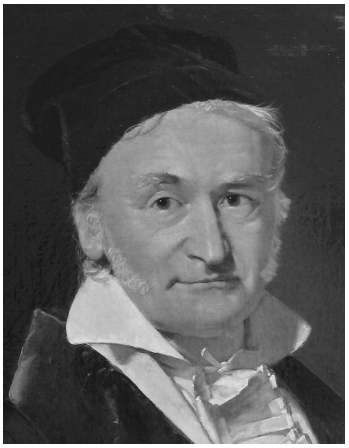
# Chapitre IV — Arithmétique des entiers et des polynômes

**Pierre de Fermat**
(1607 ?–1665)

**Étienne Bézout**
(1730–1783)



**Carl Friedrich Gauß**
(1777–1855)

## Révisions attendues

1. Le cours précédent : résultats sur les idéaux d'anneaux, définition de $\mathbb{Z}/n\mathbb{Z}$ et de l'indicatrice d'Euler, description des générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$.
2. L'intégralité du cours d'arithmétique de 1re année et du chapitre sur les polynômes.

Vos révisions sont insuffisantes si vous ne parvenez pas à faire ces exercices :

**Exercice 1.** Pour tout $n \in \mathbb{N} \setminus \{0\}$, on appelle *radical* de $n$, que l'on note $\mathrm{rad}(n)$, le plus grand diviseur positif de $n$ au sens de la relation d'ordre $\leqslant$ à être *sans facteur carré* (c'est-à-dire : pour tout $d \in \mathbb{N} \setminus \{0,1\}$, l'entier $d^2$ ne divise pas $\mathrm{rad}(n)$).

1. Soient $n \in \mathbb{N} \setminus \{0\}$ et $p$ un nombre premier. Montrer que $p$ divise $n$ si et seulement si $p$ divise $\mathrm{rad}(n)$.
2. Soit $n \in \mathbb{N} \setminus \{0\}$. Montrer que $\mathrm{rad}(n)$ est aussi son plus grand diviseur positif sans facteur carré *au sens de la relation de divisibilité* (c'est-à-dire : si $m \in \mathbb{N} \setminus \{0\}$ divise $n$ et est sans facteur carré, alors $m$ divise $\mathrm{rad}(n)$).
3. Soient $m$ et $n$ deux entiers naturels non nuls. Montrer que $m$ et $n$ sont premiers entre eux si et seulement si $\mathrm{rad}(m)$ et $\mathrm{rad}(n)$ sont premiers entre eux.

**Exercice 2.**

1. Soit $I$ un idéal d'un anneau commutatif $A$. Montrer que l'ensemble : $\sqrt{I} = \left\{x \in A \mid \exists k \in \mathbb{N} \setminus \{0\},\ x^k \in I\right\}$ est un idéal de $A$.
2. On prend $A = \mathbb{Z}$. Soit $n \in \mathbb{N}$. Expliciter $\sqrt{n\mathbb{Z}}$. On utilisera la décomposition en facteurs premiers de $n$ (pour $n \geqslant 2$).

**Exercice 3.** Calculer le reste de la division euclidienne de $3^{2023}$ par 11.

**Exercice 4.**

1. Décrire l'ensemble des carrés dans $\mathbb{Z}/7\mathbb{Z}$ c'est-à-dire : $\{y \in \mathbb{Z}/7\mathbb{Z} \mid \exists x \in \mathbb{Z}/7\mathbb{Z},\ y = x^2\}$.
2. Soit $(x, y) \in \mathbb{Z}^2$. Montrer que $x^2 + y^2$ est divisible par 7 si et seulement si $x$ et $y$ le sont.

**Exercice 5.**

1. Soit $(a_1, a_0) \in \mathbb{N}^2$. Montrer que $10a_1 + a_0$ est divisible par 13 si et seulement si $a_1 + 4a_0$ est divisible par 13.
2. Déterminer si les nombres suivants sont divisibles par 13 : 4174, 19721, 8506173.

**Exercice 6.** Résoudre l'équation $3x \equiv 7 \bmod n$ d'inconnue $x \in \mathbb{Z}$, dans les cas : $n \in \{2,3,5,7,9\}$.

**Exercice 7.**

1. Soit $(\lambda, \mu) \in \mathbb{C}^2$. Déterminer à quelle condition nécessaire et suffisante sur $(\lambda, \mu)$ le polynôme $X^4 + X^3 + \lambda X^2 + \mu X + 2$ est divisible par $X^2 + 2$.
2. Soit $a \in \mathbb{C}$. Déterminer à quelle condition nécessaire et suffisante sur $a$ le polynôme $X^4 - X + a$ est divisible par $X^2 - aX + 1$.
3. Pour tout $n \in \mathbb{N} \setminus \{0,1,2,3\}$, calculer le reste de la division euclidienne de $X^n$ par $(X-1)^4$.

**Exercice 8.**

1. Soit $P \in \mathbb{C}[X]$. Montrer que les racines de $P$ sont simples si et seulement si le pgcd de $P$ et $P'$ vaut 1.
2. On pose : $P = 4X^3 + 12X^2 - 15X + 4$. Calculer le pgcd de $P$ et $P'$, et en déduire une factorisation de $P$ en éléments irréductibles sur $\mathbb{R}$.

# 1 Autre point de vue sur l'arithmétique

## 1.1 Compléments sur les anneaux, algèbres

**Proposition 1** (Le groupe $A^\times$)**.**

**Définition 2** (Produit fini d'anneaux)**.**

**Définition 3** (Algèbre, sous-algèbre, morphisme d'algèbres)**.**

**Proposition 4** (Exemples usuels)**.**

**Définition 5** (Polynôme en un élément d'une algèbre)**.**

## 1.2 Arithmétique des idéaux

**Définition 6** (Divisibilité dans un anneau intègre, éléments associés)**.**

**Remarque.** Diviseurs et multiples de $0_A$, de $1_A$.
**Remarque.** Relation d'équivalence qui identifie les éléments associés. Ensemble $A/A^\times$.
**Remarque.** La relation de divisibilité définit une relation d'ordre sur $A/A^\times$.

**Proposition 7** (Divisibilité en termes d'idéaux)**.**

**Remarque.** Idéaux contenant un élément inversible. ♡

**Définition 8** (Éléments irréductibles)**.**

**Exemple 1.** Irréductibles de $\mathbb{Z}$.

**Définition 9** (Anneau principal)**.**

**Définition-Proposition 10** (Définition des pgcd et des ppcm dans un anneau principal)**.**

**Théorème 11** (Théorème de Bézout dans un anneau principal)**.**

**Proposition 12** (Lemme d'Euclide et théorème de Gauß dans un anneau principal)**.**

**Théorème 13** (Existence et unicité de la décomposition en éléments irréductibles dans un anneau principal)**.**

**Lemme 14** (Un lemme qui remplace les arguments de minimalité des entiers ou polynômes)**.**

*Démonstration.* On raisonne par l'absurde. Soient $A$ un anneau principal et $\mathcal{I} \subseteq \mathcal{P}(A)$ un ensemble non vide d'idéaux de $A$. On suppose qu'il n'existe pas d'élément maximal dans $\mathcal{I}$ au sens de l'inclusion.

1. Montrer l'existence d'une suite $(b_n)_{n\geqslant 0}$ d'éléments de $A$ tels que : $\forall n \in \mathbb{N}$, $b_nA \subsetneq b_{n+1}A$ (bien noter l'inclusion stricte).
2. Montrer que l'ensemble $J = \bigcup_{n\in\mathbb{N}} b_nA$ est un idéal de $A$, et en déduire l'existence de $d \in A$ tel que : $dA = J$.
3. Montrer qu'il existe $n \in \mathbb{N}$ tel que : $dA = b_nA$, et en déduire une absurdité. □

**Exercice 9.** Redémontrer l'existence de la décomposition dans les cas : $A = \mathbb{Z}$, et : $A \subseteq \mathbb{C}[X]$ (toujours sous l'hypothèse que $A$ est principal), sans utiliser le lemme 14.

**Proposition 15** (Caractérisation des éléments premiers entre eux)**.**

**Montrer qu'un anneau est principal.** Utilisation d'une division euclidienne.

# 2 Arithmétique des entiers et des polynômes

## 2.1 Arithmétique dans $\mathbb{Z}$

**Théorème 16** ($\mathbb{Z}$ est un anneau principal)**.**

↘ III lem. 19

**Corollaire 17** (On peut faire de l'arithmétique dans $\mathbb{Z}$)**.**

## 2.2 Structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$

**Proposition 18** (Inversibles de $(\mathbb{Z}/n\mathbb{Z})^\times$)**.**

↘ III prop. 24

**Exemple 2.** Calcul d'un inverse modulo 47.

**Corollaire 19** (Théorème d'Euler)**.**

↘ III th. 22

**Corollaire 20** ($\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $n$ est premier, notation $\mathbb{F}_p$)**.**

**Remarque.** Lien avec le petit théorème de Fermat.

**Théorème 21** (Théorème chinois)**.**

**Interprétation en termes de congruence.**

**Exemple 3.** Nombre de Carmichael : $\forall a \in \mathbb{Z}$, $a^{561} \equiv a \bmod 561$. ♡

**Remarque.** Construction de la bijection réciproque. ♡

**Exemple 4.** Solutions de $x^2 \equiv 1 \bmod 51$ d'inconnue $x \in \mathbb{Z}$.

**Corollaire 22** (Indicatrice d'Euler : calcul effectif)**.**

**Exemple 5.** Calcul de $\varphi(n)$ pour tout $n \in [\![1,12]\!]$.

## 2.3 Arithmétique dans $K[X]$

**Théorème 23** (L'anneau des polynômes sur un corps est un anneau principal)**.**

*Démonstration (idée).* Si $I \neq \{0_{K[X]}\}$ est un idéal, effectuer la division euclidienne de $P \in I$ par le polynôme $A$ dans $I$ de plus petit degré. Montrer que le reste appartient à $I$, et conclure par minimalité de $\deg(A)$. □

**Rappel.** Inversibles de $K[X]$ pour la multiplication.

**Corollaire 24** (On peut faire de l'arithmétique avec les polynômes)**.**

**Proposition 25** (Condition nécessaire pour être un polynôme irréductible)**.**

**Exemple 6.** Cette condition n'est pas suffisante. Contre-exemple dans $\mathbb{R}[X]$.

**Théorème 26** (Théorème de D'Alembert-Gauß, et polynômes irréductibles sur $\mathbb{C}$)**.**

**Corollaire 27** (Polynômes irréductibles sur $\mathbb{R}$)**.**

**Exemple 7.** Polynôme de degré 3 irréductible dans $\mathbb{Q}[X]$.

**Définition-Proposition 28** (Un idéal important : l'idéal annulateur, polynôme minimal)**.**

*Démonstration (idée).* Reconnaître le noyau de l'application d'évaluation $P \mapsto P(z)$. Pour l'irréductibilité : noter que si $\pi_{z,K} = QR$ alors $Q(z) = 0$ ou $R(z) = 0$, et conclure par minimalité de $\pi_{z,K}$. □

**Exemple 8.** Polynômes minimaux de 3 et $\sqrt{2}$ sur $\mathbb{Q}$, sur $\mathbb{R}$.

**Exemple 9.** Polynôme minimal de $e^{i\theta}$ sur $\mathbb{R}$. ♡

**Remarque.** L'anneau $K[X]$ a une arithmétique plus riche que $\mathbb{Z}$ !

**Exemple 10.** Pour tout $n \in \mathbb{N} \setminus \{0,1\}$, le polynôme $X^2 - 2\cos(\theta)X + 1$ divise le polynôme $\sin(\theta)X^n - \sin(n\theta)X + \sin((n-1)\theta)$.

**Exemple 11.** Soit $n \in \mathbb{N} \setminus \{0,1,2\}$. Solutions non triviales de $P^n + Q^n = R^n$ dans $\mathbb{C}[X]^3$.

— Fin du chapitre IV —

# Compléments et approfondissements

1. La résolution des équations diophantiennes, dès qu'elle fait intervenir des puissances d'entiers (surtout des carrés et des cubes, en pratique), nécessite des connaissances fines des puissances modulo $n$. On démontre en effet souvent l'inexistence de solutions (ou bien le fait qu'il y en ait « peu ») en trouvant une contradiction après réduction modulo $n$, avec $n$ bien choisi. Pour savoir comment « bien choisir » $n$, il est utile de connaître par cœur tous les carrés (ou cubes...) modulo $n$ pour $n$ une petite puissance de 2 ou un nombre premier de taille raisonnable. Pour avoir plus de connaissances sur l'ensemble des puissances modulo $n$, on a besoin de la structure cyclique de $(\mathbb{Z}/p\mathbb{Z})^\times$ (point suivant), ou de l'unique morphisme non trivial $(\mathbb{Z}/p\mathbb{Z})^\times \to \{-1,1\}$ (appelé le *symbole de Legendre*), ou des sommes de Gauß (qui sont l'outil le plus subtil de cette liste).
2. Le plus important résultat hors programme sur $\mathbb{Z}/n\mathbb{Z}$ est le fait que $(\mathbb{Z}/p\mathbb{Z})^\times$ soit cyclique si $p$ est premier. On en déduit l'existence d'éléments de tout ordre divisant $p-1$ (et on sait même exactement combien il y en a), ce qui est décisif dans la résolution d'équations de la forme $x^k \equiv 1 \bmod p$, pour dénombrer les puissances $k^{\text{es}}$ modulo $p$, etc. L'intérêt va bien au-delà : il suffit de montrer un résultat avec un générateur pour le généraliser à tout élément de $(\mathbb{Z}/p\mathbb{Z})^\times$.

   Sa démonstration utilise une spécificité du groupe multiplicatif d'un anneau : dans un tel groupe, on peut à la fois interpréter l'égalité $y^k = 1_A$ en termes d'ordre et de racines du polynôme $X^k - 1_A$. Combiner les deux points de vue (en particulier dans un corps, où il y a moins de racines que le degré) est très fécond.
3. Les polynômes irréductibles sur $\mathbb{Q}[X]$ sont, pour l'arithméticien, bien plus intéressants que ceux de $\mathbb{R}[X]$ et $\mathbb{C}[X]$ (en vue de l'étude des solutions aux équations polynomiales à coefficients entiers ou rationnels). Mais pour cela, encore faut-il savoir les reconnaître : hormis des critères d'irréductibilité, on trouvera en exercice une famille remarquable de polynômes sur $\mathbb{Q}$ (qui s'avèrent être irréductibles, même si c'est très difficile à démontrer) : les polynômes *cyclotomiques*. Leurs propriétés arithmétiques permettent d'étudier les racines primitives de l'unité et les corps qu'elles engendrent. Petit « miracle polynomial » : bien qu'ils soient définis comme polynômes dont les racines sont les éléments d'ordre $n$ dans $\mathbb{C}^*$, les racines de leurs réductions modulo $p$ permettent d'obtenir des éléments d'ordre $n$ aussi dans $(\mathbb{Z}/p\mathbb{Z})^\times$ (sous de bonnes hypothèses sur $p$ et $n$), ce qui tombe bien puisque c'est un groupe difficile à étudier ! C'est lié à l'universalité des identités polynomiales.
4. C'est relié au point précédent : une préoccupation majeure de l'algébriste est l'étude des solutions aux équations polynomiales à coefficients rationnels. Il s'avère que si $z \in \mathbb{C}$, alors munir $\mathbb{Q}[z]$ (ou $K[z]$ avec $K$ un sous-corps de $\mathbb{C}$) d'une structure d'espace vectoriel enseigne toutes sortes de choses : sa dimension nous enseigne si c'est une solution d'une équation polynomiale non triviale à coefficients dans $\mathbb{Q}$ ou $K$ (on dit dans ce cas que $z$ est *algébrique* sur $\mathbb{Q}$ ou $K$) ; si cette dimension est finie, elle nous donne même le degré minimal d'une telle équation (ce qui correspond au degré de son polynôme minimal). L'intérêt de passer par l'algèbre linéaire est que la dimension d'un espace vectoriel peut se calculer de manière indirecte, et donc montrer par des voies détournées l'existence de polynômes non nuls annulant $z$ *même sans parvenir à les expliciter*. C'est en particulier ainsi qu'on profite de la stabilité par somme d'un espace vectoriel pour obtenir la stabilité par somme de l'ensemble des nombres algébriques.

   C'est un point de départ possible de l'étude des nombres *algébriques* et *transcendants*. Pour y être à l'aise, on verra en exercice des recours possibles pour le calcul de la dimension de $K[z]$ (théorème de la base télescopique).
5. Les polynômes de $\mathbb{Z}/p\mathbb{Z}[X]$ (avec $p$ premier) vérifient subtilement des propriétés différentes des polynômes définis sur des sous-corps de $\mathbb{C}$. Il est utile d'avoir conscience de ces subtilités et d'en déduire ce qui reste valable ou non dans ces anneaux de polynômes.

# Table des matières