérifier que G/H muni de cette loi de composition interne est bien un groupe.
- Pour $g_1, g_2, g_3 \in G$, on a $\overline{g_1}(\overline{g_2 g_3}) = \overline{g_1}(\overline{g_2 g_3}) = \overline{g_1(g_2 g_3)} = \overline{(g_1 g_2)g_3} = \overline{g_1 g_2 g_3} = (\overline{g_1 g_2})\overline{g_3}$, on en déduit que cette loi est associative.
- Pour $g \in G$, on a $\overline{g}\overline{1} = \overline{g \cdot 1} = \overline{g}$, on en déduit que $\overline{1}$ est le neutre.
- Pour $g \in G$, on a $\overline{g}\overline{g^{-1}} = \overline{gg^{-1}} = \overline{1}$. On en déduit que tout élément de G/H est inversible avec $(\overline{g})^{-1} = \overline{g^{-1}}$.

Par définition de cette loi de composition interne, l'application π est surjective. □

Remarque 1.3.15. Pour H distingué dans G, le noyau de la surjection canonique est $\ker(\pi) = \{g \in G \mid \overline{g} = \overline{1}\} = \overline{1} = H$. Comme on a vu que le noyau d'un morphisme de groupe est distingué, on en déduit qu'un sous-groupe distingué de G est le noyau d'un morphisme de groupes.

Remarque 1.3.16. Dans le cas où G est commutatif, pour tout sous-groupe H de G, G/H est un groupe puisque tous les sous-groupes de G sont distingués. on note alors qu'il est aussi égal à $G\backslash H$.

Théorème 1.3.17. *Si G, G' sont deux sous-groupes et $\varphi : G \longrightarrow G'$ un morphisme de groupes, il existe alors un unique isomorphisme de groupes $\overline{\varphi} : G/\ker(\varphi) \longrightarrow Im(\varphi)$ tel que $\varphi = i \circ \overline{\varphi} \circ \pi$, où $i : Im(\varphi) \longrightarrow G'$ est l'injection canonique définie par $i(h') = h'$ pour tout $h' \in Im(\varphi)$ et $\pi : G \longrightarrow G/\ker(\varphi)$ la surjection canonique.*

Démonstration. Comme $\ker(\varphi)$ est distingué dans G, alors $G/\ker(\varphi)$ est un groupe. Si un tel isomorphisme $\overline{\varphi}$ existe, on a alors, pour tout $g \in G : \varphi(g) = i \circ \overline{\varphi} \circ \pi(g) = i \circ \overline{\varphi}(\overline{g}) = \overline{\varphi}(\overline{g})$. Ce qui prouve l'unicité $\overline{\varphi}$ s'il existe.

Vu l'analyse du problème, on montre d'abord que l'on peut définir $\overline{\varphi}$ par $\overline{\varphi}(\overline{g}) = \varphi(g)$ pour tout $\overline{g} \in G/\ker(\varphi)$. Pour justifier cette définition, on doit vérifier qu'elle ne dépend pas du choix d'un représentant de $\overline{g}$. Si $\overline{g} = \overline{h}$, on a alors $g^{-1}h \in \ker(\varphi)$, donc $(\varphi(g))^{-1}\varphi(h) = \varphi(g^{-1}h) = 1$ et $\varphi(g) = \varphi(h)$. L'application $\overline{\varphi}$ est bien définie et par construction, on a $\varphi = i \circ \overline{\varphi} \circ \pi$. Avec $\overline{\varphi}(\overline{g}\overline{h}) = \overline{\varphi}(\overline{gh}) = \varphi(gh) = \varphi(g)\varphi(h) = \overline{\varphi}(\overline{g})\overline{\varphi}(\overline{h})$. On voit que $\overline{\varphi}$ est un morphisme de groupes.

L'égalité $\overline{\varphi}(\overline{g}) = 1$ équivaut à $\varphi(g) = 1$, soit à $g \in \ker(\varphi)$ ou encore à $\overline{g} = \overline{1}$. Il est donc injective et à valeur dans $Im(\varphi) = Im(\overline{\varphi})$, il est alors surjective. □

Corollaire 1.3.18. *Soient G, G' deux groupes et $\varphi : G \longrightarrow G'$ un morphisme de groupes. Si G est fini, on a alors $card(G) = card(\ker(\varphi))card(Im(\varphi))$*

Démonstration. Comme $G/\ker(\varphi)$ et $Im(\varphi)$ sont isomorphes, dans le cas où G est fini, on a $card(Im(\varphi)) = card(G/\ker(\varphi)) = \frac{card(G)}{card(\ker(\varphi))}$. □

1.4 Ordre d'un élément dans un groupe

Soit G un groupe arbitraire, noté multiplicativement. Si $x \in G$, l'application $\varphi : (\mathbb{Z}, +) \longrightarrow G$, $n \longmapsto x^n$ est un morphisme de groupe d'image le sous-groupe $\langle x \rangle$ engendré par x. Le noyau $\ker(\varphi)$ de φ, qui est un sous-groupe de $\mathbb{Z}$, est donc de la forme $n\mathbb{Z}$ pour un unique entier $n \in \mathbb{Z}$.

Définition 1.4.1. On dit que x est *d'ordre fini* si $\ker(\varphi)$ n'est pas réduit à $\{0\}$. On dit que x est *d'ordre infini* si $\ker(\varphi) \neq \{0\}$.
Lorsque x est d'ordre fini, on appelle *ordre de* x, l'entier $\alpha \in \mathbb{N}^*$ tel que $\ker(\varphi) = \alpha\mathbb{Z}$.

Remarque 1.4.2. On dit que x est un élément de *torsion* de G si son ordre est fini. Dans ce cas, l'ordre de x est caractérisé par l'une des assertions suivantes :
1. l'ordre de x est le plus petit entier $n \in \mathbb{N}^*$ tel que $a^n = 1$,
2. l'ordre de x est l'unique entier $n \in \mathbb{N}^*$ tel que l'on ait :

$$\forall k \in \mathbb{Z},\ n \mid k \Longleftrightarrow a^k = 1.$$

Exemple 1.4.3.
1. L'ordre du neutre d'un groupe G vaut 1.
2. Un élément z non nul du groupe additif $\mathbb{C}$ est d'ordre infini.

Théorème 1.4.4. *Soit x un élément du groupe G, d'ordre fini n. Si $m \in \mathbb{Z}$, l'élément $h = g^m$ est d'ordre fini $\frac{n}{d}$ où $d = pgcd(m, n)$.*

Démonstration. Soient $m' = \frac{m}{d}$ et $n' = \frac{n}{d}$, alors $pgcd(m', n') = 1$. On a, d'une part $h^{n'} = g^{dm'n'} = (g^{dn'})^{m'} = (g^n)^{m'} = 1^{m'} = 1$. Donc h est d'ordre fini et son ordre ω divise n'. D'autre part, puisque $h^\omega = 1$, il s'en suit $g^{m\omega} = 1$. Alors, il existe entier k tel que $m\omega = kn$, i.e. $m'\omega = kn'$. Puisque $pgcd(m', n') = 1$, alors n' divise ω. Finallement, $\omega = n'$. □

Théorème 1.4.5. *Soient g et g' deux éléments commutatifs de G d'ordres finis respactifs n et n'. on suppose que n et n' sont premiers entre eux. Alors gg' est d'ordre fini et son ordre est nn'.*

Démonstration. Comme $gg' = g'g$, alors $(gg')^{nn'} = g^{nn'}g'^{nn'} = (g^n)^{n'}(g'^{n'})^n = 1$. Donc, gg' est un élément d'ordre fini et son ordre ω divise nn'. D'autre part, de $(gg')^\omega = 1$, on en déduit que $1 = (gg')^{\omega n} = (g')^{\omega n}$ entraîne n' divise ωn, i.e. n' divise ω car $pgcd(n', n) = 1$. On montre de même que n' divise ω en considérant $(gg')^{\omega n'}$. Puisque n et n' sont premiers entre eux, ω, multiple commun de n et n', est multiple de leur produit, et en fin de compte $\omega = nn'$ □

Théorème 1.4.6. *Soient $\varphi : G \longrightarrow G'$ est un morphisme de groupes injectif.*
1. *Si $x \in G$ d'ordre infini, alors $\varphi(x)$ est d'ordre infini.*
2. *Si x est fini d'ordre n, alors $\varphi(x)$ est fini d'ordre n.*

Théorème 1.4.7. *Si le groupe G est cyclique, de cardinal n, alors tout sous-groupe de G est cyclique, de cardinal un diviseur de n.*

Théorème 1.4.8 (Cauchy)**.** *Si G est un groupe fini d'ordre $n \geq 2$, alors pour tout diviseur premier p de n, il existe dans G un élément d'ordre p.*

Chapitre 2

Anneaux

2.1 Structures d'anneaux

2.1.1 Définitions et Exemples

Définition 2.1.1. On appelle *anneau* un ensemble A muni de deux lois de compositions interne ; une addition (notée en général $+$) et une multiplication (notée en général $\times$ ou sans symbole) satisfaisant aux axiomes suivants :
1. $(A, +)$ est un groupe abélien (son neutre, noté 0 ou 0_{A} est *l'élément nul* de A).
2. La multiplication est associative et distributive par rapport à l'addition.
3. La multiplication admet un élément neutre (noté en général 1 ou 1_{A}).

Un anneau est dit *commutatif* si, et seulement si, sa multiplication est commutative.

Exemple 2.1.2. $(\mathbb{Z}, +, \times)$ est un anneau commutatif non nul.

Proposition 2.1.3 (Règle de calcul)**.** *Dans un anneau A, on a les propriétés suivantes :*
1. $\forall a \in A,\ 0 \times a = a \times 0 = 0$.
2. $\forall (a, b) \in A^2,\ (-a) \times b = a \times (-b) = -(a \times b)$.

Démonstration. Pour $a \in A$, on a : $a \times 0 + a \times 0 = a \times (0 + 0) = a \times 0 = a \times 0 + 0$. Puisque $(A, +)$ est un groupe, on peut simplifier par $a \times 0$. Ce qui donne $a \times 0 = 0$. Par un raisonnement analogue, on montre que $0 \times a = 0$.

Soit $(a, b) \in A^2$, montrons que $a \times (-b)$ et $a \times b$ sont opposés. On a $a \times (-b) + a \times b = a \times (b - b) = a \times 0 = 0$. Donc $a \times (-b) = -(a \times b)$ et on prouve de même que $(-a) \times b = -(a \times b)$. □

Remarque 2.1.4. Si dans un anneau A, on a $0_{\mathrm{A}} = 1_{\mathrm{A}}$, alors $\forall x \in A,\ x = 1_{\mathrm{A}} x = 0_{\mathrm{A}} x = 0_{\mathrm{A}}$ et donc $A = \{0_{\mathrm{A}}\}$. Un tel anneau est appelé *anneau nul*.

Proposition 2.1.5 (Distributivité généralisée)**.** *Si $(a_i)_{i \in I}$ et $(b_j)_{j \in J}$ sont deux familles d'éléments d'un anneau A, indexées par des ensembles finis I et J, on a :*

$$\left(\sum_{i \in I} a_i\right) \cdot \left(\sum_{j \in I} a_j\right) = \sum_{(i,j) \times I \times J} a_i b_j$$

Proposition 2.1.6. *Soient a et b deux éléments d'un anneau A tels que $ab = ba$.*

1. ***Formule du binôme de Newton :***

$$\forall n \in \mathbb{N},\ (a+b)^n = \sum_{p=0}^{n} C_n^p a^p b^{n-p}.$$

2. *Pour $n \in \mathbb{N}$,*

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

En particulier, ces relations sont vraies quels que soient les éléments a et b d'un anneau commutatif.

Définition 2.1.7. On appelle *sous-anneau* d'un anneau d'un anneau $(A, +, \times)$, un sous-groupe de $(A, +)$ qui est stable par $\times$ et qui contient 1_A.

Exemple 2.1.8. $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$.

2.1.2 Anneaux intégres

Définition 2.1.9. Soit A un anneau commutatif. On dit que $a \in A$ est un *diviseur de* 0 si $a \neq 0$ et s'il existe un élément x de A non nul tel que $ax = 0$.

Proposition 2.1.10. *Un élément non nul d'un anneau commutatif est régulier pour la multiplication si, et seulement si, ce n'est pas un diviseur de 0.*

Démonstration. Supposons a régulier. Si $ax = 0$, alors $ax = a0$ et par conséquent $x = 0$. Donc a n'est pas diviseur de 0.

Supposons a n'est pas un diviseur de 0. Si $ax = ay$, alors $a(x-y) = 0$; donc $x - y = 0$, i.e. $x = y$ et a est régulier. □

Définition 2.1.11. Un anneau *intégre* est un anneau commutatif, différent de $\{0\}$, et sans diviseur de 0.

Exemple 2.1.12. L'anneau $(\mathbb{Z}, +, \times)$ est intègre.

2.1.3 Morphismes d'anneaux

Définition 2.1.13. Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux. On dit que $\varphi : A \longrightarrow B$ est un *morphisme d'anneaux* si :
1. $\forall (x, y) \in A^2$, $\varphi(x + y) = \varphi(x) + \varphi(y)$,
2. $\forall (x, y) \in A^2$, $\varphi(x \times y) = \varphi(x) \times \varphi(y)$,
3. $\varphi(1_{\mathrm{A}}) = \varphi(1_{\mathrm{B}})$.

Les morphismes d'anneaux de $(A, +, \times)$ dans $(B, +, \times)$ sont en particulier des morphismes de groupes de $(A, +)$ dans $(B, +)$. Ils en ont donc toutes les propriétés et on utilise la même terminologie : endomorphisme, isomorphisme, automorphisme. On définit le *noyau* de φ par $\ker(\varphi) = \varphi^{-1}(\{0_{\mathrm{B}}\})$.

Proposition 2.1.14. *L'image d'un sous-anneau de A par un morphisme d'anneaux de A dans B est un sous-anneau de B.*

2.1.4 Notion d'idéal d'un anneau commutatif

Définition 2.1.15. Soit A un anneau *commutatif.*
On appelle *idéal* de A d'un anneau commutatif A, tout sous-groupe additif I de A vérifiant la propriété suivante, dite *propriété d'absorption* :

$$\forall (u,i) \in A \times I,\ ui \in I. \tag{2.1}$$

Exemple 2.1.16. Les sous-ensembles $\{0_{\mathrm{A}}\}$ et A sont des idéaux de A.

Remarque 2.1.17.
a) Si I est un idéal de l'anneau A et si $1 \in I$, alors $I = A$. En effet, quel que soit $a \in A$, on a $1 \times a = a \in I$, donc $A \subset I$. Comme on a toujours $I \subset A$, alors $I = A$.
b) Si I est un *idéal propre* de l'anneau A, i.e. $I \neq A$, alors aucun élément de I n'est inversible (pour la multiplication). En effet, s'il existe $a \in I$ tel que a^{-1} existe, alors $a^{-1}a = 1 \in I$ et $I = A$ d'après *a*), ce qui est contraire à l'hypothèse. Donc a n'est pas inversible.

Proposition 2.1.18. *Une partie I de A est un idéal si, et seulement si, elle est non vide et vérifie :*

$$\forall (u,v) \in A^2,\ \forall (i,j) \in I^2,\ ui + vj \in I.$$

Démonstration. Le sens direct est clair. La réciproque vient des relations $i - j = (1)i + (-1)j$ et $ui = ui + 0j$. □

Proposition 2.1.19. *L'intersection d'une famille d'idéaux est un idéal de A.*

Démonstration. Soit I l'intersection d'une famille $(I_x)_{x \in X}$ d'idéaux de A. On sait que I est un sous-groupe additif de A. Soient $i \in I$ et $a \in A$; pour tout $x \in X$, on a $i \in I_x$, et par conséquent, $ai \in I_x$. Ainsi, $ai \in I$. □

Proposition 2.1.20. *Soient I et J deux idéaux de A. La somme*

$$I + J = \{i + j \ \mid \ (i,j) \in I \times J\}$$

est un idéal de A.

Démonstration. L'élément nul que l'on peut érire $0 + 0$ appartient à $I + J$. Si s et t appartiennent à $I + J$, ils s'écrivent $s = i + j$ et $t = k + l$ avec $(i,j) \in I \times J$ et $(k,l) \in I \times J$. Pour $(u,v) \in A^2$, l'expression $us + vt = (ui + vk) + (uj + vl)$ appartient donc à $I + J$. □

Proposition 2.1.21. *Si $\varphi : A \longrightarrow B$ est un morphisme d'anneaux, le noyaux de φ est un idéél de A.*

Démonstration. Nous savons que $\ker(\varphi)$ est un sous-groupe additif de A. Si $(a,x) \in A \times \ker(\varphi)$, l'égalité $\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a)0_{\mathrm{A}} = 0_{\mathrm{A}}$ montre que ax appartient à $\ker(\varphi)$. □

Remarque 2.1.22. Plus généralement, l'image réciproque de tout idéal de B est idéal de A.

2.2 Anneaux quotients

Théorème 2.2.1. *Soient A un anneau commutatif et I un idéal de A. Alors la relation définie par $x\mathcal{R}y \Leftrightarrow x - y \in I$ est une relation d'équivallence sur A, compatible avec les deux lois de A. L'ensemble quotient, noté A/I, muni des deux lois quotients est un anneau aapelé anneau-quotient de A par I. De plus, A/I est commutatif.*

Démonstration. Comme I est un sous-groupe du groupe additif A et $\mathcal{R}$ est une relation d'équivallence, on peut définir le groupe additif quotient A/I.

Montrons que la relation $\mathcal{R}$ est compatible avec la multiplication de A.

On doit démontrer que les relations $x - x' \in I$ et $y - y' \in I$ impliquent $xy - x'y' \in I$. Or si $x - x' = u \in I$ et $y - y' = v \in I$, on a :

$$x = x' + u \text{ et } y = y' + v$$

d'où

$$xy = x'y' + x'v + uy' + uv$$

Comme I est un idéal, $x'v, uy', uv \in I$ et on en déduit que :

$$xy - x'y' = x'v + uy' + uv \in I.$$

On peut donc définir la loi quotient de la multiplication en posant $(x+I)(y+I) = xy+I$ quels que soient $\overline{x} = x + I \in A/I$ et $\overline{y} = y + I \in A/I$. Ainsi, $\overline{xy} = xy + I = \overline{xy}$

Cette multiplication de A/I est commutatif. En effet, $\overline{xy} = \overline{xy} = \overline{yx} = \overline{yx}$.

On vérifie que la multiplication de A/I est associative et distributive par rapport à l'addition de A/I. Donc A/I, muni des deux lois quotient, est un anneau. □

Par exemple $\mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}$ est un anneau commutatif car $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

2.3 Idéaux maximaux et idéaux premiers

2.3.1 Idéaux maximaux

Définition 2.3.1. Soit I un idéal de l'anneau A. On dit que I est un *idéal maximal* si $I \neq A$ et si, pour tout idéal J différent de I, $I \subset J$ implique $J = A$.

Théorème 2.3.2. *Soit I un idéal d'un anneau commutatif A. Alors les assertions suivantes sont équivalentes :*

i) L'idéal I est maximal.
ii) L'idéal I est propre et, pour tout $x \in A\backslash I$, l'idéal $I + Ax$ est égal à A.
iii) L'anneau quotient A/I est un corps.

Démonstration. Si I est maximal et $x \in A\backslash I$, alors l'idéal $I + Ax$ contient strictement I, donc il est égal à A (par maximalité).

Supposons que, pour tout $x \in A\backslash I$, l'idéal $I + Ax$ est égal à A. Soit $\overline{y}$ un élément non nul de l'anneau quotient A/I. Alors $y \in A\backslash I$, et, par hypothèse, il existe $a \in A$ et $i \in I$ tels que $i + ay = 1$, ce qui entraîne que $\overline{ay} = \overline{1}$ dans A/I. Ainsi, tout élément non nul de A/I est inversible et cet anneau est un corps.

Supposons enfin que A/I est un corps. Ses seuls idéaux sont $\{0\}$ et lui-même. Il l'y a donc une bijection entre les ideuax de A contenant I et les ideaux de A/I (deuxième théorème d'isomorphisme pour les anneaux) : le seul idéal propre de A contenant I est donc I lui-même. □

Corollaire 2.3.3. *L'idéal* $\{0\}$ *est maximal si, et seulement si,* A *est un corps. Les idéaux maximaux de* A/I *sont les* $\mathcal{B}/I$*, où* $\mathcal{B}$ *est un idéal maximal de* A *de* A *contenant* I*.*

Exercice 2.3.4. Décrire les idéaux maximaux de $\mathbb{Z}$ et de $\mathbb{Z}/m\mathbb{Z}$ avec $m \in \mathbb{N}\backslash\{0,1\}$.

Théorème 2.3.5 (Théorème de Krull)**.** *Soit* A *un anneau et soit* I *un idéal de* A*. Alors,* I *est contenue dans un idéal maximal.*

2.3.2 Idéal premier

Définition 2.3.6. On appelle *idéal premier* de A, un idéal propre I de A vérifiant :

$$\forall x, y \in A,\ xy \in I \Longrightarrow x \in I \text{ ou } y \in I.$$

Théorème 2.3.7. *Soit* I *un idéal de l'anneau* A*. Alors, l'idéal* I *est un idéal premier de* A*, si et seulement si, l'anneau quotient* A/I *est intégre.*

Démonstration. Notons $\overline{x}$ la classe de $x \in A$ dans A/I, alors $\overline{x} = 0$ si et seulement si $x \in I$; et tous les éléments de A/I sont de la forme $\overline{x}$ avec $x \in A$. L'implication de la définition se réécrit donc : $\forall \overline{x}, \overline{y} \in A/I$, $\overline{xy} = 0 \Rightarrow \overline{x} = 0$ ou $\overline{y} = 0$, ce qui caractérise l'intégrité de A/I. □

Corollaire 2.3.8.
1. *Tout idéal maximal est premeir.*
2. *Tout anneau non nul admet des idéaux premiers.*
3. *L'idéal* $\{0\}$ *de* A *est premier si, et seulement si,* A *est intégre.*
4. *Les idéaux premiers de* A/I *sont les idéaux* $\mathcal{P}/I$*, où* $\mathcal{P}$ *est un idéal premier de* A*.*

Exercice 2.3.9. Décrire les idéaux premiers de $\mathbb{Z}$.

Chapitre 3

Corps

3.1 Structures de corps

3.1.1 Définitions et exemples

Définition 3.1.1. On dit $(K, +, \times)$ est un *corps* si $(K, +, \times)$ est un anneau commutatif non nul et dont tous les éléments non nuls sont inversibles pour la multiplications.

Remarque 3.1.2. Un corps est un anneau anneau intégre, puisqu'il est commutatif, non nul et que tous ses éléments non nuls sont inversibles, donc réguliers.

Exemple 3.1.3.
1. $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis des lois usuelles sont des corps.
1. $\mathbb{Z}$ muni des lois usuelles n'est pas un corps, puisque seuls 1 et -1 sont inversibles.

Notation 3.1.4. Si a et b sont deux éléments deux éléments d'un corps K, b étant non nul, on note $\frac{a}{b}$ l'élément $a \times b^{-1}$ de K

Pour $(a, b, a', b', x) \in K^5$, avec $b \neq 0$, $b' \neq 0$ et $x \neq 0$, on a alors les règles de calcul suivantes :
- $\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = a'b$.
- $\frac{ax}{bx} = \frac{a}{b}$.
- $\frac{a}{b} + \frac{a'}{b'} = \frac{ab'+a'b}{bb'}$.
- $\frac{a}{b} \times \frac{a'}{b'} = \frac{aa'}{bb'}$.
- Si $a \neq 0$, $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

Définition 3.1.5. Soit K un corps. On appelle *sous-corps* de K un sous-anneau de K qui est un corps

Exemple 3.1.6. $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont trois sous-corps de $\mathbb{C}$.

3.1.2 Corps des fractions

Définition 3.1.7. On dit qu'un corps K est un *corps des fractions* de l'anneau intègre A si les deux conditions suivantes sont vérifiées :
a) A est un sous-anneau du corps K.
b) Pour tout $x \in K$, il existe dans A des éléments a et b tels que $x = ab^{-1}$.

Théorème 3.1.8. *Tout anneau commutatif intégre A admet un corps des fractions.*

Élément de démonstration. Soit E l'ensemble des couples (p, q) où $p \in A$, $q \in A$ et $q \neq 0$. Sur E, la relation $\mathcal{R}$ définie par $(p, q)\mathcal{R}(p', q') \Leftrightarrow pq' = qp'$ est une relation d'équivallence.

Soit K l'ensemble quotient $E/\mathcal{R}$; notons φ l'application canonique de E sur $E/\mathcal{R}$.

On définit deux lois internes sur E en posant :

Addition : $(p, q) + (r, s) = (ps + qr, qs)$.

Multiplication : $(p, q) \cdot (r, s) = (pr, qs)$.

On vérifie sans peine que l'addition et la multiplication ainsi définies sont associatives, commutatives, admettant pour éléments neutre $(0, 1)$ et $(1, 1)$ respectivement, et que la multiplication est distributive par rapport à l'addition.

On vérifie également qu'elles sont compatibles avec la relation d'équivallence $\mathcal{R}$.

Dans l'ensemble quotient notons encore $+$ et $\bullet$ les lois quotients. Ces lois sont associatives, commutatives et la multiplication est distributive par rapport à l'addition.

Pour l'addition, $\varphi(0, 1)$ est l'élément neutre et $\varphi(-p, q)$ est l'opposé de $\varphi(p, q)$; donc $(K, +)$ est un groupe abélien.

Pour la multiplication, $\varphi(1, 1)$ est l'élément neutre. Donc $(K, +, \bullet)$ est un anneau commutatif.

En outre, si $\varphi(p, q)$ est différent de $\varphi(0, 1)$, i.e. si $p \neq 0$, $\varphi(p, q)$ admet pour inverse $\varphi(p, q)$. En conclusion $(K, +, \bullet)$ est un corps commutatif. □

Théorème 3.1.9. *Soit A un anneau intègre. Si K et L sont des corps des fractions de l'anneau A, alors K et L sont isomorphes.*

Exemple 3.1.10. Le corps des fractions de $\mathbb{Z}$ est appelé *corps des rationnels* et noté $\mathbb{Q}$.

3.2 Anneaux des polynômes

3.2.1 Construction

Définitions 3.2.1. Soit K un anneau commutatif.

- On appelle *polynôme à une indéterminée à coefficients dans K*, toute suite $(a_0, a_1, \ldots, a_n, \ldots)$ d'élément de K nuls à partir d'un certain rang.
  Un tel polynôme est noté $P = (a_0, a_1, \ldots, a_n, \ldots)$ ou $P = (a_n)_{n\in\mathbb{N}}$.
- Les a_n sont appelés les *coefficients* du polynôme P ; on dit que a_n est le *coefficients d'indice n* ; a_0 s'appelle le *terme constant*.
- Si tous les coefficients du polyôme P sont nuls, on dit que P est le *polynôme nul* et on le note 0. On appelle *monôme* un polynôme dont tous les coefficients sont nuls sauf, au plus, l'un d'entre eux.

Notation 3.2.2. L'ensemble des polynômes à une indéterminée à coefficients dans l'anneau commutatif K se note $K[X]$.

Définitions 3.2.3. Soient K un anneau commutatif et $P = (a_0, a_1, \ldots, a_n, \ldots)$ un polynôme à coefficients dans K.

- On appelle *degré* de P, et on note $deg(P)$, le plus grand entier n tel que $a_n \neq 0$. Cette définition s'applique à tout polynôme de $K[X]$ sauf au polynôme nul 0.
- De même, le plus petit entier k tel que $a_k \neq 0$, s'appelle la *valuation* du polynôme P et se note $val(P)$. Tout polynôme sauf 0 admet une valution

• On convient de noter $deg(0) = -\infty$ et $val(P) = +\infty$.

Exemple 3.2.4. Prenons $K = \mathbb{Z}$ et $P = (0, 1, 0, 4, 0, 0, \ldots)$. On a $deg(P) = 3$ et $val(P) = 1$.

Définition 3.2.5. On dit que deux polynômes $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ de $K[X]$ sont égaux si pour tout entier n, on a $a_n = b_n$. En particulier P est le polynôme nul si, et seulement si, pour tout n, $a_n = 0$.

3.2.2 structure d'anneau de $K[X]$

Dans ce paragraphe K désigne un anneau commutatif sauf mention expresse du contraire.

Addition de deux polynômes

Définition 3.2.6. Soient $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes de $K[X]$. On appelle *somme* de P et Q, et on note $P+Q$, le polynôme dont le coefficient d'indice n est égal $a_n + b_n$, i.e.

$$P + Q = (a_0 + b_0, \ldots, a_n + b_n, \ldots) \tag{3.1}$$

Théorème 3.2.7. *Le couple $(K[X], +)$ est un groupe abélien.*

Démonstration. Comme $(K, +)$ est un groupe abélien, pour tout $n \in \mathbb{N}$, $a_n + b_n \in K$. Donc $(a_0 + b_0, \ldots, a_n + b_n, \ldots)$ est une suite d'éléments de K. Si l'un des polynômes est nul, $P + Q$ est égal à l'autre polynôme, donc la suite $(a_n + b_n)_{n\in\mathbb{N}}$ possède un nombre fini d'éléments non nuls et $P + Q \in K[X]$. Si aucun des polynômes n'est nul, soient n et m les dégrés respectifs de P et Q respectivement. Si $k > \max(n, m)$, on aura $a_k = b_k = 0$, donc $a_k + b_k = 0$, ce qui montre que $P + Q \in K[X]$.

Les propriétés de l'addition dans $K[X]$ se déduisent facilement de celles de l'addition dans K. Ainsi, pour tout $n \in \mathbb{N}$, $(a_n + b_n) + c_n = a_n + (b_n + c_n)$, donc $(P + Q) + R = P + (Q + R)$ et pour tout $n \in \mathbb{N}$, $a_n + b_n = b_n + a_n$, donc $P + Q = Q + P$. Le polynôme 0 est l'élément neutre pour l'addition dans $K[X]$ et tout polynôme $P = (a_n)_{n\in\mathbb{N}}$ a pour opposé le polynôme, noté $-P$, tel que $-P = (-a_n)_{n\in\mathbb{N}}$. □

Théorème 3.2.8. *Posons $K[X]^* = K[X]\backslash\{0\}$. Alors si $P, Q \in K[X]^*$ et si $Q \neq -P$.*

$$deg(P + Q) \leq \max(deg(P), deg(Q)) \tag{3.2}$$
$$deg(P + Q) \geq \min(val(P), val(Q)) \tag{3.3}$$

Démonstration. Il existe deux possibilités : $deg(P) = deg(Q)$ et $deg(P) \neq deg(Q)$.

1. **Premier cas :** $deg(P) = deg(Q) = n$
   - Si $a_n + b_n = 0$, alors $deg(P + Q) < deg(P)$, l'inégalité stricte ayant lieu.
   - Si $a_n + b_n \neq 0$, alors $deg(P + Q) = deg(P)$, l'égalité ayant lieu dans ce cas.
2. **Deuxième cas :** $deg(P) \neq deg(Q)$. Nous pouvons supposer que $deg(P) < deg(Q)$. Alors par définition du dégré et de la somme, on a
   $deg(P + Q) = deg(Q) < \max(deg(P), deg(Q))$. Donc l'inégalité (3.3) est vérifiée.

On démontre de façon analogue l'inégalité (3.3). □

Multiplication de deux polynômes

Définition 3.2.9. Soient $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes de $K[X]$. On appelle *produit* de P et Q, et on note PQ, le polynôme dont le coefficient d'indice n est défini par

$$c_n = \sum_{i+j=n} a_i b_j = \sum_{k=0}^{n} a_k b_{n-k} \tag{3.4}$$

Montrons que l'on définit bien ainsi un plynôme à coefficients dans K. Si $a_i = 0$ pour $i > n_0$ et $b_j = 0$ pour $j > m_0$, on a $c_n = 0$ pour $n > n_0 + m_0$. En effet, si $n > n_0 + m_0$, dans chaque terme de c_n, on a soit $i > n_0$ et alors $a_i = 0$, soit $j > m_0$ et alors $b_j = 0$; donc chaque terme de c_n est nul, et par suite $PQ \in K[X]$.

Théorème 3.2.10.

1. *Le triplet* $(K[X], +, \cdot)$ *est un anneau commutatif et le polynôme constant* $(1, 0, 0, \ldots)$, *noté* 1, *est l'élément neutre de la multiplication.*
2. *L'anneau* $K[X]$ *est intègre si et seulement si l'anneau* K *est intègre.*
3. *Si* $P, Q \in K[X]$, *on a*

$$deg(PQ) \leq deg(P) + deg(Q) \tag{3.5}$$

$$val(PQ) \geq val(P) + val(Q) \tag{3.6}$$

Notion d'indéterminée

Définition 3.2.11. On appelle *indéterminée* le polynôme, noté X, dont tous les coefficients sont nuls, sauf le coefficient d'indice $1 \in \mathbb{N}$ qui est égal à $1 \in K$:

$$X = (0, 1, 0, 0, \ldots). \tag{3.7}$$

L'égalité (3.7) donne aisement :

$$\begin{aligned} X^2 &= (0, 0, 1, 0, \ldots) \\ X^3 &= (0, 0, 0, 1, 0, \ldots) \\ &\vdots \\ X^n &= (0, 0, \ldots, 1, 0, \ldots) \end{aligned}$$

où le coefficient 1 de X^n se trouve au $(n+1)^{\text{ème}}$ rang.

On voit que pour tout $a_n \in K$,

$$a_n X^n = (0, \ldots 0, a_n, 0, \ldots)$$

d'où, si $a_0, a_1, \ldots$, sont des éléments de K et si $a_k = 0$ pour $k > n$,

$$(a_0, a_1, \ldots, a_n, 0 \ldots) = a_0 + a_1 X + \cdots + a_n X^n$$

Nous écrivons désormais le polynôme $P = (a_0, a_1, 0, \ldots)$ de degré n sous la forme

$$a_0 + a_1 X + \cdots + a_n X^n = \sum_{k=0}^{n} a_k X^k \tag{3.8}$$

Lorsque on écrit P sous la forme $a_0 + a_1 X + \cdots + a_n X^n$, on dit que P est *ordonné suivant les puissances croissantes* de X. Si on écrit $P = a_n X^n + \cdots + a_1 X + a_0$, on dit que P est *ordonné suivant les puissances décroissantes* de X.

Le coefficient a_n est appelé *coeffeicient dominant* de P. Lorsque $a_n = 1$, on dit que le polynôme P est *unitaire ou normalisé.*

3.2.3 Propriétés arithmétiques de $K[X]$

Dans ce paragraphe, on désigne par K un corps commutatif.

Division eucidienne dans $K[X]$

Définition 3.2.12. Soient A et B deux polynômes de $K[X]$. On dit que B *divise* A, et l'on note $B \mid A$ s'il existe un polynôme Q de $K[X]$ tel que $A = BQ$. On dit aussi que A est *multiple* de B, ou que B est un *diviseur* de A.

Théorème 3.2.13. *Soient A et B deux polynômes de $K[X]$ tels que $B \neq 0$. Alors il existe un couple unique (Q, R) de polynômes de $K[X]$ tels que*

$$A = BQ + R \text{ avec } deg(R) < deq(B).$$

Q s'appelle le quotient et R le reste de la division euclidienne de A par B. A s'appelle le divideente, B le diviseur.

Exercice 3.2.14. Diviser $A = X^4 + X^2 - 4X + 2$ par $B = X^2 + 2X + 1$.

Polynômes irréductibles

Définition 3.2.15. On dit qu'un polynômes de $K[X]$ est *premier ou irréductible* sur le corps K s'il n'est pas constant et si ses seuls diviseurs dans $K[X]$ sont les polynômes associés à P et les éléments non nuls de K. **Cette de définitions dépend essentiellement du corps K.**

Remarque 3.2.16. Dire qu'un polynôme de $K[X]$ est irréductible revient à dire qu'il est impossible de l'écrire comme produit de deux polynômes non constants de $K[X]$.

Exemple 3.2.17. Tout polynôme P de $K[X]$, du premier degré, est irréductible. En effet, si $P = AB$, avec $A, B \in K[X]$, on a $1 = deg(P) = deg(A) + deg(B)$ donc, nécessairement, l'un des polynômes A ou B est de degré 0 et l'autre de degré un.

Exercice 3.2.18. Montrer que le polynôme $X^2 - 2$ est irréductible sur $\mathbb{Q}[X]$.

3.2.4 Division suivant les puissances croissantes

K désigne un corps commutatif. Nous présentons dans ce paragraphe la division suivant les puissances croissantes. Il s'agit, étant donnés deux polynômes A et B, de trouver un polynôme Q tel que $val(A - BQ)$ soit supérieure à un entier naturel fixé à l'avance.

Théorème 3.2.19. *Soient n un entier naturel, A un polynôme quelconque et B un polynôme tel que $val(B) = 0$. Il existe un couple (Q, R) de polynômes de $K[X]$ tels que*

$$A = BQ + X^{n+1}R \text{ avec } deg(Q) \leq n. \tag{3.9}$$

Définition 3.2.20. Pour un entier n donné, l'écriture (3.9) s'appelle la *division suivant les puissances croissantes de A par B à l'ordre n*. Dans cette division Q est le *quotient à l'ordre n et $X^{n+1}R$ le reste à l'ordre n.*

Exercice 3.2.21. Diviser $A = 1+X$ par $B = 1-X+X^2$ suivant les puissances croissantes de X à l'ordre 2.

3.2.5 Fonction polynômes, Racines d'un polynôme

Définition 3.2.22. Soient K un anneau commutatif et $P = a_0 + a_1X + \cdots + a_nX^n$, un polynôme de $K[X]$. On appelle *fonction polynôme ou fonction polynomiale* associée au polynôme P, l'application $\widetilde{P}$ de K dans K, associant à tout x de K l'élément

$$\widetilde{P} = a_0 + a_1x + \cdots + a_nx^n.$$

Remarque 3.2.23. La fonction polynôme associée au polynôme P se note souvent à l'aide du même symbole P, mais cette notation est dangereuse à cause des confusions possibles.

Dans la suite, on suppose que K est un corps commutatif.

Définition 3.2.24. Soient P un polynôme de $K[X]$ et a un élément de K. On dit que a est une *racine ou un zéro* de P si $\widetilde{P}(a) = 0$.

Théorème 3.2.25. *Soient $P \in K[X]$ et $a \in K$. Pour que a soit racine de P, il faut et il suffit que P soit divisible par $X - a$.*

Démonstration. Si P est divisible par $X-a$, alors il existe $Q \in K[X]$ tel que $P = (X-a)Q$; donc, pour tout $x \in K$, on a $\widetilde{P}(x) = (x-a)\widetilde{Q}(x)$. Si en particulier $x = a$, on a $\widetilde{P}(a) = 0$. Donc a est une racine de P.

Réciproquement, supposons que $\widetilde{P}(a) = 0$. Effectuons la division euclidienne de P par $X - a$. On obtient $P = (X - a)Q + R$ avec $deg(R) < deg(X - a) = 1$, donc R est un polynôme constant. En prenant les valeurs des fonctions polynômes associés au point $x = a$, il vient $0 = \widetilde{P}(0) = 0 \cdot \widetilde{Q}(a) + R$. Donc P est divisible par $X - a$. □

Définitions 3.2.26.

- Soient $P \in K[X]$, a un élément de K et $\alpha \geq 1$. On dit que a est une *racine d'ordre α ou de miltiplicité α* de P, si P est divisible par $(X - a)^\alpha$ sans l'être par $(X - a)^{\alpha+1}$.
- On dit que l'entier α est la *multiplicité ou l'ordre de multiplicité* de la racine a.
- Une racine d'ordre 1 est dite *racine simple*, une racine d'ordre 2 est dite *racine double*, ...

Définition 3.2.27. On dit qu'un polynôme P de $K[X]$ est *scindé* sur K si $P = 0$, ou, dans le cas contraire, si P est décomposable en un produit de facteurs du premier degré (distincts ou non) de $K[X]$.

3.3 Corps des fractions rationnelles

Soit K un corps commutatif. Nous savons que l'ensemble $K[X]$ des polynômes à une indéterminée à coefficients dans K est un anneau commutatif intègre dans lequel les seuls éléinversibles sont les polynômes de degré 0. $K[X]$ n'est donc pas un corps, mais on peut construire le corps des fractions de $K[X]$. Ce corps s'appelle le *corps des fractions rationnelles à une indéterminée à coefficients dans K*. On le note $K(X)$.

3.3.1 Fractions rationnelles

On pose $K[X]^* = K[X]\backslash\{0\}$.

- $K(X)$ est l'ensemble quotient de $K[X] \times K[X]^*$ par la relation d'équivallence $\mathcal{R}$:

$$(A, B)\mathcal{R}(A_1, B_1) \Leftrightarrow AB_1 = A_1B.$$

  Une fraction rationnelle F de $K(X)$ est donc une classe d'équivalence représentée par un couple (A, B) d'éléments de $K[X]$ dans lequel $B \neq 0$. Et un autre couple (A_1, B_1) représente la même fraction F si, et seulement si $AB_1 = A_1B$.
- Si (A, B) est un représentant quelconque de F, on convient d'écrire $F = \frac{A}{B}$; on dit que A est le *numérateur* et que B est le *dénominateur* de la fraction rationnelle F.
- Dans $K[X] \times K[X]^*$, on définit l'addition et la multiplication en posant :

$$\frac{A}{B} + \frac{C}{D} = \frac{AD + BC}{BD} \quad \text{et} \quad \frac{A}{B} \cdot \frac{C}{D} = \frac{AC}{BD}$$

  Les deux lois de $K(X)$ sont les lois quotients , alors le triplet $(K(X), +, \cdot)$ est un corps commutatif. L'élément neutre pour l'addition est la fraction nulle 0 qui est la classe des couples $(0, B)$ tels que $B \neq 0$. L'élément neutre pour la multiplication, appelée *fraction rationnelle unité*, et noté 1, est la classe des couples (B, B) avec $B \neq 0$.

Théorème 3.3.1. *Soit $F \in K(X)\backslash\{0\}$. Si $\frac{A}{B}$ est un représentant quelconque de F, l'entier $deg(A) - deg(B)$ ne dépend que de F. On appelle le degré de la fraction rationnelle F, et on le note $deg(F)$.*

Démonstration. Soient $\frac{A}{B}$ et $\frac{A_1}{B_1}$ deux représentants de F. On a $AB_1 = A_1B$, donc $deg(A) + deg(B_1) = deg(A_1) + deg(B)$. Comme $deg(B), deg(B_1) \in \mathbb{N}$, puisque $B \neq 0$ et $B_1 \neq 0$, on en déduit que $deg(A) - deg(B) = deg(A_1) - deg(B_1)$. □

Comme pour les polynômes, on convient de poser $deg(0) = -\infty$.

Théorème 3.3.2. *Si $\frac{A}{B}$ et $\frac{C}{D}$ sont des éléments non nuls de $K(X)$, on a*

$$\begin{aligned} deg(\frac{A}{B} + \frac{C}{D}) &\leq \max\left(deg\left(\frac{A}{B}\right), deg\left(\frac{C}{D}\right)\right) \\ deg(\frac{A}{B} \cdot \frac{C}{D}) &= deg\left(\frac{A}{B}\right) + deg\left(\frac{C}{D}\right)\end{aligned}$$

Définition 3.3.3. Soit $F \in K(X)\backslash\{0\}$. On appelle *représentant irréductible de F ou forme irréductible de F* toute représentation de F sous la forme $\frac{A}{B}$, où A et B sont des éléments de $K[X]$ premiers entre eux.

Théorème 3.3.4. *Soit F un élément de $K(X)\backslash\{0\}$. Alors :*
- *F possède des représentants irréductibles.*
- *Si (A, B) est un représentant irréductible de F, les autres représentants irréductibles de F sont de la forme $(\lambda A, \lambda B)$, où $\lambda \in K^*$, et les représentants de F sont de la forme (AC, BC), où $C \in K[X]^*$.*

Définitions 3.3.5. Soit $F = \frac{P}{Q}$ une fraction rationnelle de $K(X)$ écrite sous forme irréductible. On appelle *pôle* de F toute racine de son dénominateur. On dit $a \in K$ est un *pôle d'ordre α de F* si a est un zéro d'ordre α de Q. Toute racine de multiplicité k du polynôme P est dit racine *d'ordre k* de F.

3.3.2 Décomposition d'un fraction rationnelle en éléments simples

Théorèmes généraux

Lemme 3.3.6. *Soit F un élément de $K(X)$. Il existe un unique polynôme E tel que l'on ait $F = E + R$ où R est une fraction rationnelle de degré strictement négatif. On dit que E est la partie entière de F.*

Démonstration. Soit $\frac{A}{B}$ un représentant quelconque de F. Comme $B \neq 0$, on peut effectuer la division euclidienne de A par B. On obtient

$$A = EB + D \text{ avec } D = 0 \text{ ou } deg(D) < deg(B).$$

Si $D = 0$, $F = E + 0$ et l'existence est établie. Sinon, on a

$$\frac{A}{B} = \frac{EB + D}{B} = E + \frac{D}{B}.$$

Posons $R = \frac{D}{B}$; on a $deg(R) < 0$.

L'écriture est unique car si E et E_1 sont des polynômes tels que $F = E + R = E_1 + R_1$ avec $deg(R) < 0$ et $deg(R_1) < 0$, on a

$$deg(E_1 - E) = deg((F - E) + (E_1 - F)) \leq \max(deg(F - E), deg(E_1 - F)).$$

On en déduit que $deg(E_1 - E) < 0$ car $deg(F - E) = deg(R) < 0$ et $deg(E_1 - F)) = deg(R_1) < 0$. Donc $E_1 = E$. □

Définition 3.3.7. Toute fraction rationnelle de la forme $\frac{A}{B^\alpha}$, où B est un polynôme irréductible de $K[X]$, α un entier supérieur ou égal à 1 et ~~où~~ $deg(A) < deg(B)$, s'appelle un *élément simple.*

Théorème 3.3.8 (décomosition)**.** *Soit F une fraction rationnelle de $K(X)$ écrite sous sa forme irréducitble $\frac{P}{Q}$, Q étant un polynôme de degré au moins égal à 1. Si $Q = \lambda A^\alpha B^\beta \cdots L^\gamma$ est la décomposition de Q en facteurs irreductibles, il existe une famille unique*
$E, A_1, \ldots, A_\alpha, B_1, \ldots, B_\beta, \ldots L_1, \cdots L_\gamma$ de polynômes de $K[X]$ tels que

$$\begin{aligned} \frac{P}{Q} \quad = \quad & E + \frac{A_1}{A} + \frac{A_2}{A^2} + \cdots + \frac{A_\alpha}{A^\alpha} \\ & + \frac{B_1}{B} + \frac{B_2}{B^2} + \cdots + \frac{B_\beta}{B^\beta} \textbf{+...} \\ & + \frac{L_1}{L} + \frac{L_2}{L^2} + \cdots + \frac{L_\gamma}{L^\gamma} \end{aligned}$$

et $deg(A_i) < deg(A)$, $deg(B_i) < deg(B), \ldots, deg(L_i) < deg(L)$ pour tout i.

Calculer ces polynômes, c'est *décomposer la fraction rationnelle F en éléments simples.*

E est appelé la partie entière de F

Décomposition en éléments simples d'une fraction rationnelle sur $\mathbb{C}$

Les polynômes irréductibles de $\mathbb{C}[X]$ sont de la forme $X - a$, où $a \in \mathbb{C}$. Le Théorème 3.3.8 se simplifie de la manière suivante :

Théorème 3.3.9. *Soit F une fraction rationnelle de $\mathbb{C}[X]$ écrite sous forme irréductible $\frac{P}{Q}$ telle que $deg(Q) \geq 1$. Si $Q(X) = \lambda(X-a_1)^{\alpha_1}(X-a_2)^{\alpha_2}\cdots(X-a_n)^{\alpha_n}$ est la décomposition de Q en facteurs irréductibles, il existe un polynôme unique E et une unique famille de scalaires $(b_{ij})_{1\leq i\leq n,\ 1\leq j\leq \alpha_i}$ tels que :*

$$F = E + \sum_{i=1}^{n}\Big(\sum_{j=1}^{\alpha_i}\frac{b_{ij}}{(X-a_i)^j}\Big).$$

Remarque 3.3.10. L'expression

$$\sum_{j=1}^{\alpha_i}\frac{b_{ij}}{(X-a_i)^j},$$

s'appelle la *partie polaire ou partie principale* de F relative au pôle a_i.

Étant donné une fraction rationnelle F de $\mathbb{C}(X)$, sa partie entière s'obtient en effectuant la division euclidienne du numérateur de F par son dénominateur. Nous supposons dans la suite que cette opération a été faite et nous ne considérons que des fractions rationnelles de degré strictement négatif.

a) **Partie polaire relative à un pôle multiple :** Soit $F(X) = \frac{P(X)}{(X-a)^k Q(X)}$ une fraction rationnelle de $\mathbb{C}(X)$ de degré strictement négatif admetant a pour pôle d'ordre k. On a $P(a) \neq 0$ et $Q(a) \neq 0$, et la décomposition de F s'écrit :

$$F(X) = \frac{b_1}{X-a} + \frac{b_2}{(X-a)^2} + \cdots + \frac{b_k}{(X-a)^k} + \frac{P_1(X)}{Q(X)}.$$

D'où Posons Y =X-a=> X=Y+a

$$P(X) = (b_k + b_{k-1}(X-a) + \cdots + b_1(X-a)^{k-1})Q(X) + (X-a)^k P_1(X)$$

Prenons alors le polynôme $X - a = Y$ comme nouvelle indéterminée. On obtient alors

$$P(a+Y) = (b_k + b_{k-1}Y + \cdots + b_1 Y^{k-1})Q(a+Y) + Y^k P_1(a+Y)$$

La partie polaire relative au pôle a apparaît ainsi comme quotient de la division suivant les puissances croissantes de $P(a+Y)$ par $Q(a+Y)$ à l'ordre $k-1$.

b) **Partie polaire relative à un pôle simple :** Si $\frac{P}{Q}$ est une fraction rationnelle irréductible de $\mathbb{C}(X)$ admettant le nombre a pour pôle simple, alors en posant $Q(X) = (X-a)Q_1(X)$, on a une décomposition de la forme $\frac{P(X)}{(X-a)Q_1(X)} = \frac{A}{X-a} + \frac{R(X)}{Q_1(X)}$ avec $Q_1(a) \neq 0$.
Multiplions les deux membres par $X-a$ puis faisons $X = a$; on obtient $A = \frac{P(a)}{Q_1(a)}$.

Exercice 3.3.11. Décomposer la fraction rationnelle $F(X) = \frac{1}{X(X+1)(X-1)^3}$ en éléments simples sur $\mathbb{C}$.

Décomposition en éléments simples d'une fraction rationnelle sur $\mathbb{R}$

Dans $\mathbb{R}[X]$, les polynômes irréductibles sont les polynômes du premier degré et ceux du second degré à discriminant négatif.

Théorème 3.3.12. *Soit F une fraction rationnelle de $\mathbb{R}(X)$ admettant un représentant irréductible $\frac{P}{Q}$ tel que $deg(Q) \geq 1$. Si*

$$Q(X) = \lambda \prod_{i=1}^{n} (X-a)^{\alpha_i} \prod_{j=1}^{m} (X^2 + p_j X + q_j)^{\beta_j}$$

est la décomposition de Q en polynômes irréductibles, il existe un unique polynôme E et des familles uniques de nombres réels $(A_{ij})_{1\leq i\leq n,\ 1\leq j\leq \alpha_i}$, $(B_{kr})_{1\leq k\leq m,\ 1\leq r\leq \beta_k}$ et $(C_{kr})_{1\leq k\leq m,\ 1\leq r\leq \beta_k}$ tels que

$$F = E + \sum_{i=1}^{n} \Big(\sum_{j=1}^{\alpha_i} \frac{A_{ij}}{(X-a_i)^j} \Big) + \sum_{k=1}^{m} \Big(\sum_{r=1}^{\beta_k} \frac{B_{kr}X + C_{kr}}{(X^2 + p_k X + q_k)^r} \Big).$$

Définition 3.3.13. Dans la décomposition en éléments simples d'une fraction rationnelle de $\mathbb{R}(X)$, une fraction de la forme $\frac{A_{ij}}{(X-a_i)^j}$ s'appelle un *élément simple de première espèce*, une fraction de la forme $\frac{B_{kr}X+C_{kr}}{(X^2+p_kX+q_k)^r}$ s'appelle un *élément simple de deuxième espèce.*

a) Pour la recherche de la partie entière et les éléments simples de première espèce, tout ce qui a été dit dans la sous section précédente reste valable.
b) Pour les éléments simples de deuxième espèce, les méthodes suivantes peuvent être utilisées :
- On écrit la décomposition de F à l'aide de coefficients indéterminés et on détermine ces coefficients par des considérations numériques particulières ; l'examen de la parité de la fraction rationnelle considérée peut simplifier les calculs.
- On utilise la décomposition dans $\mathbb{C}(X)$ puis en regroupant les parties polaires relatives aux pôles conjugués, on obtient la décompositions dans $\mathbb{R}(X)$.
- Si F n'admet que deux pôles complexes conjugués, on procède par divisions successives.

Exercice 3.3.14. Décomposer les fractions rationnelle suivante en éléments simples sur $\mathbb{R}$: $F(X) = \frac{1}{(X^2-1)(X^2+1)^2}$; $G(X) = \frac{X}{(X+1)(X^2+1)}$; $H(x) = \frac{2X^4+X^3+1}{(X^2+X+1)^3}$.

Chapitre 4

Travaux dirigés

Exercice 4.0.1.
On considère la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 12 & 1 & 10 & 9 & 11 & 4 & 3 & 2 & 7 & 8 & 5 \end{pmatrix}$ de S_{12}.
1) Décomposer σ en produit de cycles à supports disjoints.
2) Décomposer σ en produit de transpositions.
3) Déterminer l'ordre, puis l'orbite de σ.
4) Quelle est la parité et la signature de σ.
5) Calculer σ^{1999}.

Exercice 4.0.2.
1) Déterminer la table de Pythagore de (S_3, o).
2) Quel est l'inverse de $\mu = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$?
3) Déterminer le sous-groupe de S_3 engendré par $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.
4) Déterminer tous les sous-groupes de S_3.

Exercice 4.0.3.
Soit $(G, \cdot)$ un groupe multiplicatif ; H et K deux sous-groupe distincts de G d'ordre un même nombre premier $p \geq 2$. Montrer que $H \cap K = \{1\}$.

Exercice 4.0.4.
Montrer que tout groupe fini G d'ordre p premier est cyclique.

Exercice 4.0.5.
Soit $(G, \cdot)$ un groupe fini d'ordre $n \geq 2$ et H un sous-groupe de G d'indice 2. Montrer que H est distingué.

Exercice 4.0.6.
Déterminer l'ordre d'un élément du groupe multiplicative $(\mathbb{C}^*, \cdot)$.

Exercice 4.0.7.
On dit qu'un anneau A est un anneau de Boole si, pour tout $x \in A$, $x^2 = x$. On fixe A un tel anneau.
1) Montrer que pour tout $x \in A$, $x = -x$.
2) Montrer que A est commutatif.