Claude Deschamps | François Moulin | Yoann Gentric
Emmanuel Delsinne | François Lussier | Chloé Mullaert
Serge Nicolas | Jean Nougayrède | Claire Tête

MATHS

MP/MP*-MPI/MPI*

j'intègre

TOUT-EN-UN

7e édition

DUNOD

Couverture : création Hokus Pokus, adaptation Studio Dunod

Retrouvez nos ouvrages pour les prépas scientifiques ici

http://dunod.link/prepassc

11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-088474-2

Table des matières

Avant-propos

Comme la précédente, cette édition du Tout-en-un de mathématiques est adaptée au programme entré en vigueur en classes préparatoires MPSI-MP2I en septembre 2021 puis en MP-MPI en septembre 2022. Grâce aux précieux retours faits par nos lecteurs (cf. adresse électronique en bas de page), des améliorations ont pu être apportées par rapport à l'édition précédente.

Rappelons l'ambition de ce livre : faire tenir, en un seul volume, cours complet et exercices corrigés.

Il nous tient à cœur de préciser quelques éléments clés de la structure du livre :

- Plutôt que de faire figurer systématiquement, à la suite de l'énoncé d'une proposition ou d'un théorème, sa démonstration entièrement rédigée, nous préférons parfois donner un principe de démonstration (la démonstration complète étant alors reléguée en fin de chapitre). L'objectif est double :
  - rendre l'exposé du cours plus concis et plus facile à lire lorsque l'étudiant ne souhaite pas s'attarder sur les démonstrations ;
  - l'étudiant, ayant à sa disposition un principe de démonstration, peut soit (en cas de première lecture) tenter de réfléchir par lui-même à la manière d'élaborer la preuve complète, soit (en cas de lecture ultérieure) se souvenir rapidement de cette preuve.
- Chaque chapitre se conclut par une série d'exercices permettant à l'étudiant de s'entraîner. Chacun de ces exercices est entièrement corrigé.
  - Certains de ces exercices ont pour mission de faire appliquer de manière ciblée un théorème ou une méthode ; sous le numéro de l'exercice est alors indiqué un renvoi vers la page du cours associée. Inversement, ces exercices sont signalés dans la marge, à l'endroit concerné du cours.

    S'il n'est pas totalement indispensable de traiter ces exercices lors d'une première lecture du cours, leur lien étroit avec celui-ci les rend particulièrement intéressants pour assimiler les nouvelles notions et méthodes.
  - L'étudiant trouvera également des exercices d'entraînement un peu plus ambitieux, demandant plus de réflexion. Certains, plus difficiles, sont étoilés.

Bien entendu, nous sommes à l'écoute de toute remarque dont les étudiants, nos collègues, tout lecteur... pourraient nous faire part, et qui nous permettra de continuer à faire évoluer cet ouvrage.

François Moulin et Yoann Gentric
touten1maths@gmail.com

« Mode d'emploi » d'un chapitre

Une introduction présente le sujet traité.

Compléments d'algèbre linéaire

Dans ce chapitre, E est un espace vectoriel sur un sous-corps $\mathbb{K}$ de $\mathbb{C}$ (on se limite en pratique au cas où $\mathbb{K}$ est égal à $\mathbb{R}$ ou $\mathbb{C}$).

Les encadrés correspondent soit à des théorèmes, propositions ou corollaires, qui partagent le même système de numérotation, soit à des définitions, qui ont leur propre numérotation.

Corollaire 46

Dans un groupe G fini de cardinal n, on a $\forall x \in G \quad x^n = e$.

Théorème 47 (Théorème d'Euler)

Soit $n \in \mathbb{N}^*$. Pour tout $a \in \mathbb{Z}$ premier avec n, on a $a^{\varphi(n)} \equiv 1\ [n]$.

Définition 7

Une **sous-algèbre** d'une algèbre A est un sous-espace vectoriel de A stable par multiplication et contenant 1_A.

La démonstration de chaque résultat encadré, lorsqu'elle ne suit pas directement celui-ci, est indiquée par un renvoi.

Proposition 4

Étant donné une partie X de A, il existe un plus petit idéal de A contenant X.

Démonstration page 26

Les points de méthode apparaissent sur fond grisé.

Point méthode Pour définir par $\overline{k} \mapsto \varphi(k)$ une application sur $\mathbb{Z}/n\mathbb{Z}$, on vérifiera bien que $\varphi(k)$ ne dépend que de la classe de congruence de k modulo n.

Les points auxquels il faut faire particulièrement attention sont signalés par un filet vertical sur la gauche.

> **Attention** La relation $a^n = e$ ne signifie pas que a est d'ordre n, mais seulement que son ordre divise n d'après la proposition suivante.

Des renvois vers des exercices peuvent apparaître en marge au sein du cours.

Exo 2.12

Définition 4

Un sous-espace vectoriel F de E est dit **stable** par u si $u(F) \subset F$.

Les exemples sont repérés par deux coins.

Ex. 48. Pour $n \in \mathbb{N}^*$, le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Des exercices sont proposés en fin de chapitre, avec éventuellement un rappel du numéro de la page de cours où se trouve la notion dont l'exercice est une application.

S'entraîner et approfondir

Séries à valeurs dans un espace vectoriel de dimension finie

10.1 (→422) Prouver la convergence et déterminer la somme de la série $\sum A^n$, où $A = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.

Certains exercices bénéficient d'indications, et les plus difficiles sont étoilés.

⋆ **3.6** Soit A et B deux matrices de $\mathcal{M}_n(\mathbb{C})$.
Montrer que A et B ont une valeur propre commune si, et seulement s'il existe une matrice U non nulle de $\mathcal{M}_n(\mathbb{C})$ telle que $AU = UB$.

Tous les exercices sont entièrement corrigés.

Solutions des exercices

1.1 Soit A un anneau fini intègre et $a \in A$ non nul. L'application $x \mapsto ax$ de A dans A est injective par intégrité de A. Comme A est fini, elle est bijective, donc 1 admet un antécédent, ce qui signifie qu'il existe $b \in A$ tel que $ab = 1$. Comme A est commutatif (puisqu'intègre), on a aussi $ba = 1$ et donc a est inversible.

Ainsi, A est un corps.

Chapitre 1 : Groupes, anneaux, arithmétique, algèbres

Groupes, anneaux, arithmétique, algèbres

Nous revenons dans ce chapitre sur les structures algébriques usuelles introduites en première année : groupes, anneaux et corps, notamment en vue de leur utilisation en arithmétique (dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$) et nous les complétons par la notion d'*algèbre* dont deux exemples importants en algèbre linéaire (algèbres des endomorphismes et des matrices carrées) seront étudiés dans le chapitre de réduction des endomorphismes. Enfin, nous conclurons par des approfondissements sur les groupes.
Dans ce chapitre, nous supposons acquises les notions suivantes vues en première année :

- groupe, sous-groupe et morphisme de groupes,
- anneau et corps, sous-anneau et morphisme d'anneaux.

I Anneaux, arithmétique

1 Rappels et notations

- Dans un anneau A, le neutre pour l'addition est noté 0 (ou 0_A), le neutre pour la multiplication 1 (ou 1_A).
- L'anneau est commutatif si la multiplication est commutative (l'addition est commutative par définition).
- Un anneau A est **trivial** si $1_A = 0_A$; dans ce cas, A est réduit à cet unique élément (on dit aussi qu'il est **nul**).
- Un anneau A est intègre s'il est commutatif, non trivial, et s'il vérifie :

Exo 1.1

$$\forall (a,b) \in A^2 \quad ab = 0 \Longrightarrow (a = 0 \quad \text{ou} \quad b = 0)\,.$$

- Rappelons qu'un corps est un anneau commutatif non trivial dans lequel tout élément non nul est inversible.

2 Anneau produit

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

Proposition 1

Étant donné des anneaux $A_1, \dots, A_n$, les opérations terme à terme :

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$$

$$(a_1, \dots, a_n) \times (b_1, \dots, b_n) = (a_1 b_1, \dots, a_n b_n)$$

munissent le produit cartésien $A_1 \times \cdots \times A_n$ d'une structure d'anneau.

Démonstration. On sait déjà que $(A_1 \times \cdots \times A_n, +)$ est un groupe (groupe produit) de neutre $(0_{A_1}, \dots, 0_{A_n})$. On vérifie facilement que $(1_{A_1}, \dots, 1_{A_n})$ est neutre pour la multiplication. Enfin, les propriétés d'associativité et de distributivité se déduisent immédiatement des propriétés correspondantes des anneaux $(A_i, +, \times)$. □

Ex. 1. Si A est un anneau, alors A^n est un anneau, comme produit de n exemplaires de A. En particulier, $\mathbb{R}^n$ et $\mathbb{C}^n$ sont des anneaux.

Ex. 2. Dans un anneau produit $A_1 \times \cdots \times A_n$, les éléments inversibles sont les $(a_1, \dots, a_n)$, où a_i est inversible dans A_i pour tout i, avec alors $(a_1, \dots, a_n)^{-1} = (a_1^{-1}, \dots, a_n^{-1})$.

Exo 1.2

3 Idéaux d'un anneau commutatif

Soit A un anneau commutatif.

Définition 1 (Idéal d'un anneau commutatif)

On dit qu'une partie I de A est un **idéal** de A si :

- I est un sous-groupe de $(A, +)$;
- I est stable par multiplication par tout élément de A, c'est-à-dire :

$$\forall x \in I \quad \forall a \in A \quad xa \in I.$$

Remarque Par commutativité de A, un idéal I de A vérifie aussi :

$$\forall x \in I \quad \forall a \in A \quad ax \in I.$$

Ex. 3. A et $\{0\}$ sont évidemment des idéaux de A, appelés **idéaux triviaux** de A.

Ex. 4. Soit X une partie de $\mathbb{R}$. L'ensemble des fonctions nulles en tout point de X est un idéal de $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

Exo 1.3

Exo 1.4

Remarque
Si I est un idéal de A contenant 1, alors $\forall a \in A \quad a = a.1 \in I$, donc $I = A$.

Attention Soit B un anneau. Le **noyau** d'un morphisme d'anneaux de A dans B, c'est-à-dire son noyau en tant que morphisme de groupes de $(A,+)$ dans $(B,+)$ n'est pas un sous-anneau de $(A,+,\times)$ si B est non trivial puisqu'alors $\varphi(1_A) = 1_B \neq 0_B$ et donc que $1_A \notin \operatorname{Ker}\varphi$.
En revanche :

Proposition 2

Le noyau de tout morphisme d'anneaux φ de A dans un anneau B est un idéal de A.

Démonstration. C'est un sous-groupe de $(A,+)$ en tant que noyau d'un morphisme de groupes. Soit $x \in \operatorname{Ker}\varphi$ et $a \in A$. On a $\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \times 0 = 0$. Donc $\operatorname{Ker}\varphi$ est un idéal de A. □

Idéal engendré par un élément

Proposition 3

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

Démonstration page 26

Proposition 4

Étant donné une partie X de A, il existe un plus petit idéal de A contenant X.

Démonstration page 26

Principe de démonstration. C'est l'intersection de tous les idéaux de A contenant X.

Terminologie

- On l'appelle **idéal** de A **engendré par** $\boldsymbol{X}$.
- Si x est un élément de A, l'**idéal engendré par** $\boldsymbol{x}$ est, par définition, l'idéal engendré par $\{x\}$, c'est-à-dire le plus petit idéal de A contenant x.

Proposition 5 (Idéal engendré par un élément)

Exo 1.5

Soit $x \in A$. L'idéal engendré par x est $xA = \{xa \mid a \in A\}$.

Démonstration page 26

Proposition 6

L'idéal de A engendré par une partie finie $\{x_1, \ldots, x_k\}$ est :

$$x_1A + \cdots + x_kA = \{x_1a_1 + \cdots + x_ka_k \mid (a_1, \ldots, a_k) \in A^k\}.$$

C'est aussi le plus petit idéal de A contenant tous les idéaux $x_1A, \ldots, x_kA$.

Démonstration page 26

4 Divisibilité dans un anneau intègre

On suppose à partir de maintenant que A est un anneau intègre.

Définition 2

Soit $(x,y) \in A^2$. On dit que x **divise** y, ou que y est un **multiple** de x, s'il existe $z \in A$ tel que $y = xz$. On note alors $x \mid y$.

Terminologie

- Lorsque x divise y, on dit aussi que x est un **diviseur** de y ou que y est un **multiple** de x.
- Lorsque x non nul divise y, il y a, par intégrité de A, unicité de $z \in A$ tel que $y = xz$. Cet élément est alors appelé **quotient** de y par x.

Remarque Pour tout $(x, y) \in A^2$, on a $x \mid y \iff y \in xA$.

La relation de divisibilité est une relation réflexive et transitive, mais n'est en général ni symétrique ni antisymétrique (ce n'est donc ni une relation d'ordre, ni une relation d'équivalence).

Ex. 5. Les diviseurs de 1 sont les éléments inversibles.

Ex. 6. Tout élément de A divise 0, mais 0 ne divise que lui-même.

Ex. 7. Grâce à l'intégrité, on a, pour tout $a \neq 0$:

$$ax \mid ay \iff (\exists z \in A \quad ay = axz) \iff (\exists z \in A \quad y = xz) \iff x \mid y.$$

Lien avec les idéaux

La proposition suivante permet de ramener la notion de divisibilité à une relation d'ordre (inclusion sur les idéaux).

Proposition 7

On a, pour tout $(x, y) \in A^2$:

$$x \mid y \iff yA \subset xA.$$

Démonstration. Soit $(x, y) \in A^2$. Comme yA est le plus petit idéal de A contenant y et que xA est un idéal, l'inclusion $yA \subset xA$ est équivalente à $y \in xA$, c'est-à-dire à $x \mid y$. □

Remarque Deux éléments engendrent le même idéal si, et seulement s'ils se divisent mutuellement. On dit alors qu'ils sont **associés**.

Terminologie Les idéaux engendrés par un élément sont appelés **idéaux principaux**. L'exemple qui suit montre qu'il existe des idéaux non principaux.

Ex. 8. Considérons l'anneau $\mathbb{Z}[X]$ des polynômes à coefficients entiers et $I = 2\mathbb{Z}[X] + X\mathbb{Z}[X]$ l'idéal engendré par 2 et X. Supposons que I soit principal, c'est-à-dire qu'il existe un polynôme $P \in \mathbb{Z}[X]$ tel que $I = P\mathbb{Z}[X]$. Les inclusions $2\mathbb{Z}[X] \subset P\mathbb{Z}[X]$ et $X\mathbb{Z}[X] \subset P\mathbb{Z}[X]$ montrent alors, d'après la proposition 7, que P divise 2, donc qu'il est constant, et qu'il divise X, donc que son coefficient dominant est ± 1. Finalement, $P = \pm 1$ et il existe donc deux polynômes $(U, V) \in \mathbb{Z}[X]^2$ tels que $\pm 1 = 2U + XV$. En évaluant en 0, cela donne $2U(0) = \pm 1$, ce qui est absurde puisque $U(0) \in \mathbb{Z}$.
Donc I n'est pas principal.

Idéaux de $\mathbb{Z}$

Commençons par un résultat sur les sous-groupes de $\mathbb{Z}$.

Proposition 8

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

Démonstration page 26

Principe de démonstration. Si H est un sous-groupe non nul de $\mathbb{Z}$, on considère le plus petit élément n strictement positif de H et l'on utilise la division euclidienne par n pour montrer que tout élément de H est un multiple de n.

On en déduit que tous les idéaux de $\mathbb{Z}$ sont principaux :

Théorème 9

Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, pour $n \in \mathbb{N}$.

Démonstration.

- Pour tout $n \in \mathbb{N}$, l'ensemble $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ des multiples de n est un idéal de $\mathbb{Z}$: c'est l'idéal de $\mathbb{Z}$ engendré par n (cf. proposition 5 de la page 4).
- Réciproquement, un idéal étant en particulier un sous-groupe, il n'y en a pas d'autres d'après la proposition 8. □

Remarque Soit I un idéal de $\mathbb{Z}$. Il existe donc $n \in \mathbb{N}$ tel que $I = n\mathbb{Z}$.

- Si m est un entier relatif tel que $I = m\mathbb{Z}$, alors $n \in m\mathbb{Z}$ et $m \in n\mathbb{Z}$, donc $m \mid n$ et $n \mid m$, ce qui donne $m = \pm n$.
- Réciproquement, il est clair que $(-n)\mathbb{Z} = n\mathbb{Z}$.

On a ainsi montré l'unicité de $n \in \mathbb{N}$ tel que $I = n\mathbb{Z}$: on l'appelle **le générateur** de l'idéal I.

5 Retour sur le PGCD dans $\mathbb{Z}$

Soit $n \in \mathbb{N}^*$ et $a_1, \ldots, a_n$ des entiers relatifs. Nous avons vu à la proposition 6 de la page 4 que l'idéal de $\mathbb{Z}$ engendré par les éléments $a_1, \ldots, a_n$ était $I = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$. Cela permet de donner une nouvelle définition du PGCD.

Proposition 10

Étant donné des entiers $a_1, \ldots, a_n$, il existe un unique entier naturel d tel que $d\mathbb{Z} = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$. Pour tout $k \in \mathbb{Z}$, on a la relation :

$$k \mid d \iff \big(\forall i \in [\![1, n]\!] \quad k \mid a_i\big).$$

On l'appelle **PGCD** de $a_1, \ldots, a_n$ et l'on dispose de la **relation de Bézout** :

$$\exists (u_1, \ldots, u_n) \in \mathbb{Z}^n \quad d = a_1u_1 + \cdots + a_nu_n.$$

Démonstration.

- Considérons le générateur de l'idéal $a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$, c'est-à-dire l'unique $d \in \mathbb{N}$ tel que $d\mathbb{Z} = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$ (cf. remarque de la présente page).

Ainsi, $d\mathbb{Z}$ est le plus petit idéal de $\mathbb{Z}$ contenant $\{a_1, \dots, a_n\}$ (proposition 6 de la page 4), donc pour tout $k \in \mathbb{Z}$, puisque $k\mathbb{Z}$ est un idéal de $\mathbb{Z}$:

$$\begin{aligned} k \mid d &\iff d\mathbb{Z} \subset k\mathbb{Z} \\ &\iff \forall i \in [\![1, n]\!] \quad a_i \in k\mathbb{Z} \\ &\iff \forall i \in [\![1, n]\!] \quad k \mid a_i. \end{aligned}$$

- Enfin, puisque $d \in d\mathbb{Z} = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$, on a par définition :

$$\exists (u_1, \dots, u_n) \in \mathbb{Z}^n \quad d = a_1u_1 + \cdots + a_nu_n.$$ □

Remarques

- Les diviseurs communs à $a_1, \dots, a_n$ sont donc exactement les diviseurs de d.
- Lorsque d est non nul, c'est-à-dire lorsqu'au moins l'un des a_i est non nul, c'est donc le plus grand parmi tous les diviseurs positifs communs à $a_1, \dots, a_n$ (et même parmi tous les diviseurs communs à $a_1, \dots, a_n$).
- De la même façon, on pourrait définir le **PPCM** de $a_1, \dots, a_n$ comme le générateur m de l'idéal $a_1\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z}$, de façon à avoir, pour tout $k \in \mathbb{Z}$, l'équivalence :

$$k \in m\mathbb{Z} \iff \big(\forall i \in [\![1, n]\!] \quad k \in a_i\mathbb{Z}\big).$$

C'est le plus petit des multiples positifs communs à $a_1, \dots, a_n$.

6 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Congruences dans $\mathbb{Z}$

Soit n un entier naturel.

Rappels Nous avons vu en première année la relation de congruence modulo n définie par :

$$x \equiv y \ [n] \iff y - x \in n\mathbb{Z}.$$

Il s'agit une relation d'équivalence sur $\mathbb{Z}$ qui est compatible avec les opérations de $\mathbb{Z}$, c'est-à-dire qui vérifie :

$$\forall (x, y, x', y') \in \mathbb{Z}^4 \quad \left\{ \begin{array}{l} x \equiv x' \ [n] \\ y \equiv y' \ [n] \end{array} \right. \implies \left\{ \begin{array}{l} x + y \equiv x' + y' \ [n] \\ x \times y \equiv x' \times y' \ [n]. \end{array} \right.$$

Notation On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence pour cette relation. La classe d'un élément k de $\mathbb{Z}$ est souvent notée $\overline{k}$.

Ex. 9. La congruence modulo 0 est la relation d'égalité, donc $\mathbb{Z}/0\mathbb{Z} = \big\{\{k\} \mid k \in \mathbb{Z}\big\}$.

Ex. 10. Deux entiers quelconques sont évidemment congrus modulo 1, donc $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$.

Ex. 11. Modulo 2, il y a deux classes : celle des entiers pairs et celle des entiers impairs. Donc $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$.

Proposition 11

Pour $n \in \mathbb{N}^*$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ a n éléments, et l'on a :

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

Démonstration page 27

Principe de démonstration. Utiliser la division euclidienne par n.

Ex. 12. Soit n et p deux entiers naturels non nuls. Pour $k \in \mathbb{Z}$, nous noterons $[k]_n$ et $[k]_p$ les classes de k respectivement modulo n et p.
Voyons à quelle condition on peut définir une application :

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ [k]_n & \longmapsto & [k]_p. \end{array}$$

- Si une telle application existe, comme $[n]_n = [0]_n$, on doit avoir $[n]_p = [0]_p$, soit $p \mid n$.
- Supposons réciproquement que p divise n. Alors si k et ℓ sont deux entiers tels que $[k]_n = [\ell]_n$, on a $n \mid k - \ell$, donc $p \mid k - \ell$, soit $[k]_p = [\ell]_p$. On peut donc bien définir l'application :

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ \alpha & \longmapsto & [k]_p \quad \text{où } k \in \alpha \end{array}$$

puisque la définition de l'image de α ne dépend que de α et non d'un de ses représentants.

Point méthode Pour définir par $\overline{k} \mapsto \varphi(k)$ une application sur $\mathbb{Z}/n\mathbb{Z}$, on vérifiera bien que $\varphi(k)$ ne dépend que de la classe de congruence de k modulo n.

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

Proposition 12

Il existe sur $\mathbb{Z}/n\mathbb{Z}$ des lois, notées $+$ et $\times$ et appelées **lois quotient**, telles que :

1. $\forall (x, y) \in (\mathbb{Z}/n\mathbb{Z})^2 \quad \overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x} \times \overline{y} = \overline{x \times y}$,
2. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ soit un anneau commutatif d'éléments neutres $\overline{0}$ et $\overline{1}$,
3. la **projection canonique** $\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto & \overline{x} \end{array}$ soit un morphisme d'anneaux surjectif de noyau $n\mathbb{Z}$.

Démonstration page 27

Principe de démonstration. Pour α et β dans $\mathbb{Z}/n\mathbb{Z}$, on définit :

$$\alpha + \beta = \overline{x+y} \quad \text{et} \quad \alpha \times \beta = \overline{x \times y} \qquad \text{où} \qquad x \in \alpha \quad \text{et} \quad y \in \beta.$$

Il faut commencer par vérifier que $\overline{x+y}$ et $\overline{x \times y}$ ne dépendent que de α et β, et non des représentants x et y choisis, grâce à la compatibilité de la relation de congruence avec les lois de $\mathbb{Z}$.

Notation Le produit de deux éléments α et β de $\mathbb{Z}/n\mathbb{Z}$ est souvent noté $\alpha\beta$ plutôt que $\alpha \times \beta$.

Ex. 13. Écrivons les tables d'addition et de multiplication de $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$. Pour alléger les notations, nous écrirons $0, 1, 2, \ldots$ à la place de $\overline{0}, \overline{1}, \overline{2}, \ldots$

$\mathbb{Z}/5\mathbb{Z}$:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}/6\mathbb{Z}$:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

On remarque que $\mathbb{Z}/5\mathbb{Z}$ est intègre puisque pour avoir $\alpha\beta = 0$ il est nécessaire d'avoir $\alpha = 0$ ou $\beta = 0$ (absence de 0 dans la portion entourée de pointillés).
En revanche, $\mathbb{Z}/6\mathbb{Z}$ est non intègre puisque, par exemple $\overline{2} \times \overline{3} = \overline{0}$.

Remarque On peut aussi prendre pour représentants des classes modulo $n \in \mathbb{N}^*$, n'importe quel n-uplet d'entiers consécutifs. Par exemple, pour étudier la multiplication sur $\mathbb{Z}/5\mathbb{Z}$, il pourra être intéressant d'écrire $\mathbb{Z}/5\mathbb{Z} = \left\{-\overline{2}, -\overline{1}, \overline{0}, \overline{1}, \overline{2}\right\}$.

Ex. 14. Pour résoudre l'équation $x^2 - \overline{1} = \overline{0}$ dans $\mathbb{Z}/12\mathbb{Z}$, il suffit de lister les carrés des éléments de $\mathbb{Z}/12\mathbb{Z}$ pour voir lesquels sont égaux à $\overline{1}$:

x	$\overline{0}$	$\pm\overline{1}$	$\pm\overline{2}$	$\pm\overline{3}$	$\pm\overline{4}$	$\pm\overline{5}$	$\overline{6}$
x^2	$\overline{0}$	$\overline{1}$	$\overline{4}$	$-\overline{3}$	$\overline{4}$	$\overline{1}$	$\overline{0}$

On en déduit que $x^2 - \overline{1} = \overline{0} \iff x \in \{-\overline{1}, \overline{1}, -\overline{5}, \overline{5}\}$.

Proposition 13 (Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$)

La classe de $k \in \mathbb{Z}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, k est premier avec n.

Démonstration page 27

Principe de démonstration. L'élément $\overline{k}$ de $\mathbb{Z}/n\mathbb{Z}$ est inversible si, et seulement s'il existe $(u, v) \in \mathbb{Z}^2$ tel que $ku + nv = 1$ et son inverse est alors $\overline{u}$.

Remarque Trouver l'inverse de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$ revient à trouver l'inverse de k modulo n (voir le cours de première année). Rappelons (c'est d'ailleurs aussi ce qui a été fait dans la démonstration précédente) qu'il suffit pour cela de trouver un couple (u, v) tel que $ku + nv = 1$ (coefficients de Bézout). L'inverse de $\overline{k}$ est alors $\overline{u}$.

Ex. 15. Déterminons l'inverse de $\overline{13}$ dans $\mathbb{Z}/34\mathbb{Z}$.
On trouve, par exemple à l'aide de l'algorithme d'Euclide (voir le cours de première année), l'égalité de Bézout $5 \times 34 - 13 \times 13 = 1$, donc l'inverse de $\overline{13}$ est $-\overline{13} = \overline{21}$ dans $\mathbb{Z}/34\mathbb{Z}$.

Théorème 14

Soit $n \in \mathbb{N}^*$. Alors $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration page 27

Principe de démonstration.

- Si n est premier, tous les éléments de $[\![1, n-1]\!]$ sont premiers avec n, donc leur classe est inversible.
- Si $n = ab$, alors $\overline{a} \times \overline{b} = \overline{ab} = \overline{0}$, ce qui permet de montrer que $\mathbb{Z}/n\mathbb{Z}$ est non intègre si n n'est pas premier.

Notation Lorsque p est un nombre premier, le corps $\mathbb{Z}/p\mathbb{Z}$ est aussi noté $\mathbb{F}_p$.

7 Théorème chinois

On note ici $[k]_n$ la classe de l'entier k modulo un entier naturel non nul n.

Proposition 15

Soit n et m des entiers naturels premiers entre eux. Les anneaux $\mathbb{Z}/(nm)\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ sont isomorphes par le morphisme d'anneaux φ :

$$\begin{array}{ccc} \mathbb{Z}/(nm)\mathbb{Z} & \longrightarrow & (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \\ [k]_{nm} & \longmapsto & \big([k]_n, [k]_m\big). \end{array}$$

Démonstration page 28

Principe de démonstration. Pour la définition de φ, vérifier que le couple $\big([k]_n, [k]_m\big)$ ne dépend que de la classe de k modulo nm.

On démontre l'injectivité de φ et l'on conclut par cardinalité.

Le corollaire suivant n'est que la traduction en termes de congruence de la proposition 15.

Corollaire 16 (Théorème chinois)

Si n et m sont des entiers premiers entre eux, alors pour tout $(a, b) \in \mathbb{Z}^2$, il existe un entier k vérifiant le système :

$$\left\{ \begin{array}{l} k \equiv a\ [n] \\ k \equiv b\ [m] \end{array} \right. \qquad (S)$$

et les solutions de ce système sont exactement les entiers congrus à k modulo nm.

Le théorème chinois permet de ramener l'étude d'une équation sur $\mathbb{Z}/n\mathbb{Z}$ lorsque n n'est pas premier, à celle d'équations sur des anneaux plus simples.

Point méthode (pour obtenir une solution de (S)) À partir d'une relation de Bézout $mu + nv = 1$, on trouve deux entiers $k_1 = mu$ et $k_2 = nv$ vérifiant respectivement les systèmes de congruences :

$$\left\{ \begin{array}{l} k_1 \equiv 1\ [n] \\ k_1 \equiv 0\ [m] \end{array} \right. \qquad \text{et} \qquad \left\{ \begin{array}{l} k_2 \equiv 0\ [n] \\ k_2 \equiv 1\ [m] \end{array} \right.$$

et une solution du système (S) est alors $k = k_1 a + k_2 b$ (vérification immédiate en prenant les congruences modulo n et m).

Ex. 16. Trouvons les entiers k tels que $k^2+k+11 \equiv 0\ [143]$, c'est-à-dire tels que l'on ait simultanément $k^2+k+11 \equiv 0\ [11]$ et $k^2+k+11 \equiv 0\ [13]$.
Cela revient à résoudre l'équation $x^2+x+11=0$ dans $\mathbb{Z}/11\mathbb{Z}$ et dans $\mathbb{Z}/13\mathbb{Z}$. Pour chaque couple de solutions $\big([a]_{11},[b]_{13}\big)$, le point méthode précédent donne la classe modulo 143 correspondante.

- Dans $\mathbb{Z}/11\mathbb{Z}$, l'équation devient $x^2+x=0$, c'est-à-dire $x(x+1)=0$.
  Comme $\mathbb{Z}/11\mathbb{Z}$ est un corps, cela équivaut à $x=0$ ou $x=-1$.
- De même, dans $\mathbb{Z}/13\mathbb{Z}$, on obtient l'équation $x^2+x-2=0$, c'est-à-dire $(x-1)(x+2)=0$, ce qui donne, puisque $\mathbb{Z}/13\mathbb{Z}$ est un corps, les deux solutions $x=1$ ou $x=-2$.
- On a donc 4 solutions modulo 143 à l'équation initiale données, en reprenant les notations du corollaire 16 de la page précédente, par $a \in \{0,-1\}$ et $b=\{1,-2\}$.
- Une relation de Bézout entre 11 et 13 est $6\times 11-5\times 13=1$. Ainsi $k_1=-65$ vérifie $k_1\equiv 1\ [11]$ et $k_1\equiv 0\ [13]$. De même, $k_2=66$ vérifie $k_2\equiv 0\ [11]$ et $k_2\equiv 1\ [13]$.
- Pour chaque couple (a,b), la solution correspondante est ak_1+bk_2. Les résultats sont récapitulés dans le tableau ci-dessous :

a \ b	1	-2
0	66	11
-1	131	76

Remarque L'obtention d'une telle solution est non triviale, mais il est très facile de vérifier qu'elle est effectivement solution, ce qui permet de repérer une erreur de calcul éventuelle. Par exemple il est immédiat que 76 est bien congru à -1 modulo 11 et à -2 modulo 13.

Corollaire 17

Étant donné des entiers naturels $n_1,\dots,n_r$ premiers entre eux deux à deux, les anneaux $\mathbb{Z}/(n_1\cdots n_r)\mathbb{Z}$ et $(\mathbb{Z}/n_1\mathbb{Z})\times\cdots\times(\mathbb{Z}/n_r\mathbb{Z})$ sont isomorphes.

Démonstration. Par récurrence sur r, en remarquant que si $n_1,\dots,n_{r+1}$ sont premiers entre eux deux à deux, alors $n_1\cdots n_r$ et n_{r+1} sont premiers entre eux et $(\mathbb{Z}/n_1\mathbb{Z})\times\cdots\times(\mathbb{Z}/n_{r+1}\mathbb{Z})$ est isomorphe à $\big((\mathbb{Z}/n_1\mathbb{Z})\times\cdots\times(\mathbb{Z}/n_r\mathbb{Z})\big)\times(\mathbb{Z}/n_{r+1}\mathbb{Z})$. □

8 Indicatrice d'Euler

Définition 3

On appelle **indicatrice d'Euler** de $n\in\mathbb{N}^*$, et l'on note $\varphi(n)$, le cardinal de l'ensemble :

$$\big\{k\in[\![1,n]\!]\ :\ k\wedge n=1\big\}.$$

Remarques

- On a évidemment $\varphi(1)=1$.
- Pour $n\geqslant 2$, $\varphi(n)$ est aussi le nombre d'éléments de $[\![1,n-1]\!]$ premiers avec n.
- Dans tous les cas, c'est aussi le nombre d'éléments de $[\![0,n-1]\!]$ premiers avec n, donc également le nombre d'éléments inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Ex. 17. Pour tout $n \geqslant 2$, on a $\varphi(n) \leqslant n-1$ avec égalité si, et seulement si, n est premier. En effet, d'après les remarques précédentes, $\varphi(n)$ est le nombre d'éléments de $[\![1, n-1]\!]$ premiers avec n (d'où l'inégalité) et n est premier si, et seulement si, tous les éléments de $[\![1, n-1]\!]$ sont premiers avec n.

Exo 1.7

Lemme 18

Soit p un nombre premier. Pour tout $k \in \mathbb{N}^*$, on a $\varphi(p^k) = p^k - p^{k-1}$.

Démonstration. Les éléments qui sont non premiers avec p^k sont les multiples de p, c'est-à-dire $p, 2p, \ldots, (p^{k-1})p$ pour ceux qui sont dans $[\![1, p^k]\!]$. Il y en a donc p^{k-1}. □

Proposition 19

Étant donné des entiers naturels $n_1, \ldots, n_r$ premiers entre eux deux à deux, on a $\varphi(n_1 \cdots n_r) = \varphi(n_1) \cdots \varphi(n_r)$.

Démonstration page 28

Principe de démonstration. L'isomorphisme d'anneaux du corollaire 17 de la page précédente entre $\mathbb{Z}/(n_1 \cdots n_r)\mathbb{Z}$ et $(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})$ induit une bijection entre leurs groupes des unités.

Corollaire 20

Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, avec $p_1, \ldots, p_r$ des nombres premiers distincts deux à deux et $\alpha_1, \ldots, \alpha_r$ des entiers naturels non nuls, alors on a :

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Démonstration. À l'aide du résultat précédent et du lemme 18, il vient :

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r}) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdots \left(p_r^{\alpha_r} - p_r^{\alpha_r - 1}\right),$$

ce qui donne le résultat après factorisation par $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. □

II Anneau des polynômes à une indéterminée

On considère ici un sous-corps $\mathbb{K}$ de $\mathbb{C}$. La structure d'anneau de $\mathbb{K}[X]$, étudiée en première année lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$, se définit de la même manière dans le cas général [1].

On conserve en particulier la notion de degré ainsi que ses propriétés qui permettent de montrer le résultat suivant.

Proposition 21

L'anneau $\mathbb{K}[X]$ est intègre.

Démonstration page 28

On conserve aussi le théorème de division euclidienne, dont la démonstration est exactement la même que celle qui a été faite en première année dans le cas de $\mathbb{R}$ ou de $\mathbb{C}$.

1. En fait, tout ce qui est fait ici est valable pour un corps quelconque, en particulier pour un corps fini $\mathbb{F}_p$, avec p premier.

Théorème 22

Soit A et B deux polynômes de $\mathbb{K}[X]$, avec $B \neq 0$.

Il existe un unique couple (Q, R) de polynômes de $\mathbb{K}[X]$ vérifiant :

$$A = BQ + R \qquad \text{et} \qquad \deg R < \deg B.$$

1 Propriétés arithmétiques élémentaires

Nous allons maintenant généraliser les propriétés arithmétiques de $\mathbb{K}[X]$ vues en première année lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$.

Ex. 18. Un polynôme B non nul divise $A \in \mathbb{K}[X]$ si, et seulement si, le reste de la division euclidienne de A par B est nul.

Ex. 19. Soit $\mathbb{K}'$ un sous-corps de $\mathbb{K}$ ainsi que A et B deux polynômes à coefficients dans $\mathbb{K}'$, avec B non nul. Montrons que le polynôme B divise A dans $\mathbb{K}'[X]$ si, et seulement s'il divise A dans $\mathbb{K}[X]$.

Il est évident que si B divise A dans $\mathbb{K}'[X]$, alors il divise A dans $\mathbb{K}[X]$. Réciproquement, supposons qu'il existe $C \in \mathbb{K}[X]$ tel que $A = BC$. La division euclidienne de A par B dans $\mathbb{K}'[X]$ s'écrit $A = BQ + R$, avec $(Q, R) \in \mathbb{K}'[X]^2$ et $\deg R < \deg B$. On dispose alors des deux égalités dans $\mathbb{K}[X]$:

$$A = BQ + R \quad \text{avec} \quad \deg R < \deg B \qquad \text{et} \qquad A = BC + 0 \quad \text{avec} \quad \deg 0 < \deg B$$

et l'unicité de la division euclidienne dans $\mathbb{K}[X]$ donne $R = 0$. Donc B divise A dans $\mathbb{K}'[X]$.

Inversibles

Proposition 23

Les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls.

Démonstration page 28

Polynômes associés

Proposition 24

Soit A et B deux éléments de $\mathbb{K}[X]$. Les propriétés suivantes sont équivalentes :

(i) $A \mid B$ et $B \mid A$;

(ii) il existe $\lambda \in \mathbb{K}^*$ tel que $B = \lambda A$.

On dit alors que A et B sont **associés**.

Démonstration page 28

Ex. 20. 0 n'est associé qu'à lui-même.

Ex. 21. Les éléments inversibles de $\mathbb{K}[X]$ sont les associés de 1.

Ex. 22. Tout élément A non nul de $\mathbb{K}[X]$ est associé à un unique polynôme unitaire, obtenu en divisant A par son coefficient dominant.

Polynômes irréductibles

Définition 4

Un **polynôme irréductible** est un polynôme non constant dont les seuls diviseurs sont ses associés et les constantes non nulles.

Ex. 23. Tout polynôme de degré 1 est irréductible.

Proposition 25

Un élément $A \in \mathbb{K}[X]$ est irréductible si, et seulement si :

- A est non constant ;
- si $A = BC$, avec $(B, C) \in \mathbb{K}[X]^2$, alors B ou C est constant.

Démonstration page 29

Rappelons la caractérisation des irréductibles de $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

Proposition 26 (Irréductibles de $\mathbb{R}[X]$ et $\mathbb{C}[X]$)

- Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
- Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est strictement négatif.

Ex. 24. Un polynôme $P \in \mathbb{K}[X]$ de degré 2 ou 3 n'ayant aucune racine dans $\mathbb{K}$ est irréductible dans $\mathbb{K}[X]$.

En effet, s'il s'écrivait $P = AB$, avec A et B non constants, on aurait $\deg A \geqslant 1$, $\deg B \geqslant 1$ et $\deg A + \deg B = \deg P \leqslant 3$. L'un des deux polynômes A ou B serait donc de degré 1, donc aurait une racine dans $\mathbb{K}$, ce qui est impossible puisqu'il divise P qui n'a pas de racine dans $\mathbb{K}$.

Ex. 25. Montrons que $P = X^3 + X + 1$ est irréductible dans $\mathbb{Q}[X]$. Comme il est de degré 3, l'exemple précédent montre qu'il suffit de prouver qu'il n'a pas de racine dans $\mathbb{Q}$.

Supposons donc, par l'absurde, $P(p/q) = 0$ avec p et q deux entiers premiers entre eux et $q \neq 0$.

Alors $p^3 + pq^2 + q^3 = 0$, donc $q \mid p^3$ et $p \mid q^3$. On en déduit $p = \pm 1$ et $q = \pm 1$ puisque $p \wedge q = 1$.

Exo 1.10

Ainsi, $p/q = \pm 1$, ce qui est contradictoire puisque $P(1) = 3 \neq 0$ et $P(-1) = -1 \neq 0$.

Polynômes premiers entre eux

Définition 5

Deux éléments de $\mathbb{K}[X]$ sont **premiers entre eux** si leurs seuls diviseurs communs sont les polynômes constants non nuls de $\mathbb{K}[X]$.

Ex. 26. Deux polynômes irréductibles non associés sont premiers entre eux. Considérons, en effet, deux polynômes irréductibles P et Q non premiers entre eux. Ils admettent alors un diviseur commun D non constant. Comme P et Q sont irréductibles, on en déduit que D est associé à P et à Q, donc que P et Q sont associés.

Plus généralement :

Proposition 27

Soit P un polynôme irréductible et A un polynôme quelconque. Alors P et A sont premiers entre eux si, et seulement si, P ne divise pas A.

Démonstration page 29

2 Utilisation des idéaux de $\mathbb{K}[X]$

Idéaux de $\mathbb{K}[X]$

Si B est un élément de $\mathbb{K}[X]$, la proposition 5 de la page 4 montre que :

$$B\mathbb{K}[X] = \{BQ \mid Q \in \mathbb{K}[X]\}$$

est un idéal de $\mathbb{K}[X]$: c'est l'idéal engendré par B.

Comme dans le cas de $\mathbb{Z}$, on obtient ainsi tous les idéaux de $\mathbb{K}[X]$.

Théorème 28

Les idéaux de $\mathbb{K}[X]$ sont les $B\mathbb{K}[X]$, pour $B \in \mathbb{K}[X]$.

Démonstration page 29

Principe de démonstration. Si I est un idéal non nul de $\mathbb{K}[X]$, on considère un élément B non nul de I de degré minimal et l'on utilise la division euclidienne par B pour montrer que tout élément de I est un multiple de B.

Ainsi, tout comme $\mathbb{Z}$, l'anneau $\mathbb{K}[X]$ a tous ses idéaux principaux (voir page 5). On dit que ce sont des **anneaux principaux**.

Grâce à cette propriété importante de $\mathbb{K}[X]$, nous allons pouvoir retrouver (et généraliser au cas d'un corps $\mathbb{K}$ quelconque) les propriétés arithmétiques de l'anneau $\mathbb{K}[X]$.

Lien avec la divisibilité

Rappelons (proposition 7 de la page 5) que la divisibilité se ramène à une inclusion d'idéaux :

$$\forall (A,B) \in \mathbb{K}[X]^2 \quad B \mid A \iff A\mathbb{K}[X] \subset B\mathbb{K}[X].$$

On en déduit, grâce à la proposition 24 de la page 13, que deux polynômes sont associés si, et seulement s'ils sont générateurs du même idéal.

Corollaire 29

Tout idéal I de $\mathbb{K}[X]$ est de la forme $A\mathbb{K}[X]$ pour un unique polynôme A nul ou unitaire. Ce polynôme A est appelé **le générateur** de I.

PGCD de polynômes

Soit $n \in \mathbb{N}^*$ et $A_1, \ldots, A_n$ des polynômes à coefficients dans $\mathbb{K}$. Nous avons vu à la proposition 6 de la page 4 que l'idéal de $\mathbb{K}[X]$ engendré par les éléments $A_1, \ldots, A_n$ était $I = A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X]$. Cela conduit à la définition :

Proposition 30 (Définition du PGCD)

Étant donné $A_1, \dots, A_n$ dans $\mathbb{K}[X]$, il existe un polynôme $D \in \mathbb{K}[X]$ tel que $D\mathbb{K}[X] = A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X]$. On a, pour tout $P \in \mathbb{K}[X]$:

$$P \mid D \iff \big(\forall i \in [\![1, n]\!] \quad P \mid A_i\big).$$

On dit que D est un **PGCD** de $A_1, \dots, A_n$ et l'on dispose de la **relation de Bézout** :

$$\exists (U_1, \dots, U_n) \in \mathbb{K}[X]^n \quad D = A_1U_1 + \cdots + A_nU_n.$$

Démonstration page 29

Remarques

- Les diviseurs communs à $A_1, \dots, A_n$ sont donc exactement les diviseurs de D.
- Ainsi, deux PGCD de $A_1, \dots, A_n$ se divisent mutuellement, donc sont associés.
- Lorsque D est non nul, c'est-à-dire lorsqu'au moins l'un des A_i est non nul, son degré est le plus grand parmi tous les degrés des diviseurs communs à $A_1, \dots, A_n$.
- Il y a unicité de D si on lui impose la condition supplémentaire d'être nul ou unitaire. On l'appelle *le* PGCD de $A_1, \dots, A_n$ et on le note $A_1 \wedge \cdots \wedge A_n$.
- De la même façon, on pourrait définir un **PPCM** de $A_1, \dots, A_n$ comme un générateur M de l'idéal $A_1\mathbb{K}[X] \cap \cdots \cap A_n\mathbb{K}[X]$, de façon à avoir, pour tout $P \in \mathbb{K}[X]$, l'équivalence :

  $$P \in M\mathbb{K}[X] \iff \big(\forall i \in [\![1, n]\!] \quad P \in A_i\mathbb{K}[X]\big).$$

  L'unique polynôme nul ou unitaire associé à M est appelé *le* PPCM de $A_1, \dots, A_n$.

Ex. 27. Deux polynômes A et B sont premiers entre eux si, et seulement si, $A \wedge B = 1$.

3 Théorème de Gauss et décomposition en produit d'irréductibles

Théorème 31 (Lemme de Gauss)

Soit A, B et C trois éléments de $\mathbb{K}[X]$.

Si A divise BC et si A est premier avec B, alors A divise C.

Démonstration page 29

Principe de démonstration. Multiplier par C une relation de Bézout $AU + BV = 1$.

Corollaire 32

Un polynôme est premier avec un produit si, et seulement s'il est premier avec chacun des facteurs.

Démonstration page 30

Théorème 33

Tout polynôme non constant de $\mathbb{K}[X]$ est produit d'irréductibles.

Démonstration page 30

Principe de démonstration. Récurrence forte sur le degré du polynôme.

Notons $\mathcal{P}$ l'ensemble des polynômes irréductibles unitaires. Les éléments de $\mathcal{P}$ sont donc deux à deux non associés et tout polynôme irréductible est associé à un unique élément de $\mathcal{P}$.

Théorème 34

Tout polynôme A non nul de $\mathbb{K}[X]$ s'écrit de façon unique sous la forme :

$$A = \lambda \prod_{P \in \mathcal{P}} P^{\alpha_P}$$

où $\lambda \in \mathbb{K}^*$ et $(\alpha_P)_{P \in \mathcal{P}}$ est une famille presque nulle d'entiers naturels.

Démonstration page 30.

Point méthode Dans la pratique, on écrit la décomposition en produit d'irréductibles d'un polynôme A non nul sous l'une des formes :

- $A = \lambda P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ où $k \in \mathbb{N}$, $\lambda \in \mathbb{K}^*$, $P_1, \ldots, P_k$ sont des éléments de $\mathcal{P}$ distincts deux à deux et $\alpha_1, \ldots, \alpha_k$ des entiers naturels non nuls ;
- $A = \lambda P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ où $k \in \mathbb{N}$, $\lambda \in \mathbb{K}^*$, $P_1, \ldots, P_k$ sont des éléments de $\mathcal{P}$ distincts deux à deux et $\alpha_1, \ldots, \alpha_k$ des entiers naturels éventuellement nuls.

Avec la deuxième forme, on peut utiliser les mêmes irréductibles pour plusieurs éléments de $\mathbb{K}[X]$.

Ex. 28. Soit A et B deux éléments non nuls de $\mathbb{K}[X]$ décomposés sous la deuxième forme :

$$A = \lambda P_1^{\alpha_1} \cdots P_k^{\alpha_k} \qquad \text{et} \qquad B = \mu P_1^{\beta_1} \cdots P_k^{\beta_k}.$$

- $B \mid A$ si, et seulement si, $\forall i \in [\![1, k]\!] \quad \beta_i \leqslant \alpha_i$;
- le PGCD de A et B est $D = P_1^{\min(\alpha_1, \beta_1)} \cdots P_k^{\min(\alpha_k, \beta_k)}$;
- le PPCM de A et B est $M = P_1^{\max(\alpha_1, \beta_1)} \cdots P_k^{\max(\alpha_k, \beta_k)}$.

On a ainsi $AB = \lambda \mu DM$.

III Algèbres

Dans toute cette section, on suppose que $\mathbb{K}$ est un sous-corps de $\mathbb{C}$.

1 Structure d'algèbre

Définition 6

Une **algèbre** est un espace vectoriel A muni d'une structure d'anneau dont les deux multiplications (interne et externe) vérifient la propriété de compatibilité :

$$\forall (\lambda, x, y) \in \mathbb{K} \times A \times A \quad \lambda(x \times y) = (\lambda x) \times y = x \times (\lambda y). \qquad (*)$$

Lorsque le produit est commutatif, on dit que l'algèbre est **commutative**.

Remarques

- De même que pour les espaces vectoriels, on peut préciser « $\mathbb{K}$-algèbre » pour spécifier le corps de base.
- Comme dans un anneau, la multiplication interne sera souvent notée implicitement xy au lieu de $x \times y$.

Ex. 29. $\mathbb{K}$, $\mathbb{K}^{\mathbb{N}}$, $\mathcal{F}(X, \mathbb{K})$ (pour X un ensemble quelconque) constituent des $\mathbb{K}$-algèbres.

Ex. 30. $\mathbb{K}[X]$, $\mathbb{K}(X)$, et $\mathcal{M}_n(\mathbb{K})$ sont des $\mathbb{K}$-algèbres pour les lois usuelles, ainsi que $\mathcal{L}(E)$ (E étant un $\mathbb{K}$-espace vectoriel quelconque).

Proposition 35

Soit A un $\mathbb{K}$-espace vectoriel muni d'une multiplication interne $(x,y) \mapsto x \times y$.

Exo 1.13

Alors A est une $\mathbb{K}$-algèbre si, et seulement si, ce produit est bilinéaire, associatif et si A possède un élément neutre multiplicatif.

Démonstration. Il suffit de montrer que la bilinéarité du produit, c'est-à-dire les relations :

$$x \times (\lambda y + \mu z) = \lambda(x \times y) + \mu(x \times z) \qquad \text{et} \qquad (\lambda x + \mu y) \times z = \lambda(x \times z) + \mu(y \times z) \quad (**)$$

est équivalente à la distributivité et à la propriété $(*)$ de compatibilité.

- En supposant $(**)$, on obtient la distributivité en prenant $\lambda = \mu = 1$ et la relation $(*)$ en prenant $\mu = 0$.
- Supposons la distributivité et $(*)$. Alors, pour tout $(x,y,z) \in A^3$ et $(\lambda,\mu) \in \mathbb{K}^2$:

$$\begin{aligned} x \times (\lambda y + \mu z) &= x \times (\lambda y) + x \times (\mu z) \quad \text{par distributivité} \\ &= \lambda(x \times y) + \mu(x \times z) \quad \text{par la relation } (*) \end{aligned}$$

et de même pour la deuxième relation de $(**)$. □

Attention Comme c'est déjà le cas pour un anneau, une algèbre est **unitaire**, c'est-à-dire possède un élément neutre multiplicatif.

2 Sous-algèbres

Définition 7

Une **sous-algèbre** d'une algèbre A est un sous-espace vectoriel de A stable par multiplication et contenant 1_A.

Remarques

- Autrement dit, une sous-algèbre est une partie de A stable par combinaison linéaire, par multiplication et contenant l'élément neutre multiplicatif 1_A.
- Une sous-algèbre est naturellement munie d'une structure d'algèbre pour les lois induites.
- Dans la plupart des cas, on démontre qu'un ensemble est muni d'une structure d'algèbre en montrant que c'est une sous-algèbre d'une algèbre connue.

Ex. 31. Si A est une algèbre, alors $\mathrm{Vect}(1_A)$ est une sous-algèbre de A.

Ex. 32. L'ensemble des suites convergentes à termes dans $\mathbb{K}$ est une sous-algèbre de $\mathbb{K}^{\mathbb{N}}$.

Ex. 33. Si I est un intervalle de $\mathbb{R}$, $\mathcal{C}(I,\mathbb{R})$ est une sous-algèbre de $\mathcal{F}(I,\mathbb{R})$.

Ex. 34. Dans $\mathcal{M}_n(\mathbb{K})$, l'ensemble des matrices triangulaires supérieures est une sous-algèbre. De même pour les matrices triangulaires inférieures ou les matrices diagonales, mais pas pour les matrices symétriques lorsque $n \geqslant 2$ (un produit de deux matrices symétriques est symétrique si, et seulement si, elles commutent).

3 Morphismes d'algèbres

Définition 8

Soit A et B deux $\mathbb{K}$-algèbres. Un **morphisme d'algèbres** de A dans B est une application linéaire de A dans B qui est également un morphisme d'anneaux.

Autrement dit, un morphisme d'algèbres de A dans B est une application de A dans B qui vérifie :

- $\forall (x,y) \in A^2 \quad \forall (\lambda,\mu) \in \mathbb{K}^2 \quad f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$,
- $\forall (x,y) \in A^2 \quad f(xy) = f(x)f(y)$,
- $f(1_A) = 1_B$.

Terminologie On dit que f est un **isomorphisme** lorsqu'il est bijectif, un **endomorphisme** lorsque $A = B$ et un **automorphisme** lorsque c'est un endomorphisme bijectif.

Ex. 35. Pour toute algèbre A non triviale, la sous-algèbre $\mathrm{Vect}(1_A)$ est isomorphe à $\mathbb{K}$ par l'isomorphisme $\lambda \mapsto \lambda 1_A$.

Ex. 36. Si $\mathcal{B}$ est une base d'un $\mathbb{K}$-espace vectoriel E de dimension finie n, l'application $u \mapsto \mathrm{Mat}_{\mathcal{B}}(u)$ est un isomorphisme d'algèbres de $\mathcal{L}(E)$ sur $\mathcal{M}_n(\mathbb{K})$.

Ex. 37. Soit $P \in \mathcal{GL}_n(\mathbb{K})$.
L'application $\begin{array}{ccc} \mathcal{M}_n(\mathbb{K}) & \longrightarrow & \mathcal{M}_n(\mathbb{K}) \\ M & \longmapsto & PMP^{-1} \end{array}$ est un automorphisme d'algèbre.

Résultats

- Une composée de morphismes d'algèbres est un morphisme d'algèbres.
- La réciproque d'un isomorphisme d'algèbres est un isomorphisme d'algèbres.
- L'image (respectivement l'image réciproque) d'une sous-algèbre par un morphisme d'algèbres est une sous-algèbre.

Attention Un morphisme d'algèbres $f : A \to B$ étant en particulier une application linéaire, son noyau est un sous-espace vectoriel, mais ce n'est en général pas une sous-algèbre puisqu'il ne contient pas 1_A si B est non trivial. Voir page 3 la notion d'idéal d'un anneau commutatif.

Ex. 38. Substitution polynomiale

Soit A une $\mathbb{K}$-algèbre. Pour $u \in A$ et $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$, on note $P(u)$ l'élément de A défini par :

$$P(u) = \sum_{k=0}^{+\infty} a_k u^k.$$

Par exemple, lorsque $A = \mathbb{K}$, l'application $\begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & P(x) \end{array}$ est l'application polynomiale associée au polynôme P.

Montrons que l'application $P \mapsto P(u)$ est un morphisme d'algèbres de $\mathbb{K}[X]$ dans A.

- La relation $1(u) = 1_A$ et la linéarité de $P \mapsto P(u)$ sont immédiates.
- Soit $P = \sum_{p=0}^{n} a_p X^p$ et $Q = \sum_{q=0}^{m} b_q X^q$. Par bilinéarité du produit polynomial, on a :

$$PQ = \sum_{\substack{0 \leqslant p \leqslant n \\ 0 \leqslant q \leqslant m}} a_p b_q X^{p+q}$$

et donc $(PQ)(u) = \sum_{\substack{0 \leqslant p \leqslant n \\ 0 \leqslant q \leqslant m}} a_p b_q u^{p+q}$, par linéarité de l'application $P \mapsto P(u)$.

De même, par bilinéarité du produit de A :

$$P(u)Q(u) = \left(\sum_{p=0}^{n} a_p u^p\right)\left(\sum_{q=0}^{m} b_q u^q\right) = \sum_{\substack{0 \leqslant p \leqslant n \\ 0 \leqslant q \leqslant m}} a_p b_q u^{p+q}$$

d'où l'égalité $(PQ)(u) = P(u)Q(u)$.

IV Approfondissements sur les groupes

Dans toute cette section, on considère un groupe $(G, \cdot)$ dont l'élément neutre est noté e.

1 Sous-groupe engendré par une partie

Proposition 36

Une intersection de sous-groupes de G est un sous-groupe de G.

Démonstration page 30

Proposition 37

Soit A une partie de G. Il existe un plus petit sous-groupe de G contenant A. On l'appelle **sous-groupe de G engendré par A**.

Démonstration. C'est l'intersection de tous les sous-groupes de G contenant A. □

Ex. 39. Il est immédiat que le sous-groupe de G engendré par l'ensemble vide est $\{e\}$.

Ex. 40. Le sous-groupe engendré par une partie A est l'ensemble H des produits d'éléments de A et d'inverses d'éléments de A :

$$H = \left\{ x_1 \cdots x_n \;\middle|\; n \in \mathbb{N} \quad \text{et} \quad \forall i \in [\![1, n]\!] \quad x_i \in A \text{ ou } x_i^{-1} \in A \right\}.$$

Montrons, en effet, que H est le plus petit sous-groupe de G contenant A.

- H contient A : pour tout $a \in A$, prendre $n = 1$ et $x_1 = a$.
- Tout sous-groupe de G contenant A contient H :
  - par stabilité par produit et passage à l'inverse, il contient tous les produits $x_1 \cdots x_n$ pour $n \in \mathbb{N}^*$, lorsque $\forall i \in [\![1, n]\!] \quad x_i \in A$ ou $x_i^{-1} \in A$;
  - comme il contient e, le résultat est également vrai pour $n = 0$.
- H est un sous-groupe de G :
  - H contient l'élément neutre e de G (prendre $n = 0$ comme ci-dessus),
  - il est stable par produit et par passage à l'inverse (l'inverse de $x_1 \cdots x_n$ est $x_n^{-1} \cdots x_1^{-1}$).

Définition 9

Une partie de G est **génératrice** de G si le sous-groupe qu'elle engendre est égal à G. On dit aussi que A **engendre** G.

Ex. 41. Nous avons vu en première année que tout élément de S_n pouvait s'écrire comme produit de cycles (à supports disjoints). Cela montre que l'ensemble des cycles constitue une partie génératrice de S_n.

Ex. 42. De même, la décomposition d'une permutation comme produit de transpositions signifie donc que l'ensemble des transpositions constitue une partie génératrice de S_n.

Point méthode Pour montrer qu'une partie de G est génératrice de G, il suffit de montrer que l'on peut obtenir, par produit et passage à l'inverse à partir de ses éléments, tous les éléments d'une partie que l'on sait génératrice.

Ex. 43. Le groupe alterné A_n (ensemble des permutations de $[\![1,n]\!]$ de signature 1) est engendré par les 3-cycles. En effet, les 3-cycles sont bien dans A_n et tout élément de A_n étant produit d'un nombre pair de transpositions (les transpositions sont de signature -1), il suffit de montrer qu'un produit de deux transpositions est aussi un produit de 3-cycles. Vérifions-le.
Soit τ_1 et τ_2 deux transpositions.

- Si $\tau_1 = \tau_2$, alors $\tau_1\tau_2$ est produit de 3-cycles (aucun !).
- Si $\tau_1 = (a\ b)$ et $\tau_2 = (b\ c)$, avec a, b, c distincts, alors $\tau_1\tau_2 = (a\ b\ c)$ est un 3-cycle.
- Si $\tau_1 = (a\ b)$ et $\tau_2 = (c\ d)$, avec a, b, c distincts, alors :

$$\tau_1\tau_2 = \tau_1(b\ c)(b\ c)\tau_2 = \big((a\ b)(b\ c)\big)\big((b\ c)(c\ d)\big) = (a\ b\ c)(b\ c\ d)$$

Exo 1.15

est un produit de 3-cycles.

2 Groupes monogènes, groupes cycliques

Sous-groupe engendré par un élément

Proposition 38

Le sous-groupe engendré par un élément a de G est $\{a^n \mid n \in \mathbb{Z}\}$.

Démonstration. Posons $H = \{a^n \mid n \in \mathbb{Z}\}$.

- On a $e = a^0 \in H$ et $\forall (p,q) \in \mathbb{Z}^2 \quad a^p(a^q)^{-1} = a^{p-q} \in H$, donc H est un sous-groupe de G.
- Il contient $a = a^1$.
- Enfin, tout sous-groupe de G contenant a contient tous les itérés de a, donc H.

Ainsi, H est bien le plus petit sous-groupe de G contenant a. □

Remarque Pour un groupe noté additivement, le sous-groupe engendré par a est :

$$\{n.a \mid n \in \mathbb{Z}\}.$$

En particulier, pour tout $a \in \mathbb{Z}$, le sous-groupe engendré par a est $a\mathbb{Z}$.
Rappelons (cf. proposition 8 de la page 6) que les sous-groupes de $\mathbb{Z}$ sont tous de cette forme.

Groupes monogènes

Définition 10

Un groupe G est **monogène** s'il est engendré par l'un de ses éléments, c'est-à-dire s'il existe $x \in G$ tel que $G = \{x^n \mid n \in \mathbb{Z}\}$.

Un tel élément x est alors appelé **générateur de G**.

Un groupe est **cyclique** s'il est monogène et fini.

Exo 1.16

Ex. 44. $\mathbb{Z}$ est monogène, engendré par 1 (ou par -1).

Ex. 45. Pour $n \in \mathbb{N}^*$, les groupes $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{U}_n$ sont cycliques, engendrés respectivement par $\overline{1}$ et $e^{2i\pi/n}$.

Ex. 46. Lorsque $n = 2p-1$ est impair, $\mathbb{Z}/n\mathbb{Z}$ est aussi engendré par $\overline{2}$ puisque $\overline{1} = p.\overline{2}$. Plus généralement, on verra à la proposition 41 de la page suivante quels sont les générateurs de $\mathbb{Z}/n\mathbb{Z}$.

Ex. 47. Si G est un groupe monogène, il est clair que tout groupe isomorphe à G est également monogène. En particulier, si p et q sont deux entiers naturels premiers entre eux, le théorème chinois (proposition 15 de la page 10) montre que $\mathbb{Z}/pq\mathbb{Z}$ et $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ sont isomorphes en tant qu'anneaux et donc, *a fortiori*, en tant que groupes. On en déduit que $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ est cyclique.

Structure des groupes monogènes

Soit G un groupe monogène et a un générateur de G.
L'application :

$$\begin{array}{rccc} \varphi_a : & \mathbb{Z} & \longrightarrow & G \\ & n & \longmapsto & a^n \end{array}$$

est donc surjective. Les règles de calcul sur les itérés :

$$\forall (p,q) \in \mathbb{Z}^2 \quad a^{p+q} = a^p a^q$$

montrent que φ_a est un morphisme de groupes de $\mathbb{Z}$ dans G. Son noyau :

$$\operatorname{Ker} \varphi_a = \{k \in \mathbb{Z} \,:\, a^k = e\}$$

est un sous-groupe de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$, pour $n \in \mathbb{N}$ (cf. proposition 8 de la page 6). On obtient la description suivante de G.

Proposition 39

Avec les notations précédentes :

- ou bien φ_a est injective et G est infini, isomorphe à $\mathbb{Z}$,
- ou bien $\operatorname{Ker} \varphi_a = n\mathbb{Z}$ avec $n \in \mathbb{N}^*$ et :

  $$G = \{e, a, a^2, \ldots, a^{n-1}\}$$

  est isomorphe à $\mathbb{Z}/n\mathbb{Z}$;

  l'entier n est alors le plus petit entier naturel k non nul tel que $a^k = e$.

Démonstration page 31

Principe de démonstration. Lorsque $\operatorname{Ker}\varphi_a = n\mathbb{Z}$, avec $n \in \mathbb{N}^*$, on vérifie que l'on peut définir l'application :

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & G \\ x & \longmapsto & a^k \quad \text{si } x = \overline{k} \end{array}$$

et que cette dernière est un isomorphisme.

Corollaire 40

Exo 1.17

1. Tout groupe monogène infini est isomorphe à $\mathbb{Z}$.
2. Tout groupe cyclique de cardinal $n \in \mathbb{N}^*$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Ex. 48. Pour $n \in \mathbb{N}^*$, le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Proposition 41

Soit $n \in \mathbb{N}^*$. Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les classes des entiers premiers avec n.

Il y en a donc $\varphi(n)$, où φ est l'indicatrice d'Euler.

Démonstration page 31

Principe de démonstration. Remarquer que $\overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, $\overline{1}$ est dans le sous-groupe engendré par $\overline{k}$.

3 Ordre d'un élément dans un groupe

Définition 11

Un élément a de G est **d'ordre fini** s'il existe $n \in \mathbb{N}^*$ tel que $a^n = e$.

L'**ordre de a** est alors le plus petit entier naturel n non nul tel que $a^n = e$.

Terminologie

Lorsqu'un élément n'est pas d'ordre fini, on dit aussi qu'il est **d'ordre infini**.

Ex. 49. L'élément neutre est d'ordre 1. C'est d'ailleurs le seul élément de G d'ordre 1.

Ex. 50. Les transpositions de S_n sont d'ordre 2.

En effet, si τ est une transposition, alors $\tau \neq \mathrm{Id}_{[\![1,n]\!]}$ et $\tau^2 = \mathrm{Id}_{[\![1,n]\!]}$.

Attention La relation $a^n = e$ ne signifie pas que a est d'ordre n, mais seulement que son ordre divise n d'après la proposition suivante.

Proposition 42

Un élément a d'un groupe G est d'ordre fini si, et seulement si, le sous-groupe engendré par a est fini et l'ordre p de a est alors le cardinal de ce sous-groupe. Il est caractérisé par la relation :

$$\forall n \in \mathbb{Z} \quad a^n = e \iff p \mid n.$$

Démonstration. C'est une conséquence de la proposition 39 de la page ci-contre. En particulier, le fait que a soit d'ordre fini est une traduction, par le noyau, de la non injectivité du morphisme φ_a. □

Exo 1.18

Remarque L'ordre de a est donc le plus petit entier naturel non nul p tel que $a^p = e$, aussi bien pour l'ordre naturel de $\mathbb{N}$ que pour la relation de divisibilité.

Ex. 51. Soit $n \geqslant 5$. La permutation $\sigma = (1\ 2)(3\ 4\ 5)$ de S_n est d'ordre 6.
En effet, pour tout $k \in \mathbb{N}^*$, $\sigma^k = (1\ 2)^k(3\ 4\ 5)^k$, puisque deux cycles à supports disjoints commutent. Donc :

$$\sigma^6 = \mathrm{Id}_{[\![1,n]\!]}, \qquad \sigma^2 = (5\ 4\ 3) \neq \mathrm{Id}_{[\![1,n]\!]} \qquad \text{et} \qquad \sigma^3 = (1\ 2) \neq \mathrm{Id}_{[\![1,n]\!]}.$$

Donc σ est d'ordre un diviseur de 6 mais pas un diviseur de 2 ni de 3. Ainsi, l'ordre de σ est égal à 6.

Exo 1.19

Corollaire 43

Dans un groupe fini, tout élément est d'ordre fini.

Remarque

- Dans un groupe infini, il y a toujours au moins un élément d'ordre fini : l'élément neutre qui est d'ordre 1. Les autres peuvent être d'ordre infini (comme dans $\mathbb{Z}$ dont tous les éléments sauf 0 sont d'ordre infini) ou d'ordre fini.
- Il se peut même que tous les éléments soient d'ordre fini, comme le montre l'exemple suivant.

Ex. 52. Soit $\mathbb{U}_\infty$ l'ensemble des racines de l'unité, c'est-à-dire l'ensemble des $z \in \mathbb{C}^*$ pour lesquels il existe $n \in \mathbb{N}^*$ tel que $z^n = 1$.

- C'est un sous-groupe de $\mathbb{C}^*$, puisqu'il contient 1, qu'il est évidemment stable par passage à l'inverse, et que si $z_1^n = 1$ et $z_2^p = 1$, alors $(z_1 z_2)^{np} = 1$.
- Par définition, tout élément de $\mathbb{U}_\infty$ est d'ordre fini.
- Il ne peut pas être fini de cardinal N, puisqu'il contient $\mathbb{U}_{N+1}$.

Proposition 44

Un groupe G de cardinal fini n est cyclique si, et seulement s'il admet un élément d'ordre n.

Démonstration. Un élément de G est d'ordre n si, et seulement si, le sous-groupe qu'il engendre est de cardinal n, c'est-à-dire est égal à G puisque G est de cardinal n.
Donc, G est cyclique si, et seulement s'il admet un élément d'ordre n. □

Ex. 53. Soit p et q deux entiers naturels non nuls. On a vu à l'exemple 47 de la page 22 que si p et q sont premiers entre eux, alors $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$, donc cyclique. Montrons la réciproque par contraposition. Posons m le PPCM de p et q. On a :

$$\forall x \in \mathbb{Z}/p\mathbb{Z} \quad p.x = 0 \qquad \text{donc} \qquad \forall x \in \mathbb{Z}/p\mathbb{Z} \quad m.x = 0 \quad \text{puisque } p \mid m.$$

Par symétrie entre p et q, on a le même résultat dans $\mathbb{Z}/q\mathbb{Z}$ et par conséquent :

$$\forall (x,y) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z}) \quad m.(x,y) = 0.$$

Ainsi, l'ordre de tout élément de $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ divise m et donc, si p et q ne sont pas premiers entre eux, il n'y a aucun élément d'ordre pq dans $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ puisqu'alors $m < pq = \mathrm{card}\left((\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})\right)$.

Remarque Comme tout groupe cyclique est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, où n est son cardinal, on a ainsi montré qu'un produit de deux groupes cycliques est cyclique si, et seulement si, leurs cardinaux sont premiers entre eux.
En particulier, un produit de groupes cycliques n'est pas en général cyclique.

Théorème 45

L'ordre de tout élément d'un groupe fini G divise le cardinal de G.

Démonstration page 31

Exo 1.20

Principe de démonstration dans le cas où G est commutatif

Pour tout $a \in G$, on a $\prod_{g\in G}(ag) = \prod_{g\in G} g$.

La démonstration dans le cas général est non exigible. Elle est proposée dans l'exercice 1.21.

Corollaire 46

Dans un groupe G fini de cardinal n, on a $\forall x \in G \quad x^n = e$.

Ex. 54. Tout groupe fini de cardinal premier est cyclique. Il est engendré par tout élément différent du neutre.
En effet, soit G un groupe de cardinal p premier. Alors $G \neq \{e\}$. Considérons donc un élément a de G différent de e. L'ordre de a est alors un diviseur de p, différent de 1 puisque $a \neq e$, donc est égal à p. Ainsi, G est cyclique (proposition 44 de la page ci-contre) et engendré par a.

Ex. 55. Montrons qu'un groupe cyclique G de cardinal n admet, pour tout diviseur d de n, un unique sous-groupe de cardinal d et que celui-ci est cyclique.
Comme deux groupes cycliques de cardinal n sont isomorphes, il suffit de montrer le résultat dans le cas où $G = \mathbb{U}_n$.
Soit d un diviseur de n.

- Le groupe $\mathbb{U}_d$ est cyclique, de cardinal d et est un sous-groupe de $\mathbb{U}_n$ puisque $d \mid n$ et donc :
$$\forall z \in \mathbb{C} \quad z^d = 1 \Longrightarrow z^n = 1.$$
- Soit H un sous-groupe de $\mathbb{U}_n$ de cardinal d. Le corollaire 46 donne :
$$\forall z \in H \quad z^d = 1 \qquad \text{c'est-à-dire} \qquad H \subset \mathbb{U}_d.$$
Cette inclusion et l'égalité des cardinaux (finis) donne alors $H = \mathbb{U}_d$.
Cela montre que $\mathbb{U}_d$ est le seul sous-groupe de cardinal d de $\mathbb{U}_n$.

Théorème 47 (Théorème d'Euler)

Soit $n \in \mathbb{N}^*$. Pour tout $a \in \mathbb{Z}$ premier avec n, on a $a^{\varphi(n)} \equiv 1\ [n]$.

Démonstration. Soit $a \in \mathbb{Z}$ premier avec n. Alors sa classe appartient au groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Ce groupe étant de cardinal $\varphi(n)$ par définition de l'indicatrice d'Euler, on en déduit que l'ordre de $\overline{a}$ divise $\varphi(n)$, soit $(\overline{a})^{\varphi(n)} = \overline{1}$.
En termes de congruences, cela se réécrit $a^{\varphi(n)} \equiv 1\ [n]$. □

Remarque Lorsque p est un nombre premier, on retrouve le petit théorème de Fermat :
$$\forall k \in \mathbb{Z} \quad k \wedge p = 1 \Longrightarrow k^{p-1} \equiv 1\ [p] \qquad \text{puis} \qquad \forall k \in \mathbb{Z} \quad k^p \equiv k\ [p].$$

Démonstrations

Proposition 3 Soit $(I_\lambda)_{\lambda\in\Lambda}$ une famille d'idéaux de A. Posons $I = \bigcap_{\lambda\in\Lambda} I_\lambda$.

- Comme tous les I_λ sont des sous-groupes de $(A,+)$, ils contiennent 0 et sont stables par somme et passage à l'opposé. Donc leur intersection également, ce qui prouve que I est un sous-groupe de $(A,+)$.
- Soit $x \in I$ et $a \in A$. Pour tout $\lambda \in \Lambda$, on a $ax \in I_\lambda$ puisque I_λ est un idéal de A. Donc $ax \in I$.

Proposition 4 Considérons l'intersection I de tous les idéaux de A contenant X (il en existe, puisque A est lui-même un idéal de A contenant X). D'après la proposition précédente, il s'agit d'un idéal de A, il contient évidemment X et, par définition, tout idéal de A contenant X contient I.

Proposition 5 Montrons que xA est le plus petit idéal de A contenant x.

- Par distributivité, l'application $a \mapsto xa$ est un endomorphisme de groupe de $(A,+)$, donc son image xA est un sous-groupe de $(A,+)$.
- Pour tout $x \in A$ et $b \in A$, on a $xa \times b = x \times (ab) \in xA$. Donc xA est un idéal de A.
- Comme $x = x \times 1_A$, on a bien $x \in xA$.
- Enfin, par définition, pour tout idéal I contenant x et pour tout $a \in A$, on a $ax \in I$, donc I contient xA.

Proposition 6 Notons $I = x_1A + \cdots + x_kA$ et montrons que c'est le plus petit idéal de A contenant tous les x_i.

- C'est un sous groupe de A, comme image du morphisme de groupes
$$\begin{array}{ccc} A^k & \longrightarrow & A \\ (a_i)_{1\leqslant i\leqslant k} & \longmapsto & \displaystyle\sum_{i=1}^{k} x_i a_i. \end{array}$$
- Il est clair que I est stable par multiplication par tout élément de A et qu'il contient tous les x_i.
- Enfin, par définition, tout idéal de A contenant $x_1, \ldots, x_k$, contient $a_1x_1, \ldots, a_kx_k$, pour tout $(a_1, \ldots, a_k) \in A^k$, donc leur somme.

Proposition 8 Soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, on a bien $H = 0\mathbb{Z}$. Sinon, H contient un élément p non nul et il contient aussi $-p$. Ainsi, l'ensemble des éléments strictement positifs de H est une partie non vide de $\mathbb{N}$. Considérons son plus petit élément n.

- Par stabilité par addition de H, on a :
$$\forall k \in \mathbb{N}^* \quad kn = \underbrace{n + n + \cdots + n}_{k \text{ fois}} \in H.$$
Comme $0 \in H$, on a $0 \times n \in H$ puis, par stabilité par passage à l'opposé :
$$\forall k \in \mathbb{Z} \quad kn \in H \qquad \text{soit} \qquad n\mathbb{Z} \subset H.$$
- Soit $a \in H$. La division euclidienne de a par n (qui est bien non nul par définition) s'écrit :
$$a = nq + r \qquad \text{avec} \qquad q \in \mathbb{Z} \quad \text{et} \quad r \in [\![0, n-1]\!].$$
Alors $r = a - nq$ appartient à H puisque $a \in H$ et $na \in n\mathbb{Z} \subset H$. Comme n est le plus petit élément strictement positif de H, on en déduit $r = 0$, ce qui donne $a = nq \in n\mathbb{Z}$. Ainsi $H \subset n\mathbb{Z}$.

Conclusion : $H = n\mathbb{Z}$.

Proposition 11 Grâce à la division euclidienne par n, tout entier est congru modulo n à un élément de $[\![0, n-1]\!]$, donc $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$.

Pour conclure, vérifions que les éléments $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ sont distincts deux à deux. Soit donc $(k, \ell) \in [\![0, n-1]\!]^2$ tel que $\overline{k} = \overline{\ell}$. Alors n divise $k-\ell$ et puisque $-(n-1) \leqslant k-\ell \leqslant n-1$, on en déduit $k - \ell = 0$, soit $k = \ell$.

Proposition 12

1. Soit α et β dans $\mathbb{Z}/n\mathbb{Z}$. Soit x et x' deux représentants de α ainsi que y et y' deux représentants de β. On a :

$$\begin{cases} x \equiv x' \ [n] \\ y \equiv y' \ [n] \end{cases} \quad \text{donc, par compatibilité,} \quad \begin{cases} x+y \equiv x'+y' \ [n] \\ x \times y \equiv x' \times y' \ [n] \end{cases} \quad \text{soit} \quad \begin{cases} \overline{x+y} = \overline{x'+y'} \\ \overline{x \times y} = \overline{x' \times y'}. \end{cases}$$

On peut donc poser $\alpha + \beta = \overline{x+y}$ et $\alpha \times \beta = \overline{x \times y}$ pour n'importe quels représentants x de α et y de β et l'on a ainsi :

$$\forall (x, y) \in (\mathbb{Z}/n\mathbb{Z})^2 \quad \overline{x} + \overline{y} = \overline{x+y} \quad \text{et} \quad \overline{x} \times \overline{y} = \overline{x \times y}.$$

2. Pour l'associativité de l'addition, on écrit, pour tout $(x, y, z) \in \mathbb{Z}^3$:

$$\overline{x} + (\overline{y} + \overline{z}) = \overline{x} + \overline{(y+z)} = \overline{x + (y+z)}$$

par définition de l'addition.

En utilisant l'associativité de l'addition de $\mathbb{Z}$, on a $x + (y+z) = (x+y) + z$ et, de la même façon que ci-dessus, on a $\overline{(x+y)+z} = (\overline{x} + \overline{y}) + \overline{z}$.

On démontre de même l'associativité de la multiplication, la commutativité de l'addition et de la multiplication, ainsi que la distributivité.

Ensuite, pour tout $x \in \mathbb{Z}$:

$$\overline{0} + \overline{x} = \overline{0+x} = \overline{x} \qquad \text{et} \qquad \overline{1} \times \overline{x} = \overline{1 \times x} = \overline{x}.$$

Enfin, pour tout $x \in \mathbb{Z}$:

$$\overline{x} + \overline{(-x)} = \overline{x - x} = \overline{0}$$

donc tout élément est symétrisable pour l'addition.

3. Le fait que la projection canonique soit un morphisme d'anneaux est une conséquence des relations suivantes déjà montrées :

$$\overline{x+y} = \overline{x} + \overline{y} \qquad \overline{x \times y} = \overline{x} \times \overline{y} \qquad \overline{x} \times \overline{1} = \overline{x}.$$

Elle est surjective par définition de $\mathbb{Z}/n\mathbb{Z}$. Son noyau est l'ensemble des entiers congrus à 0 modulo n, c'est-à-dire des multiples de n.

Proposition 13 Soit $k \in \mathbb{Z}$.

$$\begin{aligned} \overline{k} \text{ inversible dans } \mathbb{Z}/n\mathbb{Z} &\iff \exists u \in \mathbb{Z} \quad \overline{k} \times \overline{u} = \overline{1} \\ &\iff \exists u \in \mathbb{Z} \quad \overline{ku} = \overline{1} \\ &\iff \exists u \in \mathbb{Z} \quad \exists v \in \mathbb{Z} \quad ku + nv = 1 \\ &\iff k \wedge n = 1 \qquad \text{(théorème de Bézout).} \end{aligned}$$

Théorème 14

- Supposons n premier. Alors $n \geqslant 2$, donc $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif non trivial. Soit $\alpha \in \mathbb{Z}/n\mathbb{Z}$ différent de $\overline{0}$.

  Alors il existe $k \in [\![1, n-1]\!]$ tel que $\alpha = \overline{k}$ et ainsi k est premier avec n donc sa classe est inversible dans $\mathbb{Z}/n\mathbb{Z}$ d'après la proposition 13. On en déduit que α est inversible.

  Donc $\mathbb{Z}/n\mathbb{Z}$ est un corps.

- Supposons n non premier.

  Si $n = 1$, alors $\operatorname{card}(\mathbb{Z}/n\mathbb{Z}) = 1$ donc $\mathbb{Z}/n\mathbb{Z}$ est non intègre puisque trivial. Sinon, il existe deux entiers a et b tels que $n = ab$ avec $1 < a < n$ et $1 < b < n$. Par suite :

  $$\overline{a} \neq \overline{0} \quad \text{et} \quad \overline{b} \neq \overline{0} \qquad \text{tandis que} \qquad \overline{a} \times \overline{b} = \overline{0}.$$

  Donc $\mathbb{Z}/n\mathbb{Z}$ est non intègre et, *a fortiori*, n'est pas un corps.

Proposition 15

- Soit k et ℓ deux entiers tels que $k \equiv \ell\ [nm]$. Alors évidemment k et ℓ ont même classe modulo n et même classe modulo m. L'application φ est donc bien définie.
- Le fait que φ soit un morphisme découle immédiatement de la même propriété pour les trois projections canoniques de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/(nm)\mathbb{Z}$. Par exemple :

  $$\varphi\big([k]_{mn}[\ell]_{mn}\big) = \varphi\big([k\ell]_{mn}\big) = \big([k\ell]_n, [k\ell]_m\big) = \big([k]_n[\ell]_n, [k]_m[\ell]_m\big) = \varphi\big([k]_{mn}\big)\varphi\big([\ell]_{mn}\big).$$

- Soit $k \in \mathbb{Z}$ tel que $\varphi\big([k]_{nm}\big) = \big([0]_n, [0]_m\big)$. Alors k est un multiple de n et m, donc un multiple de nm puisque n et m sont premiers entre eux. On en déduit $[k]_{nm} = [0]_{nm}$. Donc φ est injective (son noyau est trivial).

  Comme $\operatorname{card}\big(\mathbb{Z}/(nm)\mathbb{Z}\big) = nm = \operatorname{card}\big((\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})\big)$, on en déduit que φ est bijective.

Ainsi, φ est un isomorphisme d'anneaux.

Proposition 19 Les anneaux $\mathbb{Z}/(n_1 \cdots n_r)\mathbb{Z}$ et $(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})$ étant isomorphes par le théorème chinois (corollaire 17 de la page 11), ils ont autant d'éléments inversibles.

Or, les inversibles de l'anneau produit $(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})$ sont les $(u_1, \ldots, u_r)$, où $u_1, \ldots, u_r$ sont inversibles respectivement dans $\mathbb{Z}/n_1\mathbb{Z}, \ldots, \mathbb{Z}/n_r\mathbb{Z}$.

Il y en a donc $\varphi(n_1) \cdots \varphi(n_r)$.

Proposition 21 Il est clair que $\mathbb{K}[X]$ est un anneau commutatif non réduit à $\{0\}$.

Soit A et B deux polynômes non nuls. Écrivons :

$$A = \sum_{i=0}^{p} a_i X^i \quad \text{et} \quad B = \sum_{j=0}^{q} b_j X^j \qquad \text{avec} \qquad p = \deg A \quad \text{et} \quad q = \deg B.$$

Par définition du produit, le coefficient du terme de degré $n = p + q$ de AB est $a_p b_q$, donc non nul comme produit d'éléments non nuls du corps $\mathbb{K}$. Ainsi $AB \neq 0$.

Proposition 23 Supposons A inversible. Il existe alors $B \in \mathbb{K}[X]$ tel que $AB = 1$ et l'on a donc $\deg A + \deg B = \deg 1 = 0$. Ainsi, $\deg A \in \mathbb{N}$ et $\deg B \in \mathbb{N}$, puis $\deg A = \deg B = 0$, c'est-à-dire $A \in \mathbb{K}^*$ et $B \in \mathbb{K}^*$.

Réciproquement, si $\lambda \in \mathbb{K}^*$, on a $\lambda\lambda^{-1} = 1$, donc λ est inversible.

Proposition 24 Supposons $A \mid B$ et $B \mid A$. Il existe alors deux polynômes Q_1 et Q_2 tels que $B = AQ_1$ et $A = BQ_2$.

- Si $A = 0$, alors $B = AQ_1 = 0$ et donc $B = 1 \times A$, avec $1 \in \mathbb{K}^*$.
- Sinon, on a $A = AQ_1Q_2$ et comme $A \neq 0$, l'intégrité de $\mathbb{K}[X]$ donne $Q_1Q_2 = 1$, donc Q_1 et Q_2 sont inversibles. On a alors $A = \lambda B$, avec $\lambda = Q_1 \in \mathbb{K}^*$ d'après la proposition 23.

Réciproquement, si $A = \lambda B$ avec $\lambda \in \mathbb{K}^*$, alors $B = \lambda^{-1}A$ donc $B \mid A$ et $A \mid B$.

Proposition 25

- Supposons A irréductible. Alors A est non constant par définition.

  Si $A = BC$, alors $B \mid A$, donc B est constant ou associé à A. Dans ce deuxième cas, $A = \lambda B$, avec $\lambda \in \mathbb{K}^*$, et comme $A = BC$, on en déduit que C est égal à la constante λ par intégrité de $\mathbb{K}[X]$.

- Réciproquement, supposons A non constant (en particulier non nul) et :

$$\forall (B,C) \in \mathbb{K}[X]^2 \quad A = BC \Longrightarrow \big(B \in \mathbb{K} \quad \text{ou} \quad C \in \mathbb{K}\big).$$

  Soit B un diviseur de A. Il existe $C \in \mathbb{K}[X]$ tel que $A = BC$. Par hypothèse, B est constant (non nul, puisque $A \neq 0$) ou C est constant (non nul pour la même raison) et dans ce cas A est associé à B.

  Comme A est non constant, on en déduit qu'il est irréductible.

Proposition 27 Il est évident que si P divise A, alors P et A ne sont pas premiers entre eux puisqu'ils admettent P comme diviseur commun non constant.

Supposons que P et A soient non premiers entre eux. Ils admettent alors un diviseur commun D non constant. Par suite D divise P irréductible, donc est associé à P. Comme D divise A, on en déduit que P divise A.

Théorème 28 Soit I un idéal de $\mathbb{K}[X]$.

- Si $I = \{0\}$, alors $I = 0\mathbb{K}[X]$.
- Sinon, parmi les éléments non nuls de I, il en existe un de degré minimal. Notons B un tel polynôme.

  Comme B appartient à I, on a $B\mathbb{K}[X] \subset I$ puisque $B\mathbb{K}[X]$ est le plus petit idéal de $\mathbb{K}[X]$ contenant B.

  Réciproquement, soit $A \in I$. Effectuons la division euclidienne de A par B : $A = BQ + R$, avec $\deg R < \deg B$. Or, $R = A - BQ$ appartient à I puisque $A \in I$ et $BQ \in B\mathbb{K}[X] \subset I$. Par minimalité du degré de B parmi les polynômes non nuls de I, on en déduit $R = 0$, c'est-à-dire $A = BQ \in B\mathbb{K}[X]$. Donc $I \subset B\mathbb{K}[X]$.

  Finalement $I = B\mathbb{K}[X]$.

Proposition 30

- Considérons le générateur de l'idéal $A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X]$, c'est-à-dire l'unique $D \in \mathbb{K}[X]$, nul ou unitaire, tel que $D\mathbb{K}[X] = A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X]$.

  Ainsi, $D\mathbb{K}[X]$ est le plus petit idéal de $\mathbb{K}[X]$ contenant $\{A_1, \ldots, A_n\}$ (proposition 6 de la page 4), donc pour tout $P \in \mathbb{K}[X]$, puisque $P\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$:

$$\begin{aligned} P \mid D &\iff D\mathbb{K}[X] \subset P\mathbb{K}[X] \\ &\iff \forall i \in [\![1,n]\!] \quad A_i \in P\mathbb{K}[X] \\ &\iff \forall i \in [\![1,n]\!] \quad P \mid A_i. \end{aligned}$$

- Enfin, puisque $D \in D\mathbb{K}[X] = A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X]$, on a par définition :

$$\exists (U_1, \ldots, U_n) \in \mathbb{K}[X]^n \quad D = A_1U_1 + \cdots + A_nU_n.$$

Théorème 31 Supposons $A \wedge B = 1$ et $A \mid BC$. D'après l'identité de Bézout, il existe des polynômes U et V tels que $AU + BV = 1$, ce qui implique $ACU + BCV = C$.

Comme A divise ACU et BCV, on a $A \mid ACU + BCV$ et donc $A \mid C$.

Corollaire 32 Par récurrence, il suffit de le montrer dans le cas de deux facteurs. Soit donc A, B et C trois polynômes.

- Si A est premier avec BC, il est évidemment premier avec B et avec C.
- Réciproquement, supposons $A \wedge B = A \wedge C = 1$. Soit D un diviseur commun à A et BC. Alors D est premier avec B (puisqu'il divise A qui est premier avec B) et comme il divise BC, le théorème de Gauss nous dit que D divise C. Ainsi, D est un diviseur commun à A et C qui sont premiers entre eux, ce qui prouve que D est constant non nul. On a donc montré que A et BC étaient premiers entre eux.

Théorème 33 Montrons par récurrence forte sur $n \in \mathbb{N}^*$:

$$H_n : \text{« tout polynôme } P \text{ de degré } n \text{ est produit d'irréductibles. »}$$

- H_1 est immédiat car tout polynôme de degré 1 est irréductible.
- Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$. Supposons $H_1, \dots, H_{n-1}$. Soit P de degré n.
  - Si P est irréductible, alors il est évidemment produit d'irréductibles (un seul).
  - Sinon, on peut écrire $P = AB$, avec $1 \leqslant \deg A, \deg B < n$. Par hypothèse de récurrence, les polynômes A et B sont des produits d'irréductibles et par suite $P = AB$ aussi.

  D'où H_n.

Théorème 34

Existence. Si A est constant non nul, on prend $\lambda = A$ et $\alpha_P = 0$ pour tout $P \in \mathcal{P}$.

Sinon, on utilise le théorème 33 pour écrire $A = P_1 \cdots P_r$, avec $P_1, \dots, P_r$ irréductibles. En factorisant chaque P_i par son coefficient dominant, cela donne $A = \lambda Q_1 \cdots Q_r$, où λ est dans $\mathbb{K}^*$ et $Q_1, \dots, Q_r$ dans $\mathcal{P}$. Pour tout $P \in \mathcal{P}$, on prend alors pour α_P le nombre de Q_i égaux à P.

Unicité. Soit $A = \lambda \prod_{P \in \mathcal{P}} P^{\alpha_P}$ une telle décomposition. Comme les éléments de $\mathcal{P}$ sont unitaires, le scalaire λ est égal au coefficient dominant de A.

Considérons une autre décomposition $A = \lambda \prod_{P \in \mathcal{P}} P^{\beta_P}$. Soit $P_0 \in \mathcal{P}$. Supposons par exemple $\alpha_{P_0} \leqslant \beta_{P_0}$. En simplifiant par $P_0^{\alpha_{P_0}} \neq 0$ ($\mathbb{K}[X]$ est intègre), on obtient :

$$\prod_{P \in \mathcal{P} \setminus \{P_0\}} P^{\alpha_P} = P_0^{\beta_{P_0} - \alpha_{P_0}} \prod_{P \in \mathcal{P} \setminus \{P_0\}} P^{\beta_P}.$$

Le membre de gauche de cette égalité est un polynôme premier avec P_0 (produit de polynômes premiers avec P_0, cf. corollaire 32 de la page 16). Donc $P_0^{\beta_{P_0} - \alpha_{P_0}}$ est premier avec P_0, ce qui prouve que $\beta_{P_0} - \alpha_{P_0} = 0$.

Les familles $(\alpha_P)_{P \in \mathcal{P}}$ et $(\beta_P)_{P \in \mathcal{P}}$ sont donc égales, ce qui montre l'unicité de la décomposition.

Proposition 36 Soit $(H_\lambda)_{\lambda \in \Lambda}$ une famille de sous-groupes de G. Posons $H = \bigcap_{\lambda \in \Lambda} H_\lambda$.

- Comme tous les H_λ sont des sous-groupes de G, ils contiennent son élément neutre e, donc $e \in H$.
- Soit $x \in H$. Pour tout $\lambda \in \Lambda$, on a $x^{-1} \in H_\lambda$ puisque H_λ est un sous-groupe de G. Donc $x^{-1} \in H$.
- Soit $(x, y) \in H^2$. Pour tout $\lambda \in \Lambda$, on a $xy \in H_\lambda$ puisque H_λ est un sous-groupe de G. Donc $xy \in H$.

Donc H est un sous-groupe de G.

Proposition 39

- Le premier cas est évident.
- Supposons $\operatorname{Ker}\varphi_a = n\mathbb{Z}$, avec $n \in \mathbb{N}^*$. On peut définir l'application :

$$\begin{array}{rccl} \widetilde{\varphi}_a : & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & G \\ & x & \longmapsto & a^k \quad \text{si } x = \overline{k} \end{array}$$

car si $\overline{k} = \overline{\ell}$, alors il existe $q \in \mathbb{Z}$ tel que $\ell = k + nq$ et alors :

$$a^\ell = a^k a^{nq} = a^k (a^n)^q = a^k e^q = a^k,$$

donc a^k ne dépend que de la classe de k modulo n.

L'application $\widetilde{\varphi}_a$ ainsi définie de $\mathbb{Z}/n\mathbb{Z}$ dans G vérifie :

$$\forall k \in \mathbb{Z} \quad \widetilde{\varphi}_a(\overline{k}) = \varphi_a(k) = a^k.$$

∗ C'est un morphisme de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans G puisque :

$$\forall (k,\ell) \in \mathbb{Z}^2 \quad \widetilde{\varphi}_a(\overline{k}+\overline{\ell}) = \widetilde{\varphi}_a(\overline{k+\ell}) = a^{k+\ell} = a^k a^\ell = \widetilde{\varphi}_a(\overline{k})\widetilde{\varphi}_a(\overline{\ell}).$$

∗ Elle est surjective puisque a engendre G.

∗ Soit $k \in \mathbb{Z}$. On a :

$$\widetilde{\varphi}_a(\overline{k}) = e \iff \varphi_a(k) = e \iff k \in \operatorname{Ker}\varphi_a \iff k \in n\mathbb{Z} \iff \overline{k} = 0.$$

Donc $\operatorname{Ker}\widetilde{\varphi}_a = \{\overline{0}\}$, ce qui prouve que $\widetilde{\varphi}_a$ est injective.

Finalement, $\widetilde{\varphi}_a$ est un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ sur G.

Comme $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\right\}$, on en déduit que :

$$G = \left\{\widetilde{\varphi}_a(\overline{0}), \widetilde{\varphi}_a(\overline{1}), \widetilde{\varphi}_a(\overline{2}), \ldots, \widetilde{\varphi}_a(\overline{n-1})\right\} = \left\{e, a, a^2, \ldots, a^{n-1}\right\}.$$

Par l'isomorphisme $\widetilde{\varphi}_a$, on a pour tout $k \in \mathbb{Z}$ les équivalences :

$$a^k = e \iff \overline{k} = \overline{0} \iff n \mid k$$

donc n est le plus petit entier naturel k non nul tel que $a^k = e$.

Proposition 41 Soit $k \in \mathbb{Z}$.

Le groupe $\mathbb{Z}/n\mathbb{Z}$ est engendré par $\overline{1}$, ce qui signifie que tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ contenant $\overline{1}$ est égal à $\mathbb{Z}/n\mathbb{Z}$.

Donc le sous-groupe engendré par $\overline{k}$ est égal à $\mathbb{Z}/n\mathbb{Z}$ si, et seulement s'il contient $\overline{1}$, ce qui équivaut successivement :

- à l'existence d'un entier ℓ tel que $\ell\overline{k} = \overline{1}$,
- à l'existence de $(\ell, a) \in \mathbb{Z}^2$ tel que $\ell k = 1 + an$,
- à $k \wedge n = 1$ d'après le théorème de Bézout.

Théorème 45 Démonstration dans le cas où G est commutatif. Notons $n = \operatorname{card} G$. Soit $a \in G$. L'application $g \mapsto ag$ est une permutation de G (de réciproque $g \mapsto a^{-1}g$). Comme le groupe G est commutatif, le produit $P = \prod_{h \in G} h$ a bien un sens et, par le changement d'indice $[h = ag]$, on a :

$$P = \prod_{h \in G} h = \prod_{g \in G} (ag).$$

Toujours par commutativité de G, on en déduit :

$$P = a^{\operatorname{card} G} \prod_{g \in G} g = a^n P.$$

Par régularité de P, cela donne $a^n = e$. D'après la proposition 42 de la page 23, cela implique que l'ordre de a divise n.

S'entraîner et approfondir

Anneaux, arithmétique de $\mathbb{Z}$

1.1 →2 Montrer que tout anneau fini intègre est un corps.

1.2 →3 Soit A et B deux anneaux. À quelle condition l'anneau produit $A \times B$ est-il intègre ? est-il un corps ?

1.3 →3 Montrer que les suites réelles convergeant vers 0 constituent un idéal de l'anneau des suites réelles bornées.
S'agit-il d'un idéal de l'anneau de toutes les suites réelles ?

1.4 →3
1. Montrer qu'un idéal contenant un élément inversible de A est égal à A.
2. Quels sont les idéaux d'un corps ?
3. Montrer que tout morphisme d'anneaux entre deux corps est injectif.

1.5 →4 Montrer qu'un anneau commutatif A non trivial ayant pour seuls idéaux A et $\{0\}$ est un corps (réciproque de la deuxième question de l'exercice 1.4).

1.6 Montrer que $\mathbb{R} \times \{0\}$ muni des lois induites par celles de l'anneau produit $\mathbb{R}^2$ est un anneau mais n'est pas un sous-anneau de $\mathbb{R}^2$.

Congruences, $\mathbb{Z}/n\mathbb{Z}$

1.7 →12 Soit $n \in \mathbb{N}^*$. Montrer :

$$\sum_{d|n} \varphi(d) = n.$$

Indication. *On pourra considérer l'ensemble des rationnels de la forme p/n, avec $p \in \mathbb{N}$.*

1.8 Déterminer les entiers $n \in \mathbb{N}^*$ tels que $\varphi(n)$ divise n.

1.9 Montrer que si n est produit de nombres premiers distincts, alors :

$$\forall k \in \mathbb{N} \quad \forall a \in \mathbb{Z} \quad a^{1+k\varphi(n)} \equiv a \ [n].$$

Arithmétique des polynômes

1.10 →14 Le polynôme $P = X^4 + X^2 + 1$
1. a-t-il des racines dans $\mathbb{C}$? dans $\mathbb{R}$? dans $\mathbb{Q}$?
2. est-il irréductible dans $\mathbb{C}[X]$? dans $\mathbb{R}[X]$? dans $\mathbb{Q}[X]$?

1.11 Montrer que le polynôme $P = X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$.

⋆ **1.12** Montrer que si A et B sont deux polynômes premiers entre eux et non tous les deux constants, il existe un unique couple $(U, V) \in \mathbb{K}[X]^2$ tel que :

$$AU + BV = 1 \qquad \text{avec} \qquad \deg U < \deg B \quad \text{et} \quad \deg V < \deg A.$$

Algèbres

1.13 Montrer que toute algèbre intègre de dimension finie A est un corps.
→18

★ **1.14** Soit A une $\mathbb{R}$-algèbre intègre de dimension finie $n \geqslant 2$.

1. Soit $a \in A$ tel que $(1_A, a)$ soit une famille libre.
   (a) Montrer qu'il existe $(\lambda_0, \dots, \lambda_n) \in \mathbb{R}^{n+1} \setminus \big\{(0, \dots, 0)\big\}$ tel que $\sum_{k=0}^{n} \lambda_k a^k = 0$.
   (b) En introduisant le polynôme $P = \sum_{k=0}^{n} \lambda_k X^k \in \mathbb{R}[X]$, montrer qu'il existe $(\alpha, \beta) \in \mathbb{R}^2$, avec $\beta \neq 0$, tel que $(a - \alpha 1_A)^2 + \beta^2 1_A = 0$.
2. Montrer qu'il existe $u \in A$ tel que $u^2 = -1_A$ puis que $(1_A, u)$ est une base de A.
3. Montrer que $\mathbb{C}$ est, à isomorphisme près, la seule $\mathbb{R}$-algèbre intègre de dimension finie $n \geqslant 2$.

Groupes

1.15 1. Soit $\sigma \in S_n$ et $(a, b) \in [\![1, n]\!]^2$ tel que $a \neq b$.
→21
Montrer que $\sigma \circ (a\ b) \circ \sigma^{-1}$ est la transposition $\big(\sigma(a)\ \sigma(b)\big)$.
2. Montrer que l'ensemble des transpositions du type $(i\ i{+}1)$ est une partie génératrice de S_n.
3. Montrer que le groupe S_n est engendré par la transposition $\tau = (1\ 2)$ et le n-cycle $\gamma = (1\ 2\ \dots\ n)$.

1.16 Montrer que $\mathbb{Z}^2$ n'est pas monogène.
→22

1.17 Montrer que $G = \left\{ \begin{pmatrix} 2^n & n2^{n-1} \\ 0 & 2^n \end{pmatrix} \,\middle|\, n \in \mathbb{Z} \right\}$ est un sous-groupe de $\mathcal{GL}_2(\mathbb{R})$ isomorphe à $\mathbb{Z}$.
→23

1.18 Soit a un élément d'ordre n d'un groupe G.
→24
1. Montrer que, pour tout diviseur d de n, l'ordre de a^d est n/d.
2. Quel est l'ordre de a^k, pour $k \in \mathbb{N}$?

1.19 Montrer que si G est fini, le sous-groupe engendré par une partie A est l'ensemble des produits d'éléments de A.
→24

1.20 Soit $n \in \mathbb{N}^*$. Montrer que $n \mid \varphi(2^n - 1)$.
→25

1.21 Théorème de Lagrange
Soit G un groupe fini et H un sous-groupe de G. On définit sur G la relation :

$$x \mathcal{R} y \iff x^{-1}y \in H.$$

1. Montrer qu'il s'agit d'une relation d'équivalence et que la classe d'équivalence d'un élément $x \in G$ est :
$$xH = \big\{xh \,\big|\, h \in H\big\}.$$
2. Montrer que les classes d'équivalence pour cette relation ont toutes même cardinal égal à celui de H.
3. En déduire que le cardinal de H divise celui de G.
4. En déduire une démonstration du théorème 45 de la page 25 : l'ordre de tout élément de G divise le cardinal de G.

1.22 Déterminer l'ordre d'une permutation $\sigma \in S_n$ en fonction des longueurs des cycles intervenant dans sa décomposition en cycles à supports disjoints.

1.23 Soit G un groupe commutatif fini, ainsi que a et b deux éléments de G d'ordres respectifs m et n.

1. (a) Montrer que si m et n sont premiers entre eux, alors ab est d'ordre mn.
   (b) Que peut-on dire de l'ordre de ab dans le cas général ?
2. (a) En déduire que si r est le PPCM des ordres des éléments de G, il existe un élément de G d'ordre r.
   (b) Qu'en est-il si G n'est plus supposé commutatif ?
3. Soit $\mathbb{K}$ un corps quelconque. Montrer, en utilisant la question 2(a), que tout sous-groupe (multiplicatif) fini de $\mathbb{K}^*$ est cyclique.

   Indication. *On pourra utiliser le fait que tout polynôme de degré n à coefficients dans $\mathbb{K}$ admet au maximum n racines.*