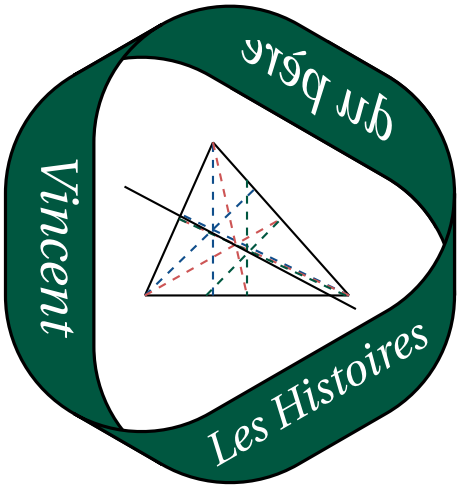


Résolution de problèmes
Licence 1

Yannick VINCENT
Université Gustave Eiffel

www.yannickvincent.fr

Table des matières

1 Groupes **3**

I. Groupes . . . 3
1. Définitions . . . 3
2. Premières propriétés . . . 4

II. Sous-groupes . . . 6
1. Généralités . . . 6
2. Intersection . . . 7
3. Sous groupe engendré . . . 7
4. Ordre d'un élément et ordre d'un sous-groupe . . . 8

III. Exemples fondamentaux de groupes . . . 9
1. Le groupe $(\mathbb{Z}, +)$ . . . 9
2. Les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{Z}/n\mathbb{Z})^*, \times)$ . . . 9
3. Le cercle unité et le groupe des racines n^e dans $\mathbb{C}$ . . . 10
4. Le groupe des permutations . . . 12

IV. Morphismes de groupes . . . 13

2 Polynômes **17**

I. Définition de l'ensemble des polynômes . . . 17
1. Définition formelle . . . 17
2. Définition des fonctions polynomiales . . . 19

II. Relation de divisibilité entre polynômes . . . 20
1. Définition et premières propriétés . . . 20
2. Division euclidienne de polynômes . . . 20

III. Application à l'étude des racines . . . 21
1. Racines d'un polynôme . . . 21
2. Existence de racines et nombre de racines . . . 22

IV. Factorisation de polynômes . . . 23
1. Factorisation dans $\mathbb{C}[X]$ . . . 23
2. Factorisation dans $\mathbb{R}[X]$ . . . 24
3. Relations entre coefficients et racines . . . 25

Chapitre 1

Groupes

I. Groupes

1. Définitions

Définition 1.1

Soit E un ensemble. Une loi de composition interne sur E est une application $\star : E \times E \longrightarrow E$. Pour désigner l'image d'un couple (x, y), plutôt que d'utiliser la notation $\star(x, y)$, on note $x \star y$.

Exemple 1. *La multiplication, notée* $\times$*, dans* $\mathbb{R}$ *est une loi de composition interne sur* $\mathbb{R}$.

Définition 1.2

Soit G un ensemble muni d'une loi de composition interne $\star$. On dit que $(G, \star)$ est un groupe lorsque les trois conditions suivantes sont vérifiées :

1. $\forall x, y, z \in G,\ (x \star y) \star z = x \star (y \star z)$ (associativité)
2. $\exists e \in G, \forall x \in G,\ x \star e = e \star x = x$ (existence d'un élément neutre)
3. $\forall x \in G, \exists y \in G,\ x \star y = y \star x = e$ (existence d'un inverse)

Étymologie – Groupe

Le mot *groupe* vient de l'italien *gruppo, noeud, assemblage*, lui-même issu de la racine germanique *kruppa* (l'anglais *crop, récolte* est de la même racine). Il apparaît en françaisau XVII^{e} siècle et donne bientôt de nombreux dérivés.
Évariste Galois utilise le mot groupe pour désigner les permutations qui agissent sur les racines d'une équation. Il s'intéresse surout à la structure obtenue en composant ces permutations.
À partir des années 1850, des mathématiciens utilisent de manière d'abord informelle l'expression *groupe de permutations* pour désigner les actions de transformations sur des ensembles. Le besoin d'une formalisation puis d'une axiomatisation de cette notion se fait sentir tout au long du XIX^{e} siècle. Les premières définitions sont dues à Arthur Cayley, camille Jordan, Leopold kronecker, Walter Dyck. La définition actuelle est donnée par Heinrich Weber en 1893.

Étymologie – Neutre

Le mot *neutre* est formé sur le latin *ne uter* qui signifie *aucun des deux*. Il est apparu en français au XVI^{e} siècle et signifiait celui qui ne prend pas partie. L'élément neutre est introduit avec la théorie des groupes vers 1900.

Exemple 2. $(\mathbb{R}^*, \times)$ *est un groupe mais* $(\mathbb{R}, \times)$ *n'est pas un groupe.*

2. Premières propriétés

Proposition 1.1

Soit $(G, \star)$ un groupe.
- L'élément neutre est unique.
- Chaque élément $x \in G$ possède un unique inverse (appelé aussi symétrique). On le note x^{-1}.
- Pour tout $x \in G$, $\left(x^{-1}\right)^{-1} = x$

Démonstration. Soit $(G, \star)$ un groupe.
- Soient e et e' deux éléments neutre de G.
  Comme e est un élément neutre, on a $e \star e' = e'$.
  De plus, comme e' est un élément neutre, on a $e \star e' = e$
  Par conséquent, $e' = e$ et l'élément neutre est donc unique.
- Soit $x \in G$. Supposons qu'il existe deux inverses y et y'.
  D'une part $yxy' = ey' = y'$ car y est un inverse de x.
  D'autre part, $yxy' = ye = y$ car y' est un inverse de x.
  On en déduit que $y = y'$ et donc que l'inverse est unique.
- Par définition de x^{-1}, $xx^{-1} = x^{-1}x = e$ donc x^{-1} est inversible et son inverse est x, ce qui s'écrit aussi $\left(x^{-1}\right)^{-1} = x$.

□

Dans la suite du cours, et sauf mention du contraire, on utilise la notation multiplicative, donc $a \star b$ sera noté simplement ab.

Proposition 1.2

Soit (G, .) un groupe. Alors pour tous éléments $a, b, x \in G$:

1. Si $ax = bx$, alors $a = b$ (simplification à droite)
2. Si $xa = xb$, alors $a = b$ (simplification à gauche)
3. Le symétrique de ab est $b^{-1}a^{-1}$.

Démonstration. Pour les points 1 et 2, il suffit de multiplier par x^{-1} à droite dans le premier cas et à gauche dans le second.
Pour le point 3, il suffit de voir que

$$(ab)\left(b^{-1}a^{-1}\right) = abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$$

De même,

$$\left(b^{-1}a^{-1}\right)(ab) = e$$

Cela prouve bien que l'inverse de ab est $b^{-1}a^{-1}$. □

Définition 1.3 – Puissance

Soit (G, .) un groupe et soit $n \in \mathbb{N}^*$.

- Pour tout $x \in G$, on note $x^n = \underbrace{x \times x \times \ldots \times x}_{n \text{ facteurs}}$.
- Par convention, pour tout $x \in G$, $x^0 = e$.
- Pour tout $x \in G$, $(x^{-1})^n = (x^n)^{-1}$. Cet élément est noté x^{-n}.

Définition 1.4

Un groupe est dit commutatif (on dit aussi abélien) si :

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

Étymologie – Abélien

L'adjéctif *abélien* vient du nom du mathématicien norvégien Niels Abel. Camille Jordan trouve dans les écrits de Galois la réponse à la question posée par Abel : une équation polynomiale est résoluble par radicaux si, et seulement si, son groupe de Galois est résoluble. Ceci ammène à étudier les groupes commutatifs qu'il nomme groupe abéliens. Ce terme apparaît dans *Traité des substitutions et des équations algébriques* publiés en 1870.

Exemple 3. $(\mathbb{Z}, +)$ *est un groupe commutatif.*

Remarque. *Dans le cas d'un groupe commutatif, on privilégie souvent la notation additive* $+$. *On note alors* 0 *l'élément neutre et* $-x$ *l'inverse de* x. *De plus, on écrit* nx *au lieu de* x^n.

Exemple 4 (Groupes concernant les ensembles de nombres usuels)**.**

- $(\mathbb{N}, +)$ *n'est pas un groupe (*2 *n'admet pas d'inverse).*
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ *sont des groupes d'élément neutre* 0.
- $(\mathbb{Z}^*, \times)$ *n'est pas un groupe (*2 *n'admet pas d'inverse).*
- $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ *sont des groupes d'élément neutre* 1.

Définition 1.5 – Ordre d'un groupe

L'ordre d'un groupe $(G,.)$ est le cardinal de G.

Définition 1.6 – Groupes produits

Soient $(G,\star)$ et (H,Δ) deux groupes d'éléments neutres respectifs e_G et e_H. On munit le produit cartésien $G\times H$ de la loi de composition interne $\wedge$ définie pour tout $(a,b),(c,d)\in G$ par $(a,b)\wedge(c,d)=(a\star c, b\Delta d)$. Alors $(G\times H,\wedge)$ est un groupe d'élément neutre (e_G,e_H). On l'appelle le groupe produit de G et de H.

II. Sous-groupes

1. Généralités

Définition 1.7 – Sous-groupe

Soit $(G,.)$ un groupe. On dit qu'un sous-ensemble H de G est un **sous-groupe** de G lorsque les trois conditions suivantes sont vérifiées :

1. L'ensemble H n'est pas vide.
2. Pour tous $x,y\in H$, $\quad xy\in H$
3. Pour tous $x\in H$, $\quad x^{-1}\in H$

Pour vérifier qu'un ensemble est un sous-groupe on peut rassembler les conditions 2 et 3 dans une seule condition :

Proposition 1.3

Soit $(G,.)$ un groupe et $H\subset G$. H est un sous-groupe de G si, et seulement si, les deux conditions suivantes sont vérifiées :

1. H contient l'élément neutre
2. $\forall x,y\in H,\ xy^{-1}\in H$

Démonstration. Laissée en exercice. □

Exemple 5.

- *Si* G *est un groupe,* $\{e\}$ *et* G *sont des sous-groupes de* G.
- *Dans* $(\mathbb{Z},+)$*, une partie de la forme* $n\mathbb{Z}$ *(avec* $n\in\mathbb{N}$*) est un sous-groupe.*
  En effet,
  — $0\in n\mathbb{Z}$
  — *Si* $x\in n\mathbb{Z}$ *et* $y\in n\mathbb{Z}$*, alors* $x+y\in n\mathbb{Z}$
  — *Si* $x\in n\mathbb{Z}$*, alors* $-x\in n\mathbb{Z}$*.*

Remarque. *Les deux derniers points peuvent être remplacés par : pour tout* $x\in n\mathbb{Z}$ *et tout* $y\in n\mathbb{Z}$*,* $x-y\in n\mathbb{Z}$*.*

Théorème 1.4

Soit (G, .) un groupe et H un sous groupe de G. La restriction à H de la loi de composition sur G fait de (H, .) un groupe.

Remarque. *On utilise souvent ce théorème pour montrer qu'un ensemble est un groupe. Par exemple,* $(n\mathbb{Z}, +)$ *est un groupe car c'est un sous-groupe de* $(\mathbb{Z}, +)$*. Cela évite d'avoir à redémontrer l'associativité notamment.*

2. Intersection

Proposition 1.5 – Cas de deux sous-groupes

Soit (G, .) un groupe et H_1 et H_2 deux sous-groupes de G. Alors $H_1 \cap H_2$ est un sous-groupe de G.

Démonstration. Soit G un groupe et H_1 et H_2 deux sous groupes.

- $e \in H_1$ et $e \in H_2$ donc $e \in H_1 \cap H_2$
- Soit $x \in H_1 \cap H_2$ et $y \in H_1 \cap H_2$.
  Alors $xy^{-1} \in H_1$ car H_1 est un sous-groupe de G.
  De même, $xy^{-1} \in H_2$ car H_2 est un sous-groupe de G.
  Ainsi, $xy^{-1} \in H_1 \cap H_2$

Finalement, on a montré que $H_1 \cap H_2$ est un sous-groupe de G. □

Proposition 1.6 – Cas général

Soit (G, .) un groupe et $\mathcal{H}$ un ensemble non vide de sous-groupes de G. L'intersection $\bigcap_{H \in \mathcal{H}} H$ est un sous-groupe de G.

Démonstration. Soit G un groupe et $\mathcal{H}$ un ensemble de sous-groupes de G.

- Pour tout $H \in \mathcal{H}$, $e \in H$. Par conséquent, $e \in \bigcap_{H \in \mathcal{H}} H$
- Soit $x \in \bigcap_{H \in \mathcal{H}} H$ et $y \in \bigcap_{H \in \mathcal{H}} H$.
  Alors, pour tout $H \in \mathcal{H}$, $xy^1 \in H$ (car H est un sous-groupe de G)
  Donc $xy^{-1} \in \bigcap_{H \in \mathcal{H}} H$.

Finalement, on a montré que $\bigcap_{H \in \mathcal{H}} H$ est un sous-groupe de G. □

3. Sous groupe engendré

Définition 1.8

Soit (G, .) un groupe et $A \subset G$ une partie non vide. On note $\mathcal{H}_A$ l'ensemble des sous groupes de G contenant A ($\mathcal{H}_A \neq \emptyset$ car il contient G). On appelle **sous-groupe engendré** par A le sous groupe $< A >= \bigcap_{H \in H_A} H$.

Remarque.
- $< \mathrm{A} >$ *est bien un groupe d'après la proposition 1.6. C'est le plus petit sous-groupe de* G *contenant* A *(au sens de l'inclusion).*
  En effet, si L *est un sous-groupe de* G *contenant* A, *alors* $\mathrm{L} \in \mathscr{H}_{\mathrm{A}}$. *On a donc* $< \mathrm{A} > \subset \bigcap_{\mathrm{H} \in \mathrm{H}_{\mathrm{A}}} \mathrm{H} \subset \mathrm{L}$
- *Si* $\mathrm{A} = a$ *est un singleton, le sous-groupe engendré par* A *est*

$$< a >= \left\{ a^k \mid k \in \mathbb{Z} \right\}.$$

Preuve : il est clair que $\{a^k \mid k \in \mathbb{Z}\}$ *est un sous-groupe (il contient e, il est stable par multiplication et par passage à l'inverse).*
De plus, c'est le plus petit sous-groupe contenant a.
En effet, si H *est un sous groupe contenant a, il contient toutes les puissances de a et toutes les puissances de* a^{-1} *donc il contient tous les éléments de la forme* a^k $(k \in \mathbb{Z})$.

- *Si* $\mathrm{G} =< \{a\} >$ *est engendré par un singleton (par abus de notation, on note* $\mathrm{G} =< a >$*), on dit que* G *est* ***monogène*** *et que a est un générateur de* G. *Si de plus* G *est un groupe fini (de cardinal fini), on dit que* G *est* ***cyclique***.

Étymologie – Monogène

Ce mot est formé avec le préfixe d'origine grecque *mono-, seul* et par une racine grecque que l'on retrouve dans *engendrer* et dans *gènes*. Le terme *monogène* apparaît en théorie des groupes dans le courant du XX$^{\mathrm{e}}$ siècle.

4. Ordre d'un élément et ordre d'un sous-groupe

Définition 1.9

Soit (G, .) un groupe d'élément neutre e et $a \in \mathrm{G}$.
- S'il existe $m \in \mathbb{N}^*$ tel que $a^m = e$, on dit que a est d'ordre fini égal à $n = \min\{m \in \mathbb{N}^* | a^m = e\}$.
- Sinon, on dit que a est d'ordre infini.

Proposition 1.7

Soit (G, .) un groupe d'élément neutre e et $a \in \mathrm{G}$ d'ordre fini n. Alors

$$< a >= \{e, a, \ldots, a^{n-1}\}.$$

Démonstration. Soit a d'ordre fini n. Alors $a^n = e$.
On a vu que $< a >= \left\{ a^k \mid k \in \mathbb{Z} \right\}$.
Il est clair que $\{e, a, \ldots, a^{n-1}\} \subset \left\{ a^k \mid k \in \mathbb{Z} \right\}$.
Montrons l'inclusion réciproque.
Soit $x \in \left\{ a^k \mid k \in \mathbb{Z} \right\}$. Alors il existe $k \in \mathbb{Z}$ tel que $x = a^k$.
On fait la division euclidienne de k par n.
Il existe q et r entiers tels que $k = nq + r$ avec $0 \leqslant r < n$.
Ainsi, $x = a^{nq+r} = (a^n)^q a^r = e a^r = a^r$ car $a^n = e$. □

Théorème 1.8 – Lagrange

Soit G un groupe fini et H un sous groupe de G. Alors Card(H) divise Card(G). Autrement dit, l'ordre de H divise l'ordre de G.

III. Exemples fondamentaux de groupes

1. Le groupe $(\mathbb{Z}, +)$

Théorème 1.9

Soit $H \subset \mathbb{Z}$. H est un sous-groupe de $\mathbb{Z}$ ssi il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$. De plus, l'entier n est unique.

Remarque. *On dit que tous les sous groupes de $\mathbb{Z}$ sont monogènes.*

Démonstration. On a déjà vu que les ensembles de la forme $n\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$.
Réciproquement, soit H un sous-groupe de $\mathbb{Z}$.
Si $H = \{0\}$, alors $H = 0\mathbb{Z}$.
Sinon, $H \cap \mathbb{N}^* \neq \emptyset$.
On pose $n_0 = \min(H \cap N^*)$
On va montrer que $H = n_0\mathbb{Z}$.
Comme $n_0 \in H$ et que H est stable par addition et passage à l'opposé, il est clair que $n_0\mathbb{Z} \subset H$.
Montrons l'inclusion inverse :
Soit $m \in n_0\mathbb{Z}$. On fait la division euclidienne de m par n_0.
Il existe ainsi deux entiers r et q tels que $m = n_0 q + r$ et $0 \leqslant r < n_0$.
Supposons par l'absurde que $r \neq 0$,
On aurait $r = m - n_0 q \in H$ (car $m \in H$ et $n_0 q \in H$).
Ainsi, $r \in H \cap N^*$ et $r < n_0$.
Cela est absurde par définition de n_0. Finalement, on a bien montré que $H \subset n_0\mathbb{Z}$ et donc que $H = n_0\mathbb{Z}$. □

2. Les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{Z}/n\mathbb{Z})^*, \times)$

Soit $n \in \mathbb{N}^*$. On définit sur $\mathbb{Z}$ la relation de congruence modulo n par :

$$a \equiv b \, mod(n) \qquad \text{ssi } n \text{ divise } (b - a).$$

Définition 1.10

$\mathbb{Z}/n\mathbb{Z}$ est défini comme l'ensemble $\{0, 1, \ldots, n-1\}$ muni de l'addition modulo n (notée +) et de la multiplication modulo n (notée ×).

Remarque. *Afin de bien différencier l'addition dans $\mathbb{Z}$ et l'addition dans $\mathbb{Z}/n\mathbb{Z}$, on prendra l'habitude de noter une barre sur les éléments de $\mathbb{Z}/n\mathbb{Z}$. Par exemple, dans $\mathbb{Z}/5\mathbb{Z}$, on a $\overline{2} + \overline{4} = \overline{1}$. Cette notation prend par ailleurs un sens plus précis en introduisant la notion de classe d'équivalence et de quotient d'un groupe par un sous-groupe. Ce sont néanmoins des concepts que nous n'aborderons pas dans ce cours.*

Proposition 1.10

- $\text{Card}(\mathbb{Z}/n\mathbb{Z}) = n$
- $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif d'élément neutre $\overline{0}$.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique ($\overline{1}$ est un générateur).
- La loi de composition interne $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ est associative, commutative, d'élément neutre $\overline{1}$.

Remarque. *Pour insister sur le fait que les opérations se font modulo n, on écrit souvent les éléments avec une barre au dessus. Cela permet par exemple de se rappeler que $\overline{x} + \overline{y}$ n'est pas nécessairement égal à l'entier $x + y$.*

Définition 1.11

L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ pour la loi $\times$ est noté $(\mathbb{Z}/n\mathbb{Z})^*$.

Proposition 1.11

$((\mathbb{Z}/n\mathbb{Z})^*, \times)$ est un groupe commutatif d'élément neutre $\overline{1}$.

Remarque.

- *L'inverse de $\overline{x}$ dans $\mathbb{Z}/n\mathbb{Z}$ n'existe pas nécessairement. De plus, écrire que l'inverse est $\frac{\overline{1}}{x}$ n'a en général pas de sens car $\frac{1}{x}$ n'est pas entier. Par exemple, l'inverse de $\overline{2}$ dans $\mathbb{Z}/5\mathbb{Z}$ est $\overline{3}$.*
- *La règle de simplification*
$$\text{Pour tout } \overline{a} \neq \overline{0}, \quad \overline{a}\overline{b} = \overline{a}\overline{c} \Longrightarrow \overline{b} = \overline{c}$$
n'est pas valide en général. On peut néanmoins simplifier si $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

3. Le cercle unité et le groupe des racines n^e dans $\mathbb{C}$

Définition 1.12

On appelle **cercle unité** et on note $\mathbb{U}$, l'ensemble des nombres complexes de module 1. On a donc :
$$\mathbb{U} = \{z \in \mathbb{C} \ / \ |z| = 1\}.$$

Géométriquement, $\mathbb{U}$ correspond au cercle de centre O et de rayon 1.

Proposition 1.12

$(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

Démonstration. Laissée en exercice. □

Remarque. $(\mathbb{U}, +)$ *n'est pas un groupe car il ne contient pas d'élément neutre et $\mathbb{U}$ n'est pas stable par addition.*

Définition 1.13

Pour $n \in \mathbb{N}^*$, on appelle **racine n^e de l'unité** et on note $\mathbb{U}_n$ l'ensemble des solutions de l'équation $z^n = 1$.

Proposition 1.13

Pour tout $n \in \mathbb{N}^*$,

- $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$.
- $\text{Card}(\mathbb{U}_n) = n$.
- $\mathbb{U}_n = \left\{ e^{\frac{2ik\pi}{n}},\ 0 \leqslant k \leqslant n-1 \right\} = < e^{\frac{2i\pi}{n}} >$.

Démonstration. Soit $n \in \mathbb{N}^*$.

- Montrons que $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$. Déjà, il est clair que $\mathrm{U}_n \subset \mathbb{U}$. En effet, si $z \in \mathbb{U}_n$, alors $z^n = 1$ donc $|z^n| = 1$ donc $|z|^n = 1$.
  Étant donné que $|z| \in \mathbb{R}^+$, on en déduit que $|z| = 1$ et on a bien $z \in \mathbb{U}$.
  On montre désormais $\mathbb{U}_n$ contient le neutre, et qu'il est stable par multiplication et passage à l'inverse.
  — Neutre : $1\mathbb{U}_n$
  — Soient $z \in \mathbb{U}_n$ et $z' \in \mathbb{U}_n$.
  Alors, $\left(zz'^{-1}\right)^n = \left(\frac{z}{z'}\right)^n = \frac{z^n}{z'^n} = 1$
- On va montrer les points 2 et 3 conjointement. Soit $z \in \mathbb{C}^*$. On pose $z = \rho e^{i\theta}$

$$\begin{aligned} z^n = 1 &\Longleftrightarrow \rho^n e^{in\theta} = 1 \\ &\Longleftrightarrow \begin{cases} \rho^n = 1 \\ n\theta = 2k\pi \ (k \in \mathbb{Z}) \end{cases} \\ &\Longleftrightarrow \begin{cases} \rho = 1 \\ n\theta = \dfrac{2k\pi}{n} \ (k \in \mathbb{Z}) \end{cases} \end{aligned}$$

Ainsi, $\mathbb{U}_n = \left\{ e^{\frac{2ik\pi}{n}} \mid k \in \mathbb{Z} \right\} = < e^{\frac{2i\pi}{n}} >$.

Montrons de plus que $\mathbb{U}_n = \left\{ e^{\frac{2ik\pi}{n}},\ 0 \leqslant k \leqslant n-1 \right\}$.
L'inclusion $\left\{ e^{\frac{2ik\pi}{n}},\ 0 \leqslant k \leqslant n-1 \right\} \subset \mathbb{U}_n$ est évidente.
Réciproquement, soit $k \in \mathbb{Z}$. En faisant la division euclidiennde de k par n, il existe deux entiers p et q tels que $k = nq + r$ avec $0 \leqslant r < n$.
Ainsi,

$$e^{\frac{2ik\pi}{n}} = e^{\frac{2i(nq+r)\pi}{n}} = e^{2iq\pi} e^{\frac{2ir\pi}{n}} = e^{\frac{2ir\pi}{n}}$$

Donc on a bien $e^{\frac{2ik\pi}{n}} \in \left\{ e^{\frac{2ik\pi}{n}},\ 0 \leqslant k \leqslant n-1 \right\}$.

Enfin, on va montrer que l'ensemble $\left\{ e^{\frac{2ik\pi}{n}},\ 0 \leqslant k \leqslant n-1 \right\}$ possède exactement n éléments. Pour cela, on va montrer que si k et k' sont deux entiers distincts, alors $e^{\frac{2ik\pi}{n}} \neq e^{\frac{2ik'\pi}{n}}$.
Par contraposée, supposons que k et k' soient des entiers tels que $e^{\frac{2ik\pi}{n}} = e^{\frac{2ik'\pi}{n}}$.
Alors $\dfrac{e^{\frac{2ik\pi}{n}}}{e^{\frac{2ik'\pi}{n}}} = 1$ et on a donc $e^{2i(k-k')\pi n} = 1$
Donc n divise $k - k'$.
Comme $|k - k'| \leqslant n - 1$, on en déduit que $k - k' = 0$, c'est-à-dire $k = k'$.
Ainsi, on a bien montré que l'ensemble $\left\{ e^{\frac{2ik\pi}{n}},\ 0 \leqslant k \leqslant n-1 \right\}$ possède exactement n éléments.

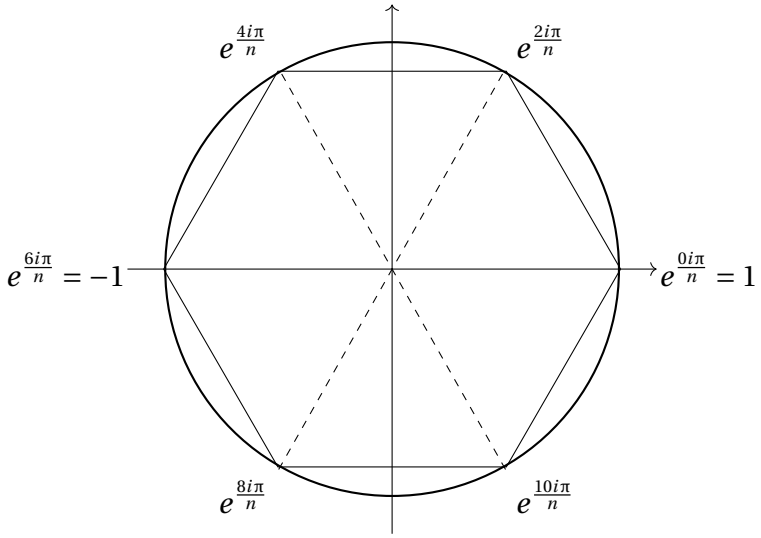
□

Remarque. *En utilisant le vocabulaire de la théorie des groupes, on aurait pu montrer que* $e^{\frac{2i\pi}{n}}$ *est d'ordre n dans* $\mathbb{U}_n$ *et appliquer la Proposition 1.7*

Exemple 6.

- $\mathbb{U}_2 = \{1;-1\}$
- $\mathbb{U}_3 = \{1;j;j^2\}$ *avec* $j = e^{\frac{2i\pi}{3}}$
- $\mathbb{U}_4 = \{1;i;-1;-i\}$

Remarque. *Si* $n \geqslant 3$*, alors les points dont les affixes sont des racines* n^e *de l'unité forment un polygône régulier à n côtés. Par exemple, le dessin ci-dessous représente les racines de l'unité pour* $n = 6$.



4. Le groupe des permutations

Définition 1.14

Soit E un ensemble. L'ensemble $\mathscr{S}(E)$ des bijections de E dans E est un groupe pour la loi de composition $\circ$. Son élément neutre est l'application Id_E. Le groupe $(\mathfrak{S}(E), \circ)$ est appelé **groupe symétrique de** E. Les éléments de $\mathfrak{S}(E)$ sont appelés des permutations.

Remarque.

- *Dans le cas où* $E = \{1,\dots,n\}$*, on note* $\mathfrak{S}_n = \mathfrak{S}(E)$*. Le groupe* $\mathfrak{S}_n$ *est appelé le groupe symétrique d'ordre n.*
- $Card(\mathfrak{S}_n) = n!$.
- *Rappel : l'identité* $Id_{\{1,\dots,n\}}$ *et les transpositions* $t_{a,b}$ *sont des permutations.*
- *Pour* $n \geqslant 3$*,* $\mathfrak{S}_n$ *est un groupe non commutatif.*
  En effet, si on choisit trois éléments distincts $a,b,c \in \{1,\dots,n\}$*, on a :*

$$t_{a,b} \circ t_{b,c} \neq t_{b,c} \circ t_{a,b}.$$

- *Dans* $\mathfrak{S}_5$*, une permutation se note par exemple* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}$*. On la note aussi* (15423)*. Avec cette notation la composée des transpositions* $t_{1,2} \circ t_{4,5}$ *se note* $(12)\circ(45)$.

Étymologie – Permutation

En latin, *permutare* signifiait *échange* et *permutatio* désignait un changement, une modification. Au Moyen Âge, la permutation était le troc ou le change. Vers le XV^{e} siècle, son sens se spécialise dans le fait d'échanger deux éléments, Leibniz appelait variation ce que nous appelons de nos jours permutation.
Au début du XIX^{e} siècle, se rapprochant du sens latin, on appelle *permutation* en mathématique la modification de l'ordre de n lettres. Certains l'utilisent cependant dans le sens d'arrangement. On rencontre souvent *permutation* chez Lagrange, Cauchy et Galois lorsqu'ils travaillent sur les racines d'une équation polynomiale. cauchy distingue curieusement une permutation dans le sens que nous venons de voir et une substitution qui représente à ses yeux réellement une bijection, c'est-à-dire le passage d'un ordre à un autre. De nos jours, les deux mots sont synonymes.

IV. Morphismes de groupes

Exemple d'introduction : Avec $G_1 = \mathbb{Z}/4\mathbb{Z}$, $G_2 = \mathbb{U}_4$ et $G_3 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Il est possible de définir un bijection entre G_1 et G_2 qui respecte la structure des opérations des groupes : effectuer les opérations dans le groupe de départ avant de calculer l'image donne le même résultat que de commencer par calculer les images puis d'effectuer les opérations dans le groupe d'arrivée. On dit que G_1 et G_2 sont isomorphes.

En notant $\omega = e^{\frac{2i\pi}{4}}$, on a $\mathbb{U}_4 = \{1, \omega, \omega^2, \omega^3\}$ et la bijection en question est :

$$\Phi : \begin{cases} \mathbb{Z}/4\mathbb{Z} & \longrightarrow & \mathbb{U}_4 \\ 0 & \longmapsto & 1 \\ 1 & \longmapsto & w \\ 2 & \longmapsto & w^2 \\ 3 & \longmapsto & w^3 \end{cases}$$

Les structures sont « identiques » : sommer dans $\mathbb{Z}/4\mathbb{Z}$ ou multiplier dans $\mathbb{U}_4$ revient pour ainsi dire au même. On a par exemple

$$w^2 \times w^3 = w^5 = w \qquad \text{et} \qquad 2 + 3 \equiv 5 \equiv 1 \mathrm{mod}(4)$$

En revanche, définir une telle bijection entre G_1 et G_3 est impossible. En effet, pour tout $x \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $x + x = 0$, ce qui n'est pas le cas dans $\mathbb{Z}/4\mathbb{Z}$.
On dit que G_1 et G_3 ne sont pas isomorphes.

Définition 1.15 – Morphisme

Soient $(G_1, \star)$ et (G_2, Δ) deux groupes. Une application $f : G_1 \longrightarrow G_2$ est un **morphisme de groupes** si pour tous $x, y \in G_1$,

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

Étymologie – Morphisme

Morphisme et ses dérivés sont apparus avec le développement et l'étude des structures abstraires, tant topologiques qu'algébriques, au début du XX^{e} siècle. *Morphe* en grec désigne la forme. Il semble que *forme*, venu du latin, soit de même racine mais modifié par une métathèse (inversion du f et du m).
Le mot *morphisme* a d'abord été employé avec un préfixe (*homo, iso, auto, homéo*). son emploi isolé date du développement de la théorie des catégories vers 1950. Il tend maintenant à supplanter *homomorphisme*.

Dans toute la suite, on considère $(G_1, \star)$ et (G_2, Δ) deux groupes d'élements neutres respectifs e_1 et e_2. De plus, $f : G_1 \longrightarrow G_2$ désigne un morphisme de groupes.

Proposition 1.14

- $f(e_1) = e_2$
- $\forall x \in G_1,\ f(x^{-1}) = f(x)^{-1}$.

Démonstration. Soit $f : G_1 \longrightarrow G_2$ un morphisme de groupes.

- $e_1 \star e_1 = e_1$ donc $f(e_1 \star e_1) = f(e_1)$
  Comme f est un morphisme, on en déduit :
  $$f(e_1)\Delta f(e_1) = f(e_1)$$
  donc
  $$f(e_1)\Delta f(e_1) = f(e_1)\Delta e_2$$
  donc, en simplifiant par $f(e_1)$ (proposition 1.2), on a :
  $$f(e_1) = e_2$$
- Soit $x \in G_1$. On a $x \star x^{-1} = e_1$
  Donc, en appliquant f :
  $$f(x \star x^{-1}) = f(e_1)$$
  Comme f est un morphisme,
  $$f(x)\Delta f(x^{-1}) = e_2.$$
  De même, on prouve que $f(x^{-1})\Delta f(x) = e_2$ et on en déduit donc que l'inverse de $f(x^{-1})$ est $f(x)$.

□

Définition 1.16

On appelle **image** du morphisme $f : G_1 \longrightarrow G_2$ l'ensemble $Im(f) = f(G_1)$.

Définition 1.17

On appelle **noyau** du morphisme $f : G_1 \longrightarrow G_2$ l'ensemble

$$\mathrm{Ker}(f) = f^{-1}(\{e_2\}) = \left\{x \in G_1 | f(x) = e_2\right\}.$$

Proposition 1.15

Soit $f : G_1 \longrightarrow G_2$ un morphisme de groupes.
f est injectif si, et seulement si, $\mathrm{Ker}(f) = \{e_1\}$.

Démonstration. Soit $f : G_1 \longrightarrow G_2$ un morphisme de groupes.
Supposons que f est injective. Un antécédent de e_2 est e_1 d'après la proposition 1.14. Comme f est injective, c'est le seul et on a bien $\text{Ker}(f) = \{e_1\}$.

Réciproquement, supposons que $\text{Ker}(f) = \{e_1\}$.
Soit $x, y \in G_1$ tels que $f(x) = f(y)$.
Alors $f(x)\Delta f(y)^{-1} = e_2$
Donc $f(x)\Delta f(y^{-1}) = e_2$ (d'après la proposition 1.14)
Donc $f(xy^{-1}) = e_2$ (par définition d'un morphisme)
Donc $xy^{-1} \in \text{Ker}(f)$
Donc $xy^{-1} = e_1$
Donc $x = y$. On a ainsi prouvé que f est injectif. □

Proposition 1.16

Soit $f : G_1 \longrightarrow G_2$ un morphisme de groupes.
- Le noyau de f est un sous-groupe de G_1.
- L'image de f est un sous-groupe de G_2.

Démonstration. Laissée en exercice □

Définition 1.18 – Isomorphisme

Soit $f : G_1 \longrightarrow G_2$ un morphisme de groupes. Si f est bijective, on dit que f est un isomorphisme de groupes et que les groupes G_1 et G_2 sont isomorphes.

Étymologie – Isomorphisme

Le terme *Isomorphisme* existe en chimie dès le début du *xix*^{e} siècle. Son utilisation en algèbre date de la fin de ce même siècle. Henri Poincaré l'introduit en topologie en 1905.

Théorème 1.17

Pour $n \in \mathbb{N}^*$, $(\mathbb{U}_n, \times)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$

Démonstration. On pose $\omega = e^{\frac{2i\pi}{n}}$ Soit

$$\Phi : \begin{cases} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{U}_n \\ \overline{k} & \longmapsto & w^k \end{cases}$$

On commence par montrer que Φ est un morphisme de groupes. Soient $k_1, k_2 \in \mathbb{Z}/n\mathbb{Z}$.
D'après la division euclidienne de $k_1 + k_2$ par n, il existe deux entiers $q, r \in \mathbb{Z}$ tels que $k_1 + k_2 = nq + r$ avec $0 \leqslant r < n$.
On a alors $\Phi(\overline{k_1} + \overline{k_2}) = \Phi(r) = \omega^r$.
De plus, $\Phi(\overline{k_1}) \times \Phi(\overline{k_2}) = \omega^{k_1} \times \omega^{k_2} = \omega k_1 + k_2 = \omega^{qn+r} = \omega^r$. On a ainsi

$$\Phi(\overline{k_1} + \overline{k_2}) = \Phi(\overline{k_1}) \times \Phi(\overline{k_2})$$

et Φ est bien un morphisme de groupes.
De plus, Φ est injective car $\ker(\Phi) = \{\overline{0}\}$. En effet, soit $\overline{k} \in \ker(\Phi)$.
On a $\Phi(\overline{k}) = 1$

Donc $w^k = 1$
Donc $e^{\frac{2ki\pi}{n}} = 1$ Donc n divise k
Donc $\overline{k} = \overline{0} \mod(n)$. On en déduit ainsi que $\ker(\Phi) = \{\overline{0}\}$.

Enfin, comme Φ est injective et que $\text{Card}(\mathbb{Z}/n\mathbb{Z}) = \text{Card}(\mathbb{U}_n)$, on en déduit que Φ est bijective.
Finalement, Φ est bien un isomorphisme.

□

Chapitre 2

Polynômes

I. Définition de l'ensemble des polynômes

1. Définition formelle

Dans tout ce chapitre, $\mathbb{K}$ désigne l'ensemble $\mathbb{R}$ ou $\mathbb{C}$. On note $\mathbb{K}^{\mathbb{N}}$ l'ensemble des suites à valeurs dans $\mathbb{K}$, c'est-à-dire l'ensemble des applications de $\mathbb{N}$ dans $\mathbb{K}$.

Définition 2.1

Un polynôme sur $\mathbb{K}$ est une suite $P = (a_k)_{k\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ dont les coefficients sont tous nuls à partir d'un certain rang, c'est à dire telle que :

$$\exists N \in \mathbb{N} \text{ tel que } \forall k > N,\ a_k = 0$$

On note $\mathbb{K}[X]$ l'ensemble des polynômes sur $\mathbb{K}$.

Définition 2.2

Soit $P = (a_k)_{k\in\mathbb{N}} \in \mathbb{K}[X]$ (avec P non identiquement nulle).
L'indice du dernier coefficient non nul de P est appelé degré de P et est noté deg(P).
Si $N = \deg(P)$, on a donc $a_N \neq 0$ et $\forall k > N$, $a_k + 0$.
On note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.

Remarque. *Par convention, si* P *est la suite nulle, on note* $P = 0_{\mathbb{K}[X]}$*, et on pose* $\deg(0_{\mathbb{K}[X]}) = -\infty$.

Exemple 7. $P = (2,0,1,-6,0,0,0,0,0,\ldots) \in \mathbb{R}[X]$. *De plus,* $\deg(P) = 3$. *Donc* $P \in \mathbb{R}_3[X]$. *On a aussi* $P \in \mathbb{R}_4[X]$ *mais* $P \notin \mathbb{R}_2[X]$.

Remarque. *Comme* $\mathbb{R} \subset \mathbb{C}$*, on a* $\mathbb{R}[X] \subset \mathbb{C}[X]$. *Autrement dit, un polynôme à coefficients réels peut toujours être considéré comme un polynôme à coefficients complexes. La réciproque est en revanche fausse.*

Définition 2.3

Soient $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ et $Q = (b_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. On définit :

- $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$
- $\lambda P = (\lambda a_n)_{n\in\mathbb{N}}$
- $P \times Q = (c_n)_{n\in\mathbb{N}}$ où, pour tout $n \in \mathbb{N}$, $c_n = \sum_{k=0}^{n} a_k b_{n-k}$.

Remarque. *Ainsi définis, on a* $P + Q \in \mathbb{K}[X]$, $\lambda P \in \mathbb{K}[X]$ *et* $P \times Q \in \mathbb{K}[X]$. *Pour le justifier, il suffit de vérifier que ces suites sont bien identiquement nulles à partir d'un certain rang (preuve laissée au lecteur).*

Remarque. *La définition du produit de deux polynômes et celle de la multiplication par un scalaire (nombre) semble naturelle. Celle du produit de deux polynômes peut paraître étrange. On va cependant voir qu'elle correspond à la notion de « multiplication de fonction polynomiales ».*

Proposition 2.1

Si $P \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$, alors :

- $\deg(P + Q) \leqslant \max(\deg(P), \deg(Q))$
- $\deg(PQ) = \deg(P) + \deg(Q)$.

Définition 2.4

On définit la suite $X = (0, 1, 0, 0, 0, 0, \ldots)$.

Exemple 8. *Soit* $p \in \mathbb{N}^*$. *Déterminer* $X^p = X \times X \times \ldots \times X$ *(on pourra raisonner par récurrence).*

Solution :
On va montrer par récurrence sur p *que* X^p *est la suite nulle partout sauf en position* p *où le coefficient est* 1. *On note* $(X^p)_l$ *le coefficient en position* l *de* X^p.
Initialisation : pour $p = 1$, *il s'agit simplement de la définition de* X.
Hérédité : Supposons la propriété vraie au rang p. $X^{p+1} = X \times X^p = (0, 1, 0, 0, 0, \ldots) \times (0, 0, 0, 0, 1, 0, 0, \ldots)$.
Ainsi, en faisant le produit avec la formule $c_n = \sum_{k=0}^{n} a_k b_{n-k}$, *on voit que le seul coefficient non nul de* X^{p+1} *est obtenu si* $n = p + 1$. *On a alors* $c_{p+1} = a_1 b_p = 1$.

Proposition 2.2

Soit $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ de degré N. On a

$$P = \sum_{k=0}^{N} a_k X^k$$

où l'on a posé, par convention, $X^0 = (1, 0, 0, 0, 0, \ldots)$.

Démonstration. Laissée au lecteur. □

Exemple 9. *Si* $P = (2, 0, 1, -6, 0, 0, 0, 0, 0, \ldots)$, *on a* $P = 2 \times X^0 + 0X^1 + 1X^2 + (-6)X^3 = 2 + X^2 - 6X^3$

Définition 2.5

- Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ un polynôme non nul. On définit le polynôme dérivé de P, noté P' de la façon suivante :

$$P' = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k$$

- Par convention, si $P = 0$, on pose $P' = 0$.
- On définit ensuite, par récurrence, les dérivées successives du polynôme P par $P^{(k)} = \left(P^{(k-1)}\right)'$

Remarque. *En faisant un changement d'indice dans la somme (en posant $i = k+1$), on vérifie que la notion de polynôme dérivé est cohérente avec le concept de la dérivée d'une fonction. Par exemple, si $P = 2 + X^2 - 6X^3$, on a $P' = 2X - 18X^2$.*

2. Définition des fonctions polynomiales

Définition 2.6

Soit $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ de degré N. La fonction $\tilde{P} : \mathbb{K} \longrightarrow \mathbb{K}$ et définie par $\tilde{P}(x) = \sum_{k=0}^{n} a_k x^k$ est appelée fonction polynomiale associée à P.

Remarque.

Si l'on note $\mathscr{F}$ l'ensemble des fonctions polynomiales, il est possible de montrer que l'application suivante est bijective (elle est clairement surjective, par définition de $\mathscr{F}$) :

$$\begin{cases} \mathbb{K}[X] & \longrightarrow & \mathscr{F} \\ P & \longmapsto & \tilde{P} \end{cases}$$

En pratique, on ne distinguera pas les deux ensembles.

L'intérêt théorique de distinguer $\mathbb{K}[X]$ et $\mathscr{F}$ apparaît lorsque $\mathbb{K}$ est différent de $\mathbb{R}$ ou $\mathbb{C}$.

Dans le cadre de ce cours, par abus de notation, on notera souvent P l'application polynomiale associée à P, sans faire de distinction entre P et $\tilde{P}$.

Il est désormais possible de voir que la définition formelle que nous avons donné du produit de deux polynômes (Définition 2.3) correspond bien au produit de fonctions polynomiales. Par exemple, si $P = a_0 + a_1X + a_2X^2$ et $Q = b_0 + b_1X + b_2X^2 + b_3X^3$, la fonction polynomiale associée à $P \times Q$ est bien $\tilde{P} \times \tilde{Q}$ (la preuve est laissée au lecteur). Autrement dit, on a

$$\widetilde{P \times Q} = \tilde{P} \times \tilde{Q}.$$

II. Relation de divisibilité entre polynômes

1. Définition et premières propriétés

Définition 2.7

Soient $P, Q \in \mathbb{K}[X]$. On dit que P **divise** Q dans $\mathbb{K}[X]$ lorsqu'il existe $S \in \mathbb{K}[X]$ tel que $Q = PS$. On dit aussi que P est un **diviseur** de Q et que Q est un **multiple** de P. On note $P|Q$.

Exemple 10. *Si* $P = X - 1$ *et* $Q = X^2 - 1$ *alors* P *divise* Q *car* $X^2 - 1 = (X-1)(X+1)$

Proposition 2.3

Soient $P, Q, R \in \mathbb{K}[X]$.
Si $P|Q$ et $Q|R$, alors $P|R$.

Proposition 2.4

Soient $P, Q, R \in \mathbb{K}[X]$ tels que $P|Q$ et $P|R$.

- Pour tous $m, n \in K$, $P|(mQ + nR)$.
- En particulier, $P|(Q+R)$ et $P|(Q-R)$.

Démonstration. La preuve de ces résultats est identique à celle des propriétés établies dans $\mathbb{Z}$. □

2. Division euclidienne de polynômes

Proposition 2.5 – (admise)

Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\}$.
Il existe un unique couple $(Q, R) \in \mathbb{K}[X] \times \mathbb{K}[X]$ tels que :

$$\begin{cases} A = BQ + R \\ \text{et} \\ \deg(R) < \deg(B) \end{cases}$$

Remarque. *La condition* $B \in \mathbb{K}[X] \setminus \{0\}$ *signifie que* B *n'est pas le polynôme nul.*

Exemple 11. *Effectuer la division euclidienne de* A *par* B *dans les cas suivants :*

1. $A(X) = X^4 + 3X^3 + X^2 - 5X + 3$ *et* $B(X) = X$
2. $A(x) = X^4 + 3X^3 + X^2 - 5X + 3$ *et* $B(x) = X^2$
3. $A(x) = X^4 + 3X^3 + X^2 - 5X + 3$ *et* $B(x) = X^2 + X + 1$

Solution :

1. $A(X) = X(X^3 + 3X^2 + X - 5) + 3$.
   Ainsi $Q(X) = X^3 + 3X^2 + X - 5$ *et* $R(X) = 3$ *(avec* $\deg(R) < \deg(B)$*).*
2. $A(X) = X^2(X^2 + 3X + 1) - 5X + 3$.
   Ainsi $Q(X) = X^2 + 3X + 1$ *et* $R(X) = -5X + 3$ *(avec* $\deg(R) < \deg(B)$*).*

3. *On pose la division euclidienne comme ci-dessous, en ordonnant les polynômes selon les puissances décroissantes de* X.

$$\begin{array}{rl|l} & X^4+3X^3+X^2-5X+3 & X^2+X+1 \\ \hline - & X^4+X^3+X^2 & X^2+2X-2 \\ \hline & 2X^3 \quad -5X+3 & \\ - & 2X^3+2X^2+2X & \\ \hline & -2X^2-7X+3 & \\ - & -2X^2-2X-2 & \\ \hline & -5X+5 & \end{array}$$

Ainsi, on a $A(X) = (X^2+X+1)(X^2+2X-2)+(-5X+5)$.
Par conséquent, $Q(X) = X^2+2X-2$ *et* $R(X) = -5X+5$ *(avec* $\deg(R) < \deg(B)$*).*

III. Application à l'étude des racines

1. Racines d'un polynôme

Définition 2.8

Soit $P \in \mathbb{K}[X]$ et soit $a \in \mathbb{C}$. On dit que a est une racine de P si $\tilde{P}(a) = 0$.

Remarque. *Même si* $P \in \mathbb{R}[X]$, P *peut admettre des racines complexes non réelles. C'est par exemple le cas de polynômes du second degré lorsque* $\Delta < 0$.

Proposition 2.6

Soit $P \in \mathbb{R}[X]$ et soit $z \in \mathbb{C}$. z est une racine de P si, et seulement si, $\overline{z}$ est une racine de P.

Démonstration. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{R}[X]$ et soit $z \in \mathbb{C}$. Alors,

$$\begin{aligned} P(z) = 0 &\iff \sum_{k=0}^{n} a_k z^k = 0 \\ &\iff \overline{\sum_{k=0}^{n} a_k z^k} = 0 \\ &\iff \sum_{k=0}^{n} \overline{a_k z^k} = 0 \\ &\iff \sum_{k=0}^{n} \overline{a_k}\,\overline{z}^k = 0 \\ &\iff \sum_{k=0}^{n} a_k \overline{z}^k = 0 \qquad (\text{car } \forall k,\ a_k \in \mathbb{R}) \\ &\iff P(\overline{z}) = 0 \end{aligned}$$

□

Remarque. *La condition* $P \in \mathbb{R}[X]$ *est essentielle. La Proposition devient fausse si* $P \in \mathbb{C}[X]$. *Il suffit de considérer par exemple le polynôme* $P(X) = (X - i)(X - 1)$.

2. Existence de racines et nombre de racines

Proposition 2.7 – Théorème de D'Alembert-Gauss (admis)

Tout polynôme $P \in \mathbb{K}[X]$ non constant admet au moins une racine complexe.

Histoire – Théorème de d'Alembert-Gauss

Au XVIII^{e} siècle, l'existence de racines complexes était globalement admise mais cela n'a été démontrée rigoureusement qu'au début du XIX^{e} siècle. Ce théorème est également connu sous le nom de « théorème fondamental de l'algèbre ». Il s'agit là d'une situation que l'on peut aujourd'hui estimer paradoxale car toutes les démonstrations connues utilisent des arguments analytiques (d'analyse complexe par exemple). Cependant, le paradoxe n'est qu'apparent car le nom de « théorème fondamental de l'algèbre » est apparu à une époque où l'algèbre désignait la théorie des équations. De nos jours, ce terme désigne plutôt la discipline qui s'intéresse aux structures et aux opérations sur les ensembles.

Proposition 2.8

Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors

$$P(a) = 0 \iff \text{Il existe } Q \in \mathbb{K}[X] \text{ tel que, } P = (X - a)Q$$

Démonstration.

- $\Longleftarrow$ Supposons qu'il existe $Q \in \mathbb{K}[X]$ tel que, pour tout $x \in \mathbb{K}$, $P = (X - a)Q$.
  Alors, $P(a) = (a - a)Q(a) = 0$.
- $\Longrightarrow$ Réciproquement, supposons que $P(a) = 0$.
  On effectue la division euclidienne de P par $X - a$.
  Ainsi, il existe des polynômes Q et R tels que

$$\begin{cases} P = (X - a)Q + R \ (\star) \\ \text{et} \\ \deg(R) < 1 \end{cases}$$

  Par conséquent, R est un polynôme constant. On note c cette constante.
  En évaluant l'égalité $(\star)$ pour $x = a$, on obtient

$$\begin{aligned} & P(a) = (X - a)Q(a) + c \\ \iff & 0 = 0 + c \\ \iff & 0 = c \end{aligned}$$

  Finalement, $R = 0$ et donc $P = (X - a)Q$.

□

Exemple 12. *On considère le polynôme* $P = X^3 - 1$.
Montrer que $(X - 1)$ *divise* P *puis établir la factorisation de* P *par* $X - 1$.

Solution :
$P(1) = 1^3 - 1 = 0$. *Ainsi,* 1 *est une racine de* P *donc* $X-1$ *divise* P.
On effectue la division euclidienne de P *par* $X-1$ *et on trouve :*

$$P = (X-1)(X^2+X+1).$$

Proposition 2.9

Pour tout $n \geqslant 1$, pour tout polynôme $P \in \mathbb{K}[X]$ de degré n, P admet au plus n racines.

Démonstration. On démontre par récurrence que la propriété $\mathscr{H}(n)$: « Pour tout $P \in \mathbb{K}[X]$ de degré n, P admet au plus n racines » est vraie pour tout entier $n \geqslant 1$.

- Initialisation : Si P est un polynôme de degré 1, $P = aX + b \quad (\text{avec } a \neq 0)$.
  Par conséquent, $-\dfrac{b}{a}$ est l'unique racine de P et donc $\mathscr{H}(1)$ est vraie.
- Hérédité : Supposons que $\mathscr{H}(n)$ soit vraie pour un certain entier $n \geqslant 1$. Montrons qu'alors $\mathscr{H}(n+1)$ est vraie.
  Soit $P \in \mathbb{K}[X]$ de degré $n+1$. On va montrer que P admet au plus $n+1$ racines.
  En fait, on peut supposer que P admet une racine (car sinon il n'y alors rien à démontrer). On note a cette racine.
  D'après la Proposition 7, il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)Q$.
  En utilisant la règle du produit nul, on voit que l'ensemble des racines de P est constitué de l'ensemble des racines de Q auquel on ajoute a.
  On a de plus $\deg(Q) = n$ et donc, d'après $\mathscr{H}(n)$, Q admet au plus n racines.
  Finalement, on en déduit que P admet au plus $n+1$ racines et donc que $\mathscr{H}(n+1)$ est vraie.

□

IV. Factorisation de polynômes

1. Factorisation dans $\mathbb{C}[X]$

Proposition 2.10

Soit $P \in \mathbb{C}[X]$. Il existe $x_1, x_2, \ldots, x_n \in \mathbb{C}$ et $a \in \mathbb{C}$ tels que

$$P = a \prod_{k=1}^{n} (X - x_k).$$

Remarque.

- *a est le coefficient dominant de* P.
- *Les nombres* x_k *ne sont pas nécessairement deux à deux distincts.*
- *On peut aussi utiliser ce résultat si* $P \in \mathbb{R}[X]$ *car* $\mathbb{R}[X] \subset \mathbb{C}[X]$.

Démonstration. On démontre par récurrence que la propriété $\mathscr{H}(n)$: « Pour tout $P \in \mathbb{C}[X]$ de degré n, il existe $x_1, x_2, \ldots, x_n \in \mathbb{C}$ et $a \in \mathbb{C}$ tels que, $P = a \prod_{k=1}^{n} (X - x_k)$ » est vraie pour tout entier $n \geqslant 1$.

- Initialisation : Si P est un polynôme de degré 1, $P(x) = aX + b$ (avec $a \neq 0$).
  En posant $x_1 = -\dfrac{b}{a}$, on a $P = a(X - x_1)$ et donc $\mathscr{H}(1)$ est vraie.
- Hérédité : Supposons que $\mathscr{H}(n)$ soit vraie pour un certain entier $n \geqslant 1$.
  Montrons qu'alors $\mathscr{H}(n+1)$ est vraie.
  Soit $P \in \mathbb{K}[X]$ de degré $n+1$.
  D'après le théorème de D'Alembert-Gauss, P admet une racine complexe (on la note x_{n+1}). De plus, d'après la Proposition 2.8, il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - x_{n+1})Q$.
  D'après l'hypothèse de récurrence, comme $\deg(Q) = n$, il existe $x_1, \ldots x_n \in \mathbb{C}$ et $a \in \mathbb{C}$ tels que $Q = a\prod_{k=1}^{n}(X - x_k)$.
  Par conséquent, on a

$$\begin{aligned} P &= (X - x_{n+1})Q \\ &= (X - x_{n+1}) \times a\prod_{k=1}^{n}(X - x_k) \\ &= a\prod_{k=1}^{n+1}(X - x_k) \end{aligned}$$

  Ainsi, on a montré que $\mathscr{H}(n+1)$ est vraie.

□

2. Factorisation dans $\mathbb{R}[X]$

Proposition 2.11

Soit $P \in \mathbb{R}[X]$. Il existe $x_1, x_2, \ldots, x_r \in \mathbb{R}$, il existe $s_1, t_1, s_2, t_2, \ldots s_l, t_l \in \mathbb{R}$ et $a \in \mathbb{R}$ tels que $P = a\prod_{k=1}^{r}(X - x_k) \times \prod_{k=1}^{l}(X^2 + s_k X + t_k)$ où les polynômes $X^2 + s_k X + t_k$ sont sans racines réelles, c'est-à-dire que $s_k^2 - 4t_k < 0$.

Démonstration. On sait, d'après la Proposition 2.10 qu'il existe $x_1, x_2, \ldots, x_n \in \mathbb{C}$ et $a \in \mathbb{C}$ tels que :

$$P = a\prod_{k=1}^{n}(X - x_k).$$

Quitte à permuter les x_i, on peut supposer que $x_1, x_2, \ldots, x_r \in \mathbb{R}$ et que $x_{r+1}, \ldots, x_n \in \mathbb{C} \setminus \mathbb{R}$.
Par conséquent, on a $P = a\prod_{k=1}^{r}(X - x_k) \times Q$ où Q admet pour racines $x_{r+1}, \ldots, x_n \in \mathbb{C} \setminus \mathbb{R}$ et, *a priori*, $Q \in \mathbb{C}[X]$.
En fait, comme les polynômes $a\prod_{k=1}^{r}(X - x_k)$ et P sont à coefficients réels, il en est de même pour Q (cela découle directement de l'unicité de la division euclidienne dans $\mathbb{R}[X]$).

Par ailleurs, d'après la Proposition 5, comme x_{r+1} est une racine de Q, $\overline{x_{r+1}}$ est également une racine de Q. Sachant que $x_{r+1} \neq \overline{x_{r+1}}$, Q est donc divisible par $(X - x_{r+1})(X - \overline{x_{r+1}})$.
Or,

$$\begin{aligned} (X - x_{r+1})(X - \overline{x_{r+1}}) &= X^2 - (x_{r+1} + \overline{x_{r+1}})X + x_{r+1}\overline{x_{r+1}} \\ &= X^2 - 2\mathrm{Re}(x_{r+1})X + (\mathrm{Re}(x_{r+1}))^2 + (\mathrm{Im}(x_{r+1}))^2 \end{aligned}$$

Cela prouve donc que $(X-x_{r+1})(X-\overline{x_{r+1}})$ est un polynôme à coefficient réel. Il existe donc des réels s_1 et t_1 tels que, pour tout $x \in \mathbb{R}$, $(X-x_{r+1})(X-\overline{x_{r+1}}) = X^2+s_1X+t_1$
Ainsi, il existe $Q' \in \mathbb{R}[X]$ tel que, $Q = (X^2+s_1X+t_1)Q'$ et les racines de Q' sont les racines de Q auxquelles on a enlevé x_{r+1} et $\overline{x_{r+1}}$.
En répétant le procédé avec Q', on voit que l'on pourra factoriser Q en produit de polynômes réels du second degré.
Finalement, on obtiendra une factorisation de P de la forme suivante :

$$P = a\prod_{k=1}^{r}(X-x_k) \times \prod_{k=1}^{l}(X^2+s_kX+t_k)$$

□

Exemple 13. *Factoriser dans* $\mathbb{R}[X]$ *et dans* $\mathbb{C}[X]$ *le polynôme* $P = X^4-1$.

Solution :
P *admet les quatre racines suivantes :* $1, -1, i, -i$.
Ainsi, $P = (X-1)(X+1)(X-i)(X+i)$ *(factorisation dans* $\mathbb{C}[X]$*)*
Par conséquent, $P = (X-1)(X+1)(X^2+1)$ *(factorisation dans* $\mathbb{R}[X]$*).*

3. Relations entre coefficients et racines

On rappelle les relations entre coefficients et racines pour un polynôme du second degré. L'objectif est ensuite de généraliser cette propriété au cas des polynômes de degré supérieur.

Proposition 2.12

Si $P = aX^2+bX+c$ avec x_1 et x_2 ses racines. Alors,

$$\begin{aligned} x_1+x_2 &= -\frac{b}{a} \\ x_1x_2 &= \frac{c}{a} \end{aligned}$$

Démonstration.
Soit $P = aX^2+bX+c$.
Comme x_1 et x_2 sont les racines de P, on sait que P se factorise de la façon suivante : $P = a(X-x_1)(X-x_2)$.
En développant, on obtient

$$\begin{aligned} P &= a\left(X^2-x_1X-x_2X+x_1x_2\right) \\ &= ax^2-a(x_1+x_2)X+ax_1x_2. \end{aligned}$$

Ainsi, en identifiant les coefficients, on obtient

$$\begin{cases} -a\left(x_1+x_2\right) = b \\ \text{et} \\ ax_1x_2 = c \end{cases}$$

Par conséquent,

$$\begin{cases} x_1 + x_2 &= -\dfrac{b}{a} \\ \text{et} & \\ x_1 x_2 &= \dfrac{c}{a} \end{cases}$$

□

Définition 2.9

Soit $P \in \mathbb{K}[X]$ tel que $P(X) = a\prod_{k=1}^{n}(X - x_k)$ avec $x_1, \dots x_n \in \mathbb{C}$ les racines de P. On définit les fonctions symétriques élémentaires des racines de la façon suivante :

$$\begin{aligned} \sigma_1 &= \sum_{1\leqslant k\leqslant n} x_k \\ \sigma_2 &= \sum_{1\leqslant k<l\leqslant n} x_k x_l \\ &\vdots \\ \sigma_k &= \sum_{1\leqslant k_1<\dots<k_s\leqslant n} x_{k_1} x_{k_2} \dots x_{k_s} \\ &\vdots \\ \sigma_n &= x_1 x_2 \dots x_n. \end{aligned}$$

Exemple 14. *Si* $P = (X - x_1)(X - x_2)(X - x_3)(X - x_4)$, *alors :*

$$\begin{aligned} \sigma_1 &= x_1 + x_2 + x_3 + x_4 \\ \sigma_2 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\ \sigma_3 &= x_1x_2x_3 + x_1x_2x_4 + x_2x_3x_4 \\ \sigma_4 &= x_1x_2x_3x_4. \end{aligned}$$

Proposition 2.13 – Relation entre coefficients et racines

Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ tel que $P(X) = a_n\prod_{k=1}^{n}(X - x_k)$ avec $x_1, \dots x_n \in \mathbb{C}$ les racines de P. On a alors, pour tout $1 \leqslant k \leqslant n$,

$$\sigma_k = (-1)^k \times \frac{a_{n-k}}{a_n}.$$

Remarque.
En particulier,

- *(pour $k = 1$)* $x_1 + x_2 \dots + x_n = -\dfrac{a_{n-1}}{a_n}$
- *(pour $k = n$)* $x_1x_2 \dots x_n = (-1)^n \times \dfrac{a_0}{a_n}$

Démonstration.
La démonstration s'effectue par récurrence et consiste, comme dans la preuve de la Proposition 2.12, à développer l'expression $a_n(X - x_1) \dots (X - x_n)$ puis à identifier le coefficient devant x^k. □