Classes préparatoires aux grandes écoles

Filière scientifique • Mathématiques

Structures algébriques

Mouad El Assadi

Professeur agrégé de mathématiques

Ingénieur d'État en génie civil — École Hassania des Travaux Publics (EHTP)

elassadimouad1@gmail.com

Table des matières

1 Groupes **2**
1.1 Rappels . . . 2
1.2 Sous-groupes . . . 3
1.3 Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ . . . 5
1.4 Groupes monogènes . . . 6
1.5 Ordre d'un élément . . . 7
1.6 Un deuxième théorème de Lagrange, HP . . . 8

2 Anneaux et idéaux **9**
2.1 Rappels . . . 9
2.2 Idéaux . . . 11
2.3 Idéaux de $\mathbb{Z}$ et arithmétique . . . 12

3 Anneau $\mathbb{Z}/n\mathbb{Z}$ **12**
3.1 Propriétés d'inversibilité . . . 12
3.2 Théorème chinois, et systèmes de congruences . . . 13
3.3 L'indicatrice d'Euler . . . 14

4 Arithmétique dans l'anneau $\mathbb{K}[X]$ **15**
4.1 Idéaux de $\mathbb{K}[X]$ . . . 15
4.2 Décomposition en facteurs irréductibles . . . 16

1. Groupes

1.1 Rappels

Définition 1.1 (Groupe). *On rappelle qu'un groupe G est un ensemble muni d'une loi de composition $\star$ telle que :*

(i) *$\star$ est associative ;*

(ii) *il existe un élément neutre e pour la loi $\star$;*

(iii) *tout élément x admet un symétrique x^e.*

Le neutre est alors unique, ainsi que le symétrique d'un élément x donné.

Définition 1.2 (Groupe abélien ou commutatif). *On dit qu'un groupe $(G, \star)$ est abélien (ou commutatif) si la loi de G est commutative.*

Remarque 1.3 (Notation additive, notation multiplicative).

- *Dans le cas général, on utilise souvent une notation multiplicative. Ainsi, la loi est $\times$, le neutre est souvent noté 1, le signe opératoire peut être omis (ab désigne $a \times b$) et on désignera sous forme de puissance l'itération de la loi, ainsi que la prise de symétrique ($x^e = x^{-1}$, on parlera alors d'inverse).*
- *Dans le cas abélien, on peut trouver la notation additive $+$, avec les conventions usuelles : le neutre est souvent noté 0, l'itération est notée nx, le symétrique est noté $-x$ et est appelé opposé.*

Définition 1.4 (Homomorphisme de groupes). *Soit $(G, \star)$ et $(H, \circ)$ deux groupes.*

- *On dit qu'une application $f : G \to H$ est un homomorphisme de groupes (ou plus simplement morphisme de groupes) si pour tout $(x, y) \in G$, $f(x \star y) = f(x) \circ f(y)$.*
- *On note $\mathrm{Hom}(G, H)$ l'ensemble des homomorphismes de G dans H.*
- *Si $(G, \star) = (H, \circ)$, on dit que f est un endomorphisme de $(G, \star)$.*
- *Un homomorphisme bijectif est appelé isomorphisme.*
- *Un endomorphisme bijectif est appelé automorphisme. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.*

Proposition 1.5 (Image du neutre par un morphisme). *Soit $f : G \to H$ un morphisme de groupes. Alors $f(e_G) = e_H$.*

Proposition 1.6 (Image par un morphisme d'un inverse). *Soit G, H deux groupes (notés multiplicativement), et f un morphisme de G dans H. Alors $f(x^{-1}) = f(x)^{-1}$. On adaptera aisément cette propriété au cas ou l'un (ou les deux) groupe(s) est (sont) en notation additive.*

Éléments de preuve. Considérer $f(x)f(x^{-1})$. □

Proposition 1.7 (Composée et réciproque de morphismes). *Soit G, H et K trois groupes.*

(i) Si $f : G \to H$ et $g : H \to K$ sont deux morphismes de groupes, alors $g \circ f$ est aussi un morphisme de groupes.

(ii) Si $f : G \to H$ est un isomorphisme, alors $f^{-1} : H \to G$ est aussi un isomorphisme.

Éléments de preuve. Vérifications faciles pour la composée. Pour la réciproque, considérer $f^{-1}(f(f^{-1}(x)f^{-1}(y)))$. □

1.2 Sous-groupes

Définition 1.8 (Sous-groupe). *Soit $(G, \star)$ un groupe. Un sous-ensemble H de G est appelé* sous-groupe de G *si H est stable pour la loi de G et si la loi induite définit sur H une structure de groupe. Le neutre de H est alors nécessairement le même que celui de G.*

Théorème 1.9 (Caractérisation des sous-groupes). *Un sous-ensemble H d'un groupe $(G, \star)$ (de neutre e_G) est un sous-groupe de G si et seulement si :*

(i) H est non vide,

(ii) H est stable pour $* : \forall (x, y) \in H, x * y \in H$,

(iii) H est stable par prise de symétrique : $\forall x \in H, x^* \in H$.

Dans la pratique, pour montrer que H est non vide, on vérifie souvent que $e_G \in H$.

Théorème 1.10 (Caractérisation des sous-groupes, version condensée). *Un sous-ensemble H d'un groupe $(G, \star)$ (de neutre e_G) est un sous-groupe de G si et seulement si :*

(i) H est non vide,

(ii) $\forall (x, y) \in H^2, x * y^* \in H$.

On traduit cette dernière propriété dans les deux cas les plus fréquents :

- *pour un sous-groupe d'un groupe additif, la vérification de stabilité à faire est donc : $\forall (x, y) \in H^2, x - y \in H$;*
- *pour un sous-groupe d'un groupe multiplicatif, la vérification de stabilité à faire est donc : $\forall (x, y) \in H^2, xy^{-1} \in H$.*

Proposition 1.11 (Image directe et réciproque de sous-groupes par un homomorphisme). *Soit G et H deux groupes, et soit $f \in Hom(G, H)$ un morphisme de groupes.*

(i) Soit G' un sous-groupe de G. Alors $f(G')$ est un sous-groupe de H.

(ii) Soit H' un sous-groupe de H. Alors $f^{-1}(H')$ est un sous-groupe de G.

Définition 1.12 (Noyau). *Soit G et H deux groupes et $f \in Hom(G, H)$ un morphisme de groupes. Le noyau de f est le sous-groupe de G défini par :*

$$Ker(f) = f^{-1}(\{e_H\}) = \{y \in G \mid f(y) = e_H\}.$$

Théorème 1.13 (Caractérisation de l'injectivité). *Soit $f \in Hom(G, H)$. Le morphisme f est injectif si et seulement si $Ker(f) = \{e_G\}$.*

Proposition 1.14 (Intersection de sous-groupes)**.** *Soit G un groupe, et $(H_i)_{i\in I}$ une famille de sous-groupes de G. Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.*

Éléments de preuve. Sans difficulté à l'aide de l'une ou l'autre des caractérisations des sous-groupes. □

Proposition 1.15 (Sous-groupe engendré par une partie)**.** *Soit $(G,\star)$ un groupe, et X une partie de G. Le sous-groupe $\langle X\rangle$ de G engendré par X est le plus petit sous-groupe de G contenant X. Ce sous-groupe est défini explicitement par*

$$\langle X\rangle = \bigcap_{X\subset H} H,$$

l'intersection étant prise sur tous les sous-groupes H de G.

Proposition 1.16 (Description par le bas du sous-groupe engendré par une partie)**.** *Soit X une partie d'un groupe G. Alors $\langle X\rangle$ est l'ensemble des éléments pouvant s'écrire sous la forme $x_1\cdots x_n, n\in\mathbb{N}$, où les x_i vérifient soit $x_i\in X$, soit $x_i^{-1}\in X$. Le produit vide est par convention égal au neutre e de G.*

Éléments de preuve. Justifier que l'ensemble de ces éléments est forcément inclus dans $\langle X\rangle$, et que c'est un sous-groupe contenant X. □

Définition 1.17 (Partie génératrice d'un groupe)**.** *Soit $X\subset G$ une partie de G. On dit que X est une partie génératrice de G si $\langle X\rangle = G$.*

Proposition 1.18. *Les sous-groupes de $\mathbb{Z}$ sont les groupes $a\mathbb{Z} = \langle a\rangle, a\in\mathbb{N}$.*

Éléments de preuve. Considérer a l'élément minimal de $G\cap\mathbb{N}^*$. Justifier que $a\mathbb{Z}\subset G$, et si l'inclusion est stricte, contredire la minimalité de a en effectuant une division euclidienne. □

Exercise 1.19.

1. *Soit G un sous-groupe de $(\mathbb{R},+)$, non réduit à 0.*
   - *(a) Justifier l'existence de $a = \inf G\cap\mathbb{R}_+^*$.*
   - *(b) Justifier que si $a>0$, alors $a\in G\cap\mathbb{R}_+^*$, puis montrer que $G = a\mathbb{Z}$.*
   - *(c) Justifier que si $a=0$, alors G est dense dans $\mathbb{R}$.*

   Ainsi, tout sous-groupe de $\mathbb{R}$ est soit de la forme $a\mathbb{Z}$, soit dense dans $\mathbb{R}$.
2. *Soit $f:\mathbb{R}\to\mathbb{R}$ une fonction périodique. Montrer que l'ensemble T de ses périodes est soit de la forme $a\mathbb{Z}$, soit dense dans $\mathbb{R}$. Donner un exemple de fonction non constante dont l'ensemble des périodes est dense dans $\mathbb{R}$.*
3. *Soit $\theta\in\mathbb{R}\setminus\mathbb{Q}$. Montrer que l'ensemble $\{a+\theta b,\ a,b\in\mathbb{Z}\}$ est dense dans $\mathbb{R}$.*
4. *Déterminer l'ensemble des valeurs d'adhérence de $(\cos(n))_{n\in\mathbb{N}}$. On admettra que π est irrationnel.*

1.3 Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Soit $n \in \mathbb{N}^*$. On rappelle les définitions suivantes, cas particulier des définitions générales liées aux relations d'équivalence.

Définition 1.20 (Classe de congruence, représentant)**.**
- *Pour $a \in \mathbb{Z}$, on note $\overline{a}$ la classe de congruence de a modulo n, c'est-à-dire la classe d'équivalence de a pour la relation de congruence modulo n.*
- *Explicitement, $\overline{a} = a + n\mathbb{Z}$.*
- *Étant donné c une classe de congruence, tout élément $a \in c$ est appelé représentant de la classe c. On a alors $c = \overline{a}$.*

On rappelle que la congruence modulo n respecte la somme et le produit, c'est-à-dire :

$$\forall (a, a', b, b') \in \mathbb{Z}^4, \begin{cases} a \equiv a'[n] \\ b \equiv b'[n] \end{cases} \implies \begin{cases} a + b \equiv a' + b'[n] \\ ab \equiv a'b'[n] \end{cases}$$

Cela permet de définir la somme et le produit directement sur les classes de congruence.

Définition 1.21 ($\mathbb{Z}/n\mathbb{Z}$ et ses lois)**.** *L'ensemble des classes de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$. Il peut être muni d'une somme et d'un produit, définis, pour $\overline{a}$ et $\overline{b}$ deux classes de $\mathbb{Z}/n\mathbb{Z}$, par*

- $\overline{a} + \overline{b} = \overline{a + b}$;
- $\overline{a} \cdot \overline{b} = \overline{ab}$.

En vertu de ce qui précède, ces définitions sont indépendantes du choix des représentants a et b des deux classes.

Exemple 1.22. *Décrire la table des lois de $\mathbb{Z}/n\mathbb{Z}$, pour $n \in \{2, 3, 4\}$.*

Proposition 1.23 (Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$)**.**
- *$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien d'ordre n.*
- *L'application $\pi : \mathbb{Z} \mapsto \mathbb{Z}/n\mathbb{Z}$ définie par $\pi(a) = \overline{a}$ est un morphisme de groupe, et $Ker(\pi) = n\mathbb{Z}$.*

Proposition 1.24 (Générateurs de $\mathbb{Z}/n\mathbb{Z}$)**.** *Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Les propositions suivantes sont équivalentes:*

(i) $\mathbb{Z}/n\mathbb{Z} = \langle \overline{a} \rangle$

(ii) *il existe $k \in \mathbb{N}$ tel que $\overline{k}a = \overline{1}$*

(iii) $a \wedge n = 1$

Éléments de preuve. Montrer $(i) \iff (ii)$, qui est assez clair, et $(ii) \iff (iii)$ qui provient de Bezout. □

Proposition 1.25 (Définir un morphisme $\mathbb{Z}/n\mathbb{Z} \to G$)**.** *Soit $(G, \times)$ un groupe, et $f : \mathbb{Z} \to G$ un morphisme de groupe. Les propositions suivantes sont équivalentes:*

(i) il existe un morphisme $g : \mathbb{Z}/n\mathbb{Z} \to G$ *tel que* $f = g \circ \pi$*;*

(ii) $n\mathbb{Z} \subset Ker(f)$.

Éléments de preuve. Le sens direct est évident. Réciproquement (ii) donne la condition pour que la valeur de f soit la même pour tout représentant d'une classe de congruence, ce qui donne une façon naturelle de définir g. Le reste n'est que de la vérification facile. □

Proposition 1.26 (Comparaison de $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{U}_n$)**.** *Les groupes* $(\mathbb{Z}/n\mathbb{Z}, +)$ *et* $(\mathbb{U}_n, \times)$ *sont isomorphes.*

Éléments de preuve. Considérer $\mathbb{Z} \longrightarrow \mathbb{U}_n$ défini par $f(k) = e^{\frac{2\pi ik}{n}}$, puis passer au quotient. □

1.4 Groupes monogènes

Définition 1.27 (Groupe monogène)**.** *(i) Un groupe* G *est monogène s'il existe* $x \in G$ *tel que* $G = \langle x \rangle$.

(ii) Si G *est fini et monogène, on dit que* G *est un groupe cyclique.*

(iii) Un générateur d'un groupe monogène est un élément x *tel que* $G = \langle x \rangle$.

Exemple 1.28. *1.* $(\mathbb{Z}, +)$ *est monogène, engendré par 1 ou par -1. Ce sont les seuls générateurs possibles de* $\mathbb{Z}$.

2. Tous les sous-groupes de $\mathbb{Z}$ *sont monogènes. En effet, ils sont de la forme* $a\mathbb{Z} = \langle a \rangle = \langle -a \rangle$. *Ce sont les seuls éléments générateurs de* $a\mathbb{Z}$.

3. $(\mathbb{Z}/n\mathbb{Z}, +)$ *est monogène, ses éléments générateurs sont les* $\overline{k}$*, avec* $k \wedge n = 1$.

4. $(\mathbb{U}_n, \times)$ *est monogène. Ses générateurs sont les images par l'isomorphisme de la proposition 7.1.25 des générateurs de* $\mathbb{Z}/n\mathbb{Z}$*, à savoir* $e^{\frac{2\pi ik}{n}}$*, avec* $k \wedge n = 1$. *Ces éléments générateurs sont appelés racines nièmes primitives de l'unité.*

Proposition 1.29 (Description explicite d'un sous-groupe monogène)**.** *Soit* $(G, \times)$ *un groupe, et* $x \in G$. *Alors*

$$\langle x \rangle = \{x^k, k \in \mathbb{N}\} = Im(\varphi_x),$$

où $\varphi_x : \mathbb{Z} \mapsto G$ *est le morphisme défini par* $\varphi_x(k) = x^k$.

Théorème 1.30 (Structure des groupes monogènes)**.** *Tout groupe monogène* $\langle x \rangle$ *est isomorphe :*

- *soit à* $(\mathbb{Z}, +)$*, si* $Ker(\varphi_x) = \{0\}$*;*
- *soit à* $(\mathbb{Z}/n\mathbb{Z}, +)$*, si* $Ker(\varphi_x) = n\mathbb{Z}$*; dans ce cas,* $n = \min\{k \in \mathbb{N}^*, x^k = e\}$.

Éléments de preuve. Dans le cas 2, passer φ_x au quotient par la proposition 7.1.24 pour définir $\widetilde{\varphi}_x : \mathbb{Z}/n\mathbb{Z} \to G$. Vérifier que c'est un isomorphisme. □

Exercise 1.31. *1. Soit* $n \in \mathbb{N}$. *Déterminer tous les sous-groupes de* $\mathbb{Z}/n\mathbb{Z}$.

2. Montrer que les sous-groupes d'un groupe cyclique sont cycliques.

1.5 Ordre d'un élément

Définition 1.32 (Ordre d'un élément)**.** *Soit $(G, \times)$ un groupe, de neutre e, et $x \in G$. L'ordre de x est*

- *$ord(x) = +\infty$ si pour tout $n \in \mathbb{N}^*, x^n \neq e$;*
- *$ord(x) = \min\{n \in \mathbb{N}^* | x^n = e\}$ sinon.*

On dit que x admet un ordre fini si $ord(x) \neq +\infty$.

Exemple 1.33. *1. Dans $(\mathbb{Z}, +)$, $ord(1) = +\infty$*

2. Dans $(\mathbb{Z}/n\mathbb{Z}, +)$, $ord(\overline{1}) = n$

3. Dans $(\mathbb{Z}/42\mathbb{Z}, +)$, $ord(\overline{12}) = 7$.

Proposition 1.34 (Résolution de $x^k = e$)**.** *Soit $(G, \times)$ un groupe de neutre e. Soit x un élément d'ordre fini n. Alors*

$$x^k = e \iff n \mid k.$$

Proposition 1.35 (Description de ord(x) par le groupe engendré)**.** *Soit $(G, \times)$ un groupe, et $x \in G$. Alors*

$$ord(x) = |\langle x \rangle|.$$

Éléments de preuve. Dans le cas où ord(x) est fini, égal à n, le théorème 7.1.29 donne $\langle x \rangle \simeq \mathbb{Z}/n\mathbb{Z}$. Passer au cardinal. □

Définition 1.36 (Ordre d'un groupe)**.** *L'ordre d'un groupe est son cardinal. C'est un élément de $\mathbb{N}^* \cup \{+\infty\}$.*

Corollaire 1.37. *Si G est un groupe fini, tout $x \in G$ admet un ordre fini.*

Éléments de preuve. Sinon, $\mathbb{Z} \simeq \langle x \rangle \subset G$. □

Exercise 1.38. *Soit G un groupe abélien fini et x et y deux éléments de G d'ordres respectifs a et b. On suppose que a et b sont premiers entre eux. Montrer que xy est d'ordre ab.*

Théorème 1.39 (Lagrange)**.** *Soit G un groupe fini, et $x \in G$. Alors $ord(x) \mid Card(G)$. Ainsi l'ordre d'un élément d'un groupe fini divise l'ordre de ce groupe.*

Éléments de preuve. La démonstration n'est exigible que dans le cas où G est abélien. Montrer que l'application $\varphi : g \mapsto xg$ est une bijection et en déduire que

$$\prod_{g \in G} g = \prod_{g \in G} (xg),$$

puis simplifier. □

1.6 Un deuxième théorème de Lagrange, HP

Lemme 1.40 (Partition par les classes à gauche modulo H)**.** *Soit G un groupe fini et H un sous-groupe de G. Alors $\{aH, a \in G\}$ est une partition de G.*

Éléments de preuve. C'est la partition associée à la relation d'équivalence définie sur G par

$$x \equiv y[H] \iff x^{-1}y \in H.$$

Cette relation est appelée relation de congruence à gauche modulo H. □

Remarque 1.41. *Lorsque $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ (et en revenant aux notations additives), la congruence modulo H correspond à la congruence modulo n bien connue.*

Lemme 1.42 (Cardinal des classes à gauche modulo H)**.** *Pour tout $a \in G$, $|aH| = |H|$.*

Éléments de preuve. L'application $h \mapsto ah$ est une bijection de H dans aH. □

Théorème 1.43 (Lagrange pour les sous-groupes)**.** *Soit G un groupe fini et H un sous-groupe de G. Alors l'ordre de H divise l'ordre de G.*

Éléments de preuve. On a partitionné G avec des parts qui ont toutes le même cardinal que H. □

Remarque 1.44 (Groupes quotients)**.**

1. *On aurait pu faire la même chose avec les classes à droite Ha.*
2. *Quand G n'est pas abélien, la partition des classes à gauche n'est en général par la même que la partition des classes à droite.*
3. *Cela peut néanmoins arriver. Cela se produit lorsque pour tout $a \in G$, $aH = Ha$, c'est-à-dire $aHa^{-1} = H$. On dit dans ce cas que H est un sous-groupe normal de G (terminologie anglaise) ou un sous-groupe distingué de G (terminologie française).*
4. *Dans ce cas, on peut montrer que la loi de G passe sur les classes, dans le sens où la classe (à droite ou gauche) de xy ne dépend pas du choix de x et y dans leur classe respective. Cela permet de définir une loi sur l'ensemble des classes modulo H, qui en fait un groupe. C'est ce qu'on appelle le groupe quotient G/H.*
5. *Cette situation se produit systématiquement lorsque G est abélien, puisque dans ce cas, les classes à gauche et à droite sont clairement confondues. Ainsi, on peut toujours définir le groupe quotient G/H dans cette situation.*
6. *Un cas particulier est le cas du sous-groupe $n\mathbb{Z}$ de $\mathbb{Z}$: en formant le groupe quotient, on retrouve le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ déjà étudié.*

Exercise 1.45. *Soit G un groupe non réduit à son élément neutre. Montrer que G n'admet aucun sous-groupe propre (i.e. distinct de $\{e\}$ et de G) si et seulement si G est cyclique d'ordre p premier.*

2. Anneaux et idéaux

2.1 Rappels

Définition 2.1 (Anneau). $(A, +, \times)$ *(ou plus simplement A) est un anneau si :*

(i) $(A, +)$ *est un groupe abélien ; le neutre est noté* 0_A *ou* 0*;*

(ii) $\times$ *est associative, et admet un neutre* 1_A*;*

(iii) $\times$ *est distributive sur* $+$*.*

On dit que A est un anneau commutatif si de plus $\times$ est commutative.

Définition 2.2 (Corps). $(K, +, \times)$ *est un corps si c'est un anneau commutatif, tel que tout $x \neq 0$ de K admet un inverse pour $\times$.*

Exemple 2.3.
1. *$\mathbb{Z}, \mathbb{R}, \mathbb{Q}$ et $\mathbb{C}$ munis des opérations usuelles sont des anneaux. $\mathbb{R}, \mathbb{Q}$ et $\mathbb{C}$ sont même des corps.*
2. *Pour tout $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif.*
3. *L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans un corps $\mathbb{K}$ est un anneau commutatif.*
4. *L'ensemble $M_n(\mathbb{R})$ des matrices carrées est un anneau non commutatif.*

Exercise 2.4. *Soit $\mathbb{K}$ un corps fini. On admet que tout polynôme non nul à coefficients dans $\mathbb{K}$, de degré $n \geq 0$, admet au plus n racines. Soit $n = |\mathbb{K}| - 1$.*

1. *Montrer que tout élément de $\mathbb{K}^*$ est racine de $X^n - 1$.*
2. *Montrer que s'il n'existe pas un élément de $\mathbb{K}^*$ dont l'ordre est n, il existe $p < n$ tel que tout élément de $\mathbb{K}^*$ soit racine de $X^p - 1$.*
3. *En déduire que $(\mathbb{K}^*, \times)$ est un groupe cyclique.*

Théorème 2.5 (Groupe des inversibles d'un anneau). *Soit A un anneau. Alors l'ensemble des éléments inversibles de A, généralement noté $A^\times$ ou $U(A)$, est stable pour la loi $\times$, et la loi induite munit $A^\times$ d'une structure de groupe multiplicatif.*

Définition 2.6 (Régularité et diviseurs de 0). *Soit A un anneau commutatif. Un élément $a \in A$ est appelé :*

- *élément régulier s'il est simplifiable : $ax = ay$ implique $x = y$;*
- *diviseur de 0 s'il est non nul, et qu'il existe $b \neq 0$ tel que $ab = 0$.*

Proposition 2.7 (Description des éléments réguliers). *Soit A un anneau commutatif et $a \in A\backslash\{0\}$. Les propositions suivantes sont équivalentes:*

(i) a *est régulier.*

(ii) a *n'est pas diviseur de 0.*

Définition 2.8 (Anneau intègre). *Un anneau A est intègre si :*

(i) $A \neq \{0\}$*;*

(ii) A *est commutatif;*

(iii) A *ne possède pas de diviseur de 0.*

La troisième propriété se traduit par : $ab = 0 \Longrightarrow (a = 0)$ *ou* $b = 0$*.*

Exemple 2.9 (Calculs dans un anneau)**.** *Sous certaines conditions de commutativité, certains outils calculatoires connus sur* $\mathbb{C}$ *restent valides dans un anneau :*

1. *la formule du binôme pour le développement de* $(A + B)^n$*, lorsque* $AB = BA$*;*
2. *la factorisation de* $A^n - B^n$ *par* $A - B$ *(factorisation de Bernoulli), lorsque* $AB = BA$*.*

Définition 2.10 (Homomorphisme d'anneaux)**.** *Soit* A *et* B *deux anneaux.*

(i) Un homomorphisme d'anneaux de A *à* B *est une application* $f : A \longrightarrow B$*, soit égale à la fonction nulle, soit vérifiant :*

$$\forall (x, y) \in A^2, f(x + y) = f(x) + f(y), \quad f(xy) = f(x)f(y) \quad \textit{et} \quad f(1_A) = 1_B.$$

(ii) Un isomorphisme est un homomorphisme bijectif. Sa réciproque est alors aussi un morphisme d'anneau.

Définition 2.11 (Sous-anneau)**.** *Soit* $(A, +, \times)$ *un anneau. Un sous-anneau de* A *est un sous-ensemble* $B \subset A$ *tel que :*

(i) B *soit stable pour les lois* $+$ *et* $\times$*,*

(ii) $1_A \in B$*,*

(iii) les lois induites sur B *définissent sur* B *une structure d'anneau.*

Proposition 2.12 (Caractérisation des sous-anneaux)**.** *Un sous-ensemble* B *d'un anneau* A *est un sous-anneau de* A *si et seulement si :*

(i) $1_A \in B$*,*

(ii) pour tout $(x, y) \in B, x - y \in B$*,*

(iii) pour tout $(x, y) \in B, xy \in B$*.*

Proposition 2.13 (Anneau produit)**.** *Soit* $(A, +, \times)$ *et* $(B, +, \times)$ *deux anneaux. On munit le produit cartésien* $A \times B$ *des deux opérations :*

$$\forall ((a, b), (a', b')) \in (A \times B)^2, (a, b) + (a', b') = (a + a', b + b') \quad \textit{et} \quad (a, b) \times (a', b') = (a \times a', b \times b').$$

Muni de ces deux lois, $A \times B$ *est un anneau, donc les neutres sont* $(0_A, 0_B)$ *et* $(1_A, 1_B)$*. Si de plus,* A *et* B *sont commutatifs, il en est de même de* $A \times B$*.*

Proposition 2.14 (Inversibles d'un anneau produit)**.** *Soit* $(A, +, \times)$ *et* $(B, +, \times)$*. Alors*

$$(A \times B)^\times = A^\times \times B^\times.$$

2.2 Idéaux

Définition 2.15 (Idéal d'un anneau commutatif)**.** *Soit A un anneau commutatif. Un idéal de A est une partie $I \subset A$ telle que :*

(i) *I est un sous-groupe de $(A, +)$,*

(ii) *I est fortement stable par produit : $A \cdot I \subset I$, c'est-à-dire :*

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

Proposition 2.16 (Noyau d'un homomorphisme)**.** *Soit A et B deux anneaux, et $f : A \to B$ un morphisme d'anneaux. On suppose A commutatif. Alors Ker(f) est un idéal de A.*

Proposition 2.17 (Idéal engendré par x)**.** *Soit A un anneau commutatif, et $x \in A$.*

(i) *$xA = \{xa, a \in A\}$ est un idéal.*

(ii) *C'est le plus petit idéal de A contenant x.*

xA est appelé idéal engendré par x.

Définition 2.18 (Idéal principal)**.** *Soit A un anneau commutatif et I un idéal de A. On dit que I est un idéal principal, s'il existe x tel que $I = xA$.*

Définition 2.19 (Anneau principal)**.** *Un anneau principal est un anneau intègre dont tous les idéaux sont principaux.*

Exercise 2.20. *Soit A un anneau principal et (I_n) une suite croissante d'idéaux. Montrer que (I_n) est stationnaire.*

Définition 2.21 (Divisibilité dans un anneau commutatif intègre)**.** *Soit A un anneau commutatif intègre, et a et b deux éléments de A. On dit que a divise b s'il existe $c \in A$ tel que $ac = b$.*

Proposition 2.22 (Caractérisation de la divisibilité par les idéaux)**.** *Soit A un anneau commutatif intègre, et a et b deux éléments de A. Les propositions suivantes sont équivalentes :*

(i) *a divise b,*

(ii) *$bA \subseteq aA$.*

Proposition 2.23 (Somme d'idéaux)**.** *Soit I et J deux idéaux d'un anneau commutatif A. Alors :*

(i) *$I \cap J$ est un idéal de A,*

(ii) *$I + J = \{x + y \mid x \in I, y \in J\}$ est un idéal de A,*

(iii) *C'est le plus petit idéal K tel que $I \subseteq K$ et $J \subseteq K$.*

Cela s'étend par récurrence immédiate à un nombre fini quelconque d'idéaux.

Exercise 2.24. *Soit A un anneau commutatif non réduit à $\{0\}$. Montrer que A est un corps si et seulement si les seuls idéaux de A sont $\{0\}$ et A.*

Exercise 2.25. *Soit K un corps et $A = K \times K$.*

1. *Définir la structure d'anneau canonique sur A.*
2. *L'anneau A est-il un corps?*
3. *Déterminer les idéaux de A.*

2.3 Idéaux de $\mathbb{Z}$ et arithmétique

Théorème 2.26 (Les idéaux de $\mathbb{Z}$)**.** *$\mathbb{Z}$ est un anneau principal, dont les idéaux sont exactement les $a\mathbb{Z}$, $a \in \mathbb{N}$.*

Éléments de preuve. Les idéaux de $\mathbb{Z}$ sont en particulier des sous-groupes, dont on connaît la description ! □

Définition 2.27 ((Re)définition du pgcd d'un nombre fini d'entiers)**.** *Soit $n \geq 2$ et $a_1, \ldots, a_n$ des entiers naturels, non tous nuls, et m un entier naturel. Le pgcd $m = a_1 \wedge a_2 \wedge \cdots \wedge a_n$ de $a_1, \ldots, a_n$ est l'unique entier positif engendrant l'idéal $a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z}$. Ainsi, il est caractérisé par l'égalité*

$$m\mathbb{Z} = a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z}.$$

Proposition 2.28 (Interprétation du pgcd par divisibilité)**.** *Le pgcd m de $a_1, \ldots, a_n$ est le plus grand entier (au sens de la divisibilité) tel que m divise chaque a_k. Ainsi, si d est un autre entier divisant chaque a_k, alors $d \mid m$.*

Remarque 2.29 (Lien avec Bézout)**.** *La définition 7.2.24 correspond en fait au théorème de Bézout. Il affirme en effet que si m désigne le pgcd de $a_1, \ldots, a_n$:*

- *il existe $u_1, \ldots, u_n$ des entiers relatifs tels que*

$$m = a_1u_1 + \cdots + a_nu_n;$$

- *réciproquement, si c vérifie*

$$c = a_1u_1 + \cdots + a_nu_n,$$

alors m divise c.

Remarque 2.30 (Définition du PGCD et du PPCM dans un anneau principal)**.** *On peut définir de la même façon un pgcd (mais non nécessairement unique) dans un anneau principal, ainsi qu'un ppcm, en remplaçant la somme par l'intersection. Par exemple, pour 2 éléments a et b :*

- *$aA + bA$ est un idéal principal de A, donc de la forme mA. Un élément m vérifiant cela est appelé pgcd de a et b.*
- *$aA \cap bA$ est un idéal principal de A, donc de la forme MA. Un élément M vérifiant cela est appelé ppcm de a et b.*

On retrouvera cette situation dans $\mathbb{K}[X]$.

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

3.1 Propriétés d'inversibilité

Proposition 3.1 (Inversibles de $\mathbb{Z}/n\mathbb{Z}$)**.** *Soit $n \in \mathbb{N}^*$ et $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$. Les propositions suivantes sont équivalentes:*

(i) $\overline{k}$ est inversible;

(ii) *il existe* u *et* v *dans* $\mathbb{Z}$ *tels que* $uk + vn = 1$*;*

(iii) $k \wedge n = 1$.

Éléments de preuve. Immédiat par traduction des congruences, et par le théorème de Bézout. □

Remarque 3.2. *Le point (ii) nous dit comment trouver un inverse de* k *modulo* n *: il suffit de déterminer une relation de Bézout, et de la réduire modulo* n*.*

Corollaire 3.3 (Le corps $\mathbb{F}_p$)**.** *En particulier, pour* $p \in \mathbb{N}^*$*,* $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ *est un corps si et seulement si* p *est premier. Ce corps est noté* $\mathbb{F}_p$*.*

Éléments de preuve. Si $p \in \mathbb{P}$, tout élément de $[1, p-1]$ est premier avec p. Réciproquement, si $p \notin \mathbb{P}$, un diviseur strict de p n'est pas premier avec p et sa classe n'est pas inversible dans $\mathbb{Z}/p\mathbb{Z}$. □

Exemple 3.4. *Le corps* $\mathbb{F}_2$ *a seulement deux éléments. Le corps* $\mathbb{F}_3$ *en a 3. Décrire leurs lois.*

3.2 Théorème chinois, et systèmes de congruences

Théorème 3.5 (Théorème chinois)**.** *Soit* m *et* n *dans* $\mathbb{N}^*$*, tels que* $m \wedge n = 1$*. Pour* $k \in \mathbb{Z}$*, on note :*

- $\hat{k}$ *la classe de* k *dans* $\mathbb{Z}/mn\mathbb{Z}$*;*
- $\check{k}$ *la classe de* k *dans* $\mathbb{Z}/m\mathbb{Z}$*;*
- $\tilde{k}$ *la classe de* k *dans* $\mathbb{Z}/n\mathbb{Z}$*;*

L'application $\varphi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ *définie par*

$$\varphi(\hat{k}) = (\check{k}, \tilde{k})$$

est bien définie, et est un isomorphisme d'anneaux. Ceci s'étend sans difficulté au cas d'un plus grand nombre d'entiers 2 à 2 premiers entre eux.

Éléments de preuve. Pour montrer que c'est un isomorphisme, étudier le noyau en se ramenant à des propriétés arithmétiques. □

Corollaire 3.6 (Unicité modulo $a_1 \cdots a_n$ de la solution d'un système)**.** *Soit* $a_1, \ldots, a_n$ *des entiers deux à deux premiers entre eux, et* $b_1, \ldots, b_n$ *des entiers. Alors le système*

$$\begin{cases} x \equiv b_1 [a_1] \\ \vdots \\ x \equiv b_n [a_n] \end{cases}$$

admet une solution, unique modulo $a_1 \cdots a_n$*.*

Corollaire 3.7 (Cas d'un second membre commun)**.** *En particulier, si* $b_1 = \cdots = b_n = b$*, la seule solution modulo* $a_1 \cdots a_n$ *est* b*.*

Remarque 3.8 (Méthode de résolution d'un système de congruence)**.** *Pour résoudre*

$$\begin{cases} x \equiv b_1[a_1] \\ \vdots \\ x \equiv b_n[a_n] \end{cases}$$

avec $a_1, \dots, a_n$ *deux à deux premiers entre eux, on combine les solutions de*

$$\begin{cases} x \equiv \delta_{1,k}[a_1] \\ \vdots \\ x \equiv \delta_{n,k}[a_n] \end{cases}$$

Pour ces dernières, par exemple pour $k = 1$*, le système équivaut à*

$$\{x \equiv 1[a_1]\ x \equiv 0[a_2 \dots a_n]\}$$

Ce système se résout en écrivant une relation de Bézout entre a_1 *et* $a_2 \dots a_n$*.*

Exemple 3.9. *Résoudre le système suivant :*

$$\begin{cases} x \equiv 2[5] \\ x \equiv 2[8] \\ x \equiv -2[11] \end{cases}$$

Exemple 3.10. *Résoudre les deux systèmes suivants :*

$$\begin{cases} x \equiv 3[42] \\ x \equiv 10[49] \end{cases} \quad \textit{et} \quad \begin{cases} x \equiv 3[42] \\ x \equiv 9[49] \end{cases}$$

3.3 L'indicatrice d'Euler

Définition 3.11 (Indicatrice d'Euler φ)**.** *Soit* $n \in \mathbb{N}^*$*. L'indicatrice d'Euler est définie par*

$$\varphi(n) = \textit{Card}(\{k \in [1, n] \mid k \wedge n = 1\}).$$

Lemme 3.12 (Ordre du groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$)**.** *Soit* $n \in \mathbb{N}^*$*. Alors* $\textit{Card}((\mathbb{Z}/n\mathbb{Z})^\times) = \varphi(n)$*.*

Théorème 3.13 (Théorème d'Euler)**.** *Soit* $(k, n) \in \mathbb{Z} \times \mathbb{N}^*$ *tels que* $n \wedge k = 1$*. Alors* $k^{\varphi(n)} \equiv 1[n]$*.*

Éléments de preuve. C'est le théorème de Lagrange dans le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$. □

Remarque 3.14 (Lien avec le petit théorème de Fermat)**.** *Pour* $n = p \in \mathbb{P}$*,* $\varphi(p) = p - 1$*, et on retrouve, pour* $k \notin p\mathbb{Z}$*,* $k^{p-1} \equiv 1[p]$*. Ainsi, le théorème d'Euler est une généralisation du petit théorème de Fermat.*

Proposition 3.15 (Multiplicativité arithmétique de φ)**.** *Soit* $(m, n) \in (\mathbb{N}^*)^2$ *tel que* $m \wedge n = 1$*. Alors* $\varphi(mn) = \varphi(m)\varphi(n)$*.*

Éléments de preuve. En passant aux inversibles dans le théorème chinois, sachant qu'un isomorphisme préserve l'inversibilité. □

Lemme 3.16 ($\varphi(p^k)$). *Soit $p \in \mathbb{P}$ et $k \in \mathbb{N}^*$. Alors $\varphi(p^k) = p^{k-1}(p-1)$.*

Éléments de preuve. Dénombrement direct, sachant que k n'est pas premier avec $p \in \mathbb{P}$ si et seulement s'il est multiple de p. □

Théorème 3.17 (Expression de $\varphi(n)$). *Soit $n \in \mathbb{N}^*$, et $n = p_1^{a_1} \cdots p_r^{a_r}$ sa décomposition en facteurs premiers, avec $a_i > 0$. Alors*

$$\varphi(n) = \prod_{\ell=1}^{r} p_\ell^{a_\ell - 1}(p_\ell - 1) = n \prod_{\ell=1}^{r} \left(1 - \frac{1}{p_\ell}\right).$$

4. Arithmétique dans l'anneau $\mathbb{K}[X]$

Conformément au programme, soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$ (mais tous les résultats de cette section restent valides si $\mathbb{K}$ est un corps quelconque).

4.1 Idéaux de $\mathbb{K}[X]$

Théorème 4.1 (Description des idéaux de $\mathbb{K}[X]$.] *Soit $\mathbb{K}$ un corps. Alors :*

(i) *$\mathbb{K}[X]$ est un anneau principal.*

(ii) *De plus, deux polynômes P et Q engendrent le même idéal si et seulement s'il existe un $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda P$.*

(iii) *En particulier, tout idéal non nul I de $\mathbb{K}[X]$ s'écrit de manière unique sous la forme $I = P \cdot \mathbb{K}[X]$, où P est un polynôme unitaire.*

Éléments de preuve. S'aider de la division euclidienne, comme pour montrer que $\mathbb{Z}$ est principal. C'est une propriété générale de tout anneau muni d'une division euclidienne (anneau euclidien). La deuxième partie provient de la description des inversibles de $\mathbb{K}[X]$. □

Définition 4.2 (Divisibilité dans $\mathbb{K}[X]$.] *Soit A et B deux polynômes de $\mathbb{K}[X]$. On dit que B divise A s'il existe un polynôme Q tel que $A = BQ$. Inversement, on dit que A est un multiple de B.*

Exercise 4.3. *Déterminer les polynômes $P \in \mathbb{C}[X]$ tels que P' divise P.*

Proposition 4.4 (Caractérisation en termes d'idéaux). *Soit A et B deux polynômes de $\mathbb{K}[X]$. Alors A divise B si et seulement si $B \in (A)$, ou encore si et seulement si $(B) \subset (A)$.*

Définition 4.5 ((Re)définition du PGCD de n polynômes). *Soit $n \geq 2$ et $P_1, \ldots, P_n$ des polynômes non tous nuls de $\mathbb{K}[X]$. Le PGCD Q de $P_1, \ldots, P_n$, noté $Q = P_1 \wedge P_2 \wedge \cdots \wedge P_n$, est l'unique polynôme unitaire tel que*

$$Q \cdot \mathbb{K}[X] = P_1 \cdot \mathbb{K}[X] + \cdots + P_n \cdot \mathbb{K}[X].$$

Proposition 4.6 (Caractérisation du PGCD par divisibilité). *Soit $n \geq 2$ et $P_1, \ldots, P_n$ des polynômes non tous nuls de $\mathbb{K}[X]$. Alors*

- *$Q = P_1 \wedge \cdots \wedge P_n$ est l'unique polynôme unitaire de plus petit degré divisant chacun des P_i;*
- *Tout autre polynôme D divisant chaque P_i vérifie $D \mid Q$.*

Exercise 4.7. *Soit K un corps, et L une extension de K (ainsi L est un corps dont K est un sous-corps). Soit $P, Q \in \mathbb{K}[X]$. Montrer que P et Q ont même PGCD dans $\mathbb{K}[X]$ et dans $L[X]$.*

4.2 Décomposition en facteurs irréductibles

Définition 4.8 (Polynôme irréductible). *Un polynôme non constant P de $\mathbb{K}[X]$ est irréductible si et seulement s'il n'est, à une constante multiplicative non nulle près, divisible que par lui-même et par 1.*

Exercise 4.9.
1. *Soit P un polynôme irréductible de $\mathbb{Q}[X]$. Montrer que P n'a pas de racine double dans $\mathbb{C}$.*
2. *Soit $P \in \mathbb{Q}[X]$ de degré 5. On suppose que P admet une racine double dans $\mathbb{C}$. Montrer que P possède une racine dans $\mathbb{Q}$.*

Exemple 4.10.
1. *Les polynômes $X - \lambda$ sont irréductibles ($\lambda \in \mathbb{K}$).*
2. *Dans $\mathbb{R}[X]$, tout polynôme $aX^2 + bX + c$ tel que $\Delta < 0$ est irréductible.*
3. *Ces polynômes ne sont pas irréductibles dans $\mathbb{C}[X]$.*

Théorème 4.11 (Polynômes irréductibles de $\mathbb{C}[X]$. *et $\mathbb{R}[X]$]*

(i) Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1 (théorème de d'Alembert-Gauss).

(ii) Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif.

Lemme 4.12 (Existence d'un diviseur irréductible). *Tout polynôme non constant $P \in \mathbb{K}[X]$ admet un diviseur irréductible.*

Éléments de preuve. Considérer un diviseur non constant de degré minimal. □

Lemme 4.13 (Euclide). *Soit A et B deux polynômes de $\mathbb{K}[X]$ et P un polynôme irréductible. Alors si P divise AB, P divise A ou P divise B. Le lemme d'Euclide se généralise facilement à davantage de facteurs, par récurrence immédiate.*

Éléments de preuve. Si P ne divise pas A, $P\mathbb{K}[X] + A\mathbb{K}[X] = \mathbb{K}[X]$. Multiplier par B pour obtenir $B\mathbb{K}[X] \subset P\mathbb{K}[X]$. □

Exercise 4.14. *Soit $n \geq 2$ et $a_1, \ldots, a_n$ des éléments de $\mathbb{Z}$ deux à deux distincts. Montrer que le polynôme $P = (X - a_1) \cdots (X - a_n) - 1$ est irréductible dans $\mathbb{Z}[X]$.*

Théorème 4.15 (Décomposition en facteurs irréductibles)**.** *Soit P un polynôme non nul de $\mathbb{K}[X]$. Il existe un unique élément $\lambda \in \mathbb{K}^*$ et des polynômes irréductibles unitaires $P_1, \ldots, P_k$, uniques à permutation près, tels que*

$$P = \lambda P_1 \cdots P_k.$$

Éléments de preuve**.** Par récurrence, en divisant par un facteur irréductible unitaire. Pour l'unicité, aussi par récurrence, en remarquant qu'un facteur irréductible unitaire de P se retrouve dans toute décomposition, d'après le lemme d'Euclide. □

Exercise 4.16. *Soit P un polynôme scindé de $\mathbb{R}[X]$ à racines simples, de degré $n \geq 2$.*

1. *Montrer que P' est scindé à racines simples.*
2. *Montrer que $P = \sum_{k=0}^{n} a_k X^k$ ne peut pas avoir deux coefficients successifs nuls.*
3. *Montrer que P ne peut pas avoir un coefficient nul entouré de deux coefficients non nuls de même signe.*