Université Mohammed Premier
Faculté Pluridisciplinaire de Nador
Département de Mathématiques
Nador

Deuxième Année Universitaire
Semestre 4
Filières : SMA

ALGÈBRE 6
COURS ET EXERCICES

Professeur : Taoufik Serraj

Année universitaire : 2020-2021
Version 1

Table des matières

1. **Introduction** 4
2. **Les groupes** 6
2.1. Définition et exemples 6
2.2. Sous-groupe 7
2.3. Homomorphismes de groupes 9
2.4. Relations modulo un sous groupe 12
2.5. Sous-groupes distingués 17
2.6. Sous-groupe engendré par une partie 23
2.7. Groupes monogènes 25
2.8. Ordre d'un élément dans un groupe 27
2.9. Retour aux groupes cycliques 30
2.10. Théorèmes d'isomorphismes 34
2.11. Exercices 38
3. **Le groupe symétrique S_n** 45
3.1. Définitions et Propriétés 45
3.2. Générateurs de $S(E)$ 52
3.3. Signature d'une permutation 53
3.4. Groupe alterné 56
3.5. Exercices 58
4. **Les Anneaux et les Corps** 59
4.1. Les anneaux : Définition et propriétés 59
4.2. Les corps 64
4.3. Homomorphismes d'anneau 65
4.4. Les idéaux d'un anneau 67
4.5. Anneaux quotients 72
4.6. Caractéristique d'un anneau 76
4.7. Idéaux étrangers 78
4.8. Idéaux premiers 80
4.9. Idéaux maximaux 81
4.10. Divisibilité dans un anneau intègre 83
4.11. PGCD et PPCM 86
4.12. Les anneaux principaux 88
4.13. Exercices 94

5. **Polynômes à plusieurs indéterminées** 98
5.1. Polynômes à une indéterminée à coefficients dans un anneau 98
5.2. Notions sur les polynômes à n indéterminées 106
5.3. Exercices 122
Références 123

1. **Introduction**

La notion de groupe joue un rôle fondamental en mathématiques. C'est l'une des principales structures algébriques, avec celles d'anneau, de corps, modules, et espaces vectoriels. D'une part, elle formalise les propriétés de plusieurs des opérations bien connues entre des objets mathématiques divers comme les : nombres, vecteurs, matrices, fonctions, etc. D'autre part, elle donne un contexte clair pour discuter de transformations de toutes sortes : rotations, translations, symétries, etc. ; ou encore de manipulations d'objets. Elle est essentielle pour comprendre des aspects fondamentaux de la physique (théorie de la relativité, théorie des quantas), de la chimie (calcul des isomères), de la cristallographie (symétries des cristaux), de la cryptographie à clé publique (système RSA, courbes elliptiques), et de l'étude des codes correcteurs d'erreurs. Elle joue aussi un rôle fondamental en théorie de Galois (qui étudie la résolution d'équations polynomiales), en théorie des nombres, en géométrie, et dans la théorie des invariants. Bref, c'est l'une des notions les plus intéressantes parmi celles élaborées par les mathématiciens.

Les origines de la théorie des groupes remontent aux travaux sur la recherche des racines de polynômes, travaux qui eurent en point d'orgue les résultats d'Evariste Galois (1811-1832) auteur de la célèbre théorie éponyme, au début du XIXème siècle.

Galois a, entre autres, introduit les notions de normalité, suites de composition, groupes résolubles, ...

Au départ, les groupes étaient des groupes de permutations de racines, ce n'est qu'avec Cayley (pour les groupes finis) en 1854 et Weber en 1889 qu'apparaît la notion abstraite de groupe. Ensuite, la théorie fut développée par Jordan, Frobenius, Burnside, Schering, Noether, et bien d'autres.

Parallèlement à cet aspect purement algébrique, la notion de groupes apparaît en géométrie avec les travaux de Klein sur la géométrie projective.

Dans une premiere partie, on pose la base de la théorie des groupes. On commence par définir ce qu'est un groupe (cours Structure). Ensuite, on regarde si un sous-ensemble d'un groupe peut conserver la structure de groupes (Sous-groupes). On étudie, les applications entre les groupes qui conservent la structure de groupe (Homomorphismes). Enfin, on construit un groupe à partir du produit direct ensemblistes de deux groupes donnés (Produit direct).

Dans une autre partie, on étudie une classe de groupes : les groupes cycliques : On commence par étudier la relation de congruence et les groupes formés à partir de celle-ci (Congruence) puis on définit la notion de groupes cycliques. Ensuite, on étudie une notion fondamentale : le groupe quotient :

On étudie, la notion de normalité d'un sous-groupe d'un groupe donné (Sous-groupes normaux). A partir des sous-groupes normaux, on construit les groupes quotients qui apparaissent très fréquemment en théorie des groupes. Ces groupes quotients interviennent en particulier dans les théorèmes d'isomorphismes, théorèmes dont le premier est l'un des théorèmes essentiels de la théorie des groupes.

On définit ensuite les groupes symétriques et on étudie leurs propriétés.

Le deuxième chapitre traite les anneaux et les corps : leurs définitions, propriétés et introduit les notions des idéaux et leurs caractéristiques.

Le dernier chapitre donne des notions préliminaires des polynômes à plusieurs indéterminées.

2. Les groupes

2.1. Définition et exemples.

Définition 1. Soit E un ensemble. Une loi de composition interne sur E est une application de $E \times E$ dans E. Si on la note $* : \quad E \times E \longrightarrow E;\ (a,b) \longmapsto a * b$ on parle alors de la loi $*$ et on dit que $a * b$ est le composé de a et b pour la loi $*$. (On utilisera aussi les notations $\perp$, $\top$, $\cdot$, $+$, $\diamond$, ...)

Définition 2. On dit qu'un couple $(G, \cdot)$, où le point désigne une loi de composition interne sur G, est un groupe si les trois axiomes suivants sont vérifiés :

i. La loi " $\cdot$ " est associative, c-à-d $\forall\, x,\, y,\, z \in G,\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$.

ii. La loi "$\cdot$" admet un élément neutre, c-à-d $\exists\, e \in G$ tel que $\forall\, x \in G\,;\, x \cdot e = e \cdot x = x$.

iii. Tout élément x de G admet un symétrique $x' \in G$ pour la loi " $\cdot$ ", c-à-d $\forall\, x \in G$, $\exists\, x' \in G$ tel que $x \cdot x' = x' \cdot x = e$.

Exemples 1.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, et $(\mathbb{C}, +)$ sont des groupes.
- $(\mathbb{Q}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes.
- $(\mathbb{N}^*, \times)$, $(\mathbb{Z}^*, \times)$, ne sont pas des groupes, car 2 n'a pas d'inverse dans $\mathbb{N}^*$ et dans $\mathbb{Z}^*$ pour $\times$.
- $(\mathcal{P}(E), \triangle)$ est un groupe.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe, $n \in \mathbb{N}$.
- $(\mathbb{Z}/p\mathbb{Z} - \{0\}, \times) = ((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est un groupe si et seulement si p est un premier.
- Soient $n \in \mathbb{N}^*$ et $K = \mathbb{Q}$ ou $\mathbb{R}$ ou $\mathbb{C}$. Soit $\mathrm{GL}_n(K)$ l'ensemble des matrices carrées de type $n \times n$ inversibles, c'est-à-dire de déterminant non nul. Alors muni du produit matriciel $\mathrm{GL}_n(K)$ est un groupe, appelé *groupe linéaire*.
- Soient E un ensemble non vide, et $S(E)$ l'ensemble des applications bijectives de E sur E. Alors $(S(E), \circ)$ est un groupe. $S(E)$ est appelé *groupe des permutations ou groupe symétrique* de E. Si $E = \{1, 2, 3, \cdots, n\}$, alors $S(E)$ est noté S_n, et est appelé *groupe symétrique* d'ordre n, et on a $\mathrm{card}(S_n) = n!$ (voir §3)

Définition 3. Un groupe peut être fini ou infini. Le cardinal d'un groupe fini G (i.e. le nombre de ses éléments) est aussi appelé ordre de G, il est noté $\mathrm{card}(G)$ ou $|G|$ ou $\#G$.

Définition 4. un groupe $(G, \cdot)$ est dit commutatif (ou abélien) si la loi " $\cdot$ " est commutative, c-à-d $\forall\, x,\, y \in G,\ x \cdot y = y \cdot x$.

Exemples 2.

1. $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{R}^*,\times)$, $(\mathbb{Q}^*,\times)$, $(\{-1,1\},\times)$ sont des groupes abéliens.
2. Soient E un ensemble et $\triangle$ la différence symétrique définie sur $\mathcal{P}(E)$. Alors $(\mathcal{P}(E),\triangle)$ est un groupe abélien.
3. Soit E un ensemble. En général, $(S(E),\circ)$ est un groupe non commutatif.
4. $S(E)$ n'est pas abélien si E a au moins 3 éléments (voir §3).
5. Pour $n \geq 2$, $\mathrm{GL}_n(K)$ est non commutatif.

Notation. Soient $(G,\cdot)$ un groupe et $x \in G$.

- Si la loi est notée multiplicativement, le symétrique d'un élément x sera noté x^{-1} et appelé l'inverse de x et le produit $x \cdot y$ est noté xy.
- Si la loi est notée additivement $(+)$, l'élément neutre sera noté 0_G ou simplement 0 et le symétrique de x sera noté $-x$ et appelé l'opposé de x.
- Soit $(n \in \mathbb{N})$; on note $x^n = \underbrace{x \cdot \cdots \cdot x}_{n \text{ fois}}$.

  Si de plus x est inversible, on note $x^{-n} = (x^{-1})^n$.

Théorème 1. *Si G est un groupe fini d'élément neutre e et d'ordre n, alors $\forall g \in G$, $g^n = e$.*

Preuve. Voir TD. □

Proposition 1. *Soient $(G,\cdot)$ un groupe et e son élément neutre. Alors*

1. *$G \neq \varnothing$, car $e \in G$.*
2. *e est unique.*
3. *Le symétrique d'un élément est unique.*
4. *Tout élément $a \in G$ est régulier, c'est-à-dire*
   $\forall\ (x,y) \in G^2$ on a : $(x \cdot a = y \cdot a \Rightarrow x = y)$ et $(a \cdot x = a \cdot y \Rightarrow x = y)$.
5. *$\forall\, a,b \in G$, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ et $(a^{-1})^{-1} = a$.*

Preuve. Facile laisser au lecteur. □

2.2. **Sous-groupe.**

Définition 5. Soit $(G,\cdot)$ un groupe. On dit qu'une partie <u>non vide</u> H de G est un sous-groupe de G si les conditions suivantes sont vérifiées :

i. H est stable pour la loi " $\cdot$ ".

ii. $(H,\cdot)$ est un groupe.

Remarques 1. Soit G un groupe d'élément neutre e.

1. G et $\{e\}$ sont des sous-groupes de G.
2. Tout sous-groupe H de G différent de G et $\{e\}$ est dit un sous-groupe propre de G.
3. Tout sous-groupe H de G contient $\{e\}$.
4. Si H est un sous-groupe de G et K un sous-groupe de H, alors K est un sous-groupe de G.

Théorème 2. *Soient G un groupe d'élément neutre e, et H une partie de G. Pour que H soit un sous-groupe de G, il faut et il suffit qu'on ait :*

1. $e \in H$.
2. *H est stable pour la loi de groupe de G.*
3. $\forall\ x \in H$ *le symétrique x' de x appartient à H.*

Preuve. Supposons que H est un sous-groupe de G, alors 1. et 2. sont vérifiés. Soient $x \in H$ et x' son symétrique dans G et x'' son symétrique dans H. On a

$$x \cdot x' = x \cdot x'' = e$$

puisque le neutre de G est celui de H, d'où $x' = x''$, car x est régulier dans G. Donc 3. est aussi vérifié.

Inversement, supposons que les assertions 1., 2. et 3. sont vérifiées, alors la loi induite par G sur H est une loi de groupe. En effet, puisque $H \neq \varnothing$ il existe $a \in H$. D'après 3. $a^{-1} \in H$, d'où par 2., $a \cdot a^{-1} = e \in H$. Donc H possède l'élément neutre e. Pour tout $x \in H$, par 3., x admet dans H un symétrique. Par suite H est un sous-groupe de G. □

Remarques 2.

1. Dans le théorème 2, on peut remplacer la condition 1. par $H \neq \emptyset$, et les conditions 2. et 3. par l'unique condition suivante : $\forall\ x, y \in H$, $xy^{-1} \in H$.
2. Dans plusieurs cas, pour montrer qu'un ensemble est un groupe, il est plus facile de montrer que c'est un sous-groupe d'un groupe connu.

Exemples 3.

1. $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$ qui est un sous-groupe de $(\mathbb{R}, +)$ qui est un sous-groupe de $(\mathbb{C}, +)$.
2. Pour tout $n \in \mathbb{N}$, posons $n\mathbb{Z} = \{na |\ a \in \mathbb{Z}\}$, alors $(n\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$.

3. Soit $(G,\cdot)$ un groupe, et soit $Z(G)=\{a\in G\,|\,ax=xa,\forall\, x\in G\}$, alors $Z(G)$ est un sous-groupe abélien de G, appelé *le centre* de G ; et on a :

$$G \text{ est commutatif si, et seulement si, } Z(G)=G.$$

Théorème 3. *Si $(H_i)_{i\in I}$ est une famille de sous-groupes d'un groupe G, alors $\bigcap_{i\in I} H_i$ est un sous groupe de G.*

Preuve.

1. $\bigcap_{i\in I} H_i \neq \varnothing$, car $e\in \bigcap_{i\in I} H_i$.
2. Soient x et y dans $\bigcap_{i\in I} H_i$, alors x et y sont dans H_i pour tout i, donc $xy^{-1}\in H_i$ pour tout i. D'où $xy^{-1}\in \bigcap_{i\in I} H_i$. Par suite $\bigcap_{i\in I} H_i$ est un sous groupe de G.

□

Remarque 1. Si $(H_i)_{i\in I}$ est une famille de sous-groupes d'un groupe G, alors $\bigcup_{i\in I} H_i$ n'est en général pas un sous-groupe de G.
Par exemple, soient H la droite d'équation $y=0$ et K la droite d'équation $x=0$ dans $\mathbb{R}^2$, qui est un groupe additif. Alors H et K sont des sous-groupes de $(\mathbb{R}^2,+)$, mais pas $H\cup K$, car $(1,0)+(0,1)=(1,1)$ n'appartient pas à $H\cup K$.

2.3. **Homomorphismes de groupes.**

Définition 6. Soient $(G,\cdot)$, $(E,\star)$ deux groupes et f une application de G dans E. On dit que f est un homomorphisme (ou morphisme) de G dans E si :

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

Si de plus f est bijectif, on dit que f est un isomorphisme de groupes (de G dans E) ou bien que G et E sont isomorphes et on écrit $G\simeq E$.
Si $G=E$ on dit que f est un endomorphisme de G ; un endomorphisme bijectif s'appelle un automorphisme, on note par $\mathrm{Aut}(\mathbf{G})$ l'ensemble des automorphismes de G.

Exemples 4.

1. La fonction exponentielle complexe $f : z\mapsto e^z$ est un homomorphisme de groupes de $(\mathbb{C},+)$ dans $(\mathbb{C}^*,\times)$. Par restriction, on obtient un isomorphisme de $(\mathbb{R},+)$ dans $(\mathbb{R}_+^*,\times)$
2. Soit $x\in\mathbb{N}^*$, alors $x\mapsto x+n$ n'est pas un automorphisme de $(\mathbb{Z},+)$ dans $(\mathbb{Z},+)$.

3. Soit a un élément d'un groupe G. L'application

$$\begin{array}{rcl} f_a : G & \longrightarrow & G \\ x & \longmapsto & a^{-1}xa \end{array}$$

est un homomorphisme, car

$$f_a(xy) = a^{-1}xya = (a^{-1}xa)(a^{-1}ya) = f_a(x)f_a(y).$$

Cet homomorphisme est en fait un automorphisme, car il est bijectif et sa réciproque est l'homomorphisme $f_a^{-1}(x) = axa^{-1}$ puisque

$$f_a \circ f_a^{-1}(x) = f_a(axa^{-1}) = a^{-1}(axa^{-1})a = x = f_a^{-1} \circ f_a(x).$$

Les automorphismes de cette forme s'appellent les *automorphismes intérieurs* de G, leur ensemble se note : $\mathrm{Int}(\mathbf{G})$.

4. Soit G un groupe d'élément neutre e, noté multiplicativement. Pour tout $n \in \mathbb{Z}$, définissons x^n, pour $x \in G$, par :

$$x^0 = e, \quad \begin{cases} x^n = x^{n-1}x & \text{si } n \geq 1, \\ n^n = (x^{-1})^{-n} & \text{si } n < 0. \end{cases}$$

Alors, pour un x fixé dans G, l'application

$$\begin{array}{rcl} f : \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & x^n \end{array}$$

est un homomorphisme de $(\mathbb{Z}, +)$ dans $(G, .)$, puisque la formule $x^{n+p} = x^n x^p$ est valable. f est l'unique homomorphisme de $(\mathbb{Z}, +)$ dans G vérifiant $f(1) = x$. Si G est noté additivement, cette application se note $f : n \longmapsto nx$ et la dernière formule s'écrit : $(n + p)x = nx + px$.

Proposition 2. *Soit $f : G \to G'$ un homomorphisme de groupes. Alors*

1. *$f(e) = e'$ avec e (resp. e') l'élément neutre de G (resp. G').*
2. *Pour tout $x \in G$, $f(x^{-1}) = (f(x))^{-1}$.*
3. *$\forall\, n \in \mathbb{Z}$, $\forall\, x \in G$, $f(x^n) = (f(x))^n$.*
4. *Pour tout sous-groupe H de G, $f(H)$ est un sous-groupe de G'.*
5. *Pour tout sous-groupe H' de G', $f^{-1}(H')$ est un sous-groupe de G.*

Preuve. Soient $(G, \cdot)$, $(G', \star)$ deux groupes et f un homomorphisme de G dans G'.

1. On a : $e' \star f(e) = f(e) = f(e \cdot e) = f(e) \star f(e)$. Puisque $f(e)$ est régulier, alors $e' = f(e)$.

2. Soit $x \in G$, alors $f(x)^{-1} \star f(x) = e' = f(e) = f(x^{-1} \cdot x) = f(x^{-1}) \star f(x)$, ce qui donne

que $f(x^{-1}) = [f(x)]^{-1}$, car $f(x)$ est régulier.

3. Par recurrence sur n.

4. Montons que $f(H)$ est sous-groupe de G'.

• On a $f(H) \subset G'$ tel $f(H) \neq \emptyset$, car $e' = f(e) \in f(H)$.

• Soient y_1 et y_2 deux élément de $f(H)$, alors il existe x_1 et $x_2 \in G$ tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$, donc

$$y_1 \star y_2^{-1} = f(x_1) \star f(x_2)^{-1} = f(x_1) \star f(x_2^{-1}) = f(x_1 \cdot x_2^{-1}) \ .$$

Or H est un sous-groupe de G, alors $x_1 \cdot x_2^{-1} \in H$, ainsi $y_1 \star y_2^{-1} \in f(H)$. On conclu que $f(H)$ est sous-groupe de G'.

5. Soit H' un sous-groupe de G', posons $H = f^{-1}(H')$ et montrons que H est un sous-groupe de G. Remarquons d'abord que $H = f^{-1}(H') \subset G$.

• On a $H \neq \emptyset$, car $e \in H$ puisque $e' = f(e) \in H'$.

• Soient x_1 et x_2 deux élément de H, alors $y_1 = f(x_1) \in H'$ et $y_2 = f(x_2) \in H'$, donc

$$y_1 \star y_2^{-1} = f(x_1) \star f(x_2)^{-1} = f(x_1) \star f(x_2^{-1}) = f(x_1 \cdot x_2^{-1}) \in H'.$$

D'où $x_1 \cdot x_2^{-1} \in H$. On conclu que $f^{-1}(H')$ est sous-groupe de G. □

Définition 7. Soit $f : G \to G'$ un homomorphisme de groupes.

i. Le sous-groupe $f(G)$ de G' est appelé image de f, et est noté $\mathrm{Im}f$.

ii. Si e' est l'élément neutre de G'. Le sous-groupe $f^{-1}(\{e'\})$ de G est appelé noyau de f, et est noté $\ker(f)$, et on a $\ker(f) = \{x \in G |\ f(x) = e'\}$

Théorème 4. *Soient $f : G \to G'$ un homomorphisme de groupes et e l'élément neutre de G. Alors on a :*

1. *f est surjectif si, et seulement si,* $\mathrm{Im}f = G'$
2. *f est injectif si, et seulement si,* $\ker(f) = \{e\}$.

Preuve. 1. Facile.

2. Soient x et x' dans G et notons par e' l'élément neutre de G', alors

$$\begin{aligned} f(x) = f(x') &\iff f(x)f(x')^{-1} = e', \\ &\iff f(xx'^{-1}) = e', \\ &\iff xx'^{-1} \in \ker(f). \end{aligned}$$

Donc si $\ker(f) = \{e\}$, alors $f(x) = f(x') \Longrightarrow xx'^{-1} = e \Longrightarrow x = x'$. D'où f est injectif. Inversement, supposons que f est injectif. Soit $x \in \ker(f)$, alors $f(x) = f(e) \Longrightarrow x = e$. D'où le résultat. □

Proposition 3. *Le composé de deux homomorphismes (resp. isomorphismes) de groupes est un homomorphisme (resp. isomorphisme) de groupes.*

Preuve. Simple à vérifier. □

2.4. **Relations modulo un sous groupe.**
On se donne un groupe multiplicatif $(G, \cdot)$. Commençons par les définitions suivantes.

Définition 8. Soient H, K deux sous-ensembles non vides d'un groupe G, on pose :

$$HK = \{hk \mid h \in H \text{ et } k \in K\}.$$

En particulier, pour tout $g \in G$ on a :

$$gH = \{gh|\ h \in H\} \qquad \text{et} \qquad Hg = \{hg|\ h \in H\}.$$

Dans le cas où G est commutatif, on a $gH = Hg$.

Remarque 2. Si H est un sous-groupe de G, alors $HH = H$.

Lemme 1. *Soit H un sous-groupe de G, et soient a, b dans G. Alors*
a. $Ha = H \Longleftrightarrow a \in H$, *et* $aH = H \Longleftrightarrow a \in H$,
b. $Ha = Hb \Longleftrightarrow ab^{-1} \in H$, *et* $aH = bH \Longleftrightarrow a^{-1}b \in H$.

Preuve. a. Si $Ha = H$, alors pour tout $h \in H$, on a $ha = h' \Longrightarrow a = h^{-1}h' \in H$, et inversement $a \in H \Longrightarrow ha \in H$ pour tout $h \in H$.
b. $Ha = Hb \Longrightarrow \forall h \in H, \exists h' \in H$ tels que $ha = h'b$, d'où $ab^{-1} = h^{-1}h' \in H$, et inversement, $ab^{-1} \in H \Longrightarrow Hab^{-1} = H$, d'où $Ha = Hb$. □

Théorème 5. *Pour tout sous-groupe H de G, la relation $\mathcal{R}_g$ définie sur G par :*

$$a\mathcal{R}_g b \Longleftrightarrow a^{-1}b \in H$$

est une relation d'équivalence.

Preuve. - Pour tout $a \in G$, on a $a^{-1}a = e \in H$, donc $\mathcal{R}_g$ est réflexive.
- Si a, b dans G sont tels que $a\mathcal{R}_g b$, donc $a^{-1}b \in H$, on a alors $(a^{-1}b)^{-1} = b^{-1}a \in H$, ce qui signifie que $b\mathcal{R}_g a$. Cette relation est donc symétrique.
- Si a, b, c dans G sont tels que $a\mathcal{R}_g b$ et $b\mathcal{R}_g c$, alors $a^{-1}b \in H$ et $b^{-1}c \in H$. On a alors $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$, ce qui signifie que $a\mathcal{R}_g c$. Cette relation est donc transitive.
Par suite $\mathcal{R}_g$ est une relation d'équivalence. □

Terminologie.

1. Avec les notations du théorème précédent 5, on note, pour tout $a \in G$, $\overline{a}$ la classe d'équivalence de a modulo $\mathcal{R}_g$ et on dit que $\overline{a}$ est la classe de a à gauche modulo H. On a donc, pour tout $a \in G$:

$$b \in \overline{a} \Longleftrightarrow a\mathcal{R}_g b \Longleftrightarrow a^{-1}b \in H \Longleftrightarrow \exists k \in H;\ b = ak \Longleftrightarrow b \in aH$$

   c'est-à-dire que $\overline{a} = aH$.
2. En particulier on a : $\overline{e} = H$, et $\overline{a} = H$ si et seulement si $a \in H$.
3. L'ensemble de toutes ces classes d'équivalence est noté $(G/H)_g$ et on l'appelle l'ensemble des classes à gauche modulo H. On a donc :

$$(G/H)_g = \{\overline{a} \mid a \in G\} = \{aH \mid a \in G\}.$$

Remarques 3.

1. On peut définir, de manière analogue, l'ensemble des classes d'équivalence à droite modulo H et on le note $(G/H)_d$, à partir de la relation d'équivalence :

$$a\mathcal{R}_d b \Longleftrightarrow ab^{-1} \in H.$$

$$(G/H)_d = \{\overline{a} \mid a \in G\} = \{Ha \mid a \in G\},$$

2. Si le groupe G est noté additivement, alors la relation d'équivalence $\mathcal{R}_d$ (resp. $\mathcal{R}_g$) est définie par : $a\mathcal{R}_d b \Longleftrightarrow a - b \in H$ (resp. $a\mathcal{R}_g b \Longleftrightarrow b - a \in H$).
3. Dans le cas où G est abélien, les notions de classes d'équivalence à droite et à gauche modulo H coincident.

Définition 9. Soit H un sous-grope d'un groupe G. L'application

$$\begin{aligned} \pi :\ & G \longrightarrow (G/H)_g \\ & a \longmapsto \overline{a} = aH \end{aligned}$$

qui à tout élément a de G associe sa classe d'équivalence modulo H, est dite la **surjection canonique**. Et on a $\pi(a) = \pi(b)$ si et seulement si $a^{-1}b \in H$.

La relation d'équivalence $\mathcal{R}_g$ (resp. $\mathcal{R}_d$) nous fournit une partition de G.

Théorème 6. *Si H est un sous-groupe de G, alors l'ensemble des classes à gauche (resp. à droite) modulo H deux à deux distinctes forment une partition de G.*

Preuve. Notons $(G/H)_g = \{\overline{g_i} = g_i H |\ i \in I\}$, où I est un ensemble d'indices, l'ensemble des classes à gauche modulo H deux à deux distinctes.

- On sait que pour tout $g \in G$, on a $\overline{g} \neq \emptyset$, car $g \in \overline{g}$.
- On a d'une part, $\bigcup_{i \in I} \overline{g_i} \subset G$. D'autre part, $\forall g \in G$, $\exists! i \in I$ tel que $\overline{g} = \overline{g_i}$, donc $G \subset \bigcup_{i \in I} \overline{g_i}$, par suite $G = \bigcup_{i \in I} \overline{g_i}$.
- Dire que g est dans $\overline{g_j} \bigcap \overline{g_k}$ signifie que g est équivalent à gauche modulo H à g_j et g_k et donc par transitivité g_j et g_k sont équivalents, ce qui revient à dire que $\overline{g_j} = \overline{g_k}$, d'où si $j \neq k$, alors $g_j \bigcap g_k = \varnothing$.

Par suite, les classes à gauche modulo H forment bien une partition de G.

On peut aussi tout simplement dire que dès qu'on a une relation d'équivalence sur G, les classes d'équivalence partitionnent G. □

Proposition 4. *Pour tout sous-groupe H de G, on a :* $\text{card}((G/H)_g) = \text{card}((G/H)_d)$.

Preuve. Nous devons définir une application de $(G/H)_d$ dans $(G/H)_g$. Soit la correspondance

$$\begin{aligned} f : \ (G/H)_g &\longrightarrow (G/H)_d \\ xH &\longmapsto Hx^{-1} \end{aligned}$$

qui à la classe gauche à xH associe la classe à droite Hx^{-1}. Cette correspondance est une application. En effet, si on prend 2 représentants de la classe xH (i.e., 2 éléments de xH), x et x', alors $xH = x'H$. La correspondance f associe donc à xH les deux éléments Hx^{-1} et Hx'^{-1}. Pour qu'elle soit une application, il faut que ces 2 classes à droite coincident. Or $x\mathcal{R}_g x'$, d'où $x^{-1}x' \in H$ ou encore $x'^{-1}x \in H \Longrightarrow x'^{-1} \in Hx^{-1}$, donc $Hx^{-1} = Hx'^{-1}$.
D'autre part, l'application f est clairement bijective, en effet :
- si $f(xH) = f(yH)$, alors $Hx^{-1} = Hy^{-1} \Longrightarrow Hx^{-1}y = H$, d'où $x^{-1}y \in H$, ce qui implique que $y \in xH$, et enfin $yH = xH$; f est parsuite injective.
- la surjection est banale.
D'où le résultat. □

Définition 10. Si H est un sous-groupe de G, le cardinal $\text{card}((G/H)_d)$ de l'ensemble $(G/H)_d$ est noté $[G : H]$ et on l'appelle **l'indice de H dans G**.

Lemme 2. *Soient G un groupe fini et H un sous-groupe de G. Pour tout $g \in G$, on a* $\text{card}(gH) = \text{card}(H)$.

Preuve. Pour g fixé dans le groupe G, la translation à gauche $T_g : h \longmapsto gh$ est une bijection de H sur gH. Il en résulte que gH et H ont même cardinal. □

Théorème 7 (**Lagrange**). *Soient G un groupe fini et H un sous-groupe de G. Alors*

$$|G| = [G : H]|H|,$$

donc l'ordre de H divise celui de G.

Preuve. L'ensemble des classes à gauche suivant H réalise une partition de G et ces classes sont en nombre fini égal à $[G : H]$. De plus, par le Lemme 2, chaque classe a le même cardinal que H, il en résulte que : $\text{card}(G) = [G : H]\text{card}(H)$. □

Remarques 4.

1. $[G : G] = 1$, $[G : \{e\}] = |G|$. Pour $|G| = 1$, on a $H = G = \{e\}$ et $[G : H] = 1$.
2. Le théorème de Lagrange peut aussi se traduire par : $[G : H] = card(G/H) = \dfrac{|G|}{|H|}$.
3. L'indice $[G : H]$ peut être fini sans que ni G, ni H le soit, il suffit de considérer $(\mathbb{Z}, +)$ et $H = n\mathbb{Z}$, avec $n \neq 0$, alors le cardinal de $\mathbb{Z}/n\mathbb{Z}$ est n, c'est-à-dire $[\mathbb{Z} : n\mathbb{Z}] = n$.

Corollaire 1 (**Formule des indices**). *Soient H un sous-groupe de G et K un sous-groupe de H $(K \subset H \subset G)$. Si l'indice de K dans G est fini, alors l'indice de H dans G et celui de K dans H sont aussi finis et on a :*

$$[G : K] = [G : H][H : K].$$

Preuve. On a

$$[G : K] = card(G/K) = \frac{|G|}{|K|} = \frac{|H|[G : H]}{|K|} = [G : H]\frac{|H|}{|K|} = [G : H][H : K].$$

D'où le rsultat. □

Corollaire 2. *Soient H et K deux sous-groupes d'un groupe fini G, alors*

$$\text{card}(HK) = \frac{|H||K|}{|H \cap K|}.$$

Preuve. Voir TD. □

Définition 11. On dit qu'une relation d'équivalence $\mathcal{R}$ sur un groupe G est compatible à droite (resp. à gauche) avec la loi de G si pour tous a, b et c dans G, on a :

$$a\mathcal{R}b \Longrightarrow ac\mathcal{R}bc \quad (\text{resp. } a\mathcal{R}b \Longrightarrow ca\mathcal{R}cb).$$

Exercice. Montrer que la relation d'équivalence $\mathcal{R}_g$ (resp. $\mathcal{R}_d$) est compatible à gauche (resp. à droite) avec la loi de G.

Définition 12. On dit qu'une relation d'équivalence $\mathcal{R}$ sur un groupe G est compatible avec la loi de G si pour tous a, b, c et d dans G, on a :

$$\begin{cases} a\mathcal{R}c \\ b\mathcal{R}d \end{cases} \Longrightarrow ab\mathcal{R}cd.$$

Proposition 5. *Une relation d'équivalence $\mathcal{R}$ sur un groupe G est compatible avec la loi de G si et seulement si elle est compatible à droite et à gauche avec cette loi, c'est-à-dire, si pour tous a, b et c dans G, on a : $a\mathcal{R}b \Longrightarrow ac\mathcal{R}bc$ et $ca\mathcal{R}cb$.*

Preuve. Preuve simple, laisser au lecteur. □

Exemple 1. La congruence modulo un entier naturel n est compatible avec l'addition et la multiplication dans $\mathbb{Z}$, car

$$\begin{cases} a \equiv b \pmod{n} \\ x \equiv y \pmod{n} \end{cases} \Longrightarrow a + x \equiv b + y \pmod{n} \text{ et } ax \equiv by \pmod{n}.$$

Soit $\mathcal{R}$ une relation d'équivalence sur un groupe $(G, .)$, posons $\overline{G} = G/\mathcal{R}$ et désignons par $\overline{g}$ la classe de g modulo la relation $\mathcal{R}$ pour tout $g \in G$.

Proposition 6. *La correspondence $\ell : \overline{G} \times \overline{G} \longrightarrow \overline{G}$, $(\overline{a}, \overline{b}) \longmapsto \overline{a.b}$ définit une loi de composition interne sur $\overline{G}$ si et seulement si $\mathcal{R}$ est compatible avec la loi de G.*

Dans ce cas, la loi de composition interne définie par ℓ est appelée loi quotient de celle de G par $\mathcal{R}$. Elle sera noté aussi ".", et on a : $\overline{a}.\overline{b} = \overline{a.b}$.

Preuve. ℓ définit une loi de composition interne sur $\overline{G}$ ssi ℓ est une application, c'est-à-dire, ssi pour tous $\overline{a}$, $\overline{b}$, $\overline{c}$ et $\overline{d}$ dans $\overline{G}$:

$$(\overline{a} = \overline{c} \text{ et } \overline{b} = \overline{d}) \Longrightarrow \overline{a.b} = \overline{c.d}.$$

Mais ceci est équivaut à la formule donné par la définition 12. D'où le résultat. □

Remarque 3. La formule $\overline{a.b} = \overline{a}.\overline{b}$ permet de transférer les propriétés de loi "." sur G à la loi quotient sur $\overline{G}$, en particulier si "." est commutative (resp. associative, admet un neutre e, tout x admet un symétrique x^{-1}), alors la loi quotient est commutative (resp. associative, admet un neutre $\overline{e}$, tout $\overline{x}$ admet un symétrique $\overline{x^{-1}} = \overline{x}^{-1}$).

Remarque 4. En général, les relations d'équivalences $\mathcal{R}_g$ et $\mathcal{R}_d$ ne sont pas compatibles avec la loi de G (elles le sont si G est abélien). Mais le théorème suivant nous donne une condition nécessaire et suffisante pour qu'elles le soient.

Théorème 8. *Si H est un sous-groupe de G, alors la relation d'équivalence $\mathcal{R}_g$ (resp. $\mathcal{R}_d$) associée à H est compatible avec la loi de G si, et seulement si, $gH = Hg$ pour tout $g \in G$.*

Preuve. Supposons $\mathcal{R}_g$ compatible avec la loi de G. Alors montrons que pour tout $g \in G$, $gH = Hg$.
- Soit $k \in gH$, alors $g\mathcal{R}_g k \Longrightarrow k\mathcal{R}_g g$ (par symétrie), et avec la compatibilité à droite, on déduit que

$$k\mathcal{R}_g g \Longrightarrow kg^{-1}\mathcal{R}_g gg^{-1} \Longrightarrow kg^{-1}\mathcal{R}_g e,$$

ce qui revient à dire que $k \in Hg$. On a donc $gH \subset Hg$.
- De manière analogue on a :

$$k \in Hg \Longrightarrow kg^{-1} \in H \Longrightarrow kg^{-1}\mathcal{R}_g e \Longrightarrow kg^{-1}g\mathcal{R}_g eg \Longrightarrow k\mathcal{R}_g g;$$

d'où avec la compatibilité de $\mathcal{R}_g$ on trouve

$$k\mathcal{R}_g g \Longrightarrow g^{-1}k\mathcal{R}_g g^{-1}g \Longrightarrow g^{-1}k\mathcal{R}_g e;$$

donc $k \in gH$, d'où $Hg \subset gH$. Par suite $gH = Hg$.

Réciproquement, supposons que pour tout $g \in G$, $gH = Hg$, alors montrons que $\mathcal{R}_g$ est compatible avec la loi de G.
Soient g, g' et h dans G. Supposons que $g\mathcal{R}_g g'$, alors $g^{-1}g' \in H$, donc

$$g^{-1}g'h \in Hh \text{ et donc } g^{-1}g'h \in hH, \text{ car } Hh = hH.$$

Par suite

$$h^{-1}g^{-1}g'h \in H \text{ c'est-à-dire } (gh)^{-1}g'h \in H, \text{ d'où } gh\mathcal{R}_g g'h.$$

D'autre part, $(hg)^{-1}hg' = g^{-1}h^{-1}hg' = g^{-1}g' \in H$, on déduit que $hg\mathcal{R}_g hg'$. Donc $\mathcal{R}_g$ est compatible avec la loi de G. Même démonstration pour $\mathcal{R}_d$. □

Ce théorème va nous permettre d'introduire une nouvelle classe de sous-groupes d'un groupe G donné.

2.5. **Sous-groupes distingués.**

Définition 13. On dit qu'un sous-groupe H d'un groupe G est **distingué** (ou **normal** ou **invariant**), et on note $H \lhd G$, si pour tout $g \in G$, on a $gH = Hg$.
Autrement dit, H est distingué si pour tout $g \in G$ et pour tout $h \in H$ on a :

$$ghg^{-1} \in H.$$

Remarques 5.

1. Par le théorème 8, la relation d'équivalence $\mathcal{R}_g$ (resp. $\mathcal{R}_d$) associée à H est compatible avec la loi de G si, et seulement si $H \lhd G$. Dans ce cas, au lieu d'écrire $a\mathcal{R}_g b$ on écrit par fois $a \equiv b \pmod{H}$.
2. Si H est distingué dans G, alors les deux relations $\mathcal{R}_g$ et $\mathcal{R}_d$ coincident. Ainsi les deux ensembles des classes d'équivalences sont identiques et on note alors
$$(G/\mathcal{R})_g = (G/\mathcal{R})_d = G/H.$$
3. Attention :$Hg = gH$ ne signifie pas : $\forall h \in H$, $hg = gh$, mais il signifie, $\forall h \in H$ $\exists h' \in H$, $hg = gh'$.

Théorème 9. *Soit H un sous-groupe d'un groupe G, alors les conditions suivantes sont équivalentes :*

a. $H \lhd G$,
b. *pour tout* $g \in G$, $gH = Hg \Longleftrightarrow gH \subset Hg$
c. *pour tout* $g \in G$, $gHg^{-1} = H \Longleftrightarrow g^{-1}Hg = H$,
d. $ghg^{-1} \in H \Longleftrightarrow g^{-1}hg \in H$ *pour tout couple* $(h, g) \in H \times G$,
e. H *est stable par tout automorphisme intérieur* $f_g : h \longmapsto ghg^{-1}$, *où* $g \in G$.

Preuve. Preuve simple laisser au lecteur. □

Exemples 5.

1. $\{e\}$ et G sont toujours distingués dans G.
2. Si le groupe G est commutatif, alors tous ses sous-groupes sont distingués.
3. Pour tout $n \in \mathbb{N}$, $n\mathbb{Z}$ est un sous groupe distingué de $(\mathbb{Z}, +)$, car $(\mathbb{Z}, +)$ est abélien.
4. Pour tout groupe G, $\mathrm{Int}(G) \lhd \mathrm{Aut}(G)$. Soit
$$\sigma_g : G \longrightarrow G,\ a \longmapsto gag^{-1} \text{ un automorphisme intérieur de } G,$$
alors pour tout $\tau \in \mathrm{Aut}(G)$ on a :
$$\tau \circ \sigma_g \circ \tau^{-1} = \sigma_{\tau(g)}.$$
5. Pour tout groupe $(G, \cdot)$, alors le centre $Z(G) = \{a \in G \,|\, ax = xa, \forall\, x \in G\}$ de G est distingué dans G, car pour tous $g \in G$ et $x \in Z(G)$, on a : $gx = xg \Longleftrightarrow gxg^{-1} = x \in Z(G)$. (Plus généralement, tout sous-groupe de G contenu dans $Z(G)$ est distingué dans G).
6. Si H est un sous-groupe d'indice 2 d'un groupe G, alors il est distingué dans G (voir TD.)

Définition 14. Un groupe G, d'élément neutre e, est dit **simple** s'il a exactement deux sous-groupes distingués : $\{e\}$ et G lui-même.

Théorème 10. *Un sous-groupe H de G est distingué si, et seulement s'il existe une unique structure de groupe sur l'ensemble quotient G/H des classes modulo H telle que la surjection canonique $\pi : G \longrightarrow G/H$ soit un homomorphisme de groupes.*

Preuve. Si G/H est muni d'une structure de groupe telle que π soit un morphisme de groupes, alors on a nécessairement pour tous g, g' dans G :

$$\overline{g}\overline{g'} = \pi(g)\pi(g') = \pi(gg') = \overline{gg'}.$$

Pour (g, h) dans $G \times H$, on a $\overline{g^{-1}hg} = \overline{g^{-1}h}\overline{g} = \overline{g^{-1}}\overline{g} = \overline{g^{-1}g} = \overline{e} = H$, ce qui signifie que $g^{-1}hg \in H$ (on rappelle que $\overline{g} = gH = \overline{e} = H$ si, et seulement si, $g \in H$). D'où H est distingué dans G.

Réciproquement, supposons que H est distingué. Alors pour tout $g \in G$, $gH = Hg$, donc par le Théorème 8 les deux relations $\mathcal{R}_g$ et $\mathcal{R}_d$ coincident et sont compatibles avec la loi du groupe G. D'où la Proposition 6 implique que l'application

$$\begin{array}{rccc} \ell : & (G/H)_d \times (G/H)d & \longrightarrow & (G/H)_d \\ & (Hg, Hg') & \longmapsto & Hgg' \end{array}$$

est bien définie, c'est-à-dire elle est définie par le choix des représentants g et g' de Hg et Hg' et elle ne dépend pas de ce choix des représentants de g et g', ce qui résulte du fait que $\mathcal{R}_g$ est compatible avec la loi de G.

Il reste à vérifier que G/H muni de cette loi de composition interne est bien un groupe. Avec :

$$\overline{g_1}(\overline{g_2 g_3}) = \overline{g_1 g_2 g_3} = \overline{g_1(g_2 g_3)} = \overline{(g_1 g_2)g_3} = \overline{g_1 g_2 g_3} = (\overline{g_1 g_2})\overline{g_3},$$

on déduit que cette loi est associative. Avec $\overline{ge} = \overline{eg} = \overline{g}$, on déduit que $\overline{e}$ est le neutre.

Avec $\overline{g}\overline{g^{-1}} = \overline{gg^{-1}} = \overline{e}$, on 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. □

Définition 15. Soit H un sous-groupe normal d'un groupe G, alors le groupe G/H est dit **groupe quotient** de G par le sous-groupe normal H.

Théorème 11. *Soit $\mathcal{R}$ une relation d'équivalence sur un groupe G d'élément neutre e. La relation $\mathcal{R}$ est compatible avec la loi de G si et seulement s'il existe un sous-groupe H distingué dans G tel que $\mathcal{R}$ est de la forme : $x \equiv y \pmod{\mathcal{R}} \Longleftrightarrow x^{-1}y \in H$.*

Preuve. Soit $\mathcal{R}$ une relation d'équivalence sur G compatible avec sa loi. Donc

$$x \equiv y \pmod{\mathcal{R}} \Longleftrightarrow x^{-1}y \equiv x^{-1}x = e \pmod{\mathcal{R}} \Longleftrightarrow x^{-1}y \equiv e \pmod{\mathcal{R}}.$$

Désignons par H la classe de e modulo $\mathcal{R}$, alors la relation $\mathcal{R}$ est équivalente à $x^{-1}y \in H$, c-à-d,

$$x \equiv y \pmod{\mathcal{R}} \Longleftrightarrow x^{-1}y \in H.$$

De plus H est un sous-groupe normal de G. En effet,
- H est non vide puisque $e \in H$,
- pour tous x et y dans H, $xy^{-1} \in H$,
- soient $a \in G$ et $h \in H$, alors $h \in H \Longleftrightarrow h \equiv e \pmod{\mathcal{R}} \Longleftrightarrow ah \equiv ae = a \pmod{\mathcal{R}}$, et comme $\mathcal{R}$ est compatible avec la loi de G, donc $aha^{-1} \equiv e \pmod{\mathcal{R}}$, d'où $aha^{-1} \in H$.

La réciproque est triviale. □

Remarques 6.

1. 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.
2. Pour un sous-groupe H de G, la compatibilité de $\mathcal{R}_g$ avec la loi de G est une condition nécessaire et suffisante pour définir naturellement une structure de groupe sur l'ensemble quotient G/H par : $\overline{g}\overline{h} = \overline{gh}$.
3. Pour tout $n \in \mathbb{N}$, $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe car $n\mathbb{Z}$ est un sous-groupe distingué de $\mathbb{Z}$, et la relation d'équivalence associée à cette structure est la congruence modulo n.

Remarque 5. Soient $H \subset K$ deux sous-groupes d'un groupe G. Si $H \lhd G$, alors $H \lhd K$. Attention la réciproque n'est pas vraie (on peut consulter exercice 9 chap IV dans [11]) et on a :

- $H \lhd K \not\Longrightarrow H \lhd G$,
- $H \lhd G \not\Longrightarrow K \lhd G$,
- $(H \lhd K \text{ et } K \lhd G) \not\Longrightarrow H \lhd G$.

Le résultat qui suit est souvent utilisé pour montrer qu'un sous-groupe est distingué.

Théorème 12. *Si G et G' sont deux groupes et f un homomorphisme de groupes de G dans G', alors* $\ker(f)$ *est un sous-groupe distingué de G.*

Preuve. Soient $g \in G$ et $h \in \ker(f)$, en notant par e et e' les éléments neutres de G et G' respectivement, on a :

$$f(g^{-1}hg) = f(g^{-1})f(h)f(g) = f(g^{-1})e'f(g) = e',$$

c'est-à-dire que $g^{-1}hg \in \ker(f)$. Le sous-groupe $\ker(f)$ de G est donc distingué. $\square$

Exemple 2.
Soit K un corps commutatif, désignons par $\mathrm{GL}_n(K)$ le groupe linéaire de degré n du corps commutatif K (c'est-à-dire le groupe des matrices $n \times n$ inversibles à coefficients dans K, muni de la multiplication matricielle). Alors l'ensemble :

$$\mathrm{SL}_n(K) = \{A \in \mathcal{M}_n(K) |\ \det(A) = 1\} \text{ (\textbf{Le groupe spécial linéaire})}$$

est un sous-groupe distingué de $\mathrm{GL}_n(K)$, car il est noyau de l'homomorphisme de groupes

$$f : \mathrm{GL}_n(K) \longrightarrow K^*,\ A \longmapsto \det(A).$$

Remarques 7.

1. En notation additive, $\ker(f) = \{x \in G \mid f(x) = 0\}$.
2. Pour un sous-groupe H distingué dans G, le noyau de la surjection canonique π est : $\ker(\pi) = \{g \in G |\ \overline{g} = \overline{e}\} = H$.
3. Comme le noyau d'un homomorphisme de groupes est distingué, on déduit qu'un sous-groupe distingué de G est toujours noyau d'un homomorphisme de groupes. Il suffit de prendre par exemple $\pi : G \longrightarrow G/H$. D'où la première caractérisation des sous groupes distingués.

Théorème 13. *Dans un groupe G, un sous groupe H de G est distingué si et seulement s'il existe un groupe G' et un morphisme de groupes f tels que $H = \ker(f)$.*

Théorème 14 (décomposition d'un morphisme)**.** *Si $f : G \longrightarrow G'$ est un homomorphisme de groupes, il existe alors un unique isomorphisme de groupes*

$$\overline{f} : G/\ker(f) \longrightarrow \mathrm{Im}(f) \qquad \textit{tel que } f = i \circ \overline{f} \circ \pi,$$

où $i : \mathrm{Im}(f) \longrightarrow G'$ est l'injection canonique (définie par $i(h) = h$ pour tout $h \in \mathrm{Im}(f)$) et $\pi : G \longrightarrow G/\ker(f)$ la surjection canonique (définie par $\pi(g) = \overline{g} = g\ker(f)$ pour tout $g \in G$).

Preuve. Comme $\ker(f)$ est distingué dans G, alors $G/\ker(f)$ est un groupe. Si un tel isomorphisme $\overline{f}$ existe, alors on a pour tout $g \in G$:

$$f(g) = i \circ \overline{f} \circ \pi(g) = i \circ \overline{f}(\overline{g}) = \overline{f}(\overline{g})$$

ce qui prouve l'unicité de $\overline{f}$.

On peut définir $\overline{f}$ par $\overline{f}(\overline{g}) = f(g)$, pour tout $g \in G/\ker(f)$. Pour justifier cette définition, on doit vérifier qu'elle ne dépend pas du choix d'un représentant de $\overline{g}$. Si $\overline{g} = \overline{h}$, alors on a $g^{-1}h \in \ker(f)$, donc $e' = f(g^{-1}h) = (f(g))^{-1}f(h) = f(g^{-1}h)$, d'où $f(g) = f(h)$. L'application $\overline{f}$ est donc bien définie et par construction, on a $f = i \circ \overline{f} \circ \pi$.

Comme $\overline{f}(\overline{g}\overline{h}) = \overline{f}(\overline{gh}) = f(gh) = f(g)f(h) = \overline{f}(\overline{g})\overline{f}(\overline{h})$, alors $\overline{f}$ est un homomorphisme de groupes. Montrons enfin que $\overline{f}$ est bijective.

Soit $\overline{g} \in \ker(\overline{f})$, alors

$$\overline{f}(\overline{g}) = e' \Longleftrightarrow f(g) = e' \Longleftrightarrow g \in \ker(f) \Longleftrightarrow \overline{g} = \ker(f) = \overline{e};$$

d'où $\overline{g} \in \ker(\overline{f}) \Longleftrightarrow \overline{g} = \ker(f) = \overline{e}$, par suite $\ker(\overline{f}) = \{\overline{e} = \ker(f)\}$, cet homomorphisme est donc injective. D'autre part,

$$\mathrm{Im}(\overline{f}) = \{\overline{f}(\overline{g}) \mid g \in G\} = \{f(g) \mid g \in G\} = \mathrm{Im}(f),$$

il est alors surjective, et par suite bijectif. □

Le théorème précédent s'exprime aussi en disant que le diagramme suivant est commutatif :

$$\begin{array}{ccc} \mathrm{G} & \xrightarrow{\quad f \quad} & G' \\ \pi \downarrow & & \uparrow i \\ G/\ker(f) & \xrightarrow{\quad \overline{f} \quad} & \mathrm{Im}(f) \end{array}$$

Corollaire 3. *Soient G et G' deux groupes et $f : G \longrightarrow G'$ un homomorphisme de groupes. Si G est fini, alors on a :*

$$|G| = |\ker(f)|\,|\mathrm{Im}(f)|$$

Preuve. On sait que $G/\ker(f)$ et $\mathrm{Im}(f)$ sont isomorphes, dans le cas où G est fini, on a : $|\mathrm{Im}(f)| = \mathrm{card}(G/\ker(f)) = \dfrac{\mathrm{card}(G)}{\mathrm{card}(\ker(f))}$. D'où le résultat. □

Définition 16. Soient G un groupe et H un sous-groupe de G. On dit qu'un élément g de G normalise H si $gHg^{-1} = H$, ce qui équivaut à $g^{-1}Hg = H$.

Remarque 6. Soient G un groupe et H un sous-groupe de G. On vérifie facilement que les éléments g de G qui normalisent H forment un sous-groupe de G.

Définition 17. Soient G un groupe et H un sous-groupe de G. On appelle normalisateur de H dans G et on note $N_G(H)$ le sous-groupe de G formé par les éléments de G qui normalisent H.

Remarque 7. Il est simple de voir que $N_G(H)$ contient H et que c'est le plus grand sous-groupe de G contenant H dans lequel H est normal. Un sous-groupe H de G est un sous-groupe normal de G si et seulement si $N_G(H) = G$.

Définition 18. Soient H et K deux sous-groupes d'un groupe G. On dit que H normalise K si H est contenu dans le normalisateur de K (dans G), autrement dit si tout élément de H normalise K.

Définition 19. Deux sous-groupes H et K de G sont dits conjugués s'il existe $g \in G$ tel que $K = gHg^{-1}$.

2.6. **Sous-groupe engendré par une partie.**

Lemme 3. *Soient G un groupe et A une partie de G. L'intersection de tous les sous-groupes de G qui contiennent A est un sous-groupe de G.*

Preuve. L'ensemble des sous-groupes de G qui contiennent A est non vide puisque G en fait partie et le théorème 3 nous dit que l'intersection de tous ces sous-groupes est un sous-groupe de G. □

Définition 20. Soit A une partie d'un groupe $(G, \cdot)$. L'intersection de tous les sous-groupes de G qui contiennent A est appelé le **sous-groupe de G engendré** par A, on le note par $\langle A \rangle$ ou $gr(A)$.

Définition 21. La partie A de G est dite **partie génératrice** de G, ou engendre G, ou est un ensemble de générateurs de G, si $\langle A \rangle = G$.

Définition 22. Un groupe G est dit de **type fini** s'il admet une partie génératrice finie, c-à-d, s'il existe une partie finie A de G telle que $\langle A \rangle = G$.

Remarques 8.

1. Tout groupe fini est bien sûr de type fini.
2. $\langle A \rangle$ est le plus petit (pour l'inclusion) des sous-groupes de G qui contiennent A. $\langle A \rangle$ est la borne inférieur de l'ensemble des sous-groupes de G qui contiennent A.
3. Dans le cas où A est l'ensemble vide, on a $\{e\} = \langle A \rangle$.

4. Si A est une partie non vide de G formée d'un nombre fini d'éléments, $a_1, \cdots, a_n$, on note $\langle A\rangle = \langle a_1, \cdots, a_n\rangle$ le groupe engendré par A.
5. Si $A = \{a\}$, on note $\langle A\rangle = \langle a\rangle$ et on parle du sous-groupe de G engendré par a.

Théorème 15. *Soient A, B deux parties d'un groupe G.*

1. *On a $A \subset \langle A\rangle$, et l'égalité est réalisée si, et seulement, si A est un sous-groupe de G.*
2. *Si $A \subset B$, alors $\langle A\rangle \subset \langle B\rangle$.*
3. *En notant, pour A non vide, A^{-1} l'ensemble formé des symétriques des éléments de A, c-à-d, $A^{-1} = \{a^{-1} |\ a \in A\}$, alors les éléments de $\langle A\rangle$ sont de la forme*

$$\prod_{i=1}^{r} a_1 \cdots a_r,$$

où $r \in \mathbb{N}^*$ et les a_k sont dans $A \cup A^{-1}$ pour tout k compris entre 1 et r.

Preuve. Les points 1. et 2. se déduisent immédiatement des définitions.
Pour le point 3., on montre tout d'abord que l'ensemble :

$$H = \{g = a_1 \cdots a_r |\ r \in \mathbb{N}^* \text{ et } a_k \in A \cup A^{-1} \text{ pour } 1 \leq k \leq r\}$$

est un sous-groupe de G.
Pour $a_1 \in A$, on a : $e = a_1 \cdot a_1^{-1} \in H$, et pour $a = a_1 \cdots a_r$, $b = b_1 \cdots b_r$ dans H, on a :

$$a \cdot b^{-1} = a_1 \cdots a_r \cdot b_r^{-1} \cdots b_1^{-1} \in H.$$

Donc H est un sous-groupe de G. Comme H est un sous-groupe de G qui contient A, on a alors $\langle A\rangle \subset H$.

Réciproquement, tout élément $a = a_1 \cdots a_r$ de H est un produit d'éléments de $A \cup A^{-1} \subset \langle A\rangle$, donc $a \in \langle A\rangle$, et par suite $\langle A\rangle = H$. □

Remarques 9.

1. Le point 3. du Théorème précédent nous affirme aussi que

$$\langle A\rangle = \langle A^{-1}\rangle = \langle A \cup A^{-1}\rangle.$$

2. On a aussi $\langle A\rangle = \left\{ \prod_{k=1}^{k=r} a_k^{\varepsilon_k} |\ r \in \mathbb{N}^*, a_k \in A, \varepsilon_k \in \{-1, 1\}, 1 \leq k \leq r \right\}$.

Dans le cas où les éléments de A sont en nombre fini et commutent, on a le résultat suivant.

Théorème 16. *Pour tout n-uplet $(g_1, \cdots, g_p)$ d'éléments de G qui commutent deux à deux (où $p \geq 1$), on a :*

$$\langle g_1, \cdots, g_p \rangle = \left\{ \prod_{k=1}^{p} g_k^{\alpha_k} |\ \alpha_k \in \mathbb{Z},\ \textit{pour tout } 1 \leq k \leq p \right\},$$

et ce groupe est commutatif.

Preuve. En notant $A = \{g_1, \cdots, g_p\}$, on a $A^{-1} = \{g_1^{-1}, \cdots, g_p^{-1}\}$, et comme les g_k commutent, on déduit que :

$$\begin{aligned} \langle g_1, \cdots, g_p \rangle &= \left\{ \prod_{k=1}^{m} h_k |\ m \in \mathbb{Z}^*, h_k \in A \cup A^{-1} \text{ pour } 1 \leq k \leq m \right\} \\ &= \left\{ \prod_{k=1}^{p} g_k^{\alpha_k} |\ \alpha_k \in \mathbb{Z},\ \text{pour tout } 1 \leq k \leq p \right\} \end{aligned}$$

($g_k g_j = g_j g_k$ entraîne $g_j^{-1} g_k = g_j^{-1} g_k g_j g_j^{-1} = g_j^{-1} g_j g_k g_j^{-1} = g_k g_j^{-1}$ et les éléments de $A \cup A^{-1}$ commutent). Comme les g_k commutent, ce groupe est commutatif. □

2.7. **Groupes monogènes.**

Définition 23. On dit qu'un groupe G est **monogène** s'il est engendré par l'un de ses éléments. Un groupe monogène fini est dit **cyclique**.

Par le théorème 16 on a :

Proposition 7. *Si G est monogéne, alors il existe $a \in G$ tel que :*

$$\begin{aligned} G &= \langle a \rangle = \{a^k |\ k \in \mathbb{Z}\} \textit{ si la loi est notée multiplicativement.} \\ G &= \langle a \rangle = \{ka |\ k \in \mathbb{Z}\} \textit{ si la loi est notée additivement.} \end{aligned}$$

Remarques 10.

1. Un groupe monogène est nécessairement commutatif. En effet, si x et y sont dans $\langle a \rangle$, alors $x = a^n$ et $y = a^m$, donc

$$xy = a^n a^m = a^{n+m} = a^{m+m} = a^m a^n = yx.$$

2. Un groupe cyclique engendré par un élément $g \neq e$ a au moins deux élément, e et g.

Exemples 6.

1. $(\mathbb{Z}, +)$ est monogène engendré par 1. Les sous-groupes de $(\mathbb{Z}, +)$ qui sont de la forme $n\mathbb{Z}$ avec $n \geq 0$ sont tous monogènes ; $n\mathbb{Z}$ est engendré par n (à titre d'exercice, montrer que les sous groupes de $(\mathbb{Z}, +)$ sont de la forme $n\mathbb{Z}$, où $n \in \mathbb{N}$).

2. Si G est le groupe additif $\mathbb{Z}$, on sait alors que ces sous-groupes sont les $n\mathbb{Z}$ où n est un entier naturel et comme $(\mathbb{Z},+)$ est commutatif, l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ est naturellement muni d'une structure de groupe. Le groupe

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$$

a n éléments. Ce groupe est cyclique d'ordre n engendré par $\overline{1}$.

Théorème 17. *Soit G un groupe monogène.*

1. *Si G est infini, alors il est isomorphe à $\mathbb{Z}$.*
2. *Si G est cyclique d'ordre n, alors il est isomorphe au groupe $\mathbb{Z}/n\mathbb{Z}$.*

Preuve. Soit $G = \langle g \rangle$ un groupe monogène, l'application

$$\begin{array}{rccc} \varphi_g : & \mathbb{Z} & \longrightarrow & G \\ & k & \longmapsto & g^k \end{array}$$

est alors un homomorphisme de groupes surjectif de $(\mathbb{Z},+)$ sur G et son noyau $\ker(\varphi_g)$ est un sous-groupe additif de $\mathbb{Z}$, donc il existe $n \in \mathbb{N}$ tel que $\ker(\varphi_g)$ est de la forme $\ker(\varphi_g) = n\mathbb{Z}$. Comme $Im(f) = G$, alors le Théorème 14 nous implique que :
- pour $n = 0$, on a $\ker(\varphi_g) = \{0\}$, d'où φ_g est injectif et G est infini isomorphe à $\mathbb{Z}$.
- pour $n \geq 1$, $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à G et $G = \langle g \rangle$ est cyclique d'ordre n. □

Théorème 18. *Les seuls groupes abéliens simples sont les groupes cycliques d'ordre premier.*

Preuve. Soit G un groupe abélien non trivial qui ne possède pas de sous-groupe distingué autre que lui-même et son sous-groupe trivial, c-à-d, G est simple.

Soit g un élément de $G - \{e\}$; donc $\langle g \rangle$ le sous-groupe engendré par g est non trivial. Comme G est simple, alors $\langle g \rangle = G$, donc G est monogène. De plus G est fini, car sinon il sera isomorphe à $\mathbb{Z}$ (voir la preuvr du Théorème 17), donc il existera un isomorphisme f de G dans $\mathbb{Z}$. Or $2\mathbb{Z}$ est un sous-groupe distingué strict de $\mathbb{Z}$, donc $f^{-1}(2\mathbb{Z})$ est un sous-groupe distingué strict de G (l'image réciproque, par un morphisme, d'un sous-groupe distingué est un sous-groupe distingué, montrer ce résultat à titre d'exercice), ce qui est absurde. D'où G est cyclique d'ordre fini n.

Soit d un diviseur de n, donc $n = md$; posons $a = g^m$, donc $a^d = a^n = e$. Par suite $\langle a \rangle$ est un sous-groupe de G, donc $\langle a \rangle = \{e\}$ ou G car G est simple ; d'où d est égal à 1 ou n, par suite les seuls diviseurs de n sont 1 et n. Ainsi, n est nécessairement premier. □

2.8. **Ordre d'un élément dans un groupe.**
Soit $(G, .)$ un groupe noté multiplicativement non réduit à l'élément neutre.

Définition 24. L'ordre d'un élément g de G est l'élément $\theta(g) \in \mathbb{N}^* \cup \{+\infty\}$ défini par : $\theta(g) = \text{card}(\langle g \rangle)$. Si $\theta(g)$ est dans $\mathbb{N}^*$, on dit alors que g est d'ordre fini, sinon on dit qu'il est d'ordre infini.

Remarques 11.

1. Seul l'élément neutre e est d'ordre 1 dans G. En effet, si $g = e$, alors $\langle g \rangle = \langle e \rangle$ et si $g \neq e$, alors $g^0 \neq g^1$ et $\langle g \rangle$ a au moins deux éléments.
2. Pour tout $g \in G$, on a $\theta(g) = \theta(g^{-1})$ puisque :
$$\langle g^{-1} \rangle = \{(g^{-1})^n |\ n \in \mathbb{Z}\} = \{g^{-n} |\ n \in \mathbb{Z}\} = \{g^m |\ m \in \mathbb{Z}\} = \langle g \rangle.$$
3. Dans le cas où le groupe G est fini d'ordre $n \geq 1$, alors le théorème de Lagrange nous dit que l'ordre de tout élément g de G divise l'ordre de G, et en conséquence on a : $g^n = e$ pour tout $g \in G$.

Proposition 8. *Soit un élément g d'un groupe G, alors*
$$\theta(g) = n \in \mathbb{N}^* \Longleftrightarrow \langle g \rangle = \{g^k |\ 0 \leq k \leq n-1\} \Longleftrightarrow \theta(g) = |\langle g \rangle|\,.$$

Preuve. D'après la Proposition 7, $\langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$.
Supposons que $\langle g \rangle$ est fini, alors il existe un entier strictement positif a tel que $g^a = e$, sinon $\langle g \rangle$ sera infini. Donc $\{a \in \mathbb{N}^* \mid g^a = e\}$ est non vide ; posons n son plus petit élément (n est le plus petit des entiers strictement positifs a tel que $g^a = e$). Pour tout entier m, il existe, par division euclidienne, un couple (i, k) d'entiers avec $0 \leq k < n$ tel que $m = in + k$. D'où $g^m = g^k$, par suite
$$\langle g \rangle = \{g^k |\ 0 \leq k \leq n-1\}.$$

Il reste à montrer que $n = \theta(g)$. Pour cela, montrons que pour tous $i \neq j \in \{1, 2, \cdots, n-1\}, g^i \neq g^j$. Rappelons que $\langle g \rangle$ est de cardinal $\theta(g)$ par définition de $\theta(g)$. Soient $1 \leq i < j < n$, supposons que $g^i = g^j$, alors $g^j(g^i)^{-1} = g^{j-i} = e$. D'où, comme $j - i > 0$, on a, par hypothèse sur n, $j - i \geq n$. Or $j < n$, donc $j - i < j < n$. Contradiction. D'où, si $1 \leq i < j < n$, alors $g^i \neq g^j$. On en déduit que $\langle g \rangle = \{g^k |\ 0 \leq k \leq n-1\}$ est de cardinal n et donc $n = \theta(g)$.

La réciproque est simple. □

Dans la démonstration précédente, on a prouvé la proposition suivante :

Proposition 9. *Soit g un élément d'ordre fini d'un groupe G. Alors, l'ordre de g est le plus petit entier strictement positif n tel que $g^n = e$.*

Remarque 8. Dire que G est cyclique d'ordre n, signifie que le cardinal de G est n et qu'il existe dans G au moins un élément g d'ordre n, i.e., $g^n = e$, et pour tout $1 \leq r \leq n-1$ on a $g^r \neq e$; de plus

$$G = \langle g \rangle = \{1, g, \cdots, g^{n-1}\}$$

Remarques 12.

1. Un groupe infini peut avoir des éléments d'ordre fini. Par exemple, -1 est d'ordre 2 dans $(\mathbb{R}, \times)$.
2. Dans un groupe, un élément est dit de torsion s'il est d'ordre fini. La torsion d'un groupe est l'ensemble de ses éléments de torsion.

   Un groupe est dit sans torsion si sa torsion ne contient que le neutre, c'est-à-dire si tout élément différent du neutre est d'ordre infini. Si le groupe est abélien, alors sa torsion est un sous-groupe.

   Un groupe de torsion est un groupe égal à sa torsion, c'est-à-dire un groupe dont tous les éléments sont d'ordre fini. Il existe des groupes de torsion infinis, par exemple $\mathbb{Q}/\mathbb{Z}$. Tout groupe fini, comme $\mathbb{Z}/n\mathbb{Z}$, est un groupe de torsion.

Proposition 10. *Soient $f : G \longrightarrow G'$ un isomorphisme de groupes. Alors $\theta(f(g)) = \theta(g)$ pour tout $g \in G$.*

Preuve. Pour $g \in G$, on a :

$$\langle f(g) \rangle = \{(f(g))^n |\ n \in \mathbb{Z}\} = \{f(g^n) |\ n \in \mathbb{Z}\} = f(\langle g \rangle).$$

Or f est bijective, donc $\text{card}(\langle f(g) \rangle) = \text{card}(\langle g \rangle)$. □

Pour $g \in G$, le sous-groupe de G engendré par g est l'image de l'homomorphisme de groupes :

$$\begin{aligned} \varphi_g :\ & \mathbb{Z} \longrightarrow G; \\ & k \longmapsto g^k. \end{aligned}$$

Pour j, k dans $\mathbb{Z}$, on a $\varphi_g(j+k) = g^{j+k} = g^j g^k = \varphi_g(j)\varphi_g(k)$ et φ_g est bien un morphisme de groupes.

Connaissant les sous-groupes additifs de $\mathbb{Z}$, on a le résultat suivant.

Théorème 19. *Pour $g \in G$, on a*

1. $\theta(g) = +\infty$ *si et seulement si* φ_g *est injectif,*
2. g *d'ordre fini si et seulement si* $\ker(\varphi_g) = \theta(g)\mathbb{Z}$.

Preuve. Le noyau de φ_g étant un sous-groupe de $\mathbb{Z}$, il existe un unique entier $n \in \mathbb{N}$ tel que $\ker(\varphi_g) = n\mathbb{Z}$.

On aura $n = 0$ si, et seulement si, φ_g est injective, ce qui revient à dire que $\varphi_g(k) = g^k \neq e$ pour tout $k \in \mathbb{Z}^*$ ou encore que $\varphi_g(k) = g^k \neq \varphi_g(j) = g^j$ pour tous $j \neq k$ dans $\mathbb{Z}$ et le sous-groupe $\langle g \rangle = \mathrm{Im}(\varphi_g)$ est infini.

Si $n \geq 1$, en effectuant, pour $k \in \mathbb{Z}$, la division euclidienne de k par n, on a $k = qn+r$ avec $0 \leq r \leq n-1$ et $g^k = (g^n)^q g^r = g^r$, ce qui nous donne :

$$\langle g \rangle = \mathrm{Im}(\varphi_g) = \{g^r |\ 0 \leq r \leq n-1\}.$$

De plus pour $1 \leq r \leq n-1$, on a $g^r \neq e$ puisque $n = \inf(\ker(\varphi_g) \cap \mathbb{N}^*)$, ce qui entraîne $g^r \neq g^s$ pour $0 \leq r \neq s \leq n-1$ (voit preuve de la Proposition 8). Le groupe $\langle g \rangle$ a donc exactement n éléments. □

Corollaire 4. *Dire que $g \in G$ est d'ordre fini $n \geq 1$ équivaut à dire que, pour $k \in \mathbb{Z}$, on a : $g^k = e$ si, et seulement si, k est un multiple de n.*

Preuve. Si g est d'ordre n, alors n est le plus petit entier vérifiant $g^n = e$. Soit $k \in \mathbb{Z}$, alors par la division euclidienne, on a pour $k = qn + r \in \mathbb{Z}$ avec $q \in \mathbb{Z}$ et $0 \leq r \leq n-1$, donc $g^k = g^r = e$ si, et seulement si $r = 0$.

Réciproquement, on a $g^k = e$ si, et seulement si, k est multiple de n. Alors $g^n = e$ et $g^k \neq 1$ si k est compris entre 1 et $n-1$, ce qui signifie que g est d'ordre n. □

Théorème 20. *Soient g, h dans G d'ordre fini et $k \in \mathbb{Z}^*$.*

1. *On a* $\theta(g^k) = \dfrac{\theta(g)}{\theta(g) \wedge k}$ *(en particulier* $\theta(g^{-1}) = \theta(g)$*).*
2. *Si k divise $\theta(g)$, alors on a* $\theta(g^k) = \dfrac{\theta(g)}{|k|}$.
3. *Si k est premier avec $\theta(g)$, on a alors* $\theta(g) = \theta(g^k)$
4. *Si $gh = hg$, alors hg est d'ordre fini divisant $\theta(g) \vee \theta(h)$.*
   Dans le cas où $\langle g \rangle \cap \langle h \rangle = \langle e \rangle$, on a $\theta(gh) = \theta(g) \vee \theta(h)$.
   De plus, si $\theta(g)$ et $\theta(h)$ sont premiers entre eux, alors $\langle g \rangle \cap \langle h \rangle = \langle e \rangle$, et $\theta(gh) = \theta(g) \vee \theta(h) = \theta(g)\theta(h)$.

Preuve. 1. Soit $\delta = \theta(g) \wedge k$, alors il existe deux entiers n', k' premiers entre eux tels que $\theta(g) = \delta n'$, $k = \delta k'$. D'une part, on a

$$(g^k)^{n'} = g^{kn'} = g^{\delta k' n'} = (g^{\theta(g)})^{k'} = e.$$

D'autre part, pour tout entier relatif j on a :

$$(g^k)^j = g^{kj} = e \iff \exists q \in \mathbb{Z},\ kj = q\theta(g) \iff \exists q \in \mathbb{Z},\ k'j = qn' \iff n' \text{ divise } j.$$

Par suite n' est le plus petit entier positif vérifiant $(g^k)^{n'} = e$, c'est-à-dire

$$\theta(g^k) = n' = \frac{\theta(g)}{\theta(g) \wedge k}.$$

2. Si k divise $\theta(g)$, alors $\theta(g) \wedge k = |k|$, donc $\theta(g^k) = \dfrac{\theta(g)}{|k|}$.

3. Si k est premier avec $\theta(g)$, alors $\theta(g) \wedge k = 1$, donc $\theta(g) = \theta(g^k)$.

4. Posons $\mu = \theta(g) \vee \theta(h)$. Dans le cas où g et h commutent, on a $(gh)^\mu = g^\mu h^\mu = e$, avec $\mu \geq 1$ donc gh est d'ordre fini et cet ordre divise μ.

Notons par $n = \theta(gh)$ l'ordre de gh, on a $g^n h^n = (gh)^n = e$ et $g^n = h^{-n} \in \langle g \rangle \cap \langle h \rangle$.

Si $\langle g \rangle \cap \langle h \rangle = \{e\}$, alors $g^n = h^n = e$ et n est multiple de $\theta(g)$ et $\theta(h)$, donc de $\theta(g) \vee \theta(h)$ et $n = \theta(g) \vee \theta(h)$.

Si $\theta(g) \wedge \theta(h) = 1$, alors $\theta(g) \vee \theta(h) = \theta(g)\theta(h)$. De plus avec $\langle g \rangle \cap \langle h \rangle \subset \langle g \rangle$ et $\langle g \rangle \cap \langle h \rangle \subset \langle h \rangle$, on déduit que $card(\langle g \rangle \cap \langle h \rangle)$ divise $\theta(g) = card(\langle g \rangle)$ et $\theta(h) = card(\langle h \rangle)$, donc $card(\langle g \rangle \cap \langle h \rangle) = 1$ et $\langle g \rangle \cap \langle h \rangle = \{e\}$, ce qui implique que $\theta(gh) = \theta(g) \vee \theta(h) = \theta(g)\theta(h)$. □

Remarques 13.

1. Si $\theta(g)$ et $\theta(h)$ ne sont pas premiers entre eux, avec g et h commutant et d'ordre fini, alors l'ordre de gh n'est pas forcement le ppcm de $\theta(g)$ et $\theta(h)$. Comme contre exemple, il suffit de prendre g d'ordre un entier $n \geq 2$ dans G et $h = g^{-1}$ qui est aussi d'ordre n, donc $gh = hg = e$ est d'ordre $1 \neq \text{ppcm}(n, n) = n$.
2. Si g et h ne commutent pas le résultat est faux (le produit gh peut être par fois d'ordre infini, même si g et h sont d'ordre fini). Comme exemple, dans le groupe symétrique S_3 qui est d'ordre 6 ; la transposition $\sigma = (12)$ est d'ordre 2 ; le cycle $\tau = (123)$ est d'ordre 3, mais les transpositions $\sigma\tau = (23) \neq \tau\sigma = (13)$ ne sont pas d'ordre 6, elles sont d'ordre 2. Si $\sigma\tau$ est d'ordre 6, S_3 sera cyclique, ce qui n'est pas le cas (S_3 n'est pas abélien).

2.9. **Retour aux groupes cycliques.**

2.9.1. **Générateurs d'un groupe cyclique.**

Théorème 21. *Soit $G = \langle g \rangle$ un groupe cyclique d'ordre n. Les générateurs de G sont les éléments g^k, où k est tel que $1 \leq k \leq n-1$ et $k \wedge n = 1$.*

Preuve. Si $k \in \{1, \cdots, n-1\}$ est premier avec n, le théorème de Bézout nous dit qu'il existe deux entiers relatifs u, v tels que $uk + vn = 1$, ce qui entraîne que pour tout $g \in G$, on a :

$$g = g^1 = g^{uk+vn} = g^{uk}g^{vn} = (g^k)^u \in \langle g^k \rangle, \text{ car } g^{vn} = (g^n)^v = e^v = e.$$

Donc $G \subset \langle g^k \rangle$, et par suite $G = \langle g^k \rangle$ puisque $\langle g^k \rangle \subset G$.

Réciproquement, soit $k \in \{1, \cdots, n-1\}$ tel que $G = \langle g^k \rangle$; comme $g \in G$, alors il existe un entier relatif u tel que $g = (g^k)^u = g^{ku}$, donc $g^{1-ku} = e$, et par suite n divise $1 - ku$ car n est l'ordre de g. Ceci signifie qu'il existe un entier relatif v tel que $1 - ku = vn$, donc $uk + vn = 1$, par suite k est premier avec n. □

Ce théorème nous donne le nombre des générateurs d'un groupe cyclique. On rappelle que la fonction indicatrice d'Euler est la fonction qui associe à tout entier naturel non nul n, le nombre, noté $\varphi(n)$, d'entiers compris entre 1 et n qui sont premiers avec n (pour $n = 1$, on a $\varphi(1) = 1$). Donc

Corollaire 5. *Soit G un groupe cyclique d'ordre n, alors le nombre des générateurs de G est $\varphi(n)$, l'indicateur d'Euler de n.*

Preuve. $\varphi(n)$ est le nombre des entiers $1 \leq k \leq n-1$ premiers avec n. □

On déduit facilement le résultat suivant.

Corollaire 6. *Un élément d'un groupe cyclique est un générateur de ce groupe si et seulement si son ordre est égal à l'ordre du groupe.*

2.9.2. **Exemples de groupes cycliques.**
Commençons par le théorème suivant qui nous dit qu'à isomorphisme près, il n'y a qu'un seul groupe d'ordre p premier, à savoir $\mathbb{Z}/p\mathbb{Z}$

Théorème 22. *Un groupe d'ordre premier p est cyclique, donc commutatif et isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

Preuve. Soit $(G, \cdot)$ un groupe de cardinal premier $p \geq 2$. Soit $g \in G$ et $g \neq e$, alors l'ordre de g est différent de celui de e, qui est 1, et divise p, donc cet ordre est p et G est cyclique engendré par g.

L'application $f : \mathbb{Z}/p\mathbb{Z} \longrightarrow G$; $\overline{k} = k + p\mathbb{Z} \longmapsto g^k$ réalise alors un isomorphisme du groupe $(\mathbb{Z}/p\mathbb{Z}, +)$ sur $(G, \cdot)$. □

Si p et q sont deux nombres premiers, un groupe d'ordre pq n'est pas nécessairement cyclique comme le montre l'exemple du groupe symétrique S_3 qui est d'ordre 6 non commutatif et donc non cyclique. Mais pour G commutatif d'ordre pq avec $p \neq q$, on a le résultat suivant.

Théorème 23. *Un groupe commutatif d'ordre pq, où p et q sont deux nombres premiers distincts, est cyclique. Il est donc commutatif et isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.*

Preuve. Soit G commutatif d'ordre pq avec $2 \leq p < q$ premiers.

- S'il existe dans G un élément g d'ordre p et un élément h d'ordre q, alors gh est d'ordre pq (Théorème 20 pour G commutatif), et donc G est cyclique engendré par gh.

- Sinon les éléments de $G\backslash\{e\}$ sont tous d'ordre p ou tous d'ordre q. Supposons les tous d'ordre p. Si $g \in G$ est d'ordre p, alors le groupe quotient $G/\langle g\rangle$ est d'ordre q premier, donc cyclique, il est donc engendré par $\overline{g}$ d'ordre q dans $G/\langle g\rangle$, ce qui entraîne que $\theta(g) = p$ divise q, ce qui est impossible pour $p \neq q$ premiers.

Le théorème de Cauchy (voir Théorème 26) nous donne une démonstration plus rapide. Ce théorème nous dit qu'il existe dans G commutatif un sous-groupe d'ordre p et un d'ordre q, ces groupes sont cycliques et on a ainsi un élément d'ordre p et un élément d'ordre q. □

Théorème 24 (**Théorème des restes Chinois**). *Le groupe $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$ est cyclique si, et seulement si, les entiers p et q sont premiers entre eux. Dans ce cas $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$ est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.*

Preuve. Le groupe $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ est commutatif et pour p, q premiers entre eux, le théorème précédent nous dit qu'il est cyclique. Si p et q ne sont pas premiers entre eux les groupes additifs $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ ne peuvent être isomorphes puisque $\overline{1}$ est d'ordre pq dans $\mathbb{Z}/pq\mathbb{Z}$ et tous les éléments de $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ ont un ordre qui divise le ppcm de p et q qui est strictement inférieur à pq. □

2.9.3. **Sous-groupes d'un groupe cyclique.**

Le théorème qui suit nous dit que les sous-groupes d'un groupe cyclique sont cycliques et que pour tout diviseur d de n, il existe un sous-groupe de G d'ordre d. Ce résultat n'est pas vrai pour un groupe fini quelconque, comme le montre l'étude du groupe symétrique A_4 qui est d'ordre 12 et n'a pas de sous-groupes d'ordre 6.

Théorème 25. *Soit $G = \langle g\rangle$ un groupe cyclique d'ordre $n \geq 2$. Pour tout diviseur d de n, il existe un unique sous-groupe d'ordre d de G, c'est le groupe cyclique $H = \langle g^{\frac{n}{d}}\rangle$.*

Preuve. Pour tout diviseur d de n, $H = \langle g^{\frac{n}{d}} \rangle$ est un sous-groupe cyclique de G, et d'après le Théorème 20, on a $\theta(g^{\frac{n}{d}}) = \dfrac{n}{n \wedge \frac{n}{d}} = d$.

Réciproquement, soit H un sous-groupe de G d'ordre d, un diviseur de n.
- Si $d = 1$, on a alors $H = \{e\} = \langle g^n \rangle$.
- Si $d \geq 2$, H n'est pas réduit à $\{e\}$, donc il existe un élément $h \in H$, or $H \subset G$, alors il existe un entier k compris entre 1 et $n-1$ tel que $h = g^k \in H$. Posons

$$p = \min(\{k \in \{1, \cdots, n-1\} |\ g^k \in H\}).$$

Donc $\langle g^p \rangle \subset H$. Soit $h \in H$, alors il existe $k \in \mathbb{N}$ tel que $h = g^k \in H$, par la division euclidienne par p on a $k = pq + r$ avec $0 \leq r \leq p-1$, d'où $g^r = g^k (g^{pq})^{-1} \in H$, donc forcement on aura $r = 0$ puisque $r < p$. On a montré donc que $h = g^k = (g^p)^q$, d'où $H \subset \langle g^p \rangle \subset H$, soit $H = \langle g^p \rangle$. Comme $g^n = 1 \in H$, alors n est multiple de p et l'ordre de H est $d = \dfrac{n}{n \wedge p} = \frac{n}{p}$, c'est-à-dire que $H = \langle g^{\frac{n}{d}} \rangle$. Un tel sous-groupe d'ordre d est donc unique. □

Réciproquement, on peut montrer qu'un groupe fini ayant la propriété du théorème précédent est nécessairement cyclique (voir [15], exercice 1.1.12.).

Exemple 3. Pour $G = \mathbb{Z}/n\mathbb{Z}$, d un diviseur de n, l'unique sous-groupe d'ordre d de G est $H = \left\langle \frac{n}{d}\overline{1} \right\rangle = \dfrac{m\mathbb{Z}}{n\mathbb{Z}}$ où $m = \frac{n}{d}$. Ce sous-groupe est isomorphe à $\mathbb{Z}/d\mathbb{Z}$, et il y en a autant de sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ que de diviseurs de n. Ce résultat est en fait un cas particulier du quatrième théorème d'isomorphisme voir Théorème 30.

Théorème 26 (**Théorème de Cauchy).** *Soit G un groupe commutatif fini d'ordre $n \geq 2$. Pour tout diviseur premier p de n il existe dans G un élément d'ordre p.*

Preuve. On procède par récurrence sur l'ordre $n \geq 2$ de G.
Pour $n = 2$, c'est clair puisque $G = \{1, g\}$ est le seul sous-groupe d'ordre 2.
Supposons le résultat vrai pour les groupes commutatifs d'ordre $m < n$, où $n \geq 3$. Soient un groupe commutatif G d'ordre n, un diviseur premier p de n et un élément $g \in G \backslash \{e\}$.

- Si $G = \langle g \rangle$, alors G est cyclique et g est d'ordre n. Pour tout diviseur premier p de n, l'élément $h = g^{\frac{n}{p}}$ est d'ordre p dans G par le Théorème 25.

- Si $G \neq \langle g \rangle$ et p divise $m = card(\langle g \rangle) < n$, alors l'hypothèse de récurrence nous assure l'existence d'un élément h dans $\langle g \rangle$ qui est d'ordre p.

- Supposons enfin que $G \neq \langle g \rangle$ et p ne divise pas $m = card(\langle g \rangle)$. Comme p est premier ne divisant pas m, il est premier avec m et le groupe quotient $G/\langle g \rangle$ est commutatif d'ordre $r = \frac{n}{m} < n$ divisible par p (p divise $n = rm$ et p est premier avec m, le théorème de Gauss nous dit alors que p divise r). L'hypothèse de récurrence nous assure alors de l'existence d'un élément $\overline{h}$ d'ordre p dans $G/\langle g \rangle$. Comme l'ordre s de h est multiple de $\theta(\overline{h}) = p$ (voit TD), alors $k = h^{\frac{s}{p}}$ est d'ordre p dans G. □

Remarque 9. Si G est un groupe commutatif non cyclique et si d est un diviseur quelconque de n, alors il n'existe pas forcement un élément d'ordre d dans G.

Le Théorème 26 reste vrai même si G n'est pas abélien.

2.10. **Théorèmes d'isomorphismes.**
Rappelons que si $f : G \to G'$ est un homomorphisme de groupes, alors $\ker(f)$ est un sous-groupe normal de G (voir Théorème 12). Ce qui permet de définir sur le groupe quotient $G/\ker(f)$ une loi de groupe compatible avec celle de G. Grâce à cette compatibilité, l'homomorphisme de groupes $f : G \to G'$ induit un isomorphisme $\overline{f} : G/\ker(f) \to \operatorname{Im} f$.

Théorème 27 (**Premier théorème d'isomorphisme).** *Soient G et G' deux groupes et $f : G \to G'$ un homomorphisme de groupes. Alors f induit un isomorphisme $\overline{f}$ de $G/\ker(f)$ vers $f(G) = \mathrm{Im(f)}$. On écrit $G/\ker(f) \simeq f(G) = \mathrm{Im(f)}$. De plus on a :*

$$f = i \circ \overline{f} \circ \pi$$

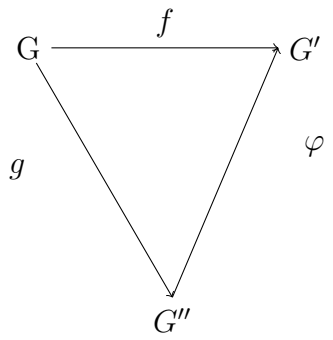
où i est l'injection canonique et π est la surjection canonique.

Preuve. Voir Théorème 14. □

Une autre formulation possible de ce théorème est que l'homomorphisme f se factorise par la surjection et l'injection canoniques, c'est-à-dire que le diagramme qui suit est commutatif.

$$\begin{array}{ccc} \mathrm{G} & \xrightarrow{\quad f \quad} & G' \\ \Big\downarrow{\scriptstyle \pi} & & \Big\uparrow{\scriptstyle i} \\ G/\ker(f) & \xrightarrow{\quad \overline{f} \quad} & \mathrm{Im}(f) \end{array}$$

Proposition 11. *Soient G, G' et G'' 3 groupes, f un homomorphisme de G dans G' et g un homomorphisme surjectif de G dans G'' ; alors il existe un homomorphisme φ de G'' dans G' tel que : $f = \varphi \circ g$ si et seulement si* $\ker(g) \subset \ker(f)$.



$f = \varphi \circ g$ si et seulement si $\ker(g) \subset \ker(f)$.

Preuve. La première implication est évidente.

Inversement, Supposons que $\ker(g) \subset \ker(f)$. Soit $y \in G''$; comme g est surjective, il existe $x \in G$ tel que $y = g(x)$. On pose : $\varphi(y) = f(x)$. Montrons que φ est une application.
Si $y = g(x) = y' = g(x')$ alors $g(x).g(x')^{-1} = e'' = g(x.x'^{-1}) = e'' \Rightarrow x.x'^{-1} \in \ker g$.
D'où $x.x'^{-1} \in \ker(f) \Rightarrow f(x.x'^{-1}) = e' \Rightarrow f(x) = f(x')$. Donc $\varphi(y) = \varphi(y')$.
Donc φ est bien une application. On vérifie aussi que φ est un homomorphisme de groupes : si $y = g(x)$ et $y' = g(x')$; alors $\varphi(y.y') = f(x.x') = f(x).f(x') = \varphi(y).\varphi(y')$.
□

Proposition 12. *Soient G un groupe et H et K deux sous-groupes de G. Alors on a :*

1. *HK est un sous-groupe de G si et seulement si $HK = KH$.*
2. *Si H est un sous-groupe distingué de G alors HK est un sous-groupe de G.*
3. *Si H est un sous-groupe distingué de G alors $H \cap K$ est distingué dans K.*

Preuve. 1. Voir TD.

2. Si H est distingué dans G, alors HK est un sous-groupe de G. Pour cela, il suffit de montrer que $HK = KH$. Comme H distingué, alors $\forall k \in K$ on a $kH = Hk$, d'où $HK = KH$.
3. Soient $x \in H \cap K$ et $k \in K$ on a : $kxk^{-1} \in K$ et puisque H distingué on a $kxk^{-1} \in H$; donc $kxk^{-1} \in H \cap K$, d'où $H \cap K$ est un sous-groupe distingué de K.

□

Théorème 28 (**Deuxième théorème d'isomorphisme).**
Soient G un groupe, H un sous-groupe distingué de G et K un sous-groupe de G alors

$$K/H \cap K \simeq HK/H.$$

Preuve. Comme H est un sous-groupe distingué de G, alors HK est un sous-groupe de G. Donc H est un sous-groupe distingué de HK. Soit

$$\begin{aligned} \pi : \ K &\longrightarrow HK/H \\ x &\longmapsto \overline{x} = Hx \end{aligned}$$

π est un homomorphisme surjectif, d'où $K/\ker\pi \simeq HK/H$.
Or $\ker\pi = \{x \in K/Hx = H\} = \{x \in K/x \in H\} = K \cap H$. Par suite $K/K \cap H \simeq HK/H$ □

Remarque 10. La conclusion de ce théorème reste vraie si l'on suppose seulement que le normalisateur de H contient K (au lieu de le supposer égal à G tout entier). Rappelons que le normalisateur de H dans G est définit comme suit :

Définition 25. Soient G un groupe et H un sous-groupe de G. Le sous-groupe de G formé par les éléments g de G tels que $gHg^{-1} = H$, est appelé le normalisateur de H (dans G) et noté $N_G(H)$.

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\} = \{g \in G \mid gH = Hg\}.$$

Définition 26. Soient G un groupe et H un sous-groupe de G. Les sous-groupes de G de la forme gHg^{-1} où $g \in G$ sont appelés les conjugués de H.

Théorème 29 (**Troisième théorème d'isomorphisme).**
Soient G un groupe et N et M deux sous-groupes normaux de G tels que M soit inclus dans N. Alors N/M est un sous-groupe normal de G/M et on a l'isomorphisme suivant :

$$(G/M)/(N/M) \simeq G/N.$$

Preuve. Considérons L'application φ : $\begin{aligned} G/M &\longrightarrow G/N \\ gM &\longmapsto (gM)N = g(MN) = gN \end{aligned}$
On a :

i. $gM = g'M \Longleftrightarrow g^{-1}g' \in M$, donc $g^{-1}g' \in N$ c'est-à-dire $gN = g'N$, d'où φ est bien défini.
ii. soient g et g' dans G, alors $\varphi(gMg'M) = \varphi(gg'M) = gg'N = gNg'N = \varphi(gM)\varphi(g'M)$, donc φ est un homomorphisme.

iii. pour tout $y = gN \in G/N$, il existe $x = gM$ tel que $\varphi(gM) = gN$. Donc φ est surjectif, d'où $\mathrm{Im}(\varphi) = \mathrm{G/N}$.

iv. le noyau de φ est

$$\begin{aligned}\ker(\varphi) &= \{gM \in G/M |\ \varphi(gM) = N\} \\ &= \{gM \in G/M |\ gN = N\} \\ &= \{gM \in G/M |\ g \in N\} \\ &= N/M.\end{aligned}$$

Par application du premier théorème d'isomorphisme, on obtient

$$(G/M)/\ker(\varphi) = (G/M)/(N/M) \simeq G/N.$$

□

Théorème 30 ($4^{\text{ème}}$ **th. d'isomorphisme ou th. de correspondance)).**
Soient G un groupe et H un sous-groupe distingué de G. Les sous-groupes du groupe quotient G/H sont de la forme K/H où K est un sous-groupe de G qui contient H.

Preuve. Soit K un sous-groupe de G qui contient H. Comme H est distingué dans G, il l'est aussi dans K et :

$$K/H = \{gH |\ g \in K\} \subset G/H = \{gH |\ g \in G\}$$

est un sous-groupe de G/H.

Réciproquement, soit L un sous-groupe de G/H, et soit $K = \{g \in G |\ gH \in L\}$. On a $H \subset K$ (pour $g \in H$, on a $gH = H = \overline{1} \in L$ puisque L est un groupe). D'autre part, K est un sous-groupe de G, en effet : si $g \in K$, alors $gH = \overline{g} \in L$, donc $g^{-1}H = \overline{g^{-1}} = \overline{g}^{-1} \in L$; et pour g_1, g_2 dans K, on a $g_1 g_2 H = \overline{g_1 g_2} \in L$. Comme H est distingué dans G, il l'est aussi dans K et $K/H = \{gH |\ g \in K\} = L$ par construction. □

Corollaire 7. *Soit H un sous-groupe distingué d'un groupe G, et soit $\pi : G \longrightarrow G/H$ la surjection canonique. Alors :*

i. *il existe une bijection entre l'ensemble des sous-groupes de G contenant H et l'ensemble des sous-groupes de G/H.*

ii. *il existe une bijection de l'ensemble des sous-groupes distingués de G contenant H sur l'ensemble des sous-groupes distingués de G/H.*

Exemple 4. Les sous-groupes de $U_n = \{z \in \mathbb{C} |\ z^n = 1\} = \left\langle e^{\frac{2i\pi}{n}} \right\rangle$ sont les $\left\langle \left(e^{\frac{2i\pi}{n}}\right)^{\frac{n}{d}} \right\rangle = \left\langle e^{\frac{2i\pi}{d}} \right\rangle = U_d$, où d est un diviseur de n et il y en a autant que de diviseurs de n.

Exercice : Montrer que R/H est un sous-groupe distingué de G/H si, et seulement si, R est un sous-groupe distingué de G.

Applications.

1. Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$. D'après le théorème de correspondance les sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $R/n\mathbb{Z}$ où R est un sous-groupe de $\mathbb{Z}$ tel que $n\mathbb{Z} \subset R$. Comme R est un sous groupe de $\mathbb{Z}$ alors $R = d\mathbb{Z}$ et puisque $n\mathbb{Z} \subset R$ alors $d|n$. Par suite les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont $d\mathbb{Z}/n\mathbb{Z}$ où $d|n$.
2. Soient m, n et d des entiers naturels tels que $m = nd$, n et d sont premiers entre eux et φ l'application de $\mathbb{Z}$ dans $d\mathbb{Z}/m\mathbb{Z}$ qui fait correspondre à k la classe de dk

$$\begin{array}{rccc} \varphi : & \mathbb{Z} & \longrightarrow & d\mathbb{Z}/m\mathbb{Z} \\ & k & \longmapsto & \overline{dk} = (dk)m\mathbb{Z} \end{array}$$

alors φ est une surjection et $Ker\varphi = n\mathbb{Z}$. Par suite on a

$$d\mathbb{Z}/m\mathbb{Z} = d\mathbb{Z}/nd\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z}.$$

2.11. **Exercices.**

Exercice 2.1. Sont G un groupe.

1. Soient H et K deux sous-groupes de G. Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$. Déduire qu'un groupe ne peut jamais être la réunion de deux de ses sous-groupes propres.
2. Déduire que $a\mathbb{Z} \cup b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ si et seulement si a divise b ou b divise a, où a et b sont dans $\mathbb{N}^*$.
3. Soit $(H_i)_{i\in I}$ une famille de sous-groupes de G ; supposons que pour tous indices i et $j \in I$, il existe un indice $k \in I$ vérifiant $H_i, H_j \subset H_k$. Montrer que $\bigcup_{i\in I} H_i$ est un sous-groupe de G.

Exercice 2.2. Montrer que $5\mathbb{Z} \cup 8\mathbb{Z}$ n'est pas un sous-groupe de $(\mathbb{Z}, +)$.

Exercice 2.3. Soient H et K deux sous-groupes d'un groupe G. Montrer que $HK = \{hk \mid h \in h \text{ et } k \in K\}$ est un sous-groupe de G si et seulement si $HK = KH$.

Exercice 2.4. Soient G un groupe et H une partie finie stable de G. Montrer que H est un sous-groupe de G. Donner un contre-exemple à la propriété précédente dans le cas d'une partie H infinie.

Exercice 2.5. Soit G un groupe d'élément neutre e tel pour tout $x \in G$, $x^2 = e$.

1. Montrer que G est commutatif.
2. Montrer que si G est fini, alors son ordre n est une puissance de 2, dans ce cas on dit que G est un 2-groupe.

Définition. Un groupe fini G est dit un p-groupe, où p est un nombre premier, lorsque tout élément de G a pour ordre une puissance de p.

Exercice 2.6. Soit un groupe $(G, \cdot)$ d'élément neutre e, on note par a^{-1} le symétrique d'un élément $a \in G$.

1. Soient H un sous groupe de G et g un élément de G. Montrer que l'ensemble $H' = \{ghg^{-1} \mid h \in H\}$ est un sous groupe de G.
2. Soit l'application $f : \begin{array}{ccc} G & \longrightarrow & G \\ a & \longmapsto & a^{-1} \end{array}$ montrer que f est un isomorphisme si et seulement si $(G, \cdot)$ est abélien.

Exercice 2.7. Soient G un groupe non commutatif et $Z(G)$ son centre. Montrer que $Z(G)$ est un sous-groupe distingué de G.

Exercice 2.8. Soient G un groupe fini et H un sous-groupe de G tel que $[G : H] = 2$. Montrer que H est un sous-groupe distingué de G.

Exercice 2.9. Soient G un groupe et $D = \{(x,x) |\ x \in G\}$. Montrer que D est un sous-groupe distingué de $G \times G$ si et seulement si G est abélien.

Exercice 2.10. Soit G un groupe. Pour tous x et y dans G, l'élément $[x, y] = x^{-1}y^{-1}xy$ est dit le commutateur de x et y. Notons par $D(G)$ le sous-groupe de G engendré par tous les commutateurs $[x, y]$ ($D(G)$ est dit le groupe dérivé de G). Soit H un sous-groupe normal de G, montrer que G/H est un groupe abélien ssi $D(G) \subseteq H$.

Exercice 2.11. Déterminer les groupes G d'ordre 1, 2, 3, 4, 5.

Exercice 2.12. Soit $\mathcal{R}$ une relation d'équivalence sur un groupe G compatible avec la loi de G. Montrer que :

1. pour tous g, h dans G, on a $g\overline{h} = \overline{gh}$ et $\overline{h}g = \overline{hg}$;

2. $H = \overline{e}$ est un sous-groupe distingué de G ;
3. pour tout $g \in G$, $\overline{g} = gH = Hg$ et $G/\mathcal{R} = G/H$.

De cet exercice, on déduit que les relations d'équivalence sur un groupe compatibles avec sa loi sont celles suivant un groupe distingué (à gauche ou à droite).

Exercice 2.13. Soit A une partie non vide d'un groupe G. On appelle normalisateur de A dans G l'ensemble $N(A) = \{g \in G |\ gA = Ag\}$ et on appelle centralisateur de A dans G l'ensemble $Z(A) = \{g \in G |\ \forall a \in A, ga = ag\}$.

1. Montrer que $N(A)$ est un sous-groupe de G.
2. Montrer que $Z(A)$ est un sous-groupe distingué de G.

Exercice 2.14. Soit H un sous-groupe d'un groupe G. Montrer que $\text{card}((G/H)_g) = \text{card}((G/H)_d)$.

Exercice 2.15. Soient H un sous-groupe d'un groupe G et K un sous-groupe de H ($K \subset H \subset G$). Montrer que si l'indice de K dans G est fini, alors l'indice de H dans G et celui de K dans H sont aussi finis et on a : $[G : K] = [G : H][H : K]$.

Exercice 2.16. Soit G un groupe de $2n$ éléments. Montrer qu'il existe un élément distinct de l'unité qui est son propre inverse.

Exercice 2.17. Soit G un groupe. Pour tout couple (g, x) de $G \times G$ on pose $g \cdot x = gxg^{-1}$.

1. Montrer que G opère ainsi sur lui-même.
2. On suppose que G est fini d'ordre p^n où p est un nombre premier et $n \in \mathbb{N}$. Montrer que $Z(G)$ n'est pas réduit à l'élément neutre.

Exercice 2.18.

1. Soit $f :\ G \longrightarrow G'$ un homomorphisme de groupes surjectif, montrer qu'il existe une bijection entre les sous-groupes distingués de G contenant $\ker(f)$ et les sous-groupes distingués de G'.
2. Étudier les cas G, $G' = G/H$, $f = \pi$ la surjection canonique et $H \lhd G$.

Exercice 2.19. Soient G un groupe fini et $Z = Z(G)$ son centre.

1. Montrer que si G/Z est cyclique, alors G est abélien.
2. Montrer que tout d'ordre p^2, p premier, est abélien.
3. Si $|G| = p^3$, p premier, déterminer $|Z|$.

Exercice 2.20. Considérons les ensembles suivants :
$G = \{f_{a,b} : \mathbb{R} \to \mathbb{R},\ x \mapsto ax + b \mid a \in \mathbb{R}^*, b \in \mathbb{R}\}$,
$H = \{g_c : \mathbb{R} \to \mathbb{R},\ x \mapsto x + c \mid c \in \mathbb{R}\}$,
$K = \{h_d : \mathbb{R} \to \mathbb{R},\ x \mapsto ax + b \mid d \in \mathbb{Q}\}$.

i. Montrer que G, H et K sont des groupes.

ii. Montrer que $H \lhd G$ et $K \lhd H$.

iii. A-t-on $K \lhd G$? Conclure.

Exercice 2.21. Montrer que l'intersection de deux sous-groupes distingués de G est un sous-groupe distingué de G.

Exercice 2.22. Soit G un groupe cyclique. Montrer que tout sous-groupe H de G est aussi cyclique.

Exercice 2.23. Soient G un groupe abélien et H un sous-groupe de G tel que G/H soit un groupe monogène infini. Montrer qu'il existe un isomorphisme de $H \times (G/H)$ sur G.

Exercice 2.24. Soient H, K deux sous-groupes d'un groupe fini G. Montrer que $\text{card}(HK) = \dfrac{|H||K|}{|H \cap K|}$, rappelons que $HK = \{hk \mid h \in H \text{ et } k \in K\}$.

Exercice 2.25. Soient G un groupe et H, K deux sous-groupes distingués de G. On dit que G est produit direct de H et K si $G = H \times K$. Déterminer les groupes G d'ordre p^2 avec p premier.

Exercice 2.26. Soit G un groupe fini d'ordre $n > 1$, et soit H un sous-groupe propre de G tel que $[G : H] = k > 1$ et n ne divise pas $k!$. Montrer que G n'est pas simple.

Exercice 2.27. Soit G un groupe fini abélien. Montrer que G est simple si et seulement si $|G|$ est premier.

Exercice 2.28. Soit G un groupe. Soit $a \in G$, alors la conjugaison par a est l'application $g_a : G \longrightarrow G,\ x \longmapsto axa^{-1}$.

1. Montrer que g_a est bien définie.
2. Montrer que g_a est un endomorphisme de G.
3. Montrer que g_a est un automorphisme de G et déterminer g_a^{-1}, g_a est dit automorphisme intérieur.
4. Montrer que $\text{Int}(G)$, l'ensemble des automorphisme intérieurs de G, est un sous-groupe de $\text{Aut}(G)$.

5. Montrer que $\mathrm{Int}(G)$ est un sous-groupe distingué de $\mathrm{Aut}(G)$.
6. Considérons l'application $\varphi : G \longrightarrow \mathrm{Aut}(G),\ a \longmapsto g_a$.
   i. Montrer que φ est un homomorphisme.
   ii. Déterminer $\ker\varphi$ et $\mathrm{Im}\varphi$. Déduire donc que $G/Z(G) \simeq \mathrm{Int}(G)$.

Exercice 2.29. Soit G un groupe non abélien tel que $|G| = 8$.

1. Montrer que G possède des éléments d'ordre 4.
2. Soit $H = \langle a \rangle$, $a \in G$ et $|a| = 4$. Soit $b \in G \backslash H$.
   i. Montrer que $b^2 \neq a$ et $b^2 \neq a^3$.
   ii. Montrer que $ba = a^3b$.
3. Montrer que G est l'un des groupes suivants :
   a. $D_4 = \langle a, b \rangle$ avec $|a| = 4$, $|b| = 2$ et $|ab| = 2$, D_4 est dit groupe diédral d'ordre 4.
   b. $Q_3 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\} = \langle a, b \rangle$ avec $|a| = |b| = 4$ et $a^2 = b^2$, Q_3 est dit groupe des quaternions.
4. Déterminer l'ordre de chaque élément de D_4.
5. Déterminer les sous-groupes de D_4.

Exercice 2.30. Soit H un sous-groupe de G. Montrer que :

$$H \lhd G \Longleftrightarrow \forall g \in G;\ gH \subset Hg \Longleftrightarrow \forall g \in G;\ gHg^{-1} \subset H.$$

Exercice 2.31. Soient G, G' deux groupes et f un homomorphisme de groupes de G dans G'.

1. Montrer que si H est un sous-groupe distingué de G et f est surjectif, alors $f(H)$ est un sous-groupe distingué de G.
2. Montrer que si H' est un sous-groupe distingué de G', alors $f^{-1}(H')$ est un sous-groupe distingué de G.

Exercice 2.32. Soient G, H deux groupes, $\varphi : G \longrightarrow H$ un homomorphisme de groupes, G' un sous-groupe distingué de G et H' un sous-groupe distingué de H tel que $\varphi(G') \subset H'$. Montrer qu'il existe un unique homomorphisme de groupes $\overline{\varphi} : G/G' \longrightarrow H/H'$ tel que $\pi_H \circ \varphi = \overline{\varphi} \circ \pi_G$, où $\pi_G : G \longrightarrow G/G'$ et $\pi_H : H \longrightarrow H/H'$ sont les surjections canoniques.

Exercice 2.33. Soit H un sous-groupe d'un groupe G. Montrer que H est distingué si et seulement si le produit de deux classes à gauche quelconques est une classe à gauche.

Exercice 2.34. Soient $(G, .)$ un groupe fini d'ordre $n \geq 2$ et H un sous-groupe distingué de G. Comparer l'ordre de $\overline{g}$ dans G/H avec l'ordre de g dans G.

Exercice 2.35. Montrer qu'un groupe G est fini si et seulement si l'ensemble de ses sous-groupes est fini. En conséquence, un groupe infini a une infinité de sous-groupes.

Exercice 2.36. Donner des exemples de groupes infinis dans lequel tous les éléments sont d'ordre fini.

Exercice 2.37. Soit $(G, .)$ un groupe tel que tout élément de G soit d'ordre au plus égal à 2.

1. Montrer que G est commutatif.
2. On suppose de plus que G est fini. Montrer qu'il existe un entier $n \in \mathbb{N}$ tel que $\text{card}(G) = 2^n$.

Exercice 2.38. Soit $(G, .)$ un groupe cyclique d'ordre m, et soit $a \in G$. .

1. Montrer que $b = a^k$, $k \in \mathbb{N}^*$, est un générateur de G si et seulement si m et k sont premiers entre eux.
2. Déterminer l'ordre du sous-groupe engendré par a^k avec $k \in \mathbb{N}^*$.
3. En déduire tous les générateurs de G.

Exercice 2.39. Soient G et G' deux groupes d'ordre un nombre premier p. Montrer que G et G' sont isomorphes.

Exercice 2.40. Soit f un isomorphisme d'un groupe G sur un groupe G'. Montrer que f conserve l'ordre de tout élément $a \in G$.

Exercice 2.41. Soient m et n deux entiers rationnels.

1. Montrer que pour qu'il existe un entier r tel que l'on ait :

$$r \equiv 0 \pmod{m} \text{ et } r \equiv 1 \pmod{n}$$

   il faut et il suffit que m et n soient premiers entre eux.
2. Déduire de là que si dans un groupe G deux éléments x et y sont d'ordres m et n premiers entre eux ($xy = yx$), alors $z = xy$ est d'ordre mn et le sous-groupe engendré par z contient x et y.

Exercice 2.42. Soient G et H deux groupes cycliques à m et n éléments respectivement. Montrer que pour que $G \times H$ soit cyclique, il faut et il suffit que m et n soient premiers entre eux. Si x et y sont des générateurs de G et H, le couple (x, y) est alors un générateur de $G \times H$.

Exercice 2.43. Montrer que tout groupe fini G d'ordre premier est cyclique, et admet pour générateur chacun de ses éléments autre que l'élément neutre.

Exercice 2.44. Soit f un homomorphisme d'un groupe fini G dans un groupe fini H. Montrer que $\text{card}(G) = \text{card}(\ker(f)) \cdot \text{card}(\text{Im}(f))$.

Exercice 2.45. Soit G un groupe. Montrer que les conditions suivantes sont équivalentes :

i. G est un groupe abélien simple.
ii. G est un groupe cyclique d'ordre premier.

Exercice 2.46. Soit G un groupe commutatif fini d'ordre p^n, p étant un nombre premier.

i. Montrer que tout élément de G est d'ordre p^m $(0 \leq m \leq n)$ et qu'il y a des éléments d'ordre p.
ii. Montrer que tout élément sous-groupe H de G est d'ordre p^m $(0 \leq m \leq n)$ et que pour tout m il existe au moins un sous-groupe d'ordre p^m.

Exercice 2.47. Soit G un groupe commutatif fini ayant m éléments. Soit $m = \prod_{i=1}^{k} p_i^{r_i}$ la décomposition de m en facteurs premiers. On pose dans tout ce qui suit : $q_i = p_i^{r_i}$, $m_i = \frac{m}{q_i}$, $i = 1, 2, \cdots, k$, et on désigne par G_i l'ensemble des éléments x de G tels que $x^{q_i} = e$, où e désigne l'élément neutre de G.

i. Montrer que G_i est un sou-groupe de G.
ii. Montrer qu'il existe des entiers $u_1, \cdots, u_k$ tels que $u_1 m_1 + \cdots + u_k m_k = 1$.
iii. Pour tout $x \in G$, on pose $x_i = x^{u_i m_i}$, $i = 1, 2, \cdots, k$, où les u_i sont donnés par la question ii.. Montrer que $x_i \in G_i$ et que $x = x_1 x_2 \cdots x_k$.
iv. On considère l'application $f : \begin{array}{ccc} G_1 \times G_2 \times \cdots \times G_k & \longrightarrow & G \\ (x_1, x_2, \cdots, x_k) & \longmapsto & x_1 x_2 \cdots x_k \end{array}$ montrer que f est un isomorphisme de groupes.
v. Montrer que G_i est d'ordre q_i.
vi. Expliciter les résultats précédents dans le cas où G est le groupe additif $\mathbb{Z}/m\mathbb{Z}$ des entiers modulo m.

Exercice 2.48. Soit G un groupe fini.

1. Soient $a \in G$ et $k \in \mathbb{N}^*$, montrer que $|a^k| = \dfrac{|a|}{k \wedge |a|}$.
2. Soient a et b dans G tels que $ab = ba$ et $\langle a \rangle \cap \langle b \rangle = \{e\}$, déterminer l'ordre de ab.

3. Le groupe symétrique S_n

Dans cette section, nous allons redéfinir le groupe symétrique et donner quelques unes de ses propriétés.

3.1. Définitions et Propriétés.

Soit E un ensemble non vide, l'ensemble des bijections de E sur lui même est noté $S(E)$, on dit aussi que $S(E)$ est l'ensemble des permutations de E.

Théorème 31. *L'ensemble $S(E)$ est un groupe pour la composition des applications.*

Preuve. C'est évident. □

Définition 27. Soit E un ensemble non vide, le groupe $S(E)$ est appelé *groupe des permutations* de E, on le note $S(E)$. Si $E = \{1, \cdots, n\}$, $n \in \mathbb{N}^*$, alors $S(E)$ est noté S_n, et il est dit *groupe symétrique* à n éléments.

Remarque 11. Dans le cas où E est réduit à un élément, on peut quand même définir $S(E)$ et il est réduit à $\{id_E\}$.

Théorème 32. *Si E, F sont deux ensembles non vides et f une bijection de E sur F, alors les groupes $S(E)$ et $S(F)$ sont isomorphes.*

Preuve. L'application $\varphi : \ S(E) \longrightarrow S(F);\ g \longmapsto f \circ g \circ f^{-1}$ est un isomorphisme. En effet, pour $g \in S(E)$, $\varphi(g) \in S(F)$ comme composée de bijections et pour g_1, g_2 dans $S(E)$, on a :

$$\varphi(g_1 \circ g_2) = f \circ g_1 \circ g_2 \circ f^{-1} = (f \circ g_1 \circ f^{-1}) \circ (f \circ g_2 \circ f^{-1}) = \varphi(g_1) \circ \varphi(g_2).$$

Donc φ est un morphisme de groupes.

Soit $g \in \ker(\varphi)$, alors $\varphi(g) = id_F$, donc $f \circ g \circ f^{-1} = id_F$; ceci implique que $g = f^{-1} \circ id_F \circ f = id_E$. D'où $\ker(\varphi) = \{id_E\}$, c-à-d φ est injective.

Pour $\tau \in S(F)$, l'application $g = f^{-1} \circ \tau \circ f$ est dans $S(E)$ et on a $\varphi(g) = \tau$, donc φ est surjective. Par suite φ est un isomorphisme. □

Remarque 12. Par le théorème 32, tout groupe de permutations d'un ensemble E à n éléments est isomorphe au groupe symétrique S_n des permutations de $\{1, 2, \cdots, n\}$. Donc il est équivalent de travailler dans le groupe $S(E)$ ou S_n.

Par suite les propriétés de $S(E)$ sont les mêmes que celles de S_n.

On rappelle que deux ensembles finis qui sont en bijection ont le même nombre d'éléments.

Proposition 13. *Soit $n \in \mathbb{N}^*$, alors $(S_n, \circ)$ est un groupe d'ordre $n!$. La composée $\sigma \circ \tau$ de deux permutations σ et τ de S_n sera noté $\sigma\tau$.*

Preuve. Laisser au lecteur. □

Le groupe symétrique joue un rôle important dans l'étude des polynômes symétriques (voir chapitre 3), l'étude de la résolubilité des équations polynomiales et en algèbre multilinéaire.

Pour toute permutation $\sigma \in S_n$ on note :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

pour signifier que σ est la bijection $\sigma : \begin{array}{ccc} E & \longrightarrow & E \\ k & \longmapsto & \sigma(k) \end{array}$

Avec cette notation, on calcule facilement la composée et l'inverse : si

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \text{ et } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$$

$$\text{alors } \sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 2 & 1 \end{pmatrix}$$

$$\text{et } \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 1 & 4 & 5 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 5 & 4 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$$

Théorème 33. *Pour $n \geq 3$, $(S_n, \circ)$ est un groupe non abélien.*

Preuve. En effet, soient les deux permutations :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots & n \end{pmatrix} \text{ et } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix}$$

on a :

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix} \text{ et } \sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 2 & 1 & 4 & \cdots & n \end{pmatrix}$$

Donc $\sigma\tau \neq \tau\sigma$. □

Définition 28. Soient $n \in \mathbb{N}^*$ et P une partie de $E = \{1, \cdots, n\}$. Soit $\sigma \in S_n$, on dit que σ opère sur P si σ laisse invariant les éléments de $\complement_E^P$, le complémentaire

de P dans E. P est dit aussi le support de la permutation $\sigma \in S(E)$ on le note : $supp(\sigma) = \{x \in E \mid \sigma(x) \neq x\}$.

Exemple 5. Soient $n = 6$ et $E = \{1, \cdots, 6\}$, alors la permutation $\sigma \in S_n$ définie par : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix}$ opère sur $supp(\sigma) = P = \{2, 3, 4\}$

Définition 29. Soient $n \in \mathbb{N}^*$ et $E = \{1, \cdots, n\}$. Une transposition est une permutation de S_n différente de l'identité qui opère sur une partie à deux éléments $\{i, j\}$. Autrement dit, une transposition est une permutation τ_{ij}, $i < j$, définie par :

$$\tau_{ij}(i) = j,\ \tau_{ij}(j) = i \text{ et } \tau_{ij}(k) = k \text{ pour } k \neq i \text{ et } k \neq j.$$

τ_{ij} se note aussi (ij).

Exemple 6. Soient $n = 6$ et $E = \{1, \cdots, 6\}$, alors la permutation $\sigma \in S_n$ suivante est une transposition.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 2 & 5 & 6 \end{pmatrix} = (2\ 4).$$

Définition 30. Soit $\sigma \in S_n$. On dit que σ est un *cycle* de longueur p ou un *p-cycle* s'il opère sur une partie $P \subset E$ à p éléments tel que si $P = \{i_1,...,i_p\}$, alors

i. $\forall k \in \{1, 2, \cdots, p-1\}$, $\sigma(i_k) = i_{k+1}$ et $\sigma(i_p) = i_1$, et

ii. $\forall k \notin \{i_1, ..., i_p\}$, $\sigma(i_k) = i_k$.

L'ensemble $P = \{i_1, ..., i_p\}$ est le *support du cycle*, et le nombre p est dit sa *longueur*. Un n-cycle dans S_n est appelé permutation circulaire.

Notation.

Le cycle σ est noté $\sigma = (i_1\ i_2\ ...\ i_p)$ ou $\begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_p & i_{p+1} & \cdots & i_n \\ i_2 & i_3 & i_4 & \cdots & i_1 & i_{p+1} & \cdots & i_n \end{pmatrix}$

Exemple 7. Soient $n = 6$ et $E = \{1, \cdots, 6\}$.

$$\sigma = (1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{pmatrix} \text{ et } \tau = (1\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 4 & 5 & 6 \end{pmatrix}$$

Sont deux cycles, σ a pour support $P = \{1, 2, 3\}$ et de longueur 3, et τ a pour support $P' = \{1, 2\}$ et de longueur 2 (τ est une transposition).

Remarques 14.

1. Les permutations : $(a_1a_2 \cdots a_p), (a_2a_3 \cdots a_pa_1), \cdots, (a_pa_1 \cdots a_{p-1})$ définissent le même p-cycle.

2. L'inverse d'un p-cycle est un p-cycle de même support. Précisément, on a : $(a_1 a_2 \cdots a_p)^{-1} = (a_p a_{p-1} \cdots a_1)$.
3. Si $\sigma = (a_1 a_2 \cdots a_p)$ est un p-cycle, alors pour tout entier k compris entre 1 et p on a :

$$a_k = \sigma^{k-1}(a_1).$$

En effet, c'est vrai pour $k = 1$; supposant le résultat vrai pour $1 \leq k-1 \leq p-1$, on a :

$$a_k = \sigma(a_{k-1}) = \sigma(\sigma^{k-2}(a_1)) = \sigma^{k-1}(a_1), \text{ car } a_{k-1} = \sigma^{k-2}(a_1).$$

Proposition 14. *Un p-cycle de longueur p est d'ordre p, i.e., $\sigma^p = id$ et $\forall k$ tel que $0 < k < p$, on a $\sigma^k \neq id$.*

Preuve. Soit $\sigma = (a_1 \cdots a_p)$ un p-cycle avec $p \geq 2$. Pour tout entier k compris entre 1 et p, on a :

- d'une part, $a_k = \sigma^{k-1}(a_1)$ (voir Remarques 14), donc pour tout $0 < k < p$, $\sigma^k \neq id$;
- d'autre part,

$$\begin{aligned} \sigma^p(a_k) &= \sigma^p(\sigma^{k-1}(a_1)) \text{ (voir Remarques 14)} \\ &= \sigma^{k-1}(\sigma^p(a_1)) \text{ (car le sous-groupe } \langle\sigma\rangle \text{ est abélien)} \\ &= \sigma^{k-1}(\sigma(\sigma^{p-1}(a_1))) = \sigma^{k-1}(\sigma(a_p)) \\ &= \sigma^{k-1}(a_1) \\ &= a_k; \end{aligned}$$

de plus, on sait que $\forall x \in E$ et $x \notin \{a_1, \cdots, a_p\}$, $\sigma^p(x) = x$. Donc $\forall x \in \{a_1, \cdots, a_p\}$, $\sigma^p(x) = x$, par suite $\sigma^p = id$.

Donc σ est d'ordre p. □

Remarques 15.

1. Du résultat précédent, On déduit que l'inverse d'un p-cycle σ est le p-cycle $\sigma^{-1} = \sigma^{p-1}$.
2. Si σ est un p-cycle, le calcul de σ^m, pour tout entier relatif m, peut alors s'obtenir en effectuant la division euclidienne de m par p : on a $m = pq + r$ avec $0 \leq r \leq p-1$, donc

$$\sigma^m = \sigma^{pq+r} = (\sigma^p)^q \sigma^r = \sigma^r.$$

3. Deux cycles σ et τ à supports disjoints commutent : $\sigma\tau = \tau\sigma$, simple à vérifier.

4. Un cycle $\tau_{ij} = (ij)$ de longueur 2 (i.e., une transposition) est d'ordre 2 puisque $\tau_{ij}^2 = id$.

Proposition 15. *Soit p un entier compris entre 2 et $\mathrm{card}(E)$. Le conjugué, dans $S(E)$, d'un p-cycle est encore un p-cycle. Précisément, pour tout p-cycle $\sigma = (x_1 x_2 \cdots x_p)$ et toute permutation τ, on a :*

$$\tau \circ \sigma \circ \tau^{-1} = (\tau(x_1)\tau(x_2)\cdots\tau(x_p)).$$

Réciproquement, deux cycles de même longueur sont conjugués dans $S(E)$, c'est-à-dire que si σ et ρ sont deux cycles de même longueur p, alors il existe une permutation τ telle que $\rho = \tau \circ \sigma \circ \tau^{-1}$.

Preuve. Soient un p-cycle $\sigma = (x_1 x_2 \cdots x_p)$ et une permutation τ. Notons

$$\mu = (\tau(x_1)\tau(x_2)\cdots\tau(x_p)),$$

alors il suffit montrer que $\tau \circ \sigma = \mu \circ \tau$.

- Si $x \in E\backslash\{x_1, \cdots, x_p\}$, on a $\sigma(x) = x$ et $\tau(x) \in E\backslash\{\tau(x_1), \cdots, \tau(x_p)\}$, ce qui implique que $\mu(\tau(x)) = \tau(x)$, d'où :

$$\tau \circ \sigma(x) = \tau(x) = \mu(\tau(x)) = \mu \circ \tau(x).$$

- Si x est l'un des x_k ($x \in \{x_1, \cdots, x_p\}$), on a donc :

$$\tau \circ \sigma(x) = \tau \circ \sigma(x_k) = \tau(\sigma(x_k)) = \tau(x_{k+1}),$$

en notant $x_{p+1} = x_1$, alors $\mu \circ \tau(x) = \mu(\tau(x_k)) = \tau(x_{k+1})$, d'où $\tau \circ \sigma = \mu \circ \tau$, donc $\tau \circ \sigma \circ \tau^{-1} = \mu$.

Inversement, Soient $\sigma = (x_1 x_2 \cdots x_p)$ et $\rho = (x'_1 x'_2 \cdots x'_p)$ deux p-cycles. Soit aussi une bijection φ de $E\backslash\{x_1, \cdots, x_p\}$ sur $E\backslash\{x'_1, \cdots, x'_p\}$, alors on peut définir une permutation τ de E en posant :
- $\tau(x_k) = x'_k$ pour $k = 1, \cdots, p$ et
- $\tau(x) = \varphi(x)$ pour $x \in E\backslash\{x_1, \cdots, x_p\}$;
on a donc : $\tau^{-1}(x'_k) = x_k$ pour $k = 1, \cdots, p$ et $\tau^{-1}(x) = \varphi^{-1}(x)$ pour $x \in E\backslash\{x'_1, \cdots, x'_p\}$.
Soit $x \in E$, on a deux cas :
- si $x \notin \{x'_1, \cdots, x'_p\}$, alors $\varphi^{-1}(x) \notin \{x_1, \cdots, x_p\}$, sinon on aura $x = \tau(\varphi^{-1}(x)) \in \{x'_1, \cdots, x'_p\}$; ce qui est faux. D'où $\tau\circ\sigma\circ\tau^{-1}(x) = \tau\circ\sigma\circ\varphi^{-1}(x) = \tau\circ\tau^{-1}(x) = x = \rho(x)$.
- si $x = x'_i \in \{x'_1, \cdots, x'_p\}$, alors $\tau \circ \sigma \circ \tau^{-1}(x'_i) = \tau \circ \sigma(x_i) = \tau(x_{i+1}) = x'_{i+1} = \rho(x'_i)$.
Par suite $\tau \circ \sigma \circ \tau^{-1} = \rho$. □

On désigne par $Z(S(E))$ le centre du groupe de $S(E)$, c'est-à-dire l'ensemble des éléments de $S(E)$ qui commutent avec tous les autres éléments de $S(E)$.

Proposition 16. $Z(S(E)) = \begin{cases} S(E) & si\ \mathrm{card}(E) = 2, \\ \{id_E\} & si\ \mathrm{card}(E) \geq 3. \end{cases}$

Preuve. Supposons que $\mathrm{card}(E) = 2$, alors le groupe $S(E)$ est commutatif et $Z(S(E)) = S(E)$.
On suppose que $\mathrm{card}(E) \geq 3$, alors $S(E)$ n'est pas abélien. On se donne σ dans $Z = Z(S(E))$. Pour $x \neq y$ dans E, on a par la proposition 15 :

$$(\sigma(x)\sigma(y)) = \sigma(xy)\sigma^{-1} = (xy)\sigma\sigma^{-1} = (xy),$$

et donc $\sigma(\{x, y\}) = \{x, y\}$. Pour $\mathrm{card}(E) \geq 3$, on peut trouver, pour tout $x \in E$, deux éléments $y \neq z$ distincts de x et avec $\{x\} = \{x, y\} \cap \{x, z\}$, on déduit, puisque σ est injective, que :

$$\{\sigma(x)\} = \sigma(\{x\}) = \sigma(\{x, y\} \cap \{x, z\}) = \sigma(\{x, y\}) \cap \sigma(\{x, z\}) = \{x, y\} \cap \{x, z\} = \{x\},$$

ce qui implique que $\forall x \in E$, $\sigma(x) = x$. Donc $\sigma = id_E$. Le centre de $S(E)$ est donc réduit à $\{id_E\}$. □

Remarque 13. Par la proposition 16, on retrouve ainsi le fait que $S(E)$ n'est pas commutatif pour $n \geq 3$, car pour les groupes G qui sont abéliens on a $Z(G) = G$.

Théorème 34. *S_n est engendré par les cycles. Autrement dit, toute permutation de S_n est un produit de cycles à supports disjoints. Cette décomposition est unique à l'ordre près des facteurs. Si $\sigma = c_1 c_2 \cdots c_\ell$ est une telle décomposition, alors on a la partition :* $supp(\sigma) = \coprod_{i=1}^{i=\ell} supp(c_i)$ *(réunion disjointe).*

Preuve. Soit $\sigma \in S_n$.
• Si $\sigma = id = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$, alors $\sigma = id = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \end{pmatrix} \cdots \begin{pmatrix} n \\ n \end{pmatrix}$
• Si $\sigma \neq id$, alors il existe $a_1 \in E = \{1, 2, \cdots, n\}$ tel que $\sigma(a_1) \neq a_1$.
Pour $j \geq 2$, posons $\sigma(a_{j-1}) = a_j$ c'est-à-dire $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\sigma(a_3) = a_4$, $\cdots$.
Soit $i \geq 2$ le plus petit entier tel que $a_{i+1} = \sigma(a_i) \in P_i = \{a_1, \cdots, a_i\}$ (cet entier existe puisque E est fini). Alors nécessairement $\sigma(a_i) = a_1$, car sinon on aura $\sigma(a_i) = a_j$ avec $2 \leq j \leq i$ et $\sigma(a_{j-1}) = a_j$, d'où $\sigma(a_i) = \sigma(a_{j-1}) = a_j$ et $a_{j-1} \neq a_i$, ce qui contredit l'injectivité de σ.

La restriction de σ à $\{a_1, \cdots, a_i\}$ est un cycle $c_i = (a_1 \cdots a_i)$. On obtient alors un cycle c_i.
Si $i = n$, alors le problème est résolu.
Sinon, c-à-d, si $i < n$, alors c_i opère sur une partie $P_i = \{a_1, \cdots, a_i\}$; on refait le même travail dans $\{a_{i+1}, a_{i+2}, \cdots, a_n\}$. Supposons construit P_i, P_j, $\cdots$, P_ℓ $(i < j < \cdots < \ell)$ tels que $\bigcup_{k=i}^{\ell} P_k = E$ et la restriction c_k de σ à chaque P_k est un cycle, alors

$$\sigma = c_i c_j \cdots c_\ell,$$

puisque $\forall x \in \{1, 2, \cdots, n\}$, il existe $k \in \{i, j, \cdots, \ell\}$ tel que $x \in P_k$, donc $c_j(x) = x$ pour tout $j \neq k$. D'où $\sigma(x) = c_k(x)$. □

Remarque 14. La somme des ordres des cycles c_i est n. Les c_i sont permutables car opèrent sur des parties disjointes.

Théorème 35. *L'ordre de la permutation $\sigma = c_1 c_2 \cdots c_\ell$ décomposée en produit de cycles deux à deux disjoints est égal au* ppcm *des longueurs des c_i.*

Preuve. Soient $\sigma \neq \mathrm{id}$ et $c_1 c_2 \cdots c_\ell$ sa décomposition en cycles disjoints. Pour tout entier k, on a $\sigma^k = c_1^k c_2^k \cdots c_\ell^k$ car les cycles commutent. Puisque les cycles c_i sont deux à deux disjoints, on a $\sigma^k = \mathrm{id}$ si et seulement si $c_1^k = \mathrm{id}$, $c_2^k = \mathrm{id}$, $\cdots$, $c_\ell^k = \mathrm{id}$. Donc si σ est d'ordre m, alors $\theta(c_i)$ divise m pour tout $i \in \{1, \cdots, \ell\}$, et donc le ppcm des $\theta(c_i)$ divise m.

Réciproquement, si s est le ppcm des $\theta(c_i)$, alors $\sigma^s = c_1^s c_2^s \cdots c_\ell^s = \mathrm{id}$ donc m divise s, d'où $m = s$. □

Remarque 15. Comme l'ordre d'un cycle est égal à sa longueur, alors l'ordre de σ est aussi le ppcm des longueurs des cycles c_i.

Définition 31. Soit $\sigma \in S_n$. Une *orbite* de σ est un ensemble de la forme $\{\sigma^k(x) \mid k \in \mathbb{Z}\}$ avec $x \in \{1, \cdots, n\}$, on le note $Orb_\sigma(1)$.

Calcul des cycles dans la décomposition d'une permutation.
Pour $E = \{1, 2, \cdots, n\}$, une décomposition d'une permutation σ s'obtient en prenant, dans le cas où il n'est pas fixe, les images de 1 par σ, σ^2, $\cdots$, jusqu'au moment où on retombe sur 1 (l'orbite de 1), puis on recommence avec le plus petit entier dans $E \backslash Orb_\sigma(1)$ qui n'est pas fixe et ainsi de suite.

Exemple. Pour : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 9 & 8 & 11 & 12 & 10 & 13 \end{pmatrix}$

On a $\sigma(1) = 2$, $\sigma^2(1) = 3$, $\sigma^3(1) = 4$, $\sigma^4(1) = 5$, $\sigma^5(1) = 1$, ce qui donne le premier cycle $c_1 = (12345)$.
Puis $\sigma(6) = 7$, $\sigma^2(6) = \sigma(7) = 6$, ce qui donne le deuxième cycle $c_2 = (67)$. On a aussi $\sigma(8) = 8$, $\sigma^2(8) = \sigma(9) = 8$, ce qui donne le troisième cycle $c_3 = (89)$. Et $\sigma(10) = 11$, $\sigma^2(10) = 12$, $\sigma^3(10) = 10$, donc $c_4 = (10\,11\,12)$, enfin $\sigma(13) = 13$. Par suite

$$\sigma = c_1c_2c_3c_4 = (12345)(67)(89)(10\,11\,12).$$

3.2. **Générateurs de $S(E)$.**
D'après le Théorème 34, on sait que $S(E)$ est engendré par les cycles. Dans la suite, on donne d'autres générateurs de $S(E)$.

Proposition 17. *Le groupe symétrique S_n est engendré par les transpositions, i.e., toute permutation est produit de transpositions* (*non unique, non commutatif*).

Preuve. Par le Théorème 34, il suffit de montrer cela pour un cycle. Si

$$\sigma = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_p & a_{p+1} & \cdots & a_n \\ a_2 & a_3 & a_4 & \cdots & a_1 & a_{p+1} & \cdots & a_n \end{pmatrix} = (a_1\ a_2\ \cdots\ a_p),$$

alors $\sigma = (a_1\ a_2\ \cdots\ a_p) = (a_1\ a_2)(a_2\ a_3)(a_3\ a_4)\cdots(a_{p-1}\ a_p)$. □

Remarque 16. La preuve de la proposition 17 montre que tout p-cycle peut s'écrire comme produit de $p-1$ transpositions.

Exemple 8. Pour $E = \{1, 2, \cdots, 7\}$, on a :

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 1 & 2 & 4 & 7 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 5 & 4 & 2 & 6 & 7 & 3 \\ 5 & 4 & 2 & 6 & 7 & 3 & 1 \end{pmatrix} \\ &= (1\ 5\ 4\ 2\ 6\ 7\ 3) = (1\ 5)(5\ 4)(4\ 2)(2\ 6)(6\ 7)(7\ 3) \end{aligned}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 5 & 2 & 3 & 7 & 6 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 4 & 2 \end{pmatrix}\begin{pmatrix} 3 & 5 \\ 5 & 3 \end{pmatrix}\begin{pmatrix} 6 & 7 \\ 7 & 6 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Remarque 17. L'écriture d'une permutation en produit de transpositions n'est pas unique : par exemple $(123) = (13)(12) = (12)(23) = (23)(13)$. De plus, si $n \geq 3$ et

$i, j \in \{2, \cdots, n\}$, $i \neq j$, alors on peut toujours remplacer la transposition (ij) par le produit $(1i)(1j)(1i)$ (voir le lemme ci-dessous 4).

Lemme 4. *S_n est engendré par les $n-1$ transpositions $(1k)$ où $2 \leq k \leq n$.*

Preuve. Il suffit de montrer ceci pour une transposition. Soit (ij) une transposition avec $1 \leq i \neq j \leq n$. Si $i = 1$ ou $j = 1$, il n'y a rien à faire ($(ij) = (ji)$). Pour $i \neq 1$ et $j \neq 1$, on a par la proposition 15 :

$$(ij) = (1i)(1j)(1i)^{-1} = (1i)(1j)(1i).$$

Le résultat se déduit alors du fait que S_n est engendré par les transpositions. □

Remarque 18. Il n'est pas possible d'enlever une de ces transpositions $(1k)$ du fait que pour $2 \leq k \leq n$ et $2 \leq j \neq k \leq n$, toutes les transposition $(1j)$ laissent fixe k.

Exemple 9. Pour : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}$
$= (12345)(67)$
$= (12)(23)(34)(45)(67)$

on a : $\sigma = (12)(12)(13)(12)(13)(14)(13)(14)(15)(14)(16)(17)(16)$
$= (13)(12)(13)(14)(13)(14)(15)(14)(16)(17)(16).$

Lemme 5. *S_n est engendré par les $n-1$ transpositions $(k\,k+1)$ où $1 \leq k \leq n-1$.*

Preuve. Comme S_n est engendré par les transpositions $(1k)$ où $2 \leq k \leq n$, il suffit d'écrire chaque transposition $(1k)$ comme produit de transpositions du type $(i\,i+1)$. Pour $3 \leq k \leq n$, on a par la proposition 15 :

$$(1k) = (k-1\,k)(1\,k-1)(k-1\,k)^{-1} = (k-1\,k)(1\,k-1)(k-1\,k).$$

Pour $k = 3$, on a $(1\,k-1) = (12)$ et c'est terminé, sinon on écrit :
$(1\,k-1) = (k-2\,k-1)(1\,k-2)(k-2\,k-1)$ et on continue ainsi de suite si nécessaire.
Pour $k = 2$, la transposition $(1\,k) = (12)$ est de la forme souhaitée. □

3.3. **Signature d'une permutation.**

Définition 32. Soient $n \in \mathbb{N}^*$, $\sigma \in S_n$ et i, j deux entiers tels que $1 \leq i < j \leq n$. On dit que $\sigma(i)$ et $\sigma(j)$ présentent une *inversions* si $\sigma(i) > \sigma(j)$.

Notons par $[\![1\ ;\ n]\!]$ l'ensemble des entiers naturels k tels que $1 \leq k \leq n$.

Définition 33. On appelle *nombre d'inversions* de $\sigma \in S_n$ l'entier

$$I(\sigma) = \text{card}\{(i,j) \in [\![1\ ;\ n]\!]^2 \mid i < j \text{ et } \sigma(i) > \sigma(j)\}.$$

C'est-à-dire le nombre total d'inversions présentés par les éléments de $\{\sigma(1), \sigma(2), \cdots, \sigma(n)\}$ pris deux à deux.

Le nombre $I(\sigma)$ vérifie la proposition suivante.

Proposition 18. *Soit $\sigma \in S_n$, posons $V_n = \prod_{1\leq i<j\leq n} (j-i)$. Alors*

$$\sigma(V_n) = \prod_{1\leq i<j\leq n} (\sigma(j) - \sigma(i)) = (-1)^{I(\sigma)} V_n.$$

Preuve. Soient les deux ensembles

$$A = \{(i,j) \mid 1 \leq i < j \leq n\} \text{ et}$$
$$B = \{(\sigma(i), \sigma(j)) \mid 1 \leq i < j \leq n\}.$$

Considérons l'application $\varphi : \begin{array}{ccc} A & \longrightarrow & B \\ (i,j) & \longmapsto & (\sigma(i), \sigma(j)) \end{array}$

φ est surjective par construction, de plus si $(\sigma(i), \sigma(j)) = (\sigma(k), \sigma(\ell))$, alors $\sigma(i) = \sigma(k)$ et $\sigma(j) = \sigma(\ell)$, d'où $i = k$ et $j = \ell$. Par suite φ est une bijection. Donc $card(A) = card(B)$. En conséquence

$$\sigma(V_n) = \prod_{1\leq i<j\leq n} (\sigma(j) - \sigma(i)) = (-1)^{I(\sigma)} V_n.$$

□

Définition 34. Le nombre $(-1)^{I(\sigma)} = \dfrac{\prod_{1\leq i<j\leq n} (\sigma(j) - \sigma(i))}{\prod_{1\leq i<j\leq n} (j-i)} \in \{-1, 1\}$ s'appelle

la signature de $\sigma \in S_n$, et est notée $\varepsilon(\sigma) = (-\mathbf{1})^{\mathbf{I}(\sigma)}$.

Définition 35.
Une permutation est dite **paire** si sa signature est 1, et elle est dite **impaire** sinon.

Remarque 19. $\sigma(V_n) = \varepsilon(\sigma) V_n$

Théorème 36. $\forall \sigma, \tau \in S_n$, $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$, *i.e., la signature est un homomorphisme de groupes de $(S_n, \circ)$ dans $\{-1,1\}$.*

Preuve. On a $\varepsilon(\sigma\tau)V_n = \sigma\tau(V_n) = \sigma(\tau(V_n)) = \varepsilon(\sigma)\tau(V_n) = \varepsilon(\sigma)\varepsilon(\tau)V_n$,
d'où $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$. □

Proposition 19.

a. *Une transposition est de signature* -1*, i.e. une transposition est impaire.*
b. *Un* p*-cycle est de signature* $(-1)^{p-1}$*.*

Preuve. *a* - Montrons que toute transposition est impaire. Soit τ la transposition sur $\{i, j\}$ et $i < j$; les couples (k, l) tels que $\tau(k) > \tau(l)$ et $k < l$ sont :

- les couples (i, k) avec $k \leq j$, au nombre $j - i$ (k prend les valeurs de $i + 1, \cdots, j$) ;
- les couples (k, j) avec $i < k < j$, au nombre $j - i - 1$ (k prend les valeurs de $i + 1$, $\cdots, j - 1$).

En tout on a : $2(j - i) - 1$ couples, et ce nombre est impaire, d'où notre assertion.
b - Par le Remarque 16, chaque p-cycle est produit de $p - 1$ transposition, d'où le résultat. □

Remarque 20. Comme conséquence de la proposition précédente on a :
si $\sigma = \tau_1\tau_2 \cdots \tau_p \in S_n$ est la décomposition de σ en produit de p transposition, alors

$$\varepsilon(\sigma) = \varepsilon(\tau_1)\varepsilon(\tau_2) \cdots \varepsilon(\tau_p) = (-1)^p.$$

Donc :

i. une permutation paire se décompose en produit d'un nombre pair de transpositions.
ii. une permutation impaire se décompose en produit d'un nombre impair de transpositions.
iii. la classe de $p \pmod 2$ est bien déterminée : p est pair si σ est paire, et est impair si σ est impaire.

Le théorème suivant permet de représenter tout groupe fini comme un sous-groupe d'un groupe symétrique.

Théorème 37 (Cayley (1878)). *Tout groupe fini d'ordre* n *est isomorphe à un sous-groupe du groupe symétrique* S_n*.*

Preuve. Soient G un groupe fini d'ordre n, et $g \in G$. Alors l'application

$$\begin{aligned} \tau_g : \ G &\longrightarrow G \\ x &\longmapsto gx \end{aligned}$$

est une bijection de bijection inverse $\tau_g^{-1} = \tau_{g^{-1}}$.
En effet, pour tout $x \in G$, $\tau_g \circ \tau_{g^{-1}}(x) = \tau_g(g^{-1}x) = gg^{-1}x = x$, et de la même manière $\tau_{g^{-1}} \circ \tau_g(x) = \tau_{g^{-1}}(gx) = g^{-1}gx = x$.
Il suit que τ_g est une permutation de G ; et en numérotant les n éléments de G par 1, 2, $\cdots$, n, alors τ_g est un élément de S_n.

L'application

$$\begin{aligned} \tau : \ G &\longrightarrow S_n; \\ g &\longmapsto \tau_g \end{aligned}$$

est un homomorphisme de groupes injectif. En effet,
pour tout $g, h \in G$ et tout $x \in G$, on a : $\tau(gh)(x) = \tau_{gh}(x) = (gh)x = g(hx) = \tau_g \circ \tau_h(x)$, donc $\tau_{gh} = \tau_g \circ \tau_h$, c'est-à-dire $\tau(gh) = \tau(g) \circ \tau(h)$.
Ensuite, τ est injectif, car

$$\begin{aligned} g \in \ker \tau &\iff \tau(g) = id_G \\ &\iff \tau_g = id_G \\ &\iff \tau_g(x) = x \ \forall x \in G \\ &\iff gx = x \ \forall x \in G \\ &\iff g = e. \end{aligned}$$

Ainsi par le premier théorème d'isomorphisme, G est isomorphe à $\tau(G)$ qui est un sous-groupe de S_n. □

3.4. **Groupe alterné.**
Dans ce paragraphe, nous nous intéressons aux permutations paires.

Définition 36. L'ensemble des permutations paires de S_n, i.e. $\{\sigma \in S_n / \varepsilon(\sigma) = 1\}$ s'appelle **le groupe alterné** sur n éléments. On le note par : $\mathcal{A}_n$.

Théorème 38. *Soit $n \geq 2$ un entier naturel. $\mathcal{A}_n$ l'ensemble des permutations paires de S_n est un sous-groupe normal de S_n. De plus $[S_n : \mathcal{A}_n] = 2$ et son cardinal est donc $\frac{n!}{2}$, et il est le noyau de l'homomorphisme ε.*

Preuve. Soit l'homomorphisme ε : $\begin{aligned} S_n &\longrightarrow \{-1, 1\} \\ \sigma &\longmapsto \varepsilon(\sigma) \end{aligned}$
il est simple de voir que ε est surjectif ($n \geq 2$). De plus $\ker \varepsilon = \{\sigma \in S_n | \ \varepsilon(\sigma) = 1\}$, donc $\mathcal{A}_n = \ker \varepsilon$; d'où $\mathcal{A}_n$ est un sous-groupe distingué de S_n.

D'autre part, par le 1er Théorème d'isomorphisme et comme ε est un homomorphisme surjectif, on a $S_n / \ker \varepsilon \simeq \{-1, 1\}$, donc $\dfrac{|S_n|}{|\{-1, 1\}|} = |\ker \varepsilon| = |\mathcal{A}_n|$, d'où $|\mathcal{A}_n| = \dfrac{n!}{2}$. □

Dans la suite, E désigne un ensemble de cardinal $n \geq 3$.

Exemple 10. Dans S_3, le sous-groupe $\mathcal{A}_3$ est cyclique engendré par $c_1 = (123)$. En effet, $\text{card}(\mathcal{A}_3) = \frac{3!}{2} = 3$ et le cycle c_1 est d'ordre 3 dans $\mathcal{A}_3$. Donc les éléments de $\mathcal{A}_3 = \{id, c_1 = (123), c_1^2 = (132)\}$, il est isomorphe à $(\mathbb{Z}/3\mathbb{Z}, +)$.

Pour continuer, nous avons besoin de la proposition suivante.

Proposition 20. *Le produit de deux transpositions est un produit de* 3*-cycles. Précisément, pour x, y, z, t deux à deux distincts dans E, on a :*

$$(xy)(xz) = (xzy) \text{ et } (xy)(zt) = (xyz)(yzt).$$

Preuve. Soient τ et σ deux transpositions.
- Si $\tau = \sigma$, alors $\tau\sigma = \tau^2 = \text{id} = \lambda^3$, pour n'importe quel 3-cycle λ.
- Si $\tau \neq \sigma$, alors on distingue deux cas :

a. si par exemple $supp(\tau) \cap supp(\sigma) = \{x\}$, alors $\tau = (xy)$ et $\sigma = (xz)$, où x, y et z sont distincts. Donc $\tau\sigma = (xy)(xz) = (xzy) = (yxz)$.

b. si $supp(\tau) \cap supp(\sigma) = \emptyset$, alors $\tau = (xy)$ et $\sigma = (zt)$, où x, y, z et t sont distincts. Donc $\tau\sigma = (xy)(zt) = (xy)(yz)^2(zt) = (xy)(yz)(yz)(zt) = (xyz)(yzt)$.

□

Théorème 39. *Pour $n \geq 3$, $\mathcal{A}_n$ est engendré par les* 3*-cycles.*

Preuve. On sait que S_n est engendré par les transpositions. Donc, par la Remarque 20, on déduit qu'une permutation paire est le produit d'un nombre pair de transpositions, et la proposition précédante nous dit que ce produit s'écrit comme produit de 3-cycles. □

Théorème 40. *Pour $n \geq 5$, les* 3*-cycles sont conjugués dans $\mathcal{A}_n$.*

Preuve. Soient c_1 et c_2 deux 3-cycles ; par la proposition 15, on sait qu'il existe $\sigma \in S_n$ tel que $c_1 = \sigma^{-1}c_2\sigma$. Si $c_1 = (i_1i_2i_3)$, $c_2 = (j_1j_2j_3)$, alors la proposition 15 implique que σ est défini par $\sigma(i_1) = j_1$, $\sigma(i_2) = j_2$, $\sigma(i_3) = j_3$. Si $\sigma \in \mathcal{A}_n$ et si $n \geq 5$, il existe deux éléments i_4 et i_5 différents de i_1, i_2, i_3. On pose alors $\tau = (i_4i_5)$, l'élément $\rho = \sigma\tau$ est dans $\mathcal{A}_n$, et on a donc $c_1 = \rho^{-1}c_2\rho$. □

Les deux théorèmes suivants sont admis.

Théorème 41. *Pour $n = 3$ ou $n \geq 5$, les sous-groupes distingués de S_n sont $\{\text{id}_\text{E}\}$, $\mathcal{A}_n$ et S_n.*

Théorème 42. *Pour $n = 3$ ou $n \geq 5$, le groupe $\mathcal{A}_n$ est simple (i.e. n'a pas de sous-groupes distingués autres que lui même et* $\{\mathrm{id}\}$*).*

Remarque 21. On a $\mathcal{A}_1 = \mathcal{A}_2 = \{id\}$. Le groupe $\mathcal{A}_3$ est d'ordre 3, donc il est cyclique d'ordre premier, d'où il est simple. Le groupe $\mathcal{A}_4$ n'est pas simple car il contient un sous groupe normal H isomorphe au groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (groupe de Klein).

3.5. **Exercices.**

Exercice 3.1. Pour $n \geq 3$, on désigne par A'_n le sous-groupe de S_n engendré par les $n-2$ cycles $(123), (124), \cdots, (12n)$.

i. Montrer que A'_n est un sous-groupe de A_n.

ii. Montrer que $(12)(ij)$, $i \neq j$, appartient à A'_n ; de même montrer que $(ij)(12)$ appartient à A'_n.

iii. Montrer que $A_n = A'_n$ (remarquer que toute permutation σ de A_n peut s'écrire :

$$\sigma = t_1 t_2 \cdots t_{2p} = t_1 t_0 t_0 t_2 t_3 t_0 \cdots t_0 t_{2p-1} t_0 t_0 t_{2p},$$

avec $t_0 = (12)$ et t_i une transposition $1 \leq i \leq 2p$.

4. Les Anneaux et les Corps

Ce chapitre rappel les notions, que vous connaissez déjà, d'anneaux, idéaux et corps. Ces notions formalisent les méthodes de calcul bien connues avec les nombres entiers : on dispose d'une addition, d'une multiplication de deux symboles 0 et 1 et des règles de calcul usuelles.

4.1. Les anneaux : Définition et propriétés.

4.1.1. **Définition d'un anneau.** Commençons par la définition d'un anneau

Définition 37. On appelle anneau un triplet $(A, +, \times)$ constitué d'un ensemble non vide A et de deux lois de composition internes $+$ et $\times$ tel que :

i. $(A, +)$ est un groupe abélien dont l'élément neutre sera noté 0_A ou 0.
ii. $\times$ est associative.
iii. $\times$ est distributive par rapport à $+$, c'est-à-dire

$$\forall\, x,\, y,\, z \in A : x \times (y + z) = (x \times y) + (x \times z) \quad \text{et} \quad (x + y) \times z = (x \times z) + (y \times z).$$

On dit que l'anneau $(A, +, \times)$ est commutatif si de plus la loi $\times$ est commutative.
On dit aussi que l'anneau $(A, +, \times)$ est unitaire (par fois on dit aussi unifère) si la loi $\times$ admet un élément neutre, on le note 1.

Exemples 7.

1. $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs unitaires (l'élément unité est 1).
2. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire fini à n éléments, l'élément unité est $\overline{1}$.
3. Soit E un ensemble, alors $(\mathcal{P}(E), \triangle, \cap)$ est un anneau commutatif unitaire, l'élément unité est E. Cet anneau est un **anneau de Boole**. Un anneau $(A, +, .)$ est dit un anneau de Boole si $\forall x \in A;\ x^2 = x$.
4. $\mathcal{L}(E)$ ensemble des endomorphismes de l'espace vectoriel E muni de l'addition et de la composition et $\mathcal{M}_n(A)$ ensemble des matrices $n \times n$ à coefficients dans un anneau A sont des anneaux non commutatifs.
5. Soit X une partie non vide de $\mathbb{R}$. Considérons $\mathcal{F} = \mathcal{F}(X, \mathbb{R})$ l'ensemble des fonctions numériques de X dans $\mathbb{R}$. Sur $\mathcal{F}$ on défini les deux lois : " $+$ " et " $\times$ " pour tous f, g de $\mathcal{F}$ par : $(f + g)(x) = f(x) + g(x)$ et $(f \times g)(x) = f(x)g(x)$. Alors $(\mathcal{F}, +, \times)$ est un anneau commutatif unitaire d'élément unité $f(x) = 1$ pour tout $x \in X$.

6. L'ensemble $K[X]$ des polynômes à une seule indéterminée X à coefficients dans un corps K, muni de l'addition et de la multiplication des polynômes, est un anneau commutatif unitaire d'élément neutre le polynôme constant égal à 1.
7. L'ensemble $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ muni de l'addition et de la multiplication habituelles, est un anneau commutatif unitaire appelé **anneau des entiers de Gauss**.

4.1.2. **Règles de calcul dans un anneau.**

Proposition 21. *Soit $(A, +, \times)$ un anneau, notons 0 l'élément neutre du groupe $(A, +)$, alors on a :*

1. *0 est absorbant, i.e. $\forall\, x \in A,\ 0 \times x = 0 = x \times 0$.*
2. *$\forall\, x \in A,\ (-1) \times x = -x$.*
3. *$\forall\, x,\ y \in A,\ (-x) \times y = -(x \times y) = x \times (-y)$.*
4. *$\forall\, x,\ y,\ z \in A,\ x \times (y - z) = x \times y - x \times z$ et $(x - y) \times z = x \times z - y \times z$.*
5. *$\forall\, x \in A,\ \forall n \in \mathbb{N}^*$, on définit $x^1 = x$ et $x^n = x^{n-1} \times x$.*
6. *$\forall\, x \in A,\ \forall n,\ m \in \mathbb{N}$, on définit $x^{n+m} = x^n \times x^m$.*
7. *$\forall\, x,\ y \in A,\ (x + y)^2 = x^2 + x \times y + y \times x + y^2$.*
8. *$\forall\, x,\ y \in A,\ (x - y)^2 = x^2 - x \times y - y \times x + y^2$.*
9. *$\forall\, x,\ y \in A,\ (x + y) \times (x - y) = x^2 - x \times y + y \times x - y^2$.*
10. *Si $x, y \in A$ commutent, alors pour tout $n \in \mathbb{N}^*$ on a les formules suivantes :*
    i. $(x + y)^n = \displaystyle\sum_{p=0}^{n} \mathrm{C}_n^p x^p y^{n-p}$, *formule du binôme.*
    ii. $x^n - y^n = (x - y)\left(x^{n-1} + y^{n-1} + \displaystyle\sum_{k=1}^{n-2} x^{n-1-k} y^k\right)$.
    iii. $x^n - 1 = (x - 1)\,(1 + x + x^2 + \cdots + x^{n-1})$.
11. *Si A est unitaire, alors l'élément neutre 1 est unique et $1 \neq 0$ sauf si $A = \{0\}$, auquel cas l'anneau est dit* **trivial ou nul**.

Preuve. La formule du binôme est prouvé par récurrence sur n en utilisant le fait que : $\mathrm{C}_n^p + \mathrm{C}_n^{p-1} = \mathrm{C}_{n+1}^p \qquad \text{et} \qquad \mathrm{C}_{n+1}^1 = \mathrm{C}_{n+1}^n = n + 1.$ □

4.1.3. **Les unités d'un anneau.**

Définition 38. Soient A un anneau unitaire et $a \in A$.

1. L'élément a est dit *inversible à droite* s'il existe $b \in A$ tel que $ab = 1$ (inversible à droite pour la multiplication de A).

2. L'élément a est dit *inversible à gauche* s'il existe $c \in A$ tel que $ca = 1$ (inversible à gauche pour la multiplication de A).
3. L'élément a est dit *inversible* s'il est inversible à droite et à gauche.

Remarque 22. Si un élément a de A est inversible, alors les inverses de a à droite et à gauche coincident, et cet élément inverse est unique, car de $ab = 1$ et $ca = 1$ on déduit que

$$cab = (ca)b = c(ab) = b = c.$$

Et de $ca = c'a = 1$, on déduit que $cab = c'ab = c = c'$ (on suppose toujours que $ab = 1$).

Remarque 23. Un élément inversible d'un anneau A est aussi dit une **unité** de A. Attention, il ne faut pas confondre une unité d'un anneau (qui est un élément inversible de l'anneau) avec son élément unité quand il existe (qui est l'élément neutre pour la multiplication).

Théorème 43. *Soit A un anneau unitaire. Notons par U_A (parfois on note aussi $A^\times$) l'ensemble des unités de A. Alors U_A muni de la loi induite par la multiplication de A est un groupe d'élément neutre* 1.

Preuve. Il suffit de montrer que U_A est stable par la multiplication de A. Soient u, $v \in \mathrm{U}_A$ et u', v' leurs inverses respectivement. Alors on a :

$$(v'u')(uv) = v'(u'u)v' = v'v = 1 \text{ et } (uv)(v'u') = u(vv')u' = uu' = 1.$$

Donc uv est inversible et admet pour inverse $v'u'$, d'où $uv \in \mathrm{U}_A$. □

Remarques 16.

1. Dans un anneau commutatif, les notions d'éléments inversibles à droite et à gauche coincident. Dans ce cas, on parle simplement d'éléments inversibles.
2. U_A s'appelle le **groupe des unités** de A. Sa connaissance donne de précieux renseignements sur la structure de A.

Exemples 8.

1. $\mathrm{U}_{\mathbb{Z}} = \{-1, 1\}$
2. $\mathrm{U}_{\mathbb{R}} = \mathbb{R} - \{0\} = \mathbb{R}^*$
3. Soient n et a deux entiers naturels. On sait, par la multiplication de l'anneau $\mathbb{Z}/n\mathbb{Z}$, que $k\overline{a} = \overline{ka}$, où $\overline{a}$ est la classe de a modulo $n\mathbb{Z}$. Donc $\overline{a}$ est inversible si et seulement s'il existe $m \in \mathbb{Z}$ tel que $\overline{m} \cdot \overline{a} = \overline{1}$; ceci est équivaut à dire, par Bézout, qu'il existe

$u \in \mathbb{Z}$ tel que $ma + nu = 1$, donc a et n sont premier entre eux. Donc les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les classes $\overline{a}$ tels que $a < n$ et $a \wedge n = 1$.

$$\mathrm{U}_{\mathbb{Z}/n\mathbb{Z}} = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid a < n \text{ et } a \wedge n = 1\}.$$

($\overline{a}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ noter que les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les éléments $\overline{a}$ tels que $0 \leq a \leq n-1$ et $a \wedge n = 1$.)

4. $\mathrm{U}_{\mathcal{M}_n(\mathbb{R})} = \mathrm{GL}_n(\mathbb{R}) = \{M \in \mathcal{M}_n(\mathbb{R}) \mid \det(M) \neq 0\}$.

4.1.4. **Anneaux intègres.**

Définition 39. Soit A un anneau non nul.
On dit que $a \in A - \{0\}$ est un diviseur de zéro s'il existe $b \in A$ tel que $b \neq 0$ et $ab = 0$.
Nous disons que A possède des diviseurs de zéro s'il existe a, $b \in A$ avec $a \neq 0$, $b \neq 0$ et $ab = 0$.

Définition 40. Un anneau non nul A est dit intègre s'il n'admet pas de diviseur de zéro.

Remarques 17.

1. Un anneau intègre et commutatif est parfois appelé **un domaine d'intégrité**.
2. Dans un anneau intègre on a l'équivalence : $ab = 0 \Longleftrightarrow a = 0$ ou $b = 0$.
3. Dans un anneau intègre tous les éléments non nuls sont réguliers.

Exemples 9.

1. $(\mathbb{Z}, +, \times)$ est un anneau intègre.
2. $(\mathbb{Z}/6\mathbb{Z}, \overline{+}, \overline{\times})$ est un anneau non intègre, car $\overline{2} \neq \overline{0}$ et $\overline{3} \neq \overline{0}$ mais $\overline{2}\overline{\times}\overline{3} = \overline{6} = \overline{0}$.
3. $(\mathbb{Z}/n\mathbb{Z}, \overline{+}, \overline{\times})$ est un anneau intègre si et seulement si $n = 0$ ou n est un premier, car pour $n > 0$ on a : $\overline{a}\overline{b} = \overline{ab} = \overline{0} \Longleftrightarrow n$ divise ab, donc ($\overline{a}\overline{b} = \overline{0} \Longleftrightarrow \overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$) si et seulement si n divise a ou b, d'où le résultat.

4.1.5. **Les sous-anneaux.**

Définition 41. Une partie B d'un anneau $(A, +, \times)$ est dite un sous-anneau de A si

- B est stable pour les deux lois $+$ et $\times$,
- $(B, +, \times)$ est aussi un anneau.

Autrement dit $(B, +)$ est un sous-groupe de $(A, +)$ et est stable pour la multiplication de A.

Théorème 44. *Une partie non vide B d'un anneau $(A,+,\times)$ est un sous-anneau de A si et seulement si : $\forall (x,y)\in B^2$ on a : $x-y\in B$ et $x\times y\in B$.*

Preuve. Simple à verifier. □

Remarques 18.

1. Soit B un sous-anneau d'un anneau A. Alors si A est commutatif (resp. intègre), alors B l'est aussi. Par contre si A est unitaire, alors B n'est pas forcément unitaire : par exemple $B=2\mathbb{Z}$ est un sous-anneau non unitaire de l'anneau unitaire $A=\mathbb{Z}$.
2. Si B est un sous-anneau unitaire d'un anneau unitaire A, il se peut que les éléments neutres de A et B soient distincts. Soit $A=M_2(K)$ l'anneau des matrices carrés d'ordres 2 sur un corps commutatif K. A est unitaire d'élément neutre la matrice $I=\begin{pmatrix}1&0\\0&1\end{pmatrix}$.
   Soit B le sous-anneau de A formé des matrices de la forme $\begin{pmatrix}\alpha&0\\0&0\end{pmatrix}$, où $\alpha\in K$. B est unitaire d'élément neutre $J=\begin{pmatrix}1&0\\0&0\end{pmatrix}$, et $I\neq J$.
3. Soit B un sous-anneau d'un anneau A ; supposons que A et B sont unitaire d'éléments neutres respectivement I et J. Si $I\neq J$, alors J est un diviseur de zéro dans A ; en effet, on a $IJ=J=J^2$, d'où $J(I-J)=0=(I-J)J$.

4.1.6. **Anneaux produits.**

Définition 42. Soient A et B deux anneaux. On appelle **anneau produit** des anneaux A et B, et on note $A\times B$, l'ensemble $A\times B$ muni des lois définies pour tous $a,a'\in A$ et $b,b'\in B$ par :

$$(a,b)+(a',b')=(a+a',b+b');\qquad (a,b)\cdot(a',b')=(aa',bb').$$

Il est simple de vérifier que ces deux lois définissent sur $A\times B$ une structure d'anneau.

Remarques 19.

1. Si A et B sont unitaires, alors $A\times B$ est aussi unitaire d'élément neutre $(1,1)$.
2. Si A et B sont commutatifs, alors $A\times B$ est aussi commutatif.
3. Si A et B sont non nuls, alors $A\times B$ n'est pas intègre, car $(a,0)\cdot(0,a)=(0,0)=0$.
4. Si A et B sont unitaires, alors $c=(a,b)\in A\times B$ est inversible si et seulement si a et b sont inversibles dans A et B. On déduit donc le résultat suivant.

Proposition 22. *Soient A et B deux anneaux unitaires. Alors $U_{A\times B} = U_A \times U_B$.*

Les notions qu'on vient de citer peuvent être généraliser.

Définition 43. Soit $(A_i)_{i\in I}$ une famille d'anneaux. L'ensemble produit $\prod_{i\in I} A_i$ muni des deux lois définies pour tous $x = (x_i)_{i\in I}$ et $y = (y_i)_{i\in I}$ par :

$$x + y = (x_i + y_i)_{i\in I} \quad \text{et} \quad x \cdot y = (x_i y_i)_{i\in I}$$

est un anneau appelé **anneau produit** des A_i.

4.2. **Les corps.**

Définition 44. On dit qu'un anneau non nul A est un corps si tout élément non nul de A est inversible, i.e. A est un corps si et seulement si $U_A = A - \{0\}$.

Proposition 23. $(A, +, \times)$ *est un corps si et seulement si :*

1. $(A, +)$ *est un groupe abélien.*
2. $(A - \{0\}, \times)$ *est un groupe.*
3. *La multiplication est distributive par rapport à l'addition.*

Preuve. Simple à vérifier. □

Exemples 10.

1. $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.
2. $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est un nombre premier.
3. $\mathbb{Z}$ est un anneau intègre qui n'est pas un corps.

Proposition 24. *Si K est un corps, alors K est intègre et $U_K = K^* = K - \{0\}$ est un groupe pour la multiplication appelé* **groupe multiplicatif** *du corps K.*

Preuve. Simple à vérifier. □

Définition 45. Soit $(K, +, \times)$ un corps et L un sous-anneau de $(K, +, \times)$. On dit que L est un sous-corps du corps $(K, +, \times)$ si $(L, +, \times)$ est un corps.
On dit que L est un sous-corps **propre** de K si L est un sous-corps de K différent de K.

Proposition 25. *Soit $(K, +, \times)$ un corps et L une partie de K. L est un sous-corps du corps $(K, +, \times)$ si, et seulement si :*

1. *L est un sous-anneau de K,*

2. *tout élément non nul $a \in L$ est inversible dans L, i.e. $a^{-1} \in L$.*

Preuve. Simple à verifier. □

Exemples 11.

1. $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$ et $\mathbb{R}$ est un sous-corps de $\mathbb{C}$.
2. $\mathbb{Q}$ ne possède pas de sous-corps propre. En effet, soit L un sous-corps de $\mathbb{Q}$, alors $0, 1 \in L$, d'où $\forall n \in \mathbb{Z}, n = n.1 \in L$. Comme L est un corps, alors $\forall n \in \mathbb{Z}^*, n^{-1} \in L$. Soit $x \in \mathbb{Q}$, alors x s'écrit sous la forme $\frac{m}{n}$ avec $(m, n) \in \mathbb{Z} \times \mathbb{Z}^*$, donc $x = \frac{m}{n} = mn^{-1} \in L$, d'où $\mathbb{Q} \subset L$, par suite $L = \mathbb{Q}$. $\mathbb{Q}$ est dit un **corps premier**.

Définition 46. Un corps K est dit premier s'il n'admet pas de sous-corps propre. L'intersection, $\Bbbk$, de tous les sous-corps d'un corps K est appelé sous-corps premier du corps K.

Remarque 24. Si L est un sous-corps de K, on dit aussi que K est un sur-corps de L. Si L et K sont, en outre, commutatifs, on dit que K est une extension de L.

On termine ce paragraphe par la définition suivante.

Définition 47. Soit A un anneau intègre. Il existe un corps K unique (à un isomorphisme près) vérifiant :

i. A est un sous-anneau de K,

ii. Pour tout $x \in K$, il existe dans A des éléments a et b tels que $x = ab^{-1}$.

K est appelé corps des fractions de A et se note $\mathrm{Fr}(A)$.

$$\mathrm{Fr}(A) = \left\{ \frac{a}{b} = ab^{-1} \mid a \in A; b \in A^* \right\}.$$

Remarque 25. K est minimal pour la condition i., i.e. si L est un corps vérifiant i. alors L admet un sous-corps isomorphe à K.

Exemple 11.

- $\mathbb{Q} = \mathrm{Fr}(\mathbb{Z})$.
- $A(X) = \mathrm{Fr}(A[X])$, corps des fractions rationnelles à coefficients dans A.

4.3. **Homomorphismes d'anneau.**

Définition 48. Une application f d'un anneau $(A, +, \times)$ dans un anneau $(B, \oplus, \star)$ est dite un homomorphisme d'anneaux si et seulement si :

1. Pour tout $x, y \in A$ on a : $f(x + y) = f(x) \oplus f(y)$.

2. Pour tout x, $y \in A$ on a : $f(x \times y) = f(x) \star f(y)$.

Remarque 26. Si A et B sont unitaires, alors un homomorphisme d'anneaux f de A dans B ne transforme pas nécessairement l'élément neutre 1_A de A en 1_B celui de B. Par exemple l'homomorphisme nul $f(x) = 0$ pour tout $x \in A$.
Un autre exemple : $f : A \longrightarrow A \times B$, $a \longmapsto (a, 0)$, alors f est un homomorphisme mais $f(1) = (1, 0) \neq (1, 1)$.

Convention.
Dans toute la suite, on appellera "homomorphisme d'anneaux" un homomorphisme transformant l'élément neutre de A en celui de B.

Définition 49.

1. On appelle isomorphisme d'anneaux de A dans B tout homomorphisme φ bijectif. Dans ce cas on dit que A et B sont isomorphes et on écrit $A \simeq B$.
2. On appelle endomorphisme de l'anneau A tout homomorphisme de A dans A.
3. On appelle automorphisme de l'anneau A tout isomorphisme de A dans A.

Proposition 26. *Si f est un homomorphisme d'un anneau $(A, +, \times)$ dans un anneau $(B, \oplus, \star)$, alors on a :*

1. $f(0_A) = 0_B$ *et* $f(-x) = -f(x)$.
2. *Si C est un sous-anneau de A, alors $f(C)$ est un sous-anneau de B.*
3. *Si C' est un sous-anneau de B, $f^{-1}(C')$ est un sous-anneau de A.*

Preuve. 1. On a $f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A) \Longrightarrow f(0_A) = 0_B$.
On a aussi $f(x) + f(-x) = f(x + (-x)) = f(0) = 0$, donc $f(-x) = -f(x)$.
2. On sait déjà que $f(C)$ est un sous-groupe de $(B, +)$, donc il suffit de montrer que $f(C)$ est stable pour la multiplication de B. Soient $y, y' \in f(C)$, alors il existe x, x' dans A tels que $f(x) = y$ et $f(x') = y'$; donc $yy' = f(x)f(x') = f(xx') \in f(C)$. D'où le résultat.
3. De même $f^{-1}(C')$ est un sous-groupe de $(A, +)$. Il suffit de montrer qu'il est stable pour la multiplication de A. Soient x, $x' \in f^{-1}(C')$, donc il existe y, $y' \in C'$ tels que $f(x) = y$ et $f(x') = y'$. Donc $yy' = f(xx')$, d'où $xx' \in f^{-1}(C')$. □

Proposition 27. *Si $f : A \longrightarrow B$ et $g : B \longrightarrow C$ sont deux homomorphismes (resp. isomorphismes) d'anneaux, alors la composée $g \circ f : A \longrightarrow C$ est un homomorphisme (resp. isomorphisme) d'anneaux.*

Preuve. Laisser au lecteur. □

4.4. **Les idéaux d'un anneau.**

Définition 50. Soient $(A, +, \times)$ un anneau et I une partie non vide de A.

1. On dit que la partie I est un idéal à gauche (resp. droite) de A si elle vérifie les deux conditions suivantes :
   i. I est un sous-groupe de $(A, +)$,
   ii. pour tous $a \in A$ et $x \in I$, $ax \in I$ (resp. $xa \in I$).
2. On dit que I est un idéal bilatère de A s'il est idéal à droite et à gauche de A.

Remarque 27. Si A est commutatif, alors les notions d'idéal à droite, à gauche et bilatère sont identiques ; on dit simplement **idéal** de A.

Exemples 12.

1. $\{0\}$ et A sont des idéaux de A, appelés idéaux triviaux de A. Tout idéal de A différent de A est dit idéal **propre** de A. Tout idéal de A contient 0.
2. Dans l'anneau $\mathbb{Z}$, soit $n \in \mathbb{Z}$, alors $n\mathbb{Z}$ est un idéal de l'anneau $\mathbb{Z}$. En effet, $(n\mathbb{Z}, +)$ est un sous-groupe abélien de $(\mathbb{Z}, +)$, et pour tous $k = na \in n\mathbb{Z}$, $h \in \mathbb{Z}$, on a $hk = kh = n(ha) \in n\mathbb{Z}$. Réciproquement, si I est un idéal de $\mathbb{Z}$, alors I est un sous-groupe de $\mathbb{Z}$, d'où I est de la forme $I = n\mathbb{Z}$ avec $n \in \mathbb{Z}$.

Proposition 28. *Soit $(A, +, \times)$ un anneau et I une partie de A. I est un idéal à gauche (resp. droite) de l'anneau A si, et seulement si :*

1. $I \neq \varnothing$,
2. $\forall x, y \in I \ ; \ x + y \in I$,
3. $\forall a \in A, \ \forall x \in I \ ; \ ax \in I \quad (resp.\ xa \in I)$.

Preuve. Si I est un idéal de A, alors les propriétés 1., 2. et 3. sont vérifiées.

Réciproquement, supposons que les trois propriétés 1., 2. et 3. sont vérifiées. Alors pour tout $x \in I$, on a $(-1)x = -x \in I$; vue la propriété 2., on déduit $(I, +)$ est un sous-groupe abélien de $(A, +)$. Tenant compte de la propriété 3., on voit que I est un idéal de A. □

Remarque 28. Dire que I est un idéal à gauche (resp. droite) de A est équivaut à dire que I est non vide et que pour tous a, $b \in A$ et x, $y \in I$ on a : $ax + by \in I$ (resp. $xa + yb \in I$).

Lemme 6. *Soient A un anneau unitaire et I un idéal de A. On a $A = I \iff 1 \in I$.*

Preuve. Il est claire que si $I = A$, alors $1 \in I$. Réciproquement, si $1 \in I$, alors $\forall a \in A$ on a $a = a1 \in I$; d'où $A \subset I$, par suite $A = I$. □

Convention. Dans toute la suite, le mot idéal signifiera un idéal bilatère.

Proposition 29. *Soit $f : A \longrightarrow B$ un homomorphisme d'anneaux. Si J est un idéal de B, alors l'image réciproque $I = f^{-1}(J) = \{a \in A \mid f(a) \in J\}$ est un idéal de A.*

Preuve. Soit J un idéal de B, et $x, y \in I = f^{-1}(J)$, $a \in A$.
Comme J est non vide, alors $I = f^{-1}(J)$ est également non vide. De plus f est un homomorphisme d'anneaux, donc $f(x - y) = f(x) - f(y)$. Or J étant un idéal et $f(x - y) = f(x) - f(y) \in J$, donc $x - y \in f^{-1}(J)$. Également, $f(ax) = f(a)f(x)$, et J étant un idéal, $f(a)f(x) \in J$, donc $ax \in f^{-1}(J)$. □

Remarque 29. L'image directe d'un idéal par un homomorphisme d'anneaux f **n'est pas forcément un idéal**, sauf si f est surjectif. Comme contre exemple, soit l'homomorphisme $f : \mathbb{Z} \longrightarrow \mathbb{Q};\ k \longmapsto k$. Alors $f(\mathbb{Z})$ n'est pas un idéal de $\mathbb{Q}$. De plus, $f(I)$ n'est un idéal de $\mathbb{Q}$ que si I est l'idéal nul.

Corollaire 8. *Le noyau d'un homomorphisme d'anneaux $f : A \longrightarrow B$ est l'ensemble des $a \in A$ tels que $f(a) = 0_B$. C'est un idéal de A noté* $\ker f$.

Preuve. On sait que $J = \{0_B\}$ est idéal de B, donc $\ker f = f^{-1}(J)$ est un idéal de A. □

Proposition 30. *Toute intersection d'idéaux d'un anneau A est un idéal de A.*

Preuve. Soit $(J_i)_{i \in I}$ une famille d'idéaux de A indexée par un ensemble I. Posons

$$J = \bigcap_{i \in I} J_i.$$

- Tous les J_i contiennent 0, donc J contient 0, et est donc non vide.
- Soient x, $y \in J$, $a \in A$. Pour tout $i \in I$, x et y sont dans J_i, qui est un idéal, donc $x - y \in J_i$ et $ax \in J_i$, donc $x - y \in J$ et $ax \in J$. □

Remarque 30. $\bigcap_{i \in I} J_i$ est la borne inférieur des (J_i) dans $\mathcal{P}(A)$, l'ensemble des parties de A, ordonné par inclusion.

La proposition précédente nous permets de considérer la notion d'idéal engendré par une partie.

Définition 51. Soit X une partie d'un anneau A. On appelle idéal engendré par X, et on note $\langle X\rangle$, l'intersection de tous les idéaux de A contenant X, c'est-à-dire

$$\langle X\rangle = \bigcap_{I \text{ idéal de } A,\ I\supset X} I.$$

C'est le plus petit idéal de A contenant X. X est appelé un système de générateurs de cet idéal.

Remarque 31. Si X est non vide, alors l'idéal engendré par X est égal à l'ensemble des éléments de la forme $\sum_{i=1}^{n} a_i x_i$ où les a_i sont des éléments quelconques de A et les x_i sont des éléments quelconques de X.

Remarque 32. Si $X = \{x_1, x_2, \cdots, x_n\}$, alors $\langle X\rangle = \left\{ \sum_{i=1}^{n} a_i x_i \mid a_i \in A \right\}$. Cet idéal est noté aussi par $\langle X\rangle = \langle x_1, x_2, \cdots, x_n\rangle$.

Proposition 31. *Soient un anneau intègre A et $a \in A$. L'idéal engendré par $X = \{a\}$, que l'on note aA ou $\langle a\rangle$, est l'ensemble $\{ax \mid x \in A\}$, c-à-d, $\langle a\rangle = \{ax \mid x \in A\}$.*

Preuve. Posons $J = \{ax \mid x \in A\}$, et montrons que c'est le plus petit idéal de A contenant a, ce qui achèvera la démonstration.

J est un idéal, en effet :
- J est non vide, car $a.0 = 0 \in J$,
- pour tous x, $y \in A$, on a : $ax - ay = a(x - y) \in J$,
- pour tout $b \in A$, comme $(ax)b = a(xb)$, alors $(ax)b \in J$,
- enfin, J contient a puisque $a = a.1 \in J$.

Soit I un idéal de A contenant a. Donc pour tout $x \in A$, on a : $ax \in I$, c'est-à-dire que $J \subset I$. □

Définition 52. Un idéal I d'un anneau intègre A est dit *principal* s'il est engendré par un seul élément.

Remarque 33. Un idéal principal peut admettre plusieurs générateurs.

Définition 53. Un idéal I d'un anneau A est dit *de type fini* s'il est engendré par une partie finie X de A.

Exemple 12. Pour tout $n \in \mathbb{N}$, $n\mathbb{Z} = \langle n\rangle$ est un idéal principal de l'anneau $\mathbb{Z}$.

Définition 54. Un anneau intègre A est dit *principal* si tout idéal I de A est principal.

Exemples 13.
- L'anneau $\mathbb{Z}$ est principal, car pour tout $n \in \mathbb{N}$, $n\mathbb{Z}$ est un idéal principal.
- Si K est un corps, alors l'anneau $K[X]$ est principal.
- L'anneau $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ est principal, il est dit l'anneau des entiers de Gauss.

Le résultat suivant est une caractérisation d'un corps.

Théorème 45. *Soit A un anneau unitaire, alors A est un corps si et seulement si ses seuls idéaux sont A et $\{0\}$.*

Preuve. Supposons que A est un corps. Soit I un idéal non nul de A, considérons $x \neq 0$ et $x \in I$, alors $x \cdot x^{-1} = 1 \in I$, donc $\forall a \in A$, $a \cdot 1 \in I$, d'où $I = A$.

Réciproquement, $x \neq 0$ et $x \in A$, alors $\langle x \rangle$ est un idéal non nul de A, donc $\langle x \rangle = A$; d'où $1 \in \langle x \rangle$, par suite il existe $y \in A$ tel que $xy = 1$, c-à-d, x est inversible. □

Proposition 32 (Somme d'idéaux).
Soient I et J deux idéaux d'un anneau A. L'ensemble des sommes $a + b$ avec $a \in I$ et $b \in J$ est un idéal de A, noté $I + J$. C'est aussi l'idéal engendré par $I \cup J$.

$$I + J = \{a + b \mid a \in I,\ b \in J\} = \langle I \cup J \rangle.$$

Plus généralement, si $(I_k)_{k \in K}$ est une famille d'idéaux d'un anneau A, alors l'ensemble des sommes (presque nulles) $\sum_{k \in K} a_k$ (K ensemble d'indices), où $a_k \in I_k$ pour tout $k \in K$, est un idéal de A, noté $\sum_{k \in K} I_k$. C'est aussi l'idéal engendré par $\bigcup_{k \in K} I_k$, et c'est la borne supérieure de cette famille dans $\mathcal{P}(A)$ ordonné par inclusion.

Preuve. Posons $I = \sum_{k \in K} I_k$. Comme $0 = \sum_k 0$ et $0 \in I_k$ pour tout k, alors $0 \in I$ c-à-d $I \neq \varnothing$.
Ensuite, si $a = \sum_{k \in K} a_k$ et $b = \sum_{k \in K} b_k$ sont deux éléments de I, alors $a + b = \sum_{k \in K} (a_k + b_k)$ où pour tout k, $a_k + b_k \in I_k$, presque tous les termes de cette somme sont nuls. Donc $a + b \in I$.
Finalement, si $a = \sum_{k \in K} a_k$ et $b \in A$, alors $ba = \sum_{k \in K} (ba_k)$. Pour tout $k \in K$, $ba_k \in I_k$, donc $ba \in I$. Ainsi, I est un idéal de A.

Pour montrer que I est l'idéal de A engendré par $\bigcup_{k \in K} I_k$, nous allons étudier deux inclusions.

Tout d'abord, si $t \in K$ et $a \in I_t$, on a $a = \sum_{k \in K} a_k$ avec $a_k = 0$ si $t \neq k$ et $a_t = a$. Donc $a \in I$ et par suite $I_t \subset I$, d'où $\bigcup_{k \in K} I_k \subset I$. Par définition de l'idéal $\left\langle \bigcup_{k \in K} I_k \right\rangle$ (plus petit idéal qui contient $\bigcup_{k \in K} I_k$) on a :

$$\left\langle \bigcup_{k \in K} I_k \right\rangle \subset I.$$

Dans l'autre sens, si J est un idéal contenant $\bigcup_{k \in K} I_k$, montrons que J contient I.

Soit $a = \sum_{k \in K} a_k \in I$; tous les termes de cette somme appartiennent à J, donc $a \in J$, car J est stable pour l'addition. D'où $I \subset J$. Ce là veut dire que I est le plus petit idéal contenant $\bigcup_{k \in K} I_k$; donc

$$\left\langle \bigcup_{k \in K} I_k \right\rangle = I.$$

□

Définition 55 (produit de deux idéaux).
Soient I et J deux idéaux d'un anneau A. L'idéal engendré par les produits ab, où $a \in I$ et $b \in J$, est appelé idéal produit de I et J, et est noté IJ. IJ est l'ensemble des combinaisons linéaires finies $\sum a_i b_j$ avec $a_i \in I$ et $b_j \in J$.

Remarque 34. L'ensemble des produits ab avec $a \in I$ et $b \in J$ n'est pas forcement un idéal de A.

Proposition 33. *Soient I et J deux idéaux d'un anneau A. Alors $IJ \subset I \cap J$.*

Preuve. Soient $a \in I$ et $b \in J$, alors $ab \in I$ (car c'est un multiple de $a \in I$) et $ab \in J$ (car c'est un multiple de $b \in J$). Donc $ab \in I \cap J$, d'où l'idéal engendré par ces produits qui est IJ est contenu dans $I \cap J$. □

Corollaire 9. *Soit une famille d'idéaux (I_i), $i = 1, \cdots, n$, alors*

$$I_1 I_2 \cdots I_n \subset \bigcap_{i=1}^{n} I_i.$$

Preuve. Par récurrence. □

Remarque 35. Dans l'ensemble des idéaux d'un anneau commutatif unitaire A, ordonné par inclusion, toute famille d'idéaux (I_i) admet une borne supérieure qui est $\sum I_i$ et une borne inférieure qui est $\cap I_i$.

4.5. **Anneaux quotients.**

Définition 56. Soit $\mathcal{R}$ une relation d'équivalence sur un anneau A. La relation $\mathcal{R}$ est dite compatible avec la structure de A si $\mathcal{R}$ est compatible avec les lois de l'anneau A, c-à-d,

$$\forall x \in A \text{ et } \forall (a,b) \in A^2,\ a \equiv b\ [\mathcal{R}] \Longrightarrow a+x \equiv b+x\ [\mathcal{R}] \text{ et } ax \equiv bx\ [\mathcal{R}].$$

Théorème 46. *Il existe une application bijective entre les relations d'équivalences compatibles avec la structure d'un anneau A et les idéaux bilatères de A.*

Preuve. Soit $\mathcal{R}$ une relation d'équivalence compatible avec la structure d'un anneau A. La classe $I = \overline{0}$ de 0, élément neutre pour la somme dans A, est un idéal de A. En effet,
- $\overline{0} \neq \varnothing$, car $0 \in \overline{0}$.
- $\forall\ x, y \in \overline{0}$, on a $x\mathcal{R}0$ et $y\mathcal{R}0$, donc $x+y\mathcal{R}0$ puisque $\mathcal{R}$ est compatible la structure de A. Donc $x+y \in \overline{0}$.
- $\forall\ x \in \overline{0}$, $\forall a \in A$, on a $x\mathcal{R}0$, donc $ax\mathcal{R}a0$ puisque $\mathcal{R}$ est compatible la structure de A. Donc $ax\mathcal{R}0$, ce qui implique que $ax \in \overline{0}$. D'où, en prenant $a = -1$, on déduit que $-x \in \overline{0}$.

Réciproquement, si I est un idéal bilatère de A, alors considérons la relation $\mathcal{R}$ définie par :

$$\forall x,\ y \in A; \qquad x\mathcal{R}y \Longleftrightarrow x - y \in I.$$

Il est facile de vérifier que $\mathcal{R}$ est une relation d'équivalence sur A. Il reste à vérifier qu'elle est compatible avec la structure de A.
- Soient $x, y \in A$ tels que $x\mathcal{R}y$, alors $x - y \in I$, donc $\forall a \in A$, $a(x-y) = ax - ay \in I$, c-à-d, $ax\mathcal{R}bx$.
- D'autre part, $x+a-(y+a) = x-y \in I$, donc $(x+a)\mathcal{R}(y+a)$; d'où $\mathcal{R}$ est compatible avec la structure de A. □

Comme conclusion, se donner un idéal bilatère I de A revient à se donner une relation d'équivalence $\mathcal{R}$ sur A compatible avec la structure de A.

Définition 57. L'ensemble des classes d'équivalences modulo la relation $\mathcal{R}$ est noté $A/\mathcal{R}$ ou A/I, et est appelé **l'ensemble quotient** modulo l'idéal I.

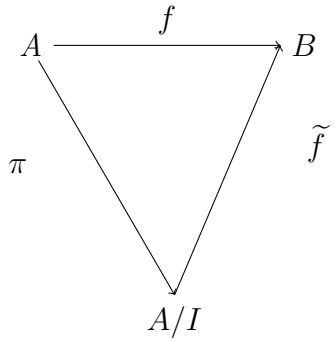
Proposition 34. *Soient A un anneau et I un idéal bilatère de A. En posant, pour tous $x, y \in A$, $\overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x} \cdot \overline{y} = \overline{xy}$; on définit sur l'ensemble quotient A/I une unique structure d'anneau telle que la surjection canonique $\pi : A \longrightarrow A/I$ soit un homomorphisme d'anneaux ;* $\ker \pi = I$. *L'anneau $(A/I, +, \cdot)$ est appelé anneau quotient de A par I, l'élément neutre pour l'addition est la classe $\overline{0} = I$.*

Preuve. Laissée au lecteur. □

Remarque 36. A/A est l'anneau nul $\{0\}$, et $A/\{0\} = A$.

Les différents théorèmes d'isomorphismes que nous avons vu pour les groupes restent valables pour les anneaux. Les démonstrations de ces Théorèmes sont presque les mêmes que pour les groupes ; il suffit de vérifier que les homomorphismes de groupes utilisés dans les preuves sont aussi des homomorphismes d'anneaux.

Théorème 47. *Soit $f : A \longrightarrow B$ un homomorphisme d'anneaux. Si I est un idéal de A* **contenu** *dans* $\ker f$ *($I \subset \ker f$), alors il existe un unique homomorphisme d'anneaux $\widetilde{f} : A/I \longrightarrow B$ tel que $f = \widetilde{f} \circ \pi$, où $\pi : A \longrightarrow A/I$ est la surjection canonique.*



$$f = \widetilde{f} \circ \pi.$$

Preuve. Supposons que $\widetilde{f}$ existe, alors nécessairement elle doit vérifier $\widetilde{f}(\pi(x)) = f(x)$ pour tout $x \in A$. Supposons qu'elle existe une autre application $\widetilde{f}'$ vérifiant la condition du théorème, alors tout $\overline{x}$ de A/I est de la forme $\pi(x)$ pour un certain $x \in A$, donc $\widetilde{f}(\overline{x}) = \widetilde{f}(\pi(x)) = f(x) = \widetilde{f}(\pi(x)) = \widetilde{f}'(\overline{x})$. Cela montre que si un homomorphisme d'anneaux $\widetilde{f} : A/I \longrightarrow B$ tel que $f = \widetilde{f} \circ \pi$ existe, alors il est unique.

Montrons maintenant l'existence de $\widetilde{f}$.
Soit $x \in A/I$, il existe $a \in A$ tel que $x = \pi(a)$. Si a' est un autre representant de x, alors $\pi(a') = \pi(a) = x$, donc $a' - a \in I$; or $I \subset \ker f$, alors $f(a' - a) = 0$, et par conséquent $f(a) = f(a')$.

Posons donc $\widetilde{f}(x) = f(a)$ et le résultat est indépendant du choix du representant a. Il reste à montrer que c'est un homomorphisme d'anneaux.

Comme $\pi(0_A) = 0_{A/I} = I$ et $\pi(1_A) = 1_{A/I} = A$, alors $f(0_A) = 0_B$ et $f(1_A) = 1_B$. De plus si $x = \pi(a)$ et $y = \pi(b)$ sont deux éléments de A/I, on a $x + y = \pi(a + b)$ et

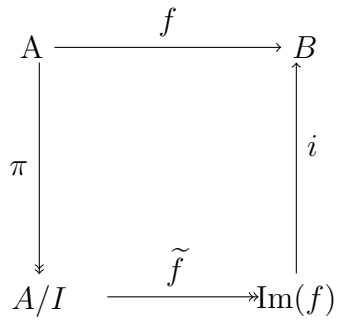
$$\widetilde{f}(x + y) = \widetilde{f}(\pi(a + b)) = f(a + b) = f(a) + f(b) = \widetilde{f}(x) + \widetilde{f}(y),$$

de même $\widetilde{f}(xy) = f(ab) = f(a)f(b) = \widetilde{f}(x)\widetilde{f}(y)$. Il en résulte que $\widetilde{f}$ est un homomorphisme d'anneaux. □

Comme $f(A)$ est un sous-anneau de B, alors f peut se décomposé comme suit :

Théorème 48 (1^{er} th. d'isomorphisme). *Soient $f : A \longrightarrow B$ un homomorphisme d'anneaux et $I = \ker f = \{x \in A \mid f(x) = 0_B\}$. Soient aussi $\pi : A \longrightarrow A/I$ la surjection canonique et $i : f(A) = \mathrm{Im}(f) \longrightarrow B$ l'injection canonique. Alors il existe un isomorphisme d'anneaux $\widetilde{f}$ de A/I dans $\mathrm{Im}(f) = f(A)$ tel que $f = i \circ \widetilde{f} \circ \pi$, on écrit*

$$A/I \simeq \mathrm{Im}(f) = f(A).$$



Preuve. Laisser au lecteur. □

Proposition 35.
Soient A, B et C trois anneaux, f un homomorphisme de A dans B et g un homomorphisme surjective de A dans C ; alors il existe un homomorphisme φ de C dans B tel que : $f = \varphi \circ g$ si et seulement si $\ker g \subset \ker f$.

Preuve. Laisser au lecteur. □

Théorème 49 ($2^{\text{ème}}$ th. d'isomorphisme).
Soient A un anneau, I et J deux idéaux bilatères de A, alors

$$J/I \cap J \simeq (I + J)/I.$$

Preuve. Laisser au lecteur. □

Théorème 50 ($3^{\text{ème}}$ **th. d'isomorphisme).**
Soient A un anneau, I et J deux idéaux bilatères de A tels que $I \subset J$; alors

$$J/I \text{ est un idéal de } A/I \quad \text{et} \quad A/J \simeq (A/I)/(J/I).$$

C'est-à-dire un quotient d'un quotient est encore un quotient.

Preuve. Comme J/I est un idéal de A/I (voir théorème suivant) et comme aussi la composée de deux homomorphismes surjectifs est un homomorphisme surjectif, alors l'application

$$\varphi : A \xrightarrow{\pi_1} A/I \xrightarrow{\pi_2} (A/I)/(J/I)$$

est un homomorphisme surjectif de A sur $(A/I)/(J/I)$. Soit $a \in A$, alors

$$\begin{aligned} a \in \ker\varphi &\iff \varphi(a) = \pi_2(\pi_1(a)) = J/I \\ &\iff \pi_1(a) \in \ker\pi_2 = J/I \\ &\iff \pi_1(a) \in \pi_1(J), \text{ car } \pi_1(J) = J/I \\ &\iff a \in J \text{ puisque } I \subset J. \end{aligned}$$

Donc le 1^{er} théorème d'isomorphisme implique que $A/J \simeq (A/I)/(J/I)$. □

Théorème 51 ($4^{\text{ème}}$ **th. d'isomorphisme ou th. de correspondance).**
Soient A un anneau et I un idéal bilatère de A.

1. *L'application $B \longmapsto B/I$ définie une application bijective entre l'ensemble des sous-anneaux de A contenant I et les sous-anneaux de A/I, i.e. C est un sous-anneau de A/I si, et seulement si, il existe un sous-anneau B de A contenant I tel que $C = B/I$.*
2. *L'application $J \longmapsto J/I$ définie une correspondance bijective entre l'ensemble des idéaux de A contenant I et l'ensemble des idéaux de A/I, i.e. R est un idéal de A/I si, et seulement si, il existe un idéal J de A contenant I tel que $R = J/I$.*

Preuve. Montrons par exemple 2.. Soit

$$\varphi : \{J \mid J \text{ est un idéal de } A \text{ contenant } I\} \longrightarrow \{K \mid K \text{ est un idéal de } A/I\}$$

définie par : $\varphi(J) = J/I$.

Si J est un idéal de A contenant I, alors J est un sous-groupe du groupe $(A, +)$ contenant le sous-groupe I de $(A, +)$ et ainsi, d'après le théorème de correspondance pour les groupes, $\varphi(J) = J/I$ est un sous-groupe du groupe quotient $(A/I, +)$. En

vérifiant que $\forall \overline{a} \in A/I$, $\forall \overline{x} \in J/I$, $\overline{a}\ \overline{x} = \overline{ax} \in J/I$, on a J/I est un idéal de l'anneau quotient A/I et ainsi φ est une application bien définie.
Montrons alors que φ est bijective : φ est injective (cf le théorème de correspondance pour les groupes).
φ est aussi surjective. En effet, Soit K un idéal de A/I, alors $J = \pi^{-1}(K)$ est un idéal de A (car $\pi : A \longrightarrow A/I$, $x \longmapsto \overline{x}$ est un homomorphisme d'anneaux) et on a $I \subset J$ (car $I = \pi^{-1}\{\overline{0}\} \subset \pi^{-1}(K) = J$) et $J/I = \pi(J) = K$ (car π est surjectif), i.e. $\varphi(J) = K$ et ainsi φ est surjective. □

4.6. **Caractéristique d'un anneau.**

Définition 58. Soit A un anneau unitaire. L'application

$$\begin{aligned} f : \ & \mathbb{Z} \longrightarrow A \\ & k \longmapsto f(k) = k \cdot 1_A \end{aligned}$$

est un homomorphisme d'anneaux. $\ker f$ est un idéal de $\mathbb{Z}$, il existe donc $n \in \mathbb{N}$ tel que $\ker f = n\mathbb{Z}$. L'entier naturel n ainsi définit est appelé **la caractéristique** de A.

Remarque 37. Si n est la caractéristique d'un anneau A, alors deux cas se distinguent :
- si $n = 0$, alors $\ker f = \{0\}$, et f est donc injective. D'où en identifiant n à $n \cdot 1_A$, on peut considérer $\mathbb{Z}$ comme un sous-anneau de A, car dans ce cas $\mathbb{Z} \simeq \mathbb{Z}/\{0\} \simeq Im(f)$.
- si $n > 0$, alors n est le plus petit entier vérifiant $n \cdot 1_A = f(n) = 0$; en effet, s'il existe $m \leq n$ tel que $n \cdot 1_A = 0$, alors $m \in \ker f = n\mathbb{Z}$, donc n divise m, ce qui implique $n = m$. On a aussi $k \cdot 1_A = 0 \Longleftrightarrow k \in n\mathbb{Z}$ et $\forall\ a \in A$, $n \cdot a = 0$. En effet $n \cdot a = n \cdot 1_A a = 0a = 0$. De plus $\mathbb{Z}/n\mathbb{Z} \simeq \mathrm{Im}(f) = f(A)$, on peut voir donc $\mathbb{Z}/n\mathbb{Z}$ comme un sous-anneau de A, en identifiant n à $n \cdot 1_A$.

Remarques 20.

1. Si $p > 0$ est un nombre premier, alors l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps, et c'est un corps premier. Plus généralement, si A est un anneau unitaire intègre de caractéristique $p > 0$ un nombre premier, le sous-anneau de A engendré par 1 dans A est un corps K isomorphe à $\mathbb{Z}/p\mathbb{Z}$: ce corps est le plus petit corps contenu dans A. Si de plus A est un corps, K est le sous-corps premier de A.
2. Si K est un corps de caractéristique 0, alors K contient $\mathbb{Z}$, donc il contient tous les éléments de la forme $(q.1)^{-1}.(p.1)$, $p \in \mathbb{Z}$ et $q \in \mathbb{Z}^*$. L'ensemble de ces éléments est un corps isomorphe à $\mathbb{Q}$.

Théorème 52. *Un anneau intègre (et donc aussi un corps) a une caractéristique nulle ou un nombre premier.*

Preuve. Soit A un anneau de caractéristique non nulle n ; comme A est intègre, alors tout sous-anneau de A est aussi intègre. Or, par identification, on a supposé que $\mathbb{Z}/n\mathbb{Z}$ est un sous-anneau de A, d'où $\mathbb{Z}/n\mathbb{Z}$ est intègre, donc n est premier. Par suite le résultat. □

Exemple 13. $\mathbb{Z}$ est de caractéristique nulle, et celle de $\mathbb{Z}/n\mathbb{Z}$ est n. Tout anneau fini a une caractéristique non nul.

La remarque suivante est basée sur le résultat suivant.

Lemme 7. *Un entier $n \geq 2$ est premier si, et seulement si, n divise $\binom{n}{k} = \mathsf{C}_n^k$ pour tout $k \in \{1, \ldots, n-1\}$.*

Preuve. Pour tout k tel que $0 < k < n$, on a

$$n\binom{n-1}{k-1} = \frac{n(n-1)!}{(k-1)!(n-k)!} = k\frac{n!}{k(k-1)!(n-k)!} = k\frac{n!}{k!(n-k)!} = k\binom{n}{k}$$

Par suite :

- si n est premier, comme il ne divise pas k (car $k < n$), il divise $\binom{n}{k}$ par le Lemme d'Euclide.
- supposons maintenant que n divise $\binom{n}{k} = \mathsf{C}_n^k$ pour tout $k \in \{1, \ldots, n-1\}$, et montrons que n est premier. Ceci est équivalent par contraposition à montrer que si n est composé (c-à-d n non premier) et si k est l'un de ses facteurs premiers, alors n ne divise pas $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$.

  Si n est composé et si k est l'un de ses facteurs premiers $n = kh$, alors k divise n et ne divise pas les $k-1$ entiers qui le précèdent, c'est-à-dire k ne divise pas $n-i$ pour $1 \leq i \leq k-1$, car sinon on aura k divise $n - n + i = i$ qui est absurde. Donc k ne divise pas $\binom{n-1}{k-1} = \frac{(n-1)(n-2)\ldots(n-k+1)}{(k-1)!}$. D'où n ne divise pas $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$.

□

Remarque 38. Soit A un anneau commutatif et admettant une caractéristique p, où p est un nombre premier. Pour tous a et b dans A on a :

$$(a+b)^p = a^p + b^p,$$

ce résultat est dû au fait que p divise $\complement_p^k$ pour tout $1 \leq k \leq p-1$.

Plus généralement et par récurrence sur l'entier naturel n, on déduit que

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

4.7. **Idéaux étrangers.**

Dans cette section, nous allons donner une version considérablement généralisée du théorème des restes chinois, et qui sert non seulement en arithmétique mais également dans d'autre discipline comme la géométrie algébrique. Commençons par énoncer une généralisation des nombres premiers entre eux.

Définition 59. Deux idéaux I et J d'un anneau unitaire A sont dits **comaximaux ou étrangers** si $I + J = A = \langle 1_A \rangle$, autrement dit, s'il existe $x \in I$ et $y \in J$ tels que $x + y = 1$.

Collectons quelques propriétés.

Proposition 36. *Soient I et J deux idéaux étrangers d'un anneau unitaire A (i.e., $I + J = A$). Alors $IJ = I \cap J$.*

Preuve. On sait déjà, par la proposition 33, que $IJ \subset I \cap J$.

Si $I + J = A$, alors il existe $x \in I$ et $y \in J$ tels que $x + y = 1$. Soit alors $a \in I \cap J$; donc

$$a = a1 = a(x+y) = ax + ay.$$

Comme $a \in I$ et $y \in J$, alors $ay \in IJ$; de même $ax \in IJ$, par suite $ax + ay \in IJ$, et alors $a \in IJ$. Donc $I \cap J \subset IJ$, d'où $IJ = I \cap J$. □

Corollaire 10. *Si les idéaux I_i, pour $i = 1, \cdots, n$, sont deux à deux comaximaux, alors*

$$\bigcap_{i=1}^{n} I_i = I_1 I_2 \cdots I_n.$$

Preuve. Par récurrence. □

Exercice. Soient K un corps commutatif et $a_1, \cdots, a_n$ des éléments distincts deux à deux de K.

a. Montrer que tout polynôme P de $K[X]$ nul en $a_1, \cdots, a_n$ est divisible par $(X - a_1) \cdots (X - a_n)$. Considérer les idéaux $I_i = \langle X - a_i \rangle$ et montrer qu'ils sont étrangers deux à deux et appliquer le corollaire précédent.

b. Montrer qu'un polynôme $P \in K[X]$ de degré $d \geq 0$ admet au plus d racines (considerer n racines de P, $a_1, \cdots, a_n$ et appliquer la question a).

Proposition 37. *Si un idéal I est étranger à J et à J', alors I est étranger à leur produit JJ'.*

Preuve. Si $x \in I$ et $y \in J$ sont tels que $x + y = 1$ et si $x' \in I$ et $y' \in J'$ sont tels que $x' + y' = 1$, alors $1 = (x+y)(x'+y') = (xx' + xy' + yx') + yy'$, or $xx' + xy' + yx' \in I$ et $yy' \in JJ'$. Donc il existe $\alpha = xx' + xy' + yx' \in I$ et $\beta = yy' \in JJ'$ tels que $\alpha + \beta = 1$, d'où I et JJ' sont étrangers. □

Proposition 38. *Si I et J sont étrangers, alors I^m et J^n sont étrangers pour tous $m, n \in N^*$.*

Preuve. Par récurrence en utilisant la proposition précédente. □

Théorème 53 (Lemme des restes chinois). *Soient I, J deux idéaux d'un anneau intègre unitaire A étrangers entre eux. Alors l'application*

$$\begin{array}{rccc} \varphi : & A/IJ & \longrightarrow & (A/I) \times (A/J) \\ & x \ (mod\ IJ) & \longmapsto & (x \ (mod\ I),\ x \ (mod\ J)) \end{array}$$

est un isomorphisme d'anneaux.

Preuve. L'application $\begin{array}{rccc} f : & A & \longrightarrow & (A/I) \times (A/J) \\ & x & \longmapsto & (x \ (mod\ I), x \ (mod\ J)) \end{array}$
est un morphisme de A sur l'anneau produit $(A/I) \times (A/J)$. On a

$$\begin{aligned} x \in \ker f &\iff f(x) = (I, J) \\ &\iff (x + I, x + J) = (I, J) \\ &\iff x + I = I \text{ et } x + J = J \\ &\iff x \in I \text{ et } x \in J. \\ &\iff x \in I \cap J. \end{aligned}$$

D'où le noyau de f est $I \cap J = IJ$ puisque I et J sont étrangers. Par le premier théorème d'isomorphisme, on obtient $A/IJ \simeq \mathrm{Im}(f)$.

Pour montrer la surjectivité, il suffit de montrer que : pour tous $a, b \in A$, il existe $c \in A$ tel que $c \equiv a \pmod{I}$ et $c \equiv b \pmod{J}$. En effet, $c \pmod{IJ}$ sera donc un antécédent de $(a \pmod{I}, b \pmod{J})$. Soient $x \in I$, $y \in J$ tels que $x + y = 1$, posons $c = bx + ay$, alors

$$c - a = bx + ay - a = bx + a(y-1) = bx - ax = (b-a)x \in I,$$

et de même $c - b \in J$. D'où f est surjective, et par suite $\mathrm{Im}(f) = (A/I) \times (A/J)$, ce qui implique que $A/IJ \simeq \mathrm{Im}(f)$. □

Corollaire 11. *Soient $I_1, \cdots, I_n$ des idéaux étrangers deux à deux d'un anneau intègre unitaire A. Alors on a un isomorphisme :*

$$A/(I_1 \cap \cdots \cap I_n) = A/(I_1 \cdots I_n) \simeq (A/I_1) \times \cdots \times (A/I_n).$$

Preuve. Par récurrence. □

4.8. **Idéaux premiers.**

Les notions d'idéaux premiers et maximaux généralisent le concept classique de nombre premier. Leur importance est apparue au XIX^e siècle avec les travaux de KUMMER en arithmétique. En effet, par définition d'un nombre premier, si un produit d'entiers ab est multiple d'un nombre premier p, alors a ou b est multiple de p. Cela amène à la définition suivante.

Définition 60. Soient A un anneau et I un idéal de A tel que $I \neq A$. On dit que I est un idéal premier de A si pour tous a, $b \in A$, $ab \in I \Longrightarrow a \in I$ ou $b \in I$.

La condition $I \neq A$ est analogue à la convention qui dit que 1 n'est pas un nombre premier. Par ailleurs, la second condition s'utilise parfois sous la forme équivalente (contraposée) :

$$\text{si } a \notin I \text{ et } b \notin I, \text{ alors } ab \notin I.$$

Théorème 54. *Soient A un anneau et I un idéal de A. Alors*

I est un idéal premier de A si et seulement si l'anneau quotient A/I est intègre.

Preuve. Dire que A/I est intègre implique d'abord que $A/I \neq \{\overline{0}\}$, c'est-à-dire que $I \neq A$. Soient a, $b \in A$, si $ab \in I$, alors $\overline{a}\overline{b} = \overline{ab} = \overline{0}$, ce qui implique que $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$ puisque A/I est intègre. Donc $a \in I$ ou $b \in I$. D'où I est premier.

Réciproquement, supposons que I est premier, soit a, $b \in A$ tels que $\overline{a}\overline{b} = \overline{ab} = \overline{0}$, alors $ab \in I$, ce qui implique que $a \in I$ ou $b \in I$. Donc $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$. D'où le résultat. □

Exemples 14.

1. L'idéal $\{0\}$ est premier si et seulement si A est intègre, car $A = A/\{0\}$.
2. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier. Comme $\mathbb{Z}$ est intègre, alors les idéaux premiers de $\mathbb{Z}$ sont $\{0\}$ et $p\mathbb{Z}$ où p est entier naturel premier.

3. Si K est un corps, alors l'idéal $\langle X\rangle$ de $K[X]$ est premier. Pour $P \in K[X]$, P est premier si et seulement si P est irréductible.
4. Soit $f : A \longrightarrow K$ un morphisme d'anneaux, avec K est un corps. Alors $\ker(f)$ est premier car, par le premier théorème d'isomorphisme, le quotient $A/\ker(f)$ est isomorphe au sous-anneau Imf de K qui est intègre.

Proposition 39. *Soit $f : A \longrightarrow B$ un homomorphisme d'anneaux. Si J est un idéal premier de B, alors $f^{-1}(J)$ est un idéal premier de A.*

Preuve. Comme $f(1) = 1 \notin J$, alors $1 \notin f^{-1}(J)$ et $f^{-1}(J) \neq A$.
Soient $a \in A$ et $b \in A$ tels que $ab \in f^{-1}(J)$, alors $f(ab) = f(a)f(b) \in J$, donc $f(a) \in J$ ou $f(b) \in J$; ce qui signifie que $a \in f^{-1}(J)$ ou $b \in f^{-1}(J)$. □

Question. Que pouvez-vous dire de l'image direct par f d'un idéal premier I de A ?

4.9. **Idéaux maximaux.**

Définition 61. Soit A un anneau unitaire.
Un idéal I de A est dit **maximal** si $I \neq A$ et s'il est maximal pour l'inclusion dans l'ensemble des idéaux de A distincts de A, c'est-à-dire,
I est maximal est équivaut à $I \neq A$ et pour tout idéal J de A, $I \subset J \Longrightarrow J = I$ ou $J = A$.

Comme pour les idéaux premiers, on peut donner une caractérisation d'un idéal maximal en termes de l'anneau quotient.

Théorème 55. *Soient A un anneau unitaire et I un idéal de A. Alors I est maximal si et seulement si tout élément non nul de A/I est inversible, i.e. $U_{A/I} = A/I - \{\overline{0}\}$. Autrement dit :*

I est maximal si et seulement si A/I est un corps.

Preuve. Supposons que $U_{A/I} = A/I - \{\overline{0}\}$, c'est à dire supposons que tout élément non nul de A/I est inversible. Soit J un idéal de A tel que $I \subsetneq J$, considérons $x \in J$ et $x \notin I$, alors $\overline{x} \neq \overline{0}$, donc $\overline{x} \in A/I - \{\overline{0}\}$, par suite il est inversible. Il existe donc $\overline{y} \in A/I$ tel que $\overline{1} = \overline{xy}$, ceci implique que $1 - xy \in I \subsetneq J$; or $xy \in J$, donc $1 \in J$. D'où $J = A$, i.e. I est maximal.

Réciproquement, supposons que I est maximal ; soit $\overline{x} \neq \overline{0}$ et $\overline{x} \in A/I$, alors $x \notin I$. Donc $I \subsetneq I + \langle x\rangle$; comme I est maximal, alors $A = I + \langle x\rangle$, d'où $1 \in I + \langle x\rangle$. Par suite il existe $\alpha \in I$, $y \in A$ tels que $1 = \alpha + xy$, d'où $\overline{1} = \overline{x} \cdot \overline{y}$, par suite $\overline{x}$ est inversible. □

Exemples 15.

1. L'idéal $\{0\}$ d'un anneau A n'est maximal que si A est un corps.
2. Les idéaux maximaux de $\mathbb{Z}$ sont les idéaux $p\mathbb{Z}$, où p un élément premier de $\mathbb{Z}$. En effet, $\{0\}$ n'est pas maximal car $\mathbb{Z}$ n'est pas un corps. Soit J un idéal de $\mathbb{Z}$, alors il existe $n \in \mathbb{Z}$ tel que $J = n\mathbb{Z}$. Donc $\langle p\rangle \subset \langle n\rangle \Longrightarrow p = nk$, ceci implique que n divise p, d'où $p = n$ ou $n = 1$; par suite $\langle p\rangle = \langle n\rangle$ ou $J = \mathbb{Z}$.
3. Dans l'anneau $K[X]$ des polynômes à coefficients dans un corps commutatif K, les idéaux sont les parties de $K[X]$ de la forme $P(X)K[X] = \langle P\rangle$, pour n'importe quel polynôme $P(X)$. Si ce polynôme est irréductible, alors il est maximal et l'anneau quotient $K[X]/\langle P\rangle$ est un corps, appelé **corps de rupture de** $P(X)$.
4. Voici un moyen commode pour démontrer qu'un idéal est maximal. Soit $\varphi : A \longrightarrow K$ un morphisme surjectif, où K est un corps. Alors $\ker(\varphi)$ est maximal. En effet, par le premier théorème d'isomorphisme on déduit que $A/\ker(\varphi)$ est isomorphe à K, donc est un corps. En fait, tout idéal maximal M peut s'obtenir de cette façon (prendre la projection canonique $\varphi : A \longrightarrow A/M$).

Remarques 21.

1. Si K est un corps, le sous-corps de K engendré par 1_K est un corps premier. C'est le sous-corps premier de K.
2. Si K est un corps de caractéristique p, alors le sous-corps premier de K est isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Corollaire 12. *Tout idéal maximal I d'un anneau A est premier.*

Preuve. Si I est un idéal maximal, alors A/I est un corps, donc A/I est intègre, ce qui implique I est premier. □

Remarque 39. La réciproque n'est généralement pas vraie, mais elle est vraie si A est un anneau principal.

Théorème 56 (**Krull** -1929)**.** *Tout anneau non nul possède au moins un idéal maximal.*

Preuve. Admise. □

Proposition 40. *Soient A un anneau et I un idéal de A. Désignons par $\pi : A \longrightarrow A/I$ la surjection canonique. La bijection donné par π^{-1} entre idéaux de A/I et idéaux de A contenant I induit des bijections entre :*

- *idéaux premiers de A/I et idéaux premiers de A contenant I ;*

- *idéaux maximaux de A/I et idéaux maximaux de A contenant I.*

Preuve. Soit J un idéal de A contenant I. Il faut montrer que J est premier (resp. maximal) si et seulement si J/I l'est. Comme I et J sont des sous-groupes distingués de $(A,+)$, alors d'après le troisième théorème d'isomorphisme on a : $A/J \simeq (A/I)/(J/I)$. En vertu des critères donnés par les théorèmes 54 et 55 sur l'anneau quotient pour qu'un idéal soit premier (resp. maximal), l'idéal J/I est premier (resp. maximal) dans A/I si et seulement si l'idéal J est premier (resp. maximal) dans A. □

Corollaire 13. *Tout idéal $I \neq A$ d'un anneau A est contenu dans un idéal maximal M de A.*

Preuve. Comme $I \neq A$, alors l'anneau A/I est non nul et possède donc un idéal maximal. D'après la proposition précédente 40, celui-ci est de la forme M/I où M est un idéal maximal de A contenant I. □

Corollaire 14. *Soit A un anneau untaire. Un élément $a \in A$ est inversible si et seulement s'il n'appartient à aucun idéal maximal de A.*

Preuve. Supposons que a est un élément inversible de A, alors il existe $b \in A$ tel que $ab = 1$, donc $1 = ab \in \langle a \rangle$. Ce qui entraîne que $\langle a \rangle = A$. D'où a n'appartient à aucun idéal maximal de A.

Réciproquement, supposons qu'un élément $a \in A$ n'appartient à aucun idéal maximal de A, alors montrons que a est inversible. Si a n'est pas inversible, alors $\langle a \rangle \neq A$. D'après le corollaire 13, l'idéal $\langle a \rangle$ est contenu dans un idéal maximal M de A, ce qui est absurde. □

Définition 62. Un anneau A est dit **local** s'il admet un seul idéal maximal.

4.10. **Divisibilité dans un anneau intègre.**
Examinons maintenant la relation de divisibilité dans un anneau commutatif ; à partir de maintenant, on préférera se limiter à un **anneau commutatif intègre** A : certaines notions pourront être définies dans des anneaux plus généraux, mais elles ont moins d'intérêt et des propriétés différentes.

Définition 63. Soient a et b deux éléments d'un anneau intègre A, on dit que a divise b ou que b est un multiple de a, et on note $a|b$, s'il existe $c \in A, b = ac$.

Proposition 41. *Soient a et b deux éléments d'un anneau intègre A. On a :*

$$a|b \Leftrightarrow b \in \langle a \rangle = aA \Leftrightarrow \langle b \rangle \subset \langle a \rangle.$$

Preuve. On a $a|b \iff \exists c \in A;\ b = ac \Leftrightarrow b \in \langle a\rangle = aA \iff \langle b\rangle \subset \langle a\rangle$. □

Remarque 40. Par la proposition 41, la relation de divisibilité $a|b$ est équivalente à la relation d'ordre $\langle b\rangle \subset \langle a\rangle$, elle a donc les propriétés suivantes, en supposant que A est unitaire :
- tout $a \in A$, a est multiple de 1.
- $\forall a \in A; a|a$;
- pour a, b et c dans A, si $a|b$ et $b|c$, alors $a|c$.

Par contre, si $a|b$ et $b|a$, on ne peut pas conclure que $a = b$, mais on a le résultat suivant.

Proposition 42. *Soient a et b deux éléments d'un anneau A. Les propriétés suivantes sont équivalentes :*

1. $\langle b\rangle = \langle a\rangle$,
2. $a|b$ *et* $b|a$,
3. *il existe une unité ε (élément inversible) de A tel que $b = a\varepsilon$.*

Preuve. Si a et b sont deux générateurs d'un idéal principal I non nul, on a d'après la propriété précédente $a|b$ et $b|a$. Donc il existe c et d tels que $b = ac$ et $a = bd$. Donc $bd = acd$, d'où $a = acd$. I étant supposé non nul, a est régulier et $cd = 1$. Donc c (ainsi que d) est inversible. Donc il existe $\varepsilon = c$ inversible dans A tel que $b = a\varepsilon$.

Réciproquement, si, pour a et b non nuls, il existe ε inversible dans A tel que $b = a\varepsilon$, on a : $b = a\varepsilon$ et $a = b\varepsilon^{-1}$, donc $a|b$ et $b|a$ et les idéaux engendrés par a et b respectivement sont égaux. Ceci est encore vrai pour a ou b nul. □

Définition 64. Soient a et b deux éléments d'un anneau intègre A, on dit que a et b sont **associés** s'il existe une unité ε de A (c-à-d ε un élément inversible de A) telle que $b = a\varepsilon$, i.e. $\langle b\rangle = \langle a\rangle$.

Remarque 41. Dans $\mathbb{Z}$, les associés d'un entier n sont n et $-n$, car $n = 1.n$ et $n = (-1).(-n)$. Dans $K[X]$, les associés d'un polynôme P sont εP, où ε est une unité de K (ne pas oublier que $U_K = K^*$).

Remarque 42. La relation "être associé" est une relation d'équivalence sur A, les classes d'équivalences de cette relation sont appelés **les classes d'éléments associés**.

Vu la Proposition 41, on peut généraliser la définition de divisibilité aux idéaux aussi comme suit :

Définition 65. On dit qu'un idéal I divise un idéal J si $J \subset I$.

Remarque 43. Désignons par $\mathcal{P}$ l'ensemble des idéaux d'un anneau intègre unitaire A. Dans $\mathcal{P}$, la relation un idéal I divise un idéal J est une relation d'ordre (opposée à l'inclusion).

Définition 66. Soient A un anneau intègre et p un élément non nul de A non inversible.

1. On dit que p est premier si pour tous a, b de A, $p|ab \Longrightarrow p|a$ ou $p|b$.
2. On dit que p est irréductible si ses seuls diviseurs sont les inversibles et ses associés. Autrement dit, dés que l'on écrit $p = ab$, alors ou bien a est inversible, ou bien b est inversible.

Exemples 16. Soit k est un corps.

1. Un nombre premier de $\mathbb{Z}$ est un élément premier de l'anneau $\mathbb{Z}$.
2. Dans l'anneau $k[X]$ un polynôme irréductible est un polynôme de degré ≥ 1 et ne s'écrit pas comme produit de deux polynômes de degrés ≥ 1.
3. Dans l'anneau $k[X]$ un polynôme ayant une racine dans k est irréductible ssi il est de degré 1.
4. Dans l'anneau $k[X]$ un polynôme de degré 2 ou 3 est irréductible ssi il n'a pas de racine dans k.
5. Dans l'anneau $\mathbb{C}[X]$ les polynômes irréductibles sont ceux de degré 1.
6. Dans l'anneau $\mathbb{R}[X]$ les polynômes irréductibles sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle.

Remarque 44. Soit a un élément non nul et non inversible d'un anneau A, alors a est irréductible si et seulement si $\langle a\rangle$ est maximal dans l'ensemble des idéaux principaux différents de A. En effet, supposons a irréductible ; soit $\langle b\rangle$ tel que $\langle a\rangle \subset \langle b\rangle$. Alors $b|a$. Comme a est irréductible, alors soit b est une unité, soit b est associé à a. Dans le premier cas $\langle b\rangle = A$, dans le second $\langle a\rangle = \langle b\rangle$.

Réciproquement, si $\langle a\rangle$ est maximal, alors pour $b|a$, on a $\langle a\rangle \subset \langle b\rangle$. Ceci implique $\langle b\rangle = A$ ou $\langle a\rangle = \langle b\rangle$, d'où le résultat.

Proposition 43. *Dans un anneau intègre unitaire A, tout élément premier est irréductible.*

Preuve. Soit p un élément premier de A. Soit $a \in A$ et $a|p$, alors il existe $b \in A$ tel que $p = ab$, d'où $p|ab$, ce qui implique que $p|a$ ou $p|b$.
- Si $p|a$, alors a et p sont associés, car $a|p$.
- Si $p|b$, alors $b = cp$, d'où $p = acp$. Ceci implique que a est inversible. □

Remarque 45. La réciproque de cette proposition n'est pas toujours vraie. Dans l'anneau

$$\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$$

l'élément 2 est irréductible mais n'est pas premier, car 2 divise $(2+\sqrt{10})(2-\sqrt{10}) = -6$ et 2 ne divise ni $2 + \sqrt{10}$ ni $2 - \sqrt{10}$.

Proposition 44. *Soient A un anneau intègre et $a \in A$. Les propriétés suivantes sont équivalentes :*

1. *l'idéal $\langle a \rangle$ est premier.*
2. *l'élément a est premier.*

Preuve. Si $\langle a \rangle$ est premier, alors pour tous x, y dans A on a :

$$\begin{aligned} a|xy &\implies xy \in \langle a \rangle \\ &\implies x \in \langle a \rangle \text{ ou } y \in \langle a \rangle \\ &\implies a|x \text{ ou } a|y \\ &\implies a \text{ est un élément premier de A.} \end{aligned}$$

Si a est premier, alors pour tous x, y dans A on a :

$$\begin{aligned} xy \in \langle a \rangle &\implies a|xy \\ &\implies a|x \text{ ou } a|y \\ &\implies x \in \langle a \rangle \text{ ou } y \in \langle a \rangle \\ &\implies \langle a \rangle \text{ est premier.} \end{aligned}$$

□

4.11. **PGCD et PPCM.**

Définition 67. Soient A un anneau intègre, a et b deux éléments de A. Un élément δ de A est appelé **plus grand commun diviseur** (pgcd) de a et b si :

1. $\delta|a$ et $\delta|b$,
2. si $d|a$ et $d|b$, alors $d|\delta$, i.e. tout diviseur commun de a et b est un diviseur de δ.

Autrement dit, δ est un pgcd de a et b si et seulement si $\langle \delta \rangle$ est le plus petit idéal principal contenant a et b, c-à-d contenant l'idéal $\langle a \rangle + \langle b \rangle$.
δ est noté $\text{pgcd}(a, b)$ ou simplement $\delta = a \wedge b$, et on a : $\delta = a \wedge b \Leftrightarrow \langle \delta \rangle = \langle a \rangle + \langle b \rangle$.

Remarques 22.

1. En général, deux éléments d'un anneau intègre n'ont pas nécessairement un pgcd.

2. Si a et b (éléments d'un anneau intègre A) admettent d comme pgcd , alors d est unique à un facteur inversible près, c-à-d, tous les associés de d sont aussi des pgcds de a et b.

   En effet, si d est un pgcd de a et b et $\delta \in A$ tel que d est associé à δ, alors δ est aussi un pgcd de a et b. En effet, puisque $\delta|a$ et $\delta|b$, car $\delta|d$ et $d|a$ et $d|b$; si $d'|a$ et $d'|b$, alors $d'|\delta$, car $d'|d$ et $d|\delta$.

   D'autre part si d et δ sont des pgcds de a et b, alors d et δ sont associés, car $d|\delta$ et $\delta|d$.
3. Si a, b et c sont des éléments de A, alors $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ (si ces pgcd existent) et ainsi un pgcd des éléments a, b et c, noté $a \wedge b \wedge c$, n'est autre que $(a \wedge b) \wedge c$ (ou $a \wedge (b \wedge c)$). De la même manière, on définit un pgcd d'un nombre fini d'éléments de A.

Définition 68. On dit que deux éléments a et b d'un anneau intègre unitaire A sont premiers entre eux (ou étrangers) s'ils ont un pgcd associé à 1, i.e. $\text{pgcd}(a, b) = 1$.

Définition 69. Un élément m de A est appelé **plus petit commun multiple** de a et b si :

1. $a|m$ et $b|m$, c-à-d m est multiples commun à a et b,
2. Si $a|d$ et $b|d$, alors $m|d$, c-à-d m divise tous les multiples communs à a et b.

Autrement dit, m est un ppcm de a et b si et seulement si $\langle m \rangle$ est le plus grand idéal principal contenu dans $\langle a \rangle$ et $\langle b \rangle$ à la fois (donc dans $\langle a \rangle \cap \langle b \rangle$).
m est noté $m = \text{ppcm}(a, b)$ ou simplement $m = a \vee b$ et on a $\langle m \rangle = \langle a \rangle \cap \langle b \rangle$,

Remarques 23.

1. En général, deux éléments d'un anneau intègre A n'ont pas nécessairement un ppcm.
2. Si a et b (éléments d'un anneau intègre A) admettent m comme ppcm, alors m est unique à un facteur inversible près, c-à-d, tous les associés de m sont aussi des ppcms de a et b.

   En effet, si m est ppcm de a et b et $m' \in A$ tel que m est associé à m', alors m' est aussi un ppcm de a et b (puisque d'une part $a|m'$ et $b|m'$, car $m|m'$ et $a|m$ et $b|m$; d'autre part, si $a|d$ et $b|d$, alors $m'|d$, car $m'|m$ et $m|d$).

   D'autre part si m et m' sont des ppcms de a et b, alors m et m' sont associés (car $m|m'$ et $m'|m$).
3. Si a, b et c sont des éléments de A, alors $a \vee (b \vee c) = (a \vee b) \vee c$ (si ces ppcms existent) et ainsi un ppcm des éléments a, b et c, noté $a \wedge b \wedge c$, n'est autre que $(a \vee b) \vee c$ (ou

$a \vee (b \vee c)$). De la même manière, on définit un ppcm d'un nombre fini d'éléments de A.

4.12. **Les anneaux principaux.**
On va étudier, dans cette section, une classe d'anneaux qui est particulièrement importante, celle des anneaux principaux. Rappelons qu'un idéal I d'un anneau A est dit principal s'il est engendré par un seul élément, c-à-d, I est de la forme aA, où a est un élément de A, qu'on note $\langle a \rangle$. Rappelons aussi la définition d'un anneau principal.

Définition 70. Un anneau principal A est un anneau commutatif intègre dont tous les idéaux sont principaux.

Comme exemples des anneaux principaux, je cite $\mathbb{Z}$, $\mathbb{Z}[i]$ et $k[X]$ l'anneau des polynômes à coefficients dans un corps. Dans toute cette section, les anneaux considérés sont principaux.

Proposition 45. *Soient A un anneau principal et $a \in A$. Les conditions suivantes sont équivalentes :*

1. *l'élément a est irréductible.*
2. *l'idéal $\langle a \rangle$ est maximal.*
3. *l'élément a est premier* (*l'idéal $\langle a \rangle$ est premier*).

Preuve. 1. $\Rightarrow$ 2. Supposons que a est irréductible, soit J un idéal de A tel que $\langle a \rangle \subset J$. Comme A est principal, alors $J = \langle x \rangle$ où $x \in A$. Donc $\langle a \rangle \subset \langle x \rangle$, d'où x divise a. Or a est irréductible, alors ses seules diviseurs sont les inversibles et ses associés, d'où x est une unité ou un associé à a ; par suite $\langle a \rangle = \langle x \rangle$ ou $\langle x \rangle = A$.
2. $\Rightarrow$ 3. Comme $\langle a \rangle$ est maximal, alors il est premier, donc a est premier.
Les autres implications sont déjà vues. □

Corollaire 15. *Dans un anneau principal, un idéal non nul est premier ssi il est maximal.*

Remarque 46. Dans un anneau principal, les notions d'éléments premiers et d'éléments irréductibles coincident.

Lemme 8. *Dans un anneau principal A, toute suite croissante d'idéaux est stationnaire, i.e. si $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$, alors il existe n tel que $m \geq n \Longrightarrow I_n = I_m$.*
Tout anneau A qui vérifie cette condition est dit **anneau noethérien**.

Preuve. Posons $I = \bigcup_n I_n$, donc I est un idéal. En effet,
- I est non nul,
- soient x et y dans I, alors il existe n et n' tels que $x \in I_n$ et $y \in I_{n'}$; donc pour $m = \max(n, n')$ on a $x, y \in I_m$. D'où $x + y \in I_m \subset I$.
- Soient $a \in I$ et $x \in A$, il existe alors $n \in \mathbb{N}$ tel que $a \in I_n$, donc $xa \in I_n$, d'où $xa \in I$.

Comme I est un idéal et A est un anneau principal, il existe alors $\alpha \in A$ tel que $I = \langle \alpha \rangle$. D'où il existe n tel que $\alpha \in I_n$, alors $I \subset I_n$. On a donc

$$m > n \Longrightarrow I_n \subset I_m \subset I \subset I_n,$$

donc $I_n = I_m$ pour tout $m > n$. □

Lemme 9. *Dans un anneau principal, tout élément non inversible possède un diviseur irréductible (premier).*

Preuve. Soit $a \in A$ et supposons que A est principal.
- Si a est irréductible c'est fini.
- Si a n'est pas irréductible, alors il existe a_1 un diviseur propre de a, $a = d_1 a_1$.
- De même si a_1 est irréductible c'est fini, sinon il existe a_2 un diviseur propre de a_1, $a_1 = d_2 a_2$. Ainsi de proche en proche, on construit une suite d'éléments :

$$a_0 = a = d_1 a_1,\ a_1 = d_2 a_2,\ a_2 = a_3 d_3,\ \cdots,\ a_{n-1} = a_n d_n.$$

De plus la suite d'idéaux $(\langle a_n \rangle)_n$ est croissante :

$$\langle a_0 \rangle = \langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots \subset \langle a_{n-1} \rangle \subset \langle a_n \rangle \subset \cdots \subset.$$

D'après le Lemme 8 précédent, la suite $(\langle a_n \rangle)_n$ est stationnaire, donc il existe un entier p tel que $\langle a_m \rangle = \langle a_p \rangle$ pour tout $m > p$. Alors a_p est irréductible, sinon il existera a_{p+1} un diviseur propre de a_p tel que $a_p = d_{p+1} a_{p+1}$ et $\langle a_p \rangle \subsetneq \langle a_{p+1} \rangle$, ce qui contredit le fait que $\langle a_m \rangle = \langle a_p \rangle$ si $m > p$. □

Proposition 46. *Soient a et b deux éléments d'un anneau principal A. Alors a et b admettent toujours un pgcd et un ppcm et on a :*

1. *$a \wedge b = d$ si, et seulement, si $\langle a \rangle + \langle b \rangle = \langle d \rangle$.*
2. *$a \vee b = m$ si, et seulement, si $\langle a \rangle \cap \langle b \rangle = \langle m \rangle$.*

Preuve. Soient a et b deux éléments de A. Puisque A est principal, l'idéal $\langle a \rangle + \langle b \rangle$ est principal et ainsi $\exists d \in A : \langle a \rangle + \langle b \rangle = \langle d \rangle$. On a $d = \text{pgcd}(a, b)$. En effet, $d|a$ et $d|b$, car $\langle a \rangle \subset \langle a \rangle + \langle b \rangle = \langle d \rangle$ et $\langle b \rangle \subset \langle a \rangle + \langle b \rangle = \langle d \rangle$. D'autre part, si $c|a$ et $c|b$, alors $\langle a \rangle \subset \langle c \rangle$

et $\langle b\rangle \subset \langle c\rangle$ d'où $\langle a\rangle + \langle b\rangle = \langle d\rangle \subset \langle c\rangle$, alors $c|d$. Ainsi, si $\langle a\rangle + \langle b\rangle = \langle d\rangle$, d est un pgcd de a et b.

Réciproquement, si $a \wedge b = d$, alors $\langle a\rangle \subset \langle d\rangle$, car $d|a$, et $\langle b\rangle \subset \langle d\rangle$, car $d|b$, d'où $\langle a\rangle + \langle b\rangle \subset \langle d\rangle$. D'autre part, l'idéal $\langle a\rangle + \langle b\rangle$ est un idéal principal (car A est principal) d'où $\exists c \in A$ tel que $\langle a\rangle + \langle b\rangle = \langle c\rangle$, alors $c|a$ (car $\langle a\rangle \subset \langle a\rangle + \langle b\rangle = \langle c\rangle$) et $c|b$ (car $\langle b\rangle \subset \langle a\rangle + \langle b\rangle = \langle c\rangle$) d'où, par définition de d, $c|d$ et ainsi $\langle d\rangle \subset \langle c\rangle = \langle a\rangle + \langle b\rangle$.

De même, on montre l'existence du ppcm et 2. □

Théorème 57 (Théorème de Bezout).
Soient a et b deux éléments d'un anneau principal A.

1. *Si $d = \text{pgcd}(a, b)$, alors il existe u et v dans A tels que $d = au + bv$.*
2. *a et b sont premiers entre eux si, et seulement si, il existe deux éléments u et v de A, tels que $au + bv = 1$.*

Preuve. En utilisant la proposition précédente on a :
1. $d = \text{pgcd}(a, b)$ si, et seulement si, $\langle a\rangle + \langle b\rangle = \langle d\rangle$, donc il existe u et v dans A tels que $d = au + bv$.
2. a et b sont premiers entre eux si, et seulement si, $\langle a\rangle + \langle b\rangle = \langle 1\rangle = A$ si, et seulement si, $\exists u, v \in A : 1 = ua + vb$. □

Proposition 47. *Soient a, b et c des éléments non nuls d'un anneau principal A.*

1. *$a \wedge b = 1$ et $a \wedge c = 1$ si et seulement si $a \wedge bc = 1$.*
2. *Si $a|bc$ et $a \wedge b = 1$, alors $a|c$ (Lemme de Gauss).*
3. *Si $a \wedge b = 1$, alors tout pgcd de a et c est aussi un pgcd de a et bc.*
4. *Si $b|a$ et $c|a$ et $b \wedge c = 1$, alors $bc|a$.*

Preuve. 1. Comme $a \wedge b = 1$ et $a \wedge c = 1$, alors il existe u, v, u' et v' dans A tels que $au + bv = 1$ et $au' + cv' = 1$. En faisant la multiplication, on obtient $a^2uu' + acuv' + bvau' + bvcv' = 1 \iff a(auu' + cuv' + bvu') + bcvv' = 1$, donc $au'' + bcv'' = 1$, d'où $a \wedge bc = 1$.
2. Puisque $a \wedge b = 1$, $\exists u, v \in A : ua + vb = 1$. En multipliant les deux membres de cette égalité par c, on obtient $c = uac + v(bc)$ et comme $bc = ad$, où $d \in A$ (car $a|bc$), on a $c = a(uc + vd)$ et ainsi $a|c$.
3. Soit $d = a \wedge c$, alors $d|a$ et $d|c$, d'où $d|a$ et $d|bc$, ceci implique que d divise $a \wedge bc$. Soit ℓ un diviseur commun de a et bc, comme $a \wedge b = 1$ et $\ell|a$, alors $\ell \wedge b = 1$, par suite $\ell|a$ et $\ell|c$, d'où $\ell|d$. Conclusion d est le pgcd de a et bc.

4. On a $b|a$ et $c|a$, donc $a = be$ et $a = cf$. Comme $b \wedge c = 1$, alors il existe u, v dans A tels que $bu + cv = 1$, d'où $a = abu + acv = cfbu + becv = bc(fu + ev)$, donc bc divise a. □

Proposition 48. *Dans un anneau principal A, si un élément premier divise un produit, alors il divise l'un des facteurs.*

Preuve. Par récurrence. □

Définition 71. Soit A un anneau intègre. On dit qu'un élément non nul $a \in A$ admet une factorisation en produit de facteurs irréductibles si a s'écrit

$$a = \mu p_1 p_2 \cdots p_m, \text{ où } \mu \in A^\times \text{ et } p_i \text{ est irréductible } \forall 1 \leq i \leq m.$$

Cette décomposition est dite unique si chaque fois que $a = \nu q_1 q_2 \cdots q_n$, où $\nu \in A^\times$, alors $n = m$ et il existe une permutation $\sigma \in S_n$ tel que p_j est associé à $q_{\sigma(j)}$ pour tout j tel que $1 \leq j \leq m$.

Théorème 58. *Dans un anneau principal A, tout élément non nul $x \in A$ admet une décomposition en facteurs irréductibles, i.e. x s'écrit sous la forme*

$$x = \mu p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}, \text{ où } \mu \in A^\times \text{ et } p_i \text{ est irréductible et } p_i \neq p_j \text{ si } i \neq j.$$

De plus si $x = \nu q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$, alors $k = n$, p_i, q_i sont associés pour tout i et $\mu = \nu$.

Preuve. Soit $x \in A$ et supposons que $x \neq 0$ et A est principal.
D'après le Lemme 9, on sait qu'il existe $p_1 \in A$ irréductible tel que $x = p_1 x_1$; si x_1 est irréductible c'est fini ; sinon $x_1 = p_2 a_2$. Ainsi on construit une chaîne d'idéaux croissante

$$\langle x_0 \rangle = \langle x \rangle \subset \langle x_1 \rangle \subset \langle x_2 \rangle \subset \cdots \subset \langle x_{n-1} \rangle \subset \langle x_n \rangle \subset \cdots \subset.$$

D'après le Lemme 8 la suite $(\langle x_n \rangle)_n$ est stationnaire, donc il existe un entier p tel que $\langle a_m \rangle = \langle a_p \rangle$ si $m > p$. Alors a_p est irréductible. D'où le résultat.

Si $\mu p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} = \nu q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$, alors chaque p_i est associé à un q_i, et par simplification on obtient que $\mu = \nu$. □

Définition 72. Un anneau intègre A est dit **factoriel** si tout élément non nul et non inversible de A admet une unique décomposition en produit d'éléments irréductibles.

Remarque 47. Tout anneau principal est factoriel, mais la réciproque n'est pas vraie. Comme contre exemple : un anneau de polynômes à coefficients dans un anneau factoriel A est toujours factoriel lui aussi, mais n'est principal que si l'anneau A est un corps.

Exemple 14. L'anneau $\mathbb{Z}$ est factoriel. L'anneau $K[X]$, où K est un corps, est factoriel.

Définition 73. Soit A anneau intègre, notons $A^* = A - \{0\}$. On dit que A est **euclidien** s'il est menu d'une division euclidienne, c-à-d, il existe une application $f : A^* \longrightarrow \mathbb{N}$ vérifiant la condition suivante :

$\forall\ a, b$ dans A, $b \neq 0$, il existe $(q, r) \in A^2$ tel que $a = bq + r$ et ($r = 0$ ou $f(r) < f(b)$).

L'application f est dite **un stathme euclidien** sur A.

Exemples 17.

i. L'anneau des entiers relatifs $\mathbb{Z}$ est euclidien pour le stathme $f(x) = |x|$ (la valeur absolue),

ii. L'anneau $K[X]$ des polynômes en une indéterminée à coefficients dans un corps commutatif K est euclidien pour le stathme $f(P) = \deg(P)$, le degré de P.

iii. L'anneau $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ des entiers de Gauss est euclidien, avec f est définie, pour tout $z = a + ib \in \mathbb{Z}[i]$, par $f(z) = z\overline{z} = |z|^2 = a^2 + b^2$.

Théorème 59. *Un anneau euclidien est principal.*

Preuve. Soit A un anneau euclidien pour une application (le stathme) $f : A^* \longrightarrow \mathbb{N}$. Soit I un idéal non nul de A. Soit b un élément non nul de I tel que $f(b)$ soit minimal (b existe car $\{f(b) \mid b \in I\}$ est une partie non vide de $\mathbb{N}^*$). Pour $a \in I$, considérons une division euclidienne $a = bq + r$ de a par b, si $r \neq 0$, alors on aura $f(r) < f(b)$, or $r = a - bq \in I$, ceci contredit la minimalité de $f(b)$. Par suite, $r = 0$ et $a \in \langle b \rangle$, d'où $I = \langle b \rangle$. □

Remarque 48. Il existe des anneaux principaux qui ne sont pas euclidiens pour aucune application f (voir par exemple le livre de Daniel Perrin ([8]) pages : 53 –55).

Dans un anneau euclidien on a un algorithme d'Euclide pour calculer le pgcd exactement comme dans le cas de $\mathbb{Z}$. On peut aussi l'utiliser pour calculer les coefficients de la formule de Bézout. En se basant sur le lemme suivant.

Lemme 10. *Soient x et y dans A, où A est un anneau principal. Soit $x = yq + r$ la division euclidienne de x par y. Alors le pgcd de x et y est égal au pgcd de y et r si $r \neq 0$, à y sinon.*

Preuve. La preuve est laissée au lecteur. □

Soient A un anneau principal, a et b deux éléments non nuls et non inversibles de A. On note $\mathcal{P}$ un ensemble d'éléments irréductibles de A tel que si p est irréductible dans

A, alors p est associé à un, et un seul, élément de $\mathcal{P}$. Comme A est principal, a et b se décomposent en produit d'éléments de $\mathcal{P}$:

$$a = \mu p_1^{\alpha_1} \cdots p_r^{\alpha_r} \qquad \text{et} \qquad b = \nu p_1^{\beta_1} \cdots p_r^{\beta_r},$$
$$\text{où } \mu, \nu \in A^\times, \text{ et } p_i \in \mathcal{P},\ p_i \neq p_j \text{ si } i \neq j,\ \alpha_i \geq 0,\ \beta_i \geq 0$$

(les décompositions de a et b contiennent les mêmes éléments de $\mathcal{P}$ quitte à ce que certains d'entre eux aient des exposants nuls).

Théorème 60. *Gardons les notations ci-dessus.*

1. $a|b$ *si, et seulement si,* $\alpha_i \leq \beta_i$ *pour tout* $i \in \{1, \cdots, r\}$.
2. $a \wedge b = p_1^{\lambda_1} \cdots p_r^{\lambda_r}$, *où* $\lambda_i = \min(\alpha_i, \beta_i)$ *pour tout* $i \in \{1, \cdots, r\}$.
3. $a \vee b = p_1^{\mu_1} \cdots p_r^{\mu_r}$, *où* $\mu_i = \max(\alpha_i, \beta_i)$ *pour tout* $i \in \{1, \cdots, r\}$.

Preuve. 1. Il est évident que si $\alpha_i \leq \beta_i$ pour tout $i \in \{1, \cdots, r\}$ alors $a|b$.
Réciproquement, supposons que $a|b$, alors $b = ac$. On distingue les deux cas suivants :
- $c \in U_A$, alors, en utilisant la définition de $\mathcal{P}$, $c = 1$ et ainsi $\alpha_i = \beta_i$.
- $c \notin U_A$, d'où c se décompose en produit d'éléments de $\mathcal{P}$ et puisque $b = ac$, alors $\alpha_i \leq \beta_i$ pour tout $i \in \{1, \cdots, r\}$. Les assertions 2. et 3. découlent de 1. □

Remarque 49. Si $a = 0$ (resp. $b = 0$), alors b (resp. a) est un pgcd de a et b. Aussi, si $a \in U_A$ ou $b \in U_A$, alors 1 est un pgcd de a et b.

Corollaire 16. *Soient a et b deux éléments d'un anneau principal A. Alors*

$$\text{pgcd}(a, b) \cdot \text{ppcm}(a, b) = ab.$$

Corollaire 17. *Si A est un anneau principal et a, b des éléments premiers entre eux, alors* $\text{ppcm}(a, b) = ab$.

Théorème 61 (Théorème des restes chinois). *Si A est un anneau principal et a_1, $\cdots$, a_n des éléments premiers entre eux deux à deux, alors*

$$A/\langle a_1 a_2 \cdots a_n \rangle \simeq A/\langle a_1 \rangle \times A/\langle a_2 \rangle \times \cdots \times A/\langle a_n \rangle.$$

Preuve. Voir Théorème 53 et Corollaire 11. □

4.13. **Exercices.**

1. i. Montrer que $\mathbb{Z}[i] = \{a + ib \mid (a, b) \in \mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{C}$.
   ii. Montrer que $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{Q}$.
2. Dans un anneau A, on suppose que $\forall\ x \in A$, $x^2 = x$. Montrer que A est commutatif. Si A contient au moins 3 éléments distincts montrer qu'il a nécessairement des diviseurs de zéro. Montrer qu'en fait A ne peut avoir exactement 3 éléments.
3. Soit A un anneau unitaire. Un élément e de A est dit un **idempotent** si $e^2 = e$.
   i. Montrer que si $e \in A$ est un idempotent, alors $1 - e$ l'est aussi.
   ii. Montrer que si $e \in A$ est un idempotent, alors $eA = \{ea \mid a \in \mathbb{Z}\}$ est un sous-anneau de A.
   iii. Montrer que si $e \in A$ est un idempotent, alors $A \simeq eA \times (1 - e)A$.
4. Soit A un anneau commutatif dont la caractéristique est un nombre premier p.
   i. Montrer que pour tous $x, y \in A$ on a : $(x + y)^p = x^p + y^p$.
   ii. Montrer que pour tous $x, y \in A$ et $n \in \mathbb{N}^*$ on a : $(x + y)^{p^n} = x^{p^n} + y^{p^n}$.
5. Soient m et n deux entiers naturels non nuls premiers entre eux. Montrer que $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
6. Répondre aux questions suivantes.
   i. Montrer que $\mathbb{Q}[i] = \{a + ib; (a; b) \in \mathbb{Q}^2\}$ est un sous-corps de $\mathbb{C}$.
   ii. Montrer que $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{R}$.
   iii. Soit $d \in \mathbb{N}$ qui ne soit pas un carré d'entier. Montrer que $\mathbb{Z}[\sqrt{d}] = \{a+b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{R}$.
7. Montrer qu'un anneau fini intègre A est un corps.
8. Considérons un un homomorphisme d'anneaux $f : A \longrightarrow B$. Montrer que si a est une unité de A, alors $f(a)$ est une unité de B. En déduire que la restriction de f à U_A définit un homomorphisme de groupes (noté encore f) $U_A \longrightarrow U_B$.
9. Soit $d \in \mathbb{N}$.
   i. Montrer que $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{R}$.
   ii. Quels sont les sous-corps de $\mathbb{Q}[\sqrt{d}]$?
10. Soit A un anneau unitaire non nul tel que : $\forall\ x \in A$, $x^2 = x$.
    i. Donner un exemple d'un tel anneau.
    ii. Quels sont les éléments inversibles de A ?
    iii. Montrer que : $\forall\ x \in A$, $x + x = 0$. En déduire que A est commutatif.
    iv. Pour x,$y \in A$ on pose : $x \leq y \iff \exists\ a \in A$ tq $x = ay$. Montrer que c'est une relation d'ordre.

Solution.

i. $\mathbb{Z}/2\mathbb{Z}$.

ii. Si x est inversible, alors $x^{-1} \cdot x^2 = x^{-1} \cdot x = 1$, donc $x = 1$.

iii. $x + y = (x + y)^2 = x^2 + y^2 + xy + yx = x + y + xy + yx$, donc $xy + yx = 0$. Si on prend $y = 1$: $x + x = 0$, ainsi $1 = -1$. Pour y quelconque : $xy = -yx = yx$.

iv. Laisser au lecteurs.

11. Soit E un ensemble non vide. Montrer que $(\mathcal{P}(E), \triangle, \cap)$ est un anneau non intègre.
12. Soit $p \in \mathbb{N}^*$ un entier sans facteur carré. Considérons l'ensemble

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

    i. Montrer que $\mathbb{Z}[i\sqrt{p}]$ est un anneau commutatif unitaire et intègre.

    ii. Montrer que $\mathbb{Z}[i\sqrt{p}]$ est contenu dans tout sous-anneau unitaire de $\mathbb{C}$ qui contient $i\sqrt{p}$, on dit que $\mathbb{Z}[i\sqrt{p}]$ est engendré par $i\sqrt{p}$.

    iii. Montrer que $\mathbb{Z}[i\sqrt{p}]$ est l'intersection de tous les sous-anneaux de $\mathbb{C}$ qui contiennent i.

    iv. Déterminer le groupe des unités de $\mathbb{Z}[i\sqrt{p}]$.

13. Soit A un anneau. Soient I un idéal de A et S une partie de A. Considérons l'ensemble $J = (I : S)$ défini par :

$$J = (I : S) = \{a \in A \mid \forall s \in S, as \in I\}.$$

    Montrer que J est un idéal de A, J est dit **le conducteur de S dans I**.

14. Soient A un anneau et I un idéal de A.

    i. Montrer que l'ensemble des éléments nilpotents de A est un idéal de A, cet ensemble est dit le **nilradical** de A, et est noté $\mathrm{Nil}(A)$.

    ii. Montrer que l'ensemble $\sqrt{I} = \{a \in A \mid$ il existe $n \in \mathbb{N}^*$, $a^n \in I\}$ est un idéal de A qui contient I. $\sqrt{I}$ est dit le **radical** de I.

    iii. Déduire que $\mathrm{Nil}(A) = \sqrt{\{0\}}$.

    iv. Quel est le radical de $\langle 12 \rangle$?

15. Montrer qu'un anneau intègre possédant un nombre fini d'idéaux est un corps. (Si $a \neq 0$, introduire les idéaux $\langle a^n \rangle$, pour $n \in \mathbb{N}^*$).
16. Soient K un corps et A un anneau non nul. Montrer que tout homomorphisme d'anneaux de K dans A est injectif.
17. Soient $\mathbb{Z}[\sqrt{2}]$ et $\mathbb{Z}[\sqrt{3}]$ les sous-anneaux de $\mathbb{C}$ engendrés par $\mathbb{Z}$ et $\sqrt{2}$ et $\sqrt{3}$ respectivement.

    1. Montrer que $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{N}\}$ et $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{N}\}$.

2. Montrer qu'il n'existe pas d'homomorphisme d'anneaux de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}[\sqrt{3}]$.

18. Soient I, J et L des idéaux d'un anneau A. Montrer les assertions suivantes :
    i. IJ est contenu dans $I \cap J$.
    ii. $IJ + IL = I(J + L)$.
    iii. $I \cap J + I \cap L$ est contenu dans $I \cap (J + L)$.
    iv. Si $J \subset I$, alors $J + I \cap L = I \cap (J + L)$.

19. Étant donné un idéal I d'un anneau A, on note $\sqrt{I}$ son radical. Soient I, J et L des idéaux d'un anneau A. Montrer les assertions suivantes :
    a. $I \subset J \Longrightarrow \sqrt{I} \subset \sqrt{J}$.
    b. $\sqrt{I.J} = \sqrt{I \cap J}$.
    c. $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
    d. $\sqrt{\sqrt{I}} = \sqrt{I}$.
    e. Si I est premier, alors $\sqrt{I} = I$.
    f. $\sqrt{I} + \sqrt{J} \subset \sqrt{I + J}$.
    g. $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.
    h. $\sqrt{(I \cap J) + (I \cap L)} = \sqrt{I \cap (J + L)}$.
    i. Soient $(\mathfrak{p}_i)_{1 \leq i \leq n}$ n idéaux premiers de A ; on suppose que I est contenu dans l'intersection des $\mathfrak{p}_i$ et cette intersection est contenu dans $\sqrt{I}$. Montrer que l'on a : $\sqrt{I} = \cap \mathfrak{p}_i$.

20. Supposons qu'un anneau A est produit fini d'anneaux A_i : $A = A_1 \times A_2 \times \cdots \times A_n$.
    i. Montrer que les idéaux de A sont de la forme $I_1 \times I_2 \times \cdots \times I_n$, où chaque I_i est un idéal de A_i.
    ii. Déterminer les idéaux premiers et maximaux de A.
    iii. Si les A_i sont des corps, montrer que A n'a qu'un nombre fini d'idéaux.

21. Soient I et J deux idéaux d'un anneau A. On suppose que $I + J = A$, montrer que $I^n + J^n = A$, $n \in \mathbb{N}^*$.

22. i. Soient A un anneau intègre, $a, b \in A$ tels que a et b admettent un ppcm, noté m, et $m' \in A$. Montrer que m' est un ppcm de a et b si, et seulement si, m et m' sont associés.
    ii. Soient $a, b \in A - \{0\}$. Montrer que si a et b possèdent un ppcm, noté m, dans A, alors il existe $d \in A : ab = md$ et que $d = a \wedge b$.

23. Soit l'anneau $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$.
    i. Déterminer $U_{\mathbb{Z}[i\sqrt{5}]}$.
    ii. Déterminer tous les diviseurs de 9 et de $3(2 + i\sqrt{5})$.

iii. Montrer que 1 est un pgcd de 3 et $2 + i\sqrt{5}$ et que 3 et $2 + i\sqrt{5}$ n'ont pas de ppcm. Conclure.

iv. Montrer que les éléments 9 et $3(2 + i\sqrt{5})$ n'ont pas de pgcd dans $\mathbb{Z}[i\sqrt{5}]$.

24. Soit $(A, +, \times)$ un anneau. On appelle centre de A l'ensemble $Z(A) = \{x \in A / \forall y \in A, xy = yx\}$. Montrer que $Z(A)$ est un sous-anneau de A.

25. Montrer que $\mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier, ne possède pas de sous-corps propre.

26. Soit K un corps commutatif.

    i. a. Montrer que l'intersection des sous-corps de K est un sous-corps de K. On l'appelle le sous-corps premier de K et on le note $P(K)$.

    b. Montrer que $P(K) = \{(n \cdot 1_K) \cdot (m \cdot 1_K)^{-1} \mid n, m \in \mathbb{Z} \text{ et } m \cdot 1_K \neq 0_K\}$.

    ii. On considère l'application $f : \mathbb{Z} \longrightarrow K$, $n \longmapsto n \cdot 1_K$.

    a. Vérifier que f est un homomorphisme d'anneaux.

    b. Montrer que si $car(K) = p$, où p est un nombre premier, alors $P(K) \simeq \mathbb{Z}/p\mathbb{Z}$.

    c. Montrer que si $carK = 0$, alors $P(K) \simeq \mathbb{Q}$.

5. Polynômes à plusieurs indéterminées

5.1. Polynômes à une indéterminée à coefficients dans un anneau.

L'idée de la construction sera peut-être bien comprit si on se demande comment stocker une fonction polynomiale de $\mathbb{R}$ dans $\mathbb{R}$ dans une mémoire d'un ordinateur :
stocker toutes les valeurs de la fonction est impossible, un bon procédé pour représenter, par exemple, la fonction

$$x \mapsto 4 + 8x + 5x^2 + 7x^3 + x^5,$$

sera de stocker la suite de ses coefficients ; on entrera donc dans l'ordinateur la suite 485701, ce qui indique que le coefficient de x^0 est 4, celui de x est 8, celui de x^2 est 5, etc.

Donc une fonction polynomiale est définie par ses coefficients.

Définition 74. Soit $(A, +)$ un groupe d'élément neutre 0.
Une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A est dite à support fini, ou bien nulle à partir d'un certain rang, si le nombre d'indices n pour les quels $a_n \neq 0$ est fini.
En d'autres termes, il existe un indice m fini tel que $a_n \neq 0$ implique $n \leqslant m$.

Exemples 18.

$$(a_n)_{n\in\mathbb{N}} = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, \dots) = (1, 0, 1, 1, 0, 1, 0, 0, \dots),$$
$$(b_n)_{n\in\mathbb{N}} = (b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7, \dots) = (1, 5, 9, 0, 0, 0, 0, 0, \dots).$$

Définition 75. Soit $(A, +, \cdot)$ un anneau commutatif. Notons par $\mathcal{P}$ l'ensemble des suites d'éléments de A à supports finis. On définit sur $\mathcal{P}$ une addition et une multiplication par les formules :

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}},$$

et

$$(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = (c_n)_{n\in\mathbb{N}} \qquad \text{où} \quad c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{n} a_{n-k} b_k = \sum_{k+t=n} a_k b_t.$$

Exemple 15.
Pour $(a_n)_{n\in\mathbb{N}} = (1, 0, 1, 1, 0, 1, 0, 0, 0, \dots)$ et $(b_n)_{n\in\mathbb{N}} = (1, 5, 9, 0, 0, 0, 0, 0, 0, \dots)$, on a :

$$(a_n + b_n)_{n\in\mathbb{N}} = (2, 5, 10, 1, 0, 1, 0, 0, \dots).$$
$$c_0 = \sum_{k=0}^{0} a_k b_{n-k} = a_0 b_0 = 1.1 = 1,$$

$$c_1 = \sum_{k=0}^{1} a_k b_{n-k} = a_0 b_1 + a_1 b_0 = 1.5 + 0.1 = 5,$$

$$c_2 = \sum_{k=0}^{2} a_k b_{n-k} = a_0 b_2 + a_1 b_1 + a_2 b_0 = 1.9 + 0.5 + 1.1 = 10,$$

$$c_3 = \sum_{k=0}^{3} a_k b_{n-k} = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 = 1.0 + 0.9 + 1.5 + 1.1 = 6,$$

$$c_4 = \sum_{k=0}^{4} a_k b_{n-k} = a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0 = 1.0 + 0.0 + 1.9 + 1.5 + 0.1 = 14,$$

$$c_5 = \sum_{k=0}^{5} a_k b_{n-k} = a_0 b_5 + a_1 b_4 + a_2 b_3 + a_3 b_2 + a_4 b_1 + a_5 b_0 =$$
$$1.0 + 0.0 + 1.0 + 1.9 + 0.5 + 1.1 = 10,$$

$$c_6 = \sum_{k=0}^{6} a_k b_{n-k} = a_0 b_6 + a_1 b_5 + a_2 b_4 + a_3 b_3 + a_4 b_2 + a_5 b_1 + a_6 b_0 =$$
$$1.0 + 0.0 + 1.0 + 1.0 + 0.9 + 1.5 + 0.1 = 5,$$

$$c_7 = \sum_{k=0}^{7} a_k b_{n-k} = 9,$$

$$c_8 = \sum_{k=0}^{8} a_k b_{n-k} = 0,$$

$$c_9 = \sum_{k=0}^{9} a_k b_{n-k} = 0,$$

etc.

Donc

$$(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = (c_n)_{n\in\mathbb{N}} = (1, 5, 10, 6, 14, 10, 5, 9, 0, 0, 0, \dots)$$

Proposition 49.
L'ensemble $\mathcal{P}$ muni des deux lois définies ci-dessus est un anneau commutatif unitaire.

Preuve. Il est facile de vérifier que $(\mathcal{P}, +)$ est un sous-groupe du groupe abélien (additif) de toutes les suites d'éléments de A.
- En effet, le neutre de A est la suite identiquement nulle, qui appartient à $\mathcal{P}$.
- La somme de deux suites à supports finis est une suite à support fini : si $a_n = 0$ pour tout $n > N$ et si $b_n = 0$ pour tout $n > M$, alors $a_n + b_n = 0$ pour tout $n > \max\{N, M\}$ (et peut-être pour d'autres indices n également mais ce n'est pas important).
- Enfin si $-a$ désigne l'opposé d'un élément a de A, alors l'opposé d'un élément $(a_n)_{n\in\mathbb{N}}$ de $\mathcal{P}$ est la suite $(-a_n)_{n\in\mathbb{N}}$, qui est effectivement à support fini.

Pour la deuxième loi, on doit tout d'abord vérifier que $(c_n)_{n\in\mathbb{N}}$ est bien une suite de $\mathcal{P}$. Avec les mêmes notations que pour l'addition, pour tout indice $n > M+N$, dans le calcul de

$$c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{N} a_k b_{n-k} + \sum_{k=N+1}^{n} a_k b_{n-k},$$

tous les termes de la première somme sont nuls, car les indices utilisés sont tels que $n-k > M+N-k \geqslant M$ donc $b_{n-k} = 0$. Tous les termes de la deuxième somme sont nuls aussi car $k > N$ donc $a_k = 0$. Tous les coefficients c_n pour $n > M+N$ sont donc nuls et $(c_n)_{n\in\mathbb{N}}$ est bien un élément de $\mathcal{P}$.

On va ensuite vérifier que pour ces formules, $\mathcal{P}$ est un anneau commutatif.

• Commutativité.

Soient $(a_i)_{i\in\mathbb{N}}$ et $(b_j)_{j\in\mathbb{N}}$ deux éléments de $\mathcal{P}$; notons $(c_k)_{k\in\mathbb{N}}$ le produit de $(a_i)_{i\in\mathbb{N}}$ par $(b_j)_{j\in\mathbb{N}}$. Alors pour tout $k \geqslant 0$, $c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{j=0}^{k} a_{k-j} b_j$ (en posant $j = k-i$) ; cette expression est bien celle qu'on trouverait en faisant le produit dans l'autre sens (en utilisant la commutativité de A).

• Associativité.

Soient $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ et $(c_n)_{n\in\mathbb{N}}$ trois éléments de $\mathcal{P}$; notons $(d_n)_{n\in\mathbb{N}}$ le produit de $(b_n)_{n\in\mathbb{N}}$ par $(c_n)_{n\in\mathbb{N}}$. Notons $(e_n)_{n\in\mathbb{N}}$ le produit de $(a_n)_{n\in\mathbb{N}}$ par $(d_n)_{n\in\mathbb{N}}$. Pour $n \geqslant 0$, calculons

$$e_n = \sum_{i=0}^{n} a_i d_{n-i} = \sum_{i=0}^{n} a_i \sum_{j=0}^{n-i} c_j b_{n-i-j} = \sum_{(i,j)} a_i b_{n-i-j} c_j,$$

où la dernière somme porte sur tous les couples $(i,j) \in \mathbb{N}^2$ tels que $i+j \leqslant n$. On trouverait la même chose en calculant de la même façon le produit de $(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}}$ par $(c_n)_{n\in\mathbb{N}}$.

• Existence d'un élément neutre.

La suite (1,0,0,0,...) est neutre pour cette multiplication.

• Distributivité.

C'est une vérification technique, fastidieuse et fatiguante, mais élémentaire, on va l'omettre.

On a bien vérifié que $\mathcal{P}$ est un anneau commutatif unitaire. □

Notations.

- On note 0 la suite nulle $0 = (0, 0, 0, 0, 0, \ldots)$.
- On appelle indéterminée l'élément $(0, 1, 0, 0, 0, \ldots)$ de $\mathcal{P}$ dont tous les termes sont nuls sauf le terme a_1 d'indice 1 qui vaut $a_1 = 1$. On note souvent X cette indéterminée, c'est-à-dire $X = (0, 1, 0, 0, 0, 0, \ldots)$.
- Avec cette définition, si n est un entier strictement positif, alors X^n est la suite nulle partout, sauf pour le terme d'indice n, qui vaut 1, d'après la règle de multiplication de l'anneau. Pour généraliser cette propriété, on définit la suite X^0 comme étant égal à la suite nulle partout, sauf pour l'indice 0 où elle vaut 1.

$$\begin{aligned} X^0 &= (1, 0, 0, 0, 0, \ldots), \\ X^1 &= (0, 1, 0, 0, 0, \ldots), \\ X^2 &= (0, 0, 1, 0, 0, \ldots), \\ X^3 &= (0, 0, 0, 1, 0, \ldots), \\ &\cdots\cdots \\ X^n &= (0, 0, 0, 0, \ldots, \overbrace{1}^{l'indice\ n}, 0, 0, \ldots). \end{aligned}$$

Ce qui permet de disposer de la règle :

$$\forall n, m \in \mathbb{N}; \quad X^n X^m = X^{n+m}.$$

- On a comme exemple la suite $(1, 0, 1, 1, 0, 1, 0, \ldots)$ s'écrit de la manière suivante :

$$\begin{aligned} (1, 0, 1, 1, 0, 1, 0, \ldots) &= (1, 0, \ldots) + (0, 0, 1, 0, \ldots) + (0, 0, 0, 1, 0, \ldots) + (0, 0, 0, 0, 0, 1, 0, \ldots) \\ &= X^0 + X^2 + X^3 + X^5. \end{aligned}$$

Dans le cas général, une suite égal à $(p_0, p_1, p_2, \ldots, p_n, 0, \ldots)$ s'écrit de manière équivalente :

$$(p_0, p_1, p_2, \ldots, p_n, 0, \ldots) = p_0 X^0 + p_1 X + p_2 X^2 + \cdots + p_n X^n.$$

Définition 76.
L'anneau $\mathcal{P}$ est noté $A[X]$ et est appelé l'anneau des polynômes à coefficients dans A.

Remarque 50. Si A est un anneau commutatif unitaire, alors $A[X]$ sera aussi un anneau commutatif unitaire.

Proposition 50. *Pour tout élément P de $A[X]$ tel que $P \neq 0$, il existe un unique entier $n \geqslant 0$ et un unique $(n+1)$-uplet $(a_i)_{0 \leqslant i \leqslant n}$ d'éléments de A tels que $a_n \neq 0$ et*

$$P = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + a_n X^n.$$

L'entier n est appelé le degré de P, et est noté $\deg(P)$. *Par convention, le degré du polynôme nul est le symbole $-\infty$.*

Preuve. Rappelons que, par définition, un polynôme est une famille $(a_k)_{k\in\mathbb{N}}$ de support fini. Soit P un polynôme de $A[X]$ tel que $P \neq 0$ de support $N = \{k \in \mathbb{N} \mid a_k \neq 0\}$. Comme $P \neq 0$, alors N est une partie non vide majorée de $\mathbb{N}$. Posons n son plus grand élément, alors pour tout $1 \leq k \leq n$, X^k est la suite dont tous les termes sont nuls sauf le terme de numéro k qui vaut 1. Ensuite, on réécrit les définitions, c'est-à-dire le polynôme P est

$$(a_k)_{0\leq k\leq n} = (a_0, a_1, \cdots, a_n) = \sum_{k=0}^{n} a_k X^k.$$

D'où le résultat. □

Exemple 16. Soient $P = X^3 - 3X^2 + 2$ et $Q = X^2 - X + 2$. Calculer le polynôme PQ.

On pourra décomposer un des deux polynômes, par exemple Q, en somme de monômes, donc X^2, $-X$ et 2, puis effectuer chacune des multiplications de P par ces monômes, et enfin tout regrouper. Une présentation claire, en alignant les monômes de mêmes degrés, est une condition nécessaire de calcul sans erreurs.

$$\begin{array}{rcccccccc}
X^2 \times P & = & X^5 & -3X^4 & & +2X^2 & & \\
-X \times P & = & & -X^4 & +3X^3 & & -2X & \\
2 \times P & = & & & 2X^3 & -6X^2 & & +4 \\
\hline
Q \times P & = & X^5 & -4X^4 & +5X^3 & -4X^2 & -2X & +4
\end{array}$$

Définition 77. Pour tout $P \in A[X]$, le coefficient dominant de P est le coefficient a_n du terme de plus haut degré dans l'écriture de P. Par convention, le coefficient dominant du polynôme nul est 0. Un polynôme est dit **unitaire** ou **normalisé** si son coefficient dominant est égal à 1.

Remarque 51. L'application $j : \begin{array}{ccc} A & \longrightarrow & A[X] \\ a & \longmapsto & j(a) = (a, 0, 0, \dots) = aX^0 \end{array}$
est un homomorphisme d'anneaux injectif. Pour cette raison, on identifie A à un sous-anneau de $A[X]$ à savoir l'image de j. Les éléments de A s'appellent alors les constantes de $A[X]$.

Proposition 51. *Soient P et Q deux polynômes de $A[X]$. On a :*

$$\deg(P + Q) \leqslant \max(\deg(P),\ \deg(Q)).$$

Preuve. • Si P ou Q est nul, alors $P + Q = P$, Q ou 0, et le résultat est évident.
• Sinon, notons $\deg(P) = n$ et $\deg(Q) = p$, puis

$$P = a_n X^n + \cdots + a_0, \text{ pour des } a_i \text{ dans } A,$$
$$Q = b_p X^p + \cdots + b_0, \text{ pour des } b_i \text{ dans } A.$$

Si $n > p$, on peut alors écrire :

$$P + Q = a_n X^n + \cdots + a_{p+1} X^{p+1} + (a_p + b_p) X^p + \cdots + (a_0 + b_0).$$

Alors il simple de voir que $\deg(P + Q) = n = \max(\deg(P), \deg(Q))$.
Le cas où $n < p$ est similaire.
Enfin, lorsque $n = p$, on a un regroupement : $P + Q = (a_n + b_n) X^n + \cdots + (a_0 + b_0)$.
Si tous les coefficients de cette somme sont nuls, alors $\deg(P + Q) = -\infty$ ce qui rend l'inégalité évidente.
Si un au moins des coefficients est non nul, alors le coefficient non nul de plus grand indice est le degré de $P + Q$ qui est bien inférieur ou égal à n. □

Proposition 52. *Soit A un anneau commutatif intègre. Soient P et Q deux polynômes de $A[X]$. Alors :*

$$\deg(PQ) = \deg(P) + \deg(Q).$$

Preuve. Si P ou Q est nul, alors $PQ = 0$, et le résultat est évident. Sinon notons $\deg(P) = n$ et $\deg(Q) = p$, puis

$$P = a_n X^n + \cdots + a_0, \text{ pour des } a_i \text{ dans } A,$$
$$Q = b_p X^p + \cdots + b_0, \text{ pour des } b_i \text{ dans } A.$$

Alors on a :

$$PQ = a_n b_p X^{n+p} + (a_n b_{p-1} + a_{n-1} b_p) X^{n+p-1} + \cdots + a_0 b_0.$$

C'est-à-dire

$$PQ = \sum_{k=0}^{n+p} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k,$$

en convenant que $a_i = 0$ pour $i > n$ et $b_i = 0$ pour $i > p$. Comme l'anneau a été supposé intègre, le produit $a_n b_p$ n'est pas nul, donc le degré de PQ est exactement égal à $n + p$. □

Remarque 52. Pour un anneau non intègre, on a $\deg(PQ) \leq \deg(P) + \deg(Q)$.

La proposition suivante est une consequence immediate de la Proposition 52.

Proposition 53.
Si l'anneau A est intègre (donc en particulier, si A est un corps), alors $A[X]$ est intègre.

Preuve. Comme A est intègre, pour tous P et Q de $A[X]$, on a $\deg(PQ) = \deg(P) + \deg(Q)$. Donc si $P \neq 0$ et $Q \neq 0$, alors $\deg(PQ) = \deg(P) + \deg(Q) \geq 0$, d'où le résultat. □

Définition 78. La *valuation* d'un polynôme non nul $P = (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$ est le plus petit des entiers k tel que $a_k \neq 0$. Par convention, la valuation du polynôme nul est $+\infty$.
La valuation d'un polynôme est aussi dite *ordre* du polynôme et on la note $\omega(P)$ ou $\mathrm{ord}(P)$.

Exemple 17. La valuation du polynôme

$$\begin{aligned} P(X) &= (0, 5, -7, 12, -87) \\ &= (a_0, a_1, a_2, a_3, a_4) = 5X - 7X^2 + 12X^3 - 87X^4 \end{aligned}$$

est $\omega(P) = 1$.

Remarques 24. Les propriétés de la valuation sont analogues à celles du degré :

$$\omega(P + Q) \geq \inf(\omega(P), \omega(Q)).$$
$$\omega(PQ) \geq \omega(P) + \omega(Q), \text{ et si l'anneau est intègre : } \omega(PQ) = \omega(P) + \omega(Q).$$
$$\omega(P) = \deg(P) \text{ si et seulement si } P \text{ est un monôme.}$$

Théorème 62. *Si l'anneau A est intègre, alors le groupe des unités de $A[X]$ coïncide avec le groupe des unités de A. En particulier si A est un corps $\mathbb{K}$, ce groupe dans ce cas est $\mathbb{K}^*$.*

Preuve. Soit $P \in A[X]$ un polynôme inversible, donc il existe $Q \in A[X]$ tel que $PQ = 1$. Comme A est intègre, alors $\deg(P) + \deg(Q) = \deg(PQ) = \deg(1) = 0$. ce qui implique que $\deg(P) = 0$ et $\deg(Q) = 0$, donc P et Q sont des constantes inversibles. □

Remarque 53. Si A n'est pas intègre le résultat précédent est faux : dans $\mathbb{Z}/4\mathbb{Z}[X]$ on a : $(1, 2, 0, 0, \cdots)(1, -2, 0, 0, \cdots) = (1, 0, 0, 0, \cdots) = 1$.

Proposition 54. *Si A, l'anneau commutatif des coefficients, est un corps, alors $A[X]$ est un espace vectoriel sur A.*

Preuve. Faire comme exercice. □

Proposition 55. *Soit $\mathbb{K}$ un corps commutatif. La suite $(X^i)_{i\in\mathbb{N}}$ est une* **base** *de $\mathbb{K}[X]$ (appelée base canonique). C'est-à-dire, pour tout $P \in \mathbb{K}[X]$, il existe une suite unique*

$(a_n)_{n\geqslant 0}$ *d'éléments de* $\mathbb{K}$*, à support fini, telle que*

$$P = \sum_{n\in\mathbb{N}} a_n X^n,$$

au sens où, si m *est tel que* $a_n = 0$ *pour tout* $n > m$*, on a* $P = \sum_{n=0}^{m} a_n X^n$.

Remarque 54. $\mathbb{K}[X]$ est un exemple des espaces vectoriels ayant une base infinie.

Proposition 56. *Soit* $\mathbb{K}$ *un corps commutatif et* $n \geqslant 0$ *un entier. On note par* $\mathbb{K}_n[X]$ *l'ensemble des polynômes sur* $\mathbb{K}$ *de degré inférieur ou égal à* n*.*
Pour tout entier $n \geqslant 0$*,* $\mathbb{K}_n[X]$ *est un sous-espace vectoriel de* $\mathbb{K}[X]$*, il admet comme base la famille* $\{1, X, \ldots, X^n\}$ *et sa dimension est* $n+1$*.*

Preuve. Il est simple de voir que $\mathbb{K}_n[X]$ est l'ensemble engendré par $\{1, X, \ldots, X^n\}$ c'est donc un sous-espace vectoriel de $\mathbb{K}[X]$. De plus cette famille génératrice est libre (par une vérification directe), c'est donc une base de $\mathbb{K}_n[X]$ □

Lemme 11. *Soit* $\mathbb{K}$ *un corps commutatif et* $\{P_0, P_1, \ldots, P_n\}$ *une famille de polynômes de* $\mathbb{K}[X]$ *tels que* $0 \leqslant \deg(P_0) < \deg(P_1) < \cdots < \deg(P_n)$*. Alors* $\{P_0, P_1, \ldots, P_n\}$ *est une famille libre.*

Preuve. - La famille $\{P_0\}$ est libre, car il résulte de l'hypothèse $0 \leqslant \deg(P_0)$ que P_0 n'est pas nul.
- Puis le système $\{P_0, P_1\}$ est libre puisque P_1, de degré strictement plus grand que P_0, ne peut lui être proportionnel.
- Puis $\{P_0, P_1, P_2\}$ est libre, puisque toute combinaison linéaire de $\{P_0, P_1\}$ est de degré inférieur ou égal à $\deg(P_1)$, donc P_2 ne peut en être une.
- Et ainsi de suite par récurrence sur n. □

Définition 79. Soient $P(X) = \sum_{k\in N_n} a_k X^k$ et $Q(X) = \sum_{k\in N_m} b_k X^k$ de $A[X]$ de support respectivement N_n et N_m. On appelle polynôme composé de P et Q et on note $P \circ Q$ ou $P(Q)$ le polynôme défini par

$$P \circ Q = \sum_{k\in N_n} a_k Q^k.$$

Dans la somme $\sum_{k\in N_n} a_k X^k$ on substitue à l'indéterminée X le polynôme Q.

Propriétés 1. *La composition des polynômes est associative et distributive à droite par rapport à l'addition, et on a $P \circ X = P$ et $X \circ P = P$ pour tout P.*

Remarque 55. La composition n'est ni commutative ni distributive à gauche par rapport à l'addition. Par exemple dans $\mathbb{Z}[X]$ on a :

$$1 \circ (X+1) = 1 \text{ et } (X+1) \circ 1 = 2,$$
$$1 \circ (X+1) = 1 \text{ et } (1 \circ X) + (1 \circ 1) = 2.$$

Nous terminons cette section par le résultat suivant, dont la preuve est simple, mais qui est important dans beaucoup d'applications.

Théorème 63. *Soit A un sous-anneau d'un corps commutatif K. L'ensemble des polynômes $P \in K[X]$ dont tous les coefficients appartiennent à A est un sous-anneau de $K[X]$. Cet sous-anneau ce n'est que l'anneau $A[X]$.*

5.2. Notions sur les polynômes à n indéterminées.

Dans toute cette section, on considère un corps K commutatif unitaire.

5.2.1. **Définitions.** Nous avons vu, dans la section précédentes, comment construire l'anneau des polynômes à coefficients dans un anneau commutatif A.

- Considérons $A_1 = K[X_1]$ l'anneau des polynômes à coefficients dans le corps K, A_1 est dit l'anneau des polynômes à coefficients dans le corps K à une indéterminée X_1.
- De la même façon, on peut construire $A_2 = A_1[X_2]$ l'anneau des polynômes à coefficients dans l'anneau A_1 à une indéterminée X_2, on écrit $A_2 = K[X_1, X_2]$ et on dit que A_2 est l'anneau des polynômes à coefficients dans le corps K à deux indéterminées.
- De même, on construit $A_3 = A_2[X_3]$ l'anneau des polynômes à coefficients dans l'anneau A_2 à une indéterminée X_3, on écrit $A_3 = K[X_1, X_2, X_3]$ et on dit que A_3 est l'anneau des polynômes à coefficients dans le corps K à trois indéterminées.
- Ainsi de proche en proche, par récurrence et pour $n \geq 2$, on construit $A_{n-1} = A_{n-2}[X_{n-1}]$ l'anneau des polynômes à coefficients dans l'anneau A_{n-2} à une indéterminée X_{n-1}, cet anneau est noté $K[X_1, X_2, X_3, \cdots, X_{n-1}]$ est dit l'anneau des polynômes à coefficients dans le corps K à $n-1$ indéterminées.
- Enfin on construit $A_n = A_{n-1}[X_n]$ l'anneau des polynômes à coefficients dans l'anneau A_{n-1} à une indéterminée X_n, on le note $K[X_1, \ldots, X_n]$ et on l'appelle l'anneau des polynômes à coefficients dans le corps K à n indéterminées.

Remarque 56. On peut admettre que K est l'anneau des polynômes à coefficients dans K à 0 indéterminée.

Définition 80. Pour tout $n \in \mathbb{N}$, l'anneau $K[X_1, \ldots, X_n]$ qu'on vient de construire est dit l'anneau des polynômes à coefficients dans K en n indéterminées.

Définition 81. Un **monôme** en les indéterminées $X_1, \ldots, X_n$ est un polynôme de la forme $aX_1^{a_1}X_2^{a_2}\ldots X_n^{a_n}$, où $a \in K$ et $a_1, a_2, \ldots, a_n$ sont des entiers naturels. Si $a \neq 0$, l'entier $k = a_1 + a_2 + \cdots + a_n$ est appelé le **degré total** de ce monôme.

Exemples 19.

1. Si $K = \mathbb{R}$, alors $7X_1^2X_2^8$ est un monôme de degré total $2 + 8 = 10$,
2. Si $K = \mathbb{R}$, alors $\sqrt{11}X_1^2X_2^7X_3^3$ est un monôme de degré total $2 + 7 + 3 = 13$,
3. Si $K = \mathbb{C}$, alors $(2 + i\sqrt{3})X_1^2X_2^8X_3^3X_4^2X_5^5$ est un monôme de degré total $2 + 8 + 3 + 2 + 5 = 20$.

Notations. Soit un n-uplet $a = (a_1, a_2, \ldots, a_n)$ d'entiers naturels, on notera

$$X^a = X_1^{a_1}X_2^{a_2}\ldots X_n^{a_n}$$

En particulier, on pose $X^{(0,0,\ldots,0)} = 1$. Le degré total du monôme X^a sera noté

$$|a| = a_1 + a_2 + \cdots + a_n.$$

Remarque 57. Un polynôme P d'indéterminées $X_1, \ldots, X_n$ à coefficients dans un corps K est une combinaison linéaire (finie) à coefficients dans K de monômes d'indéterminées $X_1, \ldots, X_n$. Avec les notations précédentes, un polynôme P de $K[X_1, \cdots, X_n]$ s'écrit d'une façon et d'une seule sous la forme

$$P = \sum_a \alpha_a X^a = \sum_a \alpha_{a_1a_2\ldots a_n} X_1^{a_1}X_2^{a_2}\ldots X_n^{a_n},$$

avec les coefficients $\alpha_a = \alpha_{a_1a_2\ldots a_n}$ sont presque tous nuls.

Exemples 20. 1. Si $n = 2$, auquel cas on désigne les deux indéterminées par X et Y ; un polynôme à deux indéterminées à coefficients dans K est une somme finie de la forme

$$\begin{aligned} P &= \sum_{a_1a_2} \alpha_{a_1a_2} X^{a_1}Y^{a_2} \\ &= \alpha_{00} + \alpha_{10}X + \alpha_{01}Y + \alpha_{20}X^2 + \alpha_{11}XY + \alpha_{02}Y^2 \\ &\quad + \alpha_{30}X^3 + \alpha_{21}X^2Y + \alpha_{11}XY^2 + \alpha_{03}Y^3 + \ldots \end{aligned}$$

Considérons par exemple dans $\mathbb{Q}[X, Y]$ les polynômes :

$$P(X, Y) = 3X^3Y + 5X^3 - 2XY + 7 \text{ et } Q(X, Y) = XY + 5X - 6Y + 1.$$

On peut calculer la somme et le produit de P et Q, on trouve des polynômes de $\mathbb{Q}[X,Y]$:

$$(P+Q)(X+Y) = P(X+Y) + Q(X+Y) = 3X^3Y + 5X^3 - XY + 5X - 6Y + 8$$

$$\begin{aligned} PQ(X,Y) = 3X^4Y^2 \quad & +20X^4Y - 18X^3Y^2 + 25X^4 - 27X^3Y - 2X^2Y^2 \\ & +5X^3 - 10X^2Y + 12XY^2 + 5XY + 35X - 42Y + 7 \end{aligned}$$

2. Si $n = 3$, on désigne les indéterminées par X, Y et Z ; et un polynôme à trois indéterminées à coefficients dans K est une somme finie de la forme

$$\begin{aligned} P &= \sum_{a_1a_2a_3} \alpha_{a_1a_2a_3} X^{a_1}Y^{a_2}Z^{a_3} \\ &= \alpha_{000} + \alpha_{100}X + \alpha_{010}Y + \alpha_{001}Z + \alpha_{200}X^2 + \alpha_{020}Y^2 + \alpha_{002}Z^2 \\ &\quad + \alpha_{110}XY + \alpha_{011}YZ + \alpha_{101}XZ + \alpha_{300}X^3 + \dots \end{aligned}$$

Par exemple

$$P(X,Y,Z) = \tfrac{-3}{5}X^4Y^3Z^7 + 2X^4Y^3 - 5Y^3Z^4 + \tfrac{7}{3},$$
$$Q(X,Y,Z) = X^3 + XYZ + X^2Z \text{ et } R(X,Y,Z) = X + Y - Z$$

sont des polynômes de $\mathbb{Q}[X,Y,Z]$. De même

$$\begin{aligned} (Q+R)(X,Y,Z) &= Q(X,Y,Z) + R(X,Y,Z) \\ &= X^3 + XYZ + X^2Z + X + Y - Z \in \mathbb{Q}[X,Y,Z], \end{aligned}$$

et

$$\begin{aligned} QR(X,Y,Z) &= Q(X,Y,Z) \times R(X,Y,Z) \\ &= X^4 + X^3Y + 2X^2YZ - X^2Z^2 + XY^2Z - XYZ^2 \in \mathbb{Q}[X,Y,Z]. \end{aligned}$$

Définition 82.
Soit $P = \sum_a \alpha_a X^a = \sum_a \alpha_{a_1a_2\dots a_n} X_1^{a_1}X_2^{a_2}\dots X_n^{a_n}$ un polynôme de $K[X_1,\dots,X_n]$.

1. Le scalaire $\alpha_{a_1a_2\dots a_n} \in K$ est appelé le coefficient du monôme $X_1^{a_1}X_2^{a_2}\dots X_n^{a_n}$.
2. Si $\alpha_{a_1a_2\dots a_n} \neq 0$, alors $\alpha_{a_1a_2\dots a_n}X_1^{a_1}X_2^{a_2}\dots X_n^{a_n}$ est un terme du polynôme P.
3. le degré total du polynôme P, noté $\deg(P)$, est le degré total maximum $|a|$, tel que le coefficient $\alpha_a = \alpha_{a_1a_2\dots a_n}$ soit non nul.
4. Si $P = 0$, alors $\deg(P) = -\infty$.

Exemple 18.
Soit dans $\mathbb{R}[X,Y,Z]$ le polynôme

$$P = \frac{7}{3} + 2X^4Y^9 - \frac{3}{5}X^4Y^2Z^7 - 5Y^3Z^4 + Z^{13} + \sqrt{2}XYZ.$$

Le polynôme P est constitué de 6 termes de degrés respectivement 0, 13, 13, 7, 13 et 3, il est de degré total 13. Notons que trois termes sont de même degré total maximal 13 avec des monômes différents. Cette situation n'est pas possible avec des polynômes d'une seule indéterminée.

Définition 83. Soit $P = \sum_a \alpha_a X^a = \sum_a \alpha_{a_1 a_2 \dots a_n} X_1^{a_1} X_2^{a_2} \dots X_n^{a_n}$ un polynôme de $K[X_1, \dots, X_n]$. Le degré partiel en X_k d'un monôme (resp. polynôme P) est la plus grande puissance avec laquelle intervient X_k dans ce monôme (resp. ce polynôme P), i.e. si on écrit $P = \sum_j P_j X_k^j$, tel que pour tout j, $P_j \in A[X_1, \dots X_{k-1}, X_{k+1}, \cdots, X_n]$, le degré partiel de P en X_k est le degré de P considéré comme polynôme en X_k, on le note $\deg_{X_k}(P)$.

Exemple 19.
Soit dans $\mathbb{R}[X, Y, Z]$ le polynôme

$$P = \frac{7}{3} + 2X^4Y^9 - \frac{3}{5}X^4Y^2Z^7 - 5Y^3Z^4 + Z^{13} + \sqrt{2}XYZ.$$

Le degré partiel de P en X est 4, en Y est 9 et en Z est 13.

5.2.2. **Quelques propriétés de l'anneau $K[X_1, \dots, X_n]$.** Commençons par la proposition suivante qui se démontre par récurrence sur n.

Proposition 57. *Soit K un corps commutatif unitaire. Alors l'anneau $K[X_1, \dots, X_n]$ des polynômes d'indéterminées $X_1, \dots, X_n$ muni de l'addition et de la multiplication est un anneau commutatif intègre unitaire.*

Preuve. Par récurrence sur n en utilisant les propriétés de la section précédente 5.1. □

Proposition 58. *Pour tous polynômes P et Q de $K[X_1, \dots, X_n]$, on a :*

$$\deg(P + Q) \leqslant \max(\deg(P),\ \deg(Q)),$$

$$\deg(PQ) = \deg(P) + \deg(Q)).$$

Si K est un anneau non intègre, alors $\deg(PQ) \leqslant \deg(P) + \deg(Q))$.

Preuve. Même démonstration que le cas d'une indéterminée. □

Proposition 59. *L'anneau $B = K[X_1, X_2, \dots, X_n]$ est un K-espace vectoriel de dimension infinie. Une base est constituée des monômes de la forme $X_1^{a_1} X_2^{a_2} \dots X_n^{a_n}$.*

Preuve. Puisque $(B,+,\times)$ est un anneau, alors $(B,+)$ est un groupe abélien. Soient $\alpha,\beta\in K$ et $P,Q\in A$, alors il est simple de voir que :
$(\alpha+\beta).P=\alpha.P+\beta.P,\quad \alpha.(P+Q)=\alpha.P+\alpha.Q$, $\alpha.(\beta.P)=(\alpha\beta).P$ et $1.P=P$. D'où $(B,+,.)$ est un espace vectoriel sur K. □

Remarque 58. En réalité $(K[X_1,\ldots,X_n],+,.,\times)$ est une algèbre sur K.

Rappelons que si $a=(a_1,a_2,\ldots,a_n)$, alors le monôme $X^a=X_1^{a_1}X_2^{a_2}\ldots X_n^{a_n}$ a pour degré total $|a|=a_1+a_2+\cdots+a_n$. Ainsi, un polynôme P de degré total égal à n sera de la forme

$$P=\sum_{|a|=n}\alpha_a X^a=\sum_{|a|=n}\alpha_{a_1a_2\ldots a_n}X_1^{a_1}X_2^{a_2}\ldots X_n^{a_n},$$

et un polynôme P de degré total inférieur à n sera de la forme

$$P=\sum_{|a|\leq n}\alpha_a X^a=\sum_{|a|\leq n}\alpha_{a_1a_2\ldots a_n}X_1^{a_1}X_2^{a_2}\ldots X_n^{a_n},$$

Lemme 12 (Propriété universelle des anneaux de polynômes)**.** *Soient A et B deux anneaux et $f:A\longrightarrow B$ un morphisme d'anneaux. Alors, pour tout entier $n\geq 1$ et pour tous éléments $b_1,b_2,\cdots,b_n$ de B, il existe un unique morphisme d'anneaux*

$$\varphi:A[X_1,X_2,\cdots,X_n]\longrightarrow B$$

qui prolonge f (c'est-à-dire $\varphi(a)=f(a)$ pour tout $a\in A$), et tel que $\varphi(X_i)=b_i$ pour tout $1\leq i\leq n$.

Preuve. Si φ existe, alors il vérifie nécessairement :

$$\begin{aligned}\varphi\left(\sum_a\alpha_a X^a\right) &= \varphi\left(\sum_a\alpha_{a_1a_2\ldots a_n}X_1^{a_1}X_2^{a_2}\ldots X_n^{a_n}\right)\\ &=\sum_a\varphi\left(\alpha_{a_1a_2\ldots a_n}X_1^{a_1}X_2^{a_2}\ldots X_n^{a_n}\right)\\ &=\sum_a\varphi(\alpha_{a_1a_2\ldots a_n})\varphi(X_1^{a_1})\varphi(X_2^{a_2})\ldots\varphi(X_n^{a_n})\\ &=\sum_a f(\alpha_{a_1a_2\ldots a_n})b_1^{a_1}b_2^{a_2}\ldots b_n^{a_n},\ \text{ car } \varphi(a)=f(a)\ \forall a\in A\end{aligned}$$

donc φ est aussi nécessairement unique.

Réciproquement, on vérifie facilement que l'application $\varphi:A[X_1,X_2,\cdots,X_n]\longrightarrow B$ définie par

$$\varphi\left(\sum_a\alpha_{a_1a_2\ldots a_n}X_1^{a_1}X_2^{a_2}\ldots X_n^{a_n}\right)=\sum_a f(\alpha_{a_1a_2\ldots a_n})b_1^{a_1}b_2^{a_2}\ldots b_n^{a_n}$$

vérifie les propriétés demandées : il est clair que
- $\varphi(a) = f(a)\ \forall a \in A$,
- $\varphi(X_k) = b_k\ \forall k$,
- on vérifie aussi que φ est bien un morphisme d'anneaux (admis). □

On admet la proposition suivante.

Proposition 60 (Fondamentale)**.** *Soit A un anneau.*

1. *Pour tout entier $n \geq 2$, il existe dans $A[X_1, X_2, \cdots, X_n]$ un sous-anneau isomorphe à $A[X_1, X_2, \cdots, X_{n-1}]$, et on a alors $A[X_1, X_2, \cdots, X_n] \simeq A[X_1, X_2, \cdots, X_{n-1}][X_n]$.*
2. *En particulier, $A[X, Y] \simeq A[X][Y]$, et $A[X, Y, Z] \simeq A[X, Y][Z] \simeq A[X][Y][Z]$.*

5.2.3. **Quelques propriétés de la divisibilité dans $K[X_1, \ldots, X_n]$.**
Commençons par la proposition suivante.

Proposition 61. *Un polynôme $P \in K[X_1, X_2, \ldots, X_n]$ est divisible par $X_n - B$, où B est un polynôme $K[X_1, X_2, \ldots, X_{n-1}]$ si et seulement si le polynôme obtenu en substituant, dans P le polynôme B à l'indéterminée X_n soit nul, i.e., ssi*

$$P(X_1, X_2, \ldots, X_{n-1}, B) = 0.$$

Preuve. Dans $K[X_1, X_2, \ldots, X_{n-1}][X_n]$, effectuons la division euclidienne

$$P = (X_n - B)Q + R \qquad \text{et} \qquad \deg_{X_n}(R) < \deg_{X_n}(X_n - B).$$

Or $\deg_{X_n}(X_n - B) = 1$, alors $\deg_{X_n}(R) = 0$, donc $R \in K[X_1, X_2, \ldots, X_{n-1}]$.
En substituant B à X_n dans la relation $P = (X_n - B)Q + R$, on trouve que :

$$P(X_1, X_2, \ldots, X_{n-1}, B(X_1, X_2, \ldots, X_{n-1})) = R(X_1, X_2, \ldots, X_{n-1}).$$

D'où $X_n - B$ divise P ssi $R = 0$ ssi $P(X_1, X_2, \ldots, X_{n-1}, B(X_1, X_2, \ldots, X_{n-1})) = 0$. □

Exemple 20. Dans $\mathbb{Q}[X, Y, Z]$ à quelle condition sur m le polynôme

$$P(X, Y, Z) = X^3 + Y^3 + Z^3 + mXYZ$$

est-il divisible par $Q = Z + X + Y$?

On a $Z + X + Y = Z - (-X - Y) = Z - B$, où $B = -X - Y$,
donc $Q = Z - B$ divise P ssi $P(X, Y, B) = 0$ ceci est équivaut à

$$X^3 + Y^3 + (-X - Y)^3 + mXY(-X - Y) = 0,$$

On a donc $-3XY(X + Y) - mXY(X + Y) = 0$, la condition cherchée est $m = -3$.

Proposition 62. *Un polynôme $P \in K[X_1, X_2, \ldots, X_n]$ est divisible par $\prod_{1 \leq i < j \leq n} (X_j - X_i)$ si et seulement si $P(X_1, X_2, \ldots, X_n)$ est divisible séparément par chacun des polynômes $X_j - X_i$, $1 \leq i < j \leq n$.*

Preuve. La condition est visiblement nécessaire. Inversement, supposons que $X_j - X_i$, pour $1 \leq i < j \leq n$, divise P, alors P est divisible par $X_2 - X_1$. On peut donc écrire que

$$P = (X_2 - X_1)Q$$

avec $Q \in K[X_1, X_2, \ldots, X_n]$. On sait que P est divisible par $X_3 - X_1$ (c-à-d, $P = (X_3 - X_1)Q'$), alors en remplaçant, dans P, X_3 par X_1 on obtient 0, c'est-à-dire

$$P(X_1, X_2, X_1, \ldots, X_n) = (X_2 - X_1)Q(X_1, X_2, X_1, \ldots, X_n) = 0.$$

Or $K[X_1, X_2, \ldots, X_n]$ est intègre et $X_2 - X_1 \neq 0$, alors $Q(X_1, X_2, X_1, \ldots, X_n) = 0$, ceci exige que Q est divisible par $X_3 - X_1$, ce qui donne que

$$P = (X_2 - X_1)(X_3 - X_1)R,$$

où $R \in K[X_1, X_2, \ldots, X_n]$. On continuera donc par récurrence. □

Proposition 63. *Un polynôme $P \in K[X_1, X_2, \ldots, X_n]$ est divisible par $X_1 - X_2$ si et seulement si $P(X_1, X_1, \ldots, X_n) = O$.*

Preuve. Il est clairement que si $P = (X_1 - X_2)Q$, alors $P(X_1, X_1, X_3, \ldots, X_n) = 0$. Pour la réciproque, posons $B = K[X_3, X_4, \ldots, X_n]$ et on considère P comme élément de $B[X_1, X_2]$; alors

$$P(X_1, X_2) = \sum_{(i,j) \in I} \alpha_{ij} X_1^i X_2^j \quad \text{et} \quad P(X_1, X_1) = \sum_{(i,j) \in I} \alpha_{ij} X_1^i X_1^j = 0,$$

où I est un ensemble fini de couples d'indices. Par soustraction on a :

$$P(X_1, X_2) = P(X_1, X_2) - P(X_1, X_1) = \sum_{(i,j) \in I} \alpha_{ij} X_1^i (X_2^j - X_1^j).$$

Or

$$X_2^j - X_1^j = (X_2 - X_1) \sum_{k=0}^{j-1} X_2^{j-1-k} X_1^k,$$

pour j non nul. D'où

$$\begin{aligned} P(X_1, X_2) &= \sum_{(i,j)\in I} \alpha_{ij} X_1^i (X_2 - X_1) \left(\sum_{k=0}^{j-1} X_2^{j-1-k} X_1^k \right), \\ &= (X_2 - X_1) \sum_{(i,j)\in I} \alpha_{ij} X_1^i \left(\sum_{k=0}^{j-1} X_2^{j-1-k} X_1^k \right), \end{aligned}$$

par suite P est divisible par $X_2 - X_1$. □

Avec un procédé analogue, on prouve la proposition suivante qui généralise la précédente.

Proposition 64. *Un polynôme $P \in K[X_1, X_2, \ldots, X_n]$ est divisible par $X_i - X_j$, $i, j \in \{1, 2, \ldots, n\}$, si et seulement si $P(X_1, X_2, \ldots, X_i, \ldots, X_i, \ldots, X_n) = 0$.*

Nous achevons cette section par le théorème suivant.

Théorème 64. *Pour $n \geq 2$, l'anneau $K[X_1, X_2, \ldots, X_n]$ n'est pas principal.*

Preuve. Considérons dans $K[X_1, X_2, \ldots, X_n]$ l'idéal I engendré par $X_1, \cdots, X_n$, c-à-d $I = \langle X_1, \cdots, X_n \rangle$. Donc I est l'ensemble des polynômes de la forme

$$\sum_{i=1}^{n} P_i X_i \text{ avec } P_i \in K[X_1, X_2, \ldots, X_n].$$

Si I est principal, alors son générateur P divisera chacun des X_i ; donc P est un élément non nul de K, d'où $1 \in I$. Ceci implique $I = K[X_1, X_2, \ldots, X_n]$, ce qui est faux, car les constantes non nuls n'appartiennent pas à I. □

5.2.4. **Polynômes homogènes.**
Rappelons que pour $\alpha \in K^*$, l'écriture $\alpha X_1^{a_1} X_2^{a_2} \ldots X_n^{a_n}$, où $a_i \in \mathbb{N}$, est dite monôme de degré total $k = a_1 + a_2 + \cdots + a_n$.

Définition 84.
Soit $P = \sum_a \alpha_a X^a = \sum_a \alpha_{a_1 a_2 \ldots a_n} X_1^{a_1} X_2^{a_2} \ldots X_n^{a_n}$ un polynôme de $K[X_1, \ldots, X_n]$. P est dit un **polynôme homogène** de degré k, si tous les monômes de P sont de degré total k.

Remarque 59. Le polynôme $P = \sum_a \alpha_a X^a = \sum_a \alpha_{a_1 a_2 \ldots a_n} X_1^{a_1} X_2^{a_2} \ldots X_n^{a_n}$ est homogène de degré k s'il vérifie la condition :

$$\alpha_{a_1 a_2 \ldots a_n} \neq 0 \Longrightarrow a_1 + a_2 + \cdots + a_n = k.$$

Exemples 21.
- Le polynôme $P = \sqrt{2}X^4Y^9 + \frac{-3}{5}X^4Y^2Z^7 - 5Y^5Z^8 + Z^{13}$ de $\mathbb{R}[X, Y, Z]$ est homogène de degré 13.
- Le polynôme $Q = 2X^2Y^3 - 11XY^4 + \sqrt{7}Y^5$ de $\mathbb{R}[X, Y]$ est homogène de degré 5.
- Le polynôme $R = \frac{\sqrt{7}}{5} + \sqrt{2}X^3Y^6Z + \frac{-3}{5}X^4YZ^7 - 5Y^4Z^8 + Y^2Z^{10}$ de $\mathbb{R}[X, Y, Z]$ n'est pas homogène.

Remarque 60. Tout polynôme P de $K[X_1, X_2, \ldots, X_n]$ s'écrit de manière unique comme somme de polynômes homogènes, que l'on appelle **composantes homogènes de** P.
Les composantes homogènes de

$$R(X, Y, Z) = \frac{\sqrt{7}}{5} + \sqrt{2}X^3Y^6Z + \frac{-3}{5}X^4YZ^7 - 5Y^4Z^8 + Y^2Z^{10}$$

sont :

- $R_1(X, Y, Z) = \frac{\sqrt{7}}{5}$ de degré 0,
- $R_2(X, Y, Z) = \sqrt{2}X^3Y^6Z$ de degré 10 et
- $R_3(X, Y, Z) = \frac{-3}{5}X^4YZ^7 - 5Y^4Z^8 + Y^2Z^{10}$ de degré 12.

Proposition 65. *Si P est homogène de degré k et Q homogène de degré ℓ, alors PQ est homogène de degré $k + \ell$.*

Preuve. Soient $X_1^{a_1}X_2^{a_2}\ldots X_n^{a_n}$ un monôme de P et $X_1^{b_1}X_2^{b_2}\ldots X_n^{b_n}$ un monôme de Q, donc

$$a_1 + a_2 + \cdots + a_n = k \qquad \text{et} \qquad b_1 + b_2 + \cdots + b_n = \ell,$$

d'où $X_1^{a_1}X_2^{a_2}\ldots X_n^{a_n}X_1^{b_1}X_2^{b_2}\ldots X_n^{b_n} = X_1^{a_1+b_1}X_2^{a_2+b_2}\ldots X_n^{a_n+b_n}$ qui de degré total $k + \ell$. □

5.2.5. **Polynômes symétriques.**
Considérons le groupe symétrique S_n, l'ensemble des permutations de l'ensemble $\{1, 2, \ldots, n\}$. Soit $\sigma \in S_n$, à chaque polynôme P à n variables, notons par Q le polynôme suivant $Q = \sigma.P$ définit par :

$$Q(X_1, X_2, \ldots, X_n) = (\sigma.P)(X_1, X_2, \ldots, X_n) = P(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}).$$

Exemple 21. Si σ est la transposition $\sigma = \tau_{12}$ et $P = X_1^2 + X_2 + 3X_3X_1 - X_4^5X_1^4$ de l'anneau $\mathbb{R}[X_1, X_2, X_3, X_4]$, alors

$$\begin{aligned} Q(X_1, X_2, X_3, X_4) &= (\tau_{12}.P)(X_1, X_2, X_3, X_4) \\ &= P(X_{\tau_{12}(1)}, X_{\tau_{12}(2)}, X_{\tau_{12}(3)}, X_{\tau_{12}(4)}) \\ &= P(X_2, X_1, X_3, X_4) \\ &= X_2^2 + X_1 + 3X_3X_2 - X_4^5X_2^4 \end{aligned}$$

Définition 85.

Un polynôme $P \in K[X_1, X_2, \ldots, X_n]$ est dit un **polynôme symétrique** si

$$\forall \sigma \in S_n; \quad \sigma.P = P, \text{ c'est-à-dire}$$
$$\forall \sigma \in S_n; \ P(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}) = P(X_1, X_2, \ldots, X_n).$$

Exemple 22.

1. Dans $\mathbb{R}[X_1, X_2, X_3]$, le polynôme $P(X_1, X_2, X_3) = X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2$ est un polynôme symétrique. En effet, on sait que le groupe symétrique S_3 est donné par :
$$S_3 = \{id, \tau_{12}, \tau_{13}, \tau_{23}, c_1 = (123), c_2 = (132)\}.$$

$$\begin{aligned} (id.P)(X_1, X_2, X_3) &= P(X_1, X_2, X_3) = X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2, \\ (\tau_{12}.P)(X_1, X_2, X_3) &= P(X_2, X_1, X_3) = X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2 = P(X, Y, Z), \\ (\tau_{13}.P)(X_1, X_2, X_3) &= P(X_3, X_2, X_1) = X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2 = P(X_1, X_2, X_3), \\ (\tau_{23}.P)(X_1, X_2, X_3) &= P(X_1, X_3, X_2) = X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2 = P(X_1, X_2, X_3), \\ (c_1.P)(X_1, X_2, X_3) &= P(X_{c_1(1)}, X_{c_1(2)}, X_{c_1(3)}) = P(X_2, X_3, X_1) \\ &= X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2 = P(X_1, X_2, X_3), \\ (c_2.P)(X_1, X_2, X_3) &= P(X_{c_2(1)}, X_{c_2(2)}, X_{c_2(3)}) = P(X_3, X_1, X_2) \\ &= X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2 = P(X_1, X_2, X_3). \end{aligned}$$

2. Dans $\mathbb{R}[X_1, X_2, X_3]$, le polynôme $P(X_1, X_2, X_3) = X_1X_2 + X_2X_3 + X_3X_1$ est un polynôme symétrique.
3. Le polynôme $P(X, Y, Z) = X^2 + Y^2 + Z^2$ est un polynôme symétrique de $\mathbb{Q}[X,Y, Z]$ (mais pas de $\mathbb{Q}[X,Y, Z, T]$).
4. Dans $\mathbb{R}[X, Y]$, le polynôme $P(X, Y) = X^2Y + XY^2$ est un polynôme symétrique.
5. Soit $m \in \mathbb{N}$; le polynôme $P = X_1^m + X_2^m + \cdots + X_n^m$ est un polynôme symétrique dans $\mathbb{R}[X_1, X_2, \cdots, X_n]$.
6. Le polynôme $P(X, Y, Z) = X^3Y + Y^3Z + Z^3X$ n'est pas un polynôme symétrique de $\mathbb{Q}[X,Y, Z]$.

Proposition 66. *Un polynôme $P \in K[X_1, X_2, \ldots, X_n]$ est symétrique si, et seulement, si pour tous $i, j \in \{1, 2, \cdots, n\}$ tels que $i < j$ on a*

$$P(X_1, X_2, \ldots, \mathbf{X_i}, \ldots, \mathbf{X_j}, \ldots, X_n) = P(X_1, X_2, \ldots, \mathbf{X_j}, \cdots, \mathbf{X_i}, \cdots, X_n).$$

Preuve. Simple à vérifier. Le sens direct est banal. Pour l'inverse, on peut utiliser le fait que chaque permutation de S_n est produit de transposition τ_{ij} avec $i < j$. □

Exemple 23.

1. Dans $\mathbb{R}[X, Y]$, le polynôme $P(X, Y) = X^2Y + XY^2$ est symétrique, car $P(X, Y) = P(Y, X)$.
2. Dans $\mathbb{R}[X, Y, Z]$, le polynôme $P(X, Y, Z) = XY + XZ + YZ$ est symétrique, car $P(X, Y, Z) = P(Y, X, Z)$, $P(X, Y, Z) = P(Z, Y, X)$ et $P(X, Y, Z) = P(X, Z, Y)$.

Remarque 61. Si P est un polynôme symétrique, alors le degré partiel de P par rapport à chacune de ses variables est le même.

Notons par $\mathbf{S}$ l'ensemble des polynômes symétriques. Alors

Proposition 67. $\mathbf{S}$ *est un sous-anneau de* $K[X_1, X_2, \ldots, X_n]$.

Preuve. - $\mathbf{S}$ est non nul, car $P = 0 \in \mathbf{S}$,
- Si $P = \sum_a \alpha_a X^a = \sum_a \alpha_{a_1 a_2 \ldots a_n} X_1^{a_1} X_2^{a_2} \ldots X_n^{a_n}$ et $Q = \sum_b \alpha_b X^b = \sum_b \alpha_{b_1 b_2 \ldots b_n} X_1^{b_1} X_2^{b_2} \ldots X_n^{b_n}$ sont dans $\mathbf{S}$, alors $\forall \sigma \in S_n$; $\sigma.P = P$ et $\sigma.Q = Q$, donc

$$\sigma.(P - Q) = \sum_a \alpha_{a_1 a_2 \ldots a_n} X_{\sigma(1)}^{a_1} X_{\sigma(2)}^{a_2} \ldots X_{\sigma(n)}^{a_n} - \sum_b \alpha_{b_1 b_2 \ldots b_n} X_{\sigma(1)}^{b_1} X_{\sigma(2)}^{b_2} \ldots X_{\sigma(n)}^{b_n} = P - Q.$$

D'où $P - Q \in \mathbf{S}$.
De même

$$\sigma.(P \times Q) = \left(\sum_a \alpha_{a_1 a_2 \ldots a_n} X_{\sigma(1)}^{a_1} X_{\sigma(2)}^{a_2} \ldots X_{\sigma(n)}^{a_n} \right) \times \left(\sum_b \alpha_{b_1 b_2 \ldots b_n} X_{\sigma(1)}^{b_1} X_{\sigma(2)}^{b_2} \ldots X_{\sigma(n)}^{b_n} \right) = P \times Q.$$

D'où $P \times Q \in \mathbf{S}$. □

Remarque 62. $\mathbf{S}$ est un sous-anneau strict dès qu'il y a plus d'une variable.

Définition 86. On appelle k-ième polynôme symétrique élémentaire de n variables le polynôme :

$$\sigma_{k,n} = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} X_{i_1} X_{i_2} \ldots X_{i_k}$$

La somme porte sur tous les k-uplets tels que la condition $1 \leq i_1 < i_2 < \cdots < i_k \leq n$ soit satisfaite. Ainsi :

$$\begin{aligned}
\sigma_{1,n} &= X_1 + X_2 + \cdots + X_n, \\
\sigma_{2,n} &= X_1X_2 + X_1X_3 + \cdots + X_1X_n + X_2X_3 + \cdots + X_{n-1}X_n, \\
\sigma_{3,n} &= X_1X_2X_3 + X_1X_2X_4 + X_1X_2X_5 + X_1X_2X_6 + \cdots + X_1X_2X_n \\
&\quad + X_1X_3X_4 + X_1X_3X_5 + X_1X_3X_6 + X_1X_3X_7 + \cdots + X_1X_3X_n \\
&\quad + X_2X_3X_4 + X_2X_3X_5 + X_2X_3X_6 + X_2X_3X_7 + \cdots + X_2X_3X_n + \cdots + X_{n-2}X_{n-1}X_n, \\
&\quad \ldots \\
\sigma_{n,n} &= X_1X_2 \ldots X_n.
\end{aligned}$$

Exemples :

Pour $n = 2$, on a :

$$\begin{aligned}
\sigma_{1,2} &= X_1 + X_2, \\
\sigma_{2,2} &= X_1X_2.
\end{aligned}$$

Pour $n = 3$, on a :

$$\begin{aligned}
\sigma_{1,3} &= X_1 + X_2 + X_3, \\
\sigma_{2,3} &= X_1X_2 + X_1X_3 + X_2X_3, \\
\sigma_{3,3} &= X_1X_2X_3.
\end{aligned}$$

Pour $n = 4$, on a :

$$\begin{aligned}
\sigma_{1,4} &= X_1 + X_2 + X_3 + X_4, \\
\sigma_{2,4} &= X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4, \\
\sigma_{3,4} &= X_1X_2X_3 + X_1X_2X_4 + X_1X_3X_4 + X_2X_3X_4, \\
\sigma_{4,4} &= X_1X_2X_3X_4.
\end{aligned}$$

Pour $n = 5$, on a :

$$\begin{aligned}
\sigma_{1,5} &= X_1 + X_2 + X_3 + X_4 + X_5, \\
\sigma_{2,5} &= X_1X_2 + X_1X_3 + X_1X_4 + X_1X_5 + X_2X_3 + X_2X_4 + X_2X_5 + X_3X_4 \\
&\quad + X_3X_5 + X_4X_5, \\
\sigma_{3,5} &= X_1X_2X_3 + X_1X_2X_4 + X_1X_2X_5 + X_1X_3X_4 + X_1X_3X_5 + X_1X_4X_5 \\
&\quad + X_2X_3X_4 + X_2X_3X_5 + X_2X_4X_5 + X_3X_4X_5, \\
\sigma_{4,5} &= X_1X_2X_3X_4 + X_1X_2X_3X_5 + X_1X_2X_4X_5 + X_1X_3X_4X_5 + X_2X_3X_4X_5, \\
\sigma_{5,5} &= X_1X_2X_3X_4X_5.
\end{aligned}$$

Remarque 63. Si $\sigma_{k,n}$ est un polynôme symétrique élémentaire, alors $\deg(\sigma_{k,n}) = k$.

Théorème 65. *L'anneau des polynômes symétriques est engendré algébriquement par les polynômes symétriques élémentaires. De plus, ces polynômes symétriques élémentaires*

sont algébriquement indépendants. Cela signifie que pour tout polynôme symétrique $P \in K[X_1, X_2, \ldots, X_m]$*, il existe un unique polynôme* $Q \in K[X_1, X_2, \ldots, X_m]$ *tel que* $P = Q(\sigma_{1,n}, \sigma_{2,n}, \cdots, \sigma_{1,n})$.

Preuve. Admis. □

Ce théorème signifie que tout polynôme symétrique est un polynôme en les polynômes symétriques élémentaires, avec la précision que cette écriture est unique. Précisons également que des polynômes $P_1, P_2, \ldots, P_m$ sont dits algébriquement indépendants si :

$$\forall Q \in K[X_1, X_2, \ldots, X_m],\ Q(P_1, P_2, ..., P_m) = 0 \Longrightarrow Q = 0.$$

Exemples 22.

1. $X^2 + Y^2 = (X + Y)^2 - 2XY = \sigma_{1,2}^2 - 2\sigma_{2,2}$
2. $X^2 + Y^2 + Z^2 = (X + Y + Z)^2 - 2(XY + YZ + ZX) = \sigma_{1,3}^2 - 2\sigma_{2,3}$
3. $\begin{aligned} XY^2 + X^2Y + YZ^2 + Y^2Z + XZ^2 + X^2Z &= (X + Y + Z)(XY + YZ + ZX) - 3XYZ \\ &= \sigma_{1,3}\sigma_{2,3} - 3\sigma_{3,3} \end{aligned}$
4. $\begin{aligned} X^3 + Y^3 + Z^3 &= (X + Y + Z)^3 - 3(X + Y + Z)(XY + YZ + ZX) + 3XYZ \\ &= \sigma_{1,3}^3 - 3\sigma_{1,3}\sigma_{2,3} + 3\sigma_{3,3} \end{aligned}$

Un corollaire du théorème est le suivant :

Corollaire 18. *L'anneau* $K[X_1, X_2, \ldots, X_n]$ *est isomorphe à l'anneau* $\mathbf{S}$.

C'est donc un exemple de sous-anneau strict isomorphe à l'anneau tout entier.

Preuve. Soit l'application Φ : $\begin{aligned} K[X_1, X_2, \ldots, X_n] &\longrightarrow \mathbf{S} \\ P(X_1, X_2, \ldots, X_n) &\longmapsto P(\sigma_{1,n}, \sigma_{2,n}, \ldots, \sigma_{n,n}) \end{aligned}$

Par exemple pour $n = 3$ et $P(X_1, X_2, X_3) = X_1^2 - 2X_2$, on a :

$$\begin{aligned} \Phi(P) &= P(\sigma_{1,3}, \sigma_{2,3}, \sigma_{3,3}) = \sigma_{1,3}^2 - 2\sigma_{2,3} \\ &= (X_1 + X_2 + X_3)^2 - 2(X_1X_2 + X_1X_3 + X_2X_3) \\ &= X_1^2 + X_2^2 + X_3^2 + 2X_1X_2 + 2X_1X_3 + 2X_2X_3 - 2X_1X_2 - 2X_1X_3 - 2X_2X_3 \\ &= X_1^2 + X_2^2 + X_3^2. \end{aligned}$$

On montre que :

- Φ est un homomorphisme d'anneau :

$$\Phi(P + Q) = \Phi(P) + \Phi(Q), \text{ et } \Phi(PQ) = \Phi(P)\Phi(Q), \text{ et } \Phi(1) = 1.$$

- De plus, le théorème 65 affirme que Φ est surjectif, et que son noyau est réduit à 0. □

5.2.6. **Dérivées partielles.**

Définition 87. Soient n un entier naturel et $i \in [1, n]$. Soit le monôme $P = X_1^{a_1} X_2^{a_2} \dots X_i^{a_i} \dots X_n^{a_n}$. Posons :

$$D_i(X_1^{a_1} X_2^{a_2} \dots X_i^{a_i} \dots X_n^{a_n}) = a_i X_1^{a_1} X_2^{a_2} \dots X_i^{a_i - 1} \dots X_n^{a_n}.$$

D_i est appelé la $i^{\text{ième}}$ dérivation partielle ou dérivation partielle par rapport à X_i.

On peut étendre, de façon unique, D_i en un endomorphisme linéaire de $K[X_1, X_2, \dots, X_n]$, appelé aussi $i^{\text{ième}}$ dérivation partielle ou dérivation partielle par rapport à X_i.

De façon équivalente, si $P \in K[X_1, X_2, \dots, X_n]$, alors la dérivée partielle est la dérivée de P par rapport à X_i, lorsque P est considéré comme polynôme en X_i à coefficient dans $K[X_1, X_2, \dots, X_{i-1}, X_{i+1}, \dots, X_n]$. D_i est noté P'_{X_i} ou $\dfrac{\partial P}{\partial X_i}$.

Exemple 24. Si $P = 7 + 3X^2Y^6 - 5XY^2 + 11Y^9$, alors

$$\frac{\partial P}{\partial X} = 6XY^6 - 5Y^2 \text{ et}$$
$$\frac{\partial P}{\partial Y} = 18X^2Y^5 - 10XY + 99Y^8.$$

Remarque 64. L'application $\dfrac{\partial}{\partial X_i} : K[X_1, X_2, \dots, X_n] \longrightarrow K[X_1, X_2, \dots, X_n]$ est linéaire et vérifie

$$\frac{\partial}{\partial X_i}(PQ) = \frac{\partial P}{\partial X_i}.Q + P.\frac{\partial Q}{\partial X_i}.$$

Proposition 68. *Pour tous $i, j \in \{1, 2, \dots, n\}$, on a :*

$$\frac{\partial}{\partial X_i} \circ \frac{\partial}{\partial X_j} = \frac{\partial}{\partial X_j} \circ \frac{\partial}{\partial X_i}.$$

Preuve. Par linéarité, il suffit de le vérifier sur les monômes :

$$\begin{aligned}
\frac{\partial}{\partial X_i}\left(\frac{\partial}{\partial X_j}(X_1^{a_1} X_2^{a_2} \dots X_i^{a_i} \dots X_j^{a_j} \dots X_n^{a_n})\right) &= \frac{\partial}{\partial X_i}\left(a_j X_1^{a_1} X_2^{a_2} \dots X_i^{a_i} \dots X_j^{a_j - 1} \dots X_n^{a_n}\right) \\
&= a_i a_j X_1^{a_1} X_2^{a_2} \dots X_i^{a_i - 1} \dots X_j^{a_j - 1} \dots X_n^{a_n} \\
&= \frac{\partial}{\partial X_j}\left(\frac{\partial}{\partial X_i}(X_1^{a_1} X_2^{a_2} \dots X_i^{a_i} \dots X_j^{a_j} \dots X_n^{a_n})\right)
\end{aligned}$$

□

Définition 88. Soit $a = (a_1, a_2, \dots, a_n) \in \mathbb{N}^n$. L'application

$$\frac{\partial^a}{\partial X_1^{a_1} \partial X_2^{a_2} \dots \partial X_n^{a_n}} : K[X_1, X_2, \dots, X_n] \longrightarrow K[X_1, X_2, \dots, X_n]$$

est la composée de a_1 fois de $\dfrac{\partial}{\partial X_1}$ par elle-même, a_2 fois de $\dfrac{\partial}{\partial X_2}$ par elle-même, ... etc. Cet opérateur est K-linéaire.

Lemme 13. *Soient $a = (a_1, a_2, \ldots, a_n)$ et $k = (k_1, k_2, \cdots, k_n) \in \mathbb{N}^n$ et un monôme $P = \alpha_a X_1^{a_1} X_2^{a_2} \ldots X_n^{a_n}$, alors*

$$\frac{\partial^k P}{\partial X_1^{a_1} \partial X_2^{a_2} \ldots \partial X_n^{a_n}} = \begin{cases} a_1! a_2! \ldots a_n! \alpha_a & si\ \forall i, k_i = a_i, \\ 0 & si\ k_i > a_i\ pour\ au\ moins\ un\ i\ . \end{cases}$$

Ce résultat reste vrai si on remplace X_i par $X_i + h_i$, où $h_i \in K$.

Exemple 25. Soit $P(X, Y) = 2X^4Y^3 + 5X^2Y^4$. Pour $k = (2, 4)$, calculer $\dfrac{\partial^k P}{\partial X^2 \partial Y^4}$.

Théorème 66 (Formule d'Euler). *Soit $P \in K[X_1, X_2, \ldots, X_n]$ un* **polynôme homogène de degré** *k. Alors on a :*

$$\sum_{i=1}^{n} X_i \frac{\partial P}{\partial X_i} = X_1 P'_{X_1} + X_2 P'_{X_2} + \cdots + X_n P'_{X_n} = kP.$$

Cette formule est dite **Formule d'Euler**.

Preuve. Par linéarité de $\dfrac{\partial}{\partial X_i}$, il suffit de le vérifier sur les monômes.
Soit alors $P = X_1^{a_1} X_2^{a_2} \ldots X_i^{a_i} \ldots X_n^{a_n}$ tel que $k = a_1 + a_2 + \cdots + a_n$. On a pour tout i :

$$\begin{aligned} X_i P'_{X_i} = X_i \frac{\partial}{\partial X_i} \left(X_1^{a_1} X_2^{a_2} \ldots X_i^{a_i} \ldots X_n^{a_n} \right) &= X_i a_i X_1^{a_1} X_2^{a_2} \ldots X_i^{a_i - 1} \ldots X_n^{a_n} \\ &= a_i X_1^{a_1} X_2^{a_2} \ldots X_i^{a_i} \ldots X_n^{a_n} \\ &= a_i P. \end{aligned}$$

Donc

$$\begin{aligned} X_1 P'_{X_1} + X_2 P'_{X_2} + \cdots + X_n P'_{X_n} &= a_1 P + a_2 P + \cdots + a_n P \\ &= (a_1 + a_2 + \cdots + a_n) P \\ &= kP. \end{aligned}$$

□

Remarque 65. Si K est un corps de caractéristique zéro et si P est un polynôme qui satisfait la formule d'Euler, pour un entier k, alors P est homogène de degré k.

Théorème 67 (Formule de Taylor). *Soient K un corps de caractéristique nulle et $a = (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n$. Soient $P \in K[X_1, \cdots, X_n]$ et $(\alpha_1, \alpha_2, \cdots, \alpha_n) \in K^n$, alors*

$$P = \sum_a \frac{(X_1 - \alpha_1)^{a_1} \cdots (X_n - \alpha_n)^{a_n}}{a_1! a_2! \cdots a_n!} \frac{\partial^a P}{\partial X_1^{a_1} \partial X_2^{a_2} \ldots \partial X_n^{a_n}} (\alpha_1, \alpha_2, \cdots, \alpha_n)$$

Preuve. Notons d'abord que ce résultat a un sens car la somme du second membre est finie puisque les dérivées sont nulles pour $|a|$ assez grand. D'autre part, chaque élément

de $K[X_1, \cdots, X_n]$ est somme d'éléments de la forme $\lambda(X_1 - \alpha_1)^{r_1} \cdots (X_1 - \alpha_1)^{r_n}$, où $\lambda \in K$, et les r_i sont dans $\mathbb{N}$. En effet, pour un monôme $X_1^{a_1} X_2^{a_2} \dots X_i^{a_i} \dots X_n^{a_n}$, on a

$$X_1^{a_1} X_2^{a_2} \dots X_i^{a_i} \dots X_n^{a_n} = ((X_1 - \alpha_1) + \alpha_1)^{a_1} \dots ((X_i - \alpha_n) + \alpha_n)^{a_n}.$$

La formule du binôme nous donne

$$X_1^{a_1} X_2^{a_2} \dots X_i^{a_i} \dots X_n^{a_n} = \sum_{k=0}^{a_1} C_{a_1}^k \alpha_1^{a_1 - k} (X_1 - \alpha_1)^k \cdots \sum_{k=0}^{a_n} C_{a_n}^k \alpha_n^{a_n - k} (X_n - \alpha_n)^k.$$

Mais cette expression peut toujours s'écrire sous la forme indiquée.

Par linéarité, il suffit donc de démontrer le théorème pour les monômes

$$P = (X_1 - \alpha_1)^{a_1} \cdots (X_1 - \alpha_1)^{a_n}.$$

On a, pour $k \in \mathbb{N}^n$, $\dfrac{\partial^k P}{\partial X_1^{a_1} \partial X_2^{a_2} \dots \partial X_n^{a_n}}(\alpha_1, \alpha_2, \cdots, \alpha_n) = 0$ si $k \neq a$ et $\dfrac{\partial^k P}{\partial X_1^{a_1} \partial X_2^{a_2} \dots \partial X_n^{a_n}}(\alpha_1, \alpha_2, \cdots, \alpha_n) = a_1! a_2! \cdots a_n!$ si $k = a$. Donc

$$\begin{aligned} P &= \frac{1}{a_1! a_2! \cdots a_n!} a_1! a_2! \cdots a_n! (X_1 - \alpha_1)^{a_1} \cdots (X_1 - \alpha_1)^{a_n} \\ &= \frac{1}{a_1! a_2! \cdots a_n!} \frac{\partial^k P}{\partial X_1^{a_1} \partial X_2^{a_2} \dots \partial X_n^{a_n}}(\alpha_1, \alpha_2, \cdots, \alpha_n)(X_1 - \alpha_1)^{a_1} \cdots (X_1 - \alpha_1)^{a_n} \\ &= \frac{(X_1 - \alpha_1)^{a_1} \cdots (X_1 - \alpha_1)^{a_n}}{a_1! a_2! \cdots a_n!} \frac{\partial^k P}{\partial X_1^{a_1} \partial X_2^{a_2} \dots \partial X_n^{a_n}}(\alpha_1, \alpha_2, \cdots, \alpha_n). \end{aligned}$$

□

5.3. **Exercices.**

1. On dit qu'un anneau est local s'il n'a qu'un seul idéal maximal. Montrer qu'un anneau est local ssi l'ensemble de ses éléments non inversibles est un idéal.
2. Soit K un anneau, montrer que K est un corps si et seulement si $K[X]$ est un anneau principal.
3. Soient K un corps et a, b deux éléments de K. Montrer les assertions suivantes :
   i. l'anneau $K[X]/(X-a)$ est isomorphe à K.
   ii. l'anneau $K[X,Y]/(Y-b)$ est isomorphe à $K[X]$.
   iii. l'anneau $K[X,Y]/(X-a,Y-b)$ est isomorphe à K.
   iv. l'idéal engendré par X et Y est maximal dans l'anneau $K[X,Y]$.
4. Soit K un corps, on pose $A = K[X,Y]/(X^2, XY, Y^2)$.
   i. Déterminer les éléments inversibles de A.
   ii. Déterminer tous les idéaux principaux de A.
   iii. Déterminer tous les idéaux de A.
5. Soient K un corps et $\varphi : K[U,V] \longrightarrow K[X]$ l'homomorphisme d'anneaux défini par les égalités $\varphi(U) = X^3$, $\varphi(V) = -X^2$ et $\varphi(a) = a$ pour tout $a \in K$. Quels sont les noyau et image de φ. Soit A l'image de φ, montrer que A est intègre et que son corps de fractions est isomorphe à $K[X]$.
6. Soit K un corps. Montrer que l'anneau $K[X,Y]$ n'est pas principal. Indication : vous pouvez montrer que l'idéal (X,Y) engendré par X et Y n'est pas principal.
7. Soit P un polynôme à coefficient dans $\mathbb{R}$.
   1. Montrer que, dans l'anneau $\mathbb{R}[X,Y]$, le polynôme $R(X,Y) = P(X) - P(Y)$ est divisible par $X - Y$.
   2. En déduire que $P(P(X)) - P(X)$ est divisible par $P(X) - X$.
8. Soient $A = \mathbb{Z}[X,Y]$, p un nombre premier et I un idéal de A engendré par p et X. Supposons que I est principal, i.e. $I = P_0A = (P_0)$, où P_0 est un polynôme de A.
   1. Montrer que P_0 est une unité de A.
   2. En déduire que p est inversible dans $\mathbb{Z}$.
   3. Conclure.
9. Montrer que le polynôme $P(X,Y) = X^3 - Y^3 - X$ est irréductible dans $\mathbb{C}[X,Y]$.
10. Factoriser en un produit de polynômes de premier degré le polynôme suivant :

$$P(X,Y,Z) = X^3(Y-Z) + Y^3(Z-X) + Z^3(X-Y).$$

Références

[1] J. Dixmier, *Cours de mathématiques du premier cycle : première année*, Gauthier Villars (1973).

[2] J. Lelong-Ferrand et J. M. Arnaudiès, *Cours de mathématiques Tome* 1 *: Algèbre,* 3^e *édition*, Dunod Université (1978).

[3] Roger Codment, *Cours d'Algèbre,* (1996).

[4] Demazure, *Cours d'algèbre,* éditions Cassini, (1997).

[5] Serge Lang, *Algebra,* éditions Addison-Welsey.

[6] P. Samuel, *Théorie des nombres,* Collection Méthodes, éditions Hermann.

[7] J. P. Serre, *Cours d'arithmétique,* éditions PUF.

[8] Daniel Perrin, *Cours d'algèbre*, Ellipses, 1996.

[9] Alain Bouvier, Denis Richard, *Groupes. Observation, théorie, pratique,* Hermann, 1994.

[10] Josette Calais, *Éléments de théorie des groupes,* Puf, 1998.

[11] Josette Calais, *Éléments de théorie des anneaux : anneaux commutatifs, niveau L3.* Ellipses, 2006.

[12] Eric Lehman, *Mathématiques pour l'étudiant de première année. Algèbre et géométrie,* Belin, 1984.

[13] Saliou Touré, *Algèbre,* Premier Cycle MP1, EDICEF, 1991.

[14] S. Francinou, H. Gianella, *Exercices de mathématiques pour l'agrégation. Algèbre 1,* Masson (1994).

[15] J. Delcourt, *Théorie des groupes.* Dunod, (2001).