Cours

Anneaux et corps

Mathieu Mansuy - Préparation à l'Agrégation Interne de Mathématiques, Université de Franche Comté
mansuy.mathieu@hotmail.fr

1 Généralités sur les anneaux

1.1 Définitions

Définition.

Soit A un ensemble muni de deux lois internes notées « $+$ » et « $\times$ ». On dit que $(A,+,\times)$ est un *anneau* si :

(i) $(A,+)$ est un groupe abélien ;

(ii) la loi $\times$ est associative ;

(iii) la loi $\times$ est distributive par rapport à la loi $+$.

Si la loi $\times$ admet un élément neutre, on parle d'anneau *unitaire*. Si la loi $\times$ est commutative, on parle d'anneau *commutatif*.

Notation. Le neutre pour la loi $+$ sera noté 0_A ou simplement 0, celui pour la loi $\times$ sera noté 1_A ou 1. Dans le suite, on supposera que $0_A \neq 1_A$.

Exemples.

- $(\mathbb{Z},+,\times)$, $(\mathbb{K}[X],+,\times)$ (où $\mathbb{K}$ corps) sont des anneaux commutatifs et unitaires.
- $(\mathscr{M}_n(\mathbb{R}),+,\times)$ est un anneau unitaire non commutatif.

Définition.

Un sous-ensemble B de A est un *sous-anneau* de $(A,+,\times)$ si $(B,+,\times)$ est un anneau.

Propriété 1 (Caractérisation des sous-anneaux)

Un sous-ensemble B de A est un sous-anneau de $(A,+,\times)$ si et seulement si elle vérifie les conditions :

(i) B est un sous-groupe de $(A,+)$: $\quad \forall x,y \in B, \quad x-y \in B$;

(ii) B est stable par multiplication : $\quad \forall x,y \in B, \quad x \times y \in B$;

Propriété 2 (*Formule du binôme*)

Soit A un anneau, et $a,b \in A$ deux éléments qui **commutent** (i.e. $a \times b = b \times a$). Alors pour tout $n \in \mathbb{N}$, on a :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Définition.

Soit $(A,+,\times)$ un anneau unitaire.

- Un élément $x \in A$ est *inversible* dans A s'il existe $y \in A$ tel que :

  $$x \times y = y \times x = 1_A$$

  Par associativité de $\times$, un tel élément y est unique. On l'appelle *l'inverse* de x et on le note x^{-1}.
- On note $\mathscr{U}(A)$ ou A^* l'ensemble des éléments inversibles de A.
- A est un *corps* si $\mathscr{U}(A) = A \setminus \{0_A\}$.

Exemples.

- $\mathscr{U}(\mathbb{Z}) = \{-1, 1\}$, $\mathscr{U}(\mathbb{K}[X]) = \mathbb{K}^*$.
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps.

Propriété 3

Soit $(A, +, \times)$ un anneau unitaire. Alors $(\mathscr{U}(A), \times)$ est un groupe.

Preuve. On revient à la définition d'un groupe.

- $\times$ est une loi de composition interne sur $\mathscr{U}(A)$. En effet, pour tout $x, y \in \mathscr{U}(A)$, on a :

$$(x \times y) \times (y^{-1} \times x^{-1}) \underbrace{=}_{\times \text{ ass.}} x \times (y \times y^{-1}) \times x^{-1} = x \times 1_A \times x^{-1} = 1_A.$$

  On montre de même que $(y^{-1} \times x^{-1}) \times (x \times y) = 1_A$, de sorte que $x \times y \in \mathscr{U}(A)$. On obtient de plus que $(x \times y)^{-1} = y^{-1} \times x^{-1}$.

- $\times$ est associatif par définition d'un anneau.
- $1_A \in \mathscr{U}(A)$ et est un élément neutre pour la loi $\times$. En effet, on a :

$$1_A \times 1_A = 1_A \quad \Rightarrow \quad 1_A \in \mathscr{U}(A).$$

  Et 1_A est un élément neutre pour la loi $\times$.

- Tout élément est symétrisable dans $\mathscr{U}(A)$. En effet, on a pour tout $x \in \mathscr{U}(A)$:

$$x \times x^{-1} = x^{-1} \times x = 1_A.$$

  Donc x^{-1} appartient bien à $\mathscr{U}(A)$. On obtient de plus que $(x^{-1})^{-1} = x$.

□

Définition.

Un anneau A est dit *intègre* si on a :

(i) $A \neq \{0_A\}$,

(ii) $\forall a, b \in A$, $a \times b = 0_A \Rightarrow a = 0_A$ ou $b = 0_A$.

Remarques.

- Si A est un corps, alors A est intègre.
- Un sous-anneau d'un anneau intègre est intègre.

Exemple. $(\mathbb{Z}, +, \times)$ et $(\mathbb{K}[X], +, \times)$ sont des anneaux intègres, $(\mathscr{M}_n(\mathbb{R}), +, \times)$ n'est pas intègre.

Propriété 4

Si A est intègre, l'anneau $A[X]$ des polynômes à coefficients dans A est intègre.

Preuve. Comme A est intègre, on a $A \neq \{0_A\}$, et donc aussi $A[X] \neq \{0_{A[X]}\}$. Soient P et Q des polynômes non nuls de $A[X]$, et notons a_p et b_q les coefficients dominants de P et Q. Alors le coefficient dominant $a_p \times_A b_q$ de $P \times_{A[X]} Q$ est non nul car a_p et b_q sont non nuls et que A est intègre. Ainsi $P \times_{A[X]} Q \neq 0_{A[X]}$, et $A[X]$ est un anneau intègre. □

Dans toute la suite, les anneaux considérés seront supposés unitaires et commutatifs.

1.2 Idéaux d'un anneau commutatif

Définition.

Soit $I \subset A$. On dit que I est un *idéal* de l'anneau A si :

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

(ii) I est absorbant : $\forall (x, a) \in I \times A,\ a \times x \in I$.

On dit que I est un idéal *propre* si de plus $I \neq A$.

Remarques.

- Un idéal est un sous-anneau.
- $\{0_A\}$ et A sont des idéaux de A.
- Soit $\mathscr{N} = \{a \in A,\ \exists n \in \mathbb{N}^*,\ a^n = 0_A\}$ l'ensemble des éléments nilpotents de A. Alors $\mathscr{N}$ est un idéal de A.

Exercice. Montrer que les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

Propriété 5

- Une intersection quelconque d'idéaux de A est un idéal de A.
- Si $I_1, \dots, I_k$ sont des idéaux de A, la *somme* de $I_1, \dots, I_k$, notée $\sum_{j=1}^{k} I_j$ et définie par :

$$\sum_{j=1}^{k} I_j = \{i_1 + \cdots + i_k,\ \forall j \in [\![1, k]\!],\ i_j \in I_j\}$$

est un idéal de A.

Preuve. Laissée en exercice. □

Définition.

- Soit $X \subset A$. On appelle *idéal engendré par* X l'intersection de tous les idéaux de A contenant X. C'est le plus petit idéal de A contenant X au sens de l'inclusion. On le note $\langle X \rangle$
- Si $X = \{x\}$, alors
$$\langle X \rangle = \{x \times a,\ a \in A\}.$$
On l'appelle *l'idéal engendré par* x, et on le note xA ou $\langle x \rangle$.
Un idéal I de la forme $\langle x \rangle$ est dit *principal*.
- Si $X = \{x_1, \dots, x_k\}$ est fini, alors
$$\langle X \rangle = \{x_1 a_1 + \cdots + x_k a_k,\ a_i \in A\} = x_1 A + \cdots + x_k A.$$
On l'appelle *l'idéal engendré par* $x_1, \dots, x_k$, et on le note $\langle x_1, \dots, x_k \rangle$.
Un idéal I de la forme $\langle x_1, \dots, x_k \rangle$ est dit *de type fini*.

Propriété 6

Soit I un idéal de A.

(1) $I = A \quad \Leftrightarrow \quad I \cap \mathscr{U}(A) \neq \emptyset$.

(2) A est un corps si et seulement si ses seuls idéaux sont $\{0_A\}$ et A.

Preuve.

(1) Si $I = A$, alors 1_A appartient à $I \cap \mathscr{U}(A)$ qui est donc non vide.

Réciproquement, supposons $I \cap \mathscr{U}(A) \neq \emptyset$ et notons que u un élément de $I \cap \mathscr{U}(A)$. Pour tout $x \in A$, on a :

$$x = \underbrace{u}_{\in I} \times \underbrace{(u^{-1} \times x)}_{\in A} \in I$$

car I est absorbant, et donc $I = A$.

(2) Supposons que A soit un corps. $\{0_A\}$ et A sont des idéaux de A. Et ce sont les seuls puisque si I est un idéal distinct de $\{0_A\}$, alors $I \cap \mathscr{U}(A) = I \cap (A \setminus \{0_A\}) \neq \emptyset$ et donc $I = A$ d'après le point précédent.

Réciproquement, supposons que $\{0_A\}$ et A sont les seuls idéaux de A. Soit alors x un élément non nul de A. L'idéal $\langle x \rangle$ est distinct de $\{0_A\}$ puisqu'il contient x. On a donc par hypothèse que $\langle x \rangle = A$, de sorte que $1_A \in \langle x \rangle$. Il existe donc $y \in A$ tel que :

$$x \times y = y \times x = 1_A.$$

□

1.3 Morphismes d'anneaux

Définition.

Soient A, B des anneaux unitaires. Une application $f : A \to B$ est un *morphisme d'anneaux* si :

- $\forall x, y \in A,\ f(x + y) = f(x) + f(y)$,
- $\forall x, y \in A,\ f(x \times y) = f(x) \times f(y)$,
- $f(1_A) = 1_B$.

Lorsque f est bijective, on parle d'*isomorphisme d'anneaux*.

Propriété 7

Soit $f : A \to B$ un morphisme d'anneaux.

- L'image et l'image réciproque par f d'un sous-anneau est un sous-anneau.
- Si J est un idéal de B, alors l'image réciproque $f^{-1}(J)$ de l'idéal J est un idéal de A.
- Si I est un idéal de A et f **surjective**, alors $f(I)$ est un idéal de B.

Preuve. Laissée en exercice. □

Propriété 8

- L'ensemble $f^{-1}(\{0_B\})$ est un idéal de A. On le note $\mathrm{Ker}(f)$ et on l'appelle le *noyau de* f. On a de plus :
$$\mathrm{Ker}(f) = \{0_A\} \quad \Leftrightarrow \quad f \text{ injective.}$$
- L'ensemble $f(A)$ est un sous-anneau de B. On le note $\mathrm{Im}(f)$ et on l'appelle l'*image de* f. On a de plus :
$$\mathrm{Im}(f) = B \quad \Leftrightarrow \quad f \text{ surjective.}$$

Preuve. Comme $\{0_B\}$ et A sont des idéaux respectivement de B et de A, $f^{-1}(\{0_B\})$ et $f(A)$ sont des idéaux de A et de B respectivement par la proposition précédente. Le reste est bien connu et laissé en exercice. □

Remarque. Un morphisme d'anneaux f d'un corps $\mathbb{K}$ dans un anneau non nul B est injectif : en effet, $\mathrm{Ker}(f)$ est un idéal de $\mathbb{K}$, donc égal à $\{0_\mathbb{K}\}$ ou $\mathbb{K}$. Et comme f est non nul (puisque $f(1_\mathbb{K}) = 1_B$), on a $\mathrm{Ker}(f) = \{0_\mathbb{K}\}$ et f est injective.

Propriété 9

Soit $f : A \to B$ un morphisme d'anneaux. Alors $f(\mathscr{U}(A)) \subset \mathscr{U}(B)$ et pour tout $x \in \mathscr{U}(A)$, $f(x)^{-1} = f(x^{-1})$.

Preuve. Soit $x \in \mathscr{U}(A)$. Il existe $y \in A$ tel que :

$$x \times_A y = y \times_A x = 1_A.$$

On obtient en composant par f morphisme d'anneaux :

$$f(x \times_A y) = f(y \times_A x) = f(1_A) \underbrace{\Rightarrow}_{f \text{ morph. d'ann.}} f(x) \times_B f(y) = f(y) \times_B f(x) = 1_B.$$

Ainsi $f(x)$ appartient à $\mathscr{U}(B)$ et on a $f(x)^{-1} = f(y) = f(x^{-1})$. □

1.4 Anneaux quotients

Théorème 10

Soit A un anneau commutatif et unitaire, et soit I un idéal de A.

- $(I, +)$ est un sous-groupe distingué de $(A, +)$, ce qui permet de définir le groupe quotient $(A/I, +)$ qui est abélien. On a pour rappel :
  - $A/I = \{x + I,\ x \in A\}$,
  - pour tout $x, y \in A$, $x + I = y + I \Leftrightarrow x - y \in I$,
  - la loi $+$ du groupe A/I est définie par : $(x + I) + (y + I) = (x + y) + I$,
  - l'élément neutre pour la loi $+$ est $0_{A/I} = 0_A + I = I$.
- Pour tout $a, b, a', b' \in A$, on a :

$$\begin{cases} a + I = a' + I \\ b + I = b' + I \end{cases} \quad \Rightarrow \quad a \times b + I = a' \times b' + I.$$

  On définit ainsi une loi de composition interne sur A/I, toujours notée $\times$, en posant :

$$(a + I) \times (b + I) = a \times b + I.$$

- $(A/I, +, \times)$ est un anneau commutatif et unitaire, avec $1_{A/I} = 1_A + I$. On l'appelle *l'anneau quotient de A par I*.
- L'application $\pi : \begin{cases} A & \to A/I \\ a & \mapsto a + I \end{cases}$ est un morphisme d'anneaux surjectif, de noyau $\mathrm{Ker}(\pi) = I$, appelée la *projection* ou *surjection canonique*.

Preuve. Pour le premier point, je vous renvoie par exemple à mon cours **Groupes et actions de groupes**.

Montrons le deuxième point. Soient pour cela $a, b, a', b' \in A$ tels que $\begin{cases} a + I = a' + I \\ b + I = b' + I \end{cases} \Leftrightarrow \begin{cases} a - a' \in I \\ b - b' \in I \end{cases}$. On a :

$$a \times b - a' \times b' = a \times b - a \times b' + a \times b' - a' \times b' = a \times \underbrace{(b - b')}_{\in I} + \underbrace{(a - a')}_{\in I} \times b' \in I.$$

Ainsi, on a bien $a \times b + I = a' \times b' + I$. Ce qui permet de (bien) définir une loi de composition interne sur A/I, indépendante des représentants choisis, toujours notée $\times$, en posant :

$$(a + I) \times (b + I) = a \times b + I.$$

Les axiomes définissant un anneau commutatif unitaire sont alors trivialement vérifiés pour $(A/I, +, \times)$ puisqu'ils le sont pour $(A, +, \times)$. D'où le troisième point. Et le quatrième point est immédiat. □

Exemple. Pour tout $n \in \mathbb{N}$, $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$. On dispose donc de l'anneau quotient $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

Propriété 11

Soit A un anneau, I un idéal, et $\pi : A \to A/I$ la surjection canonique. Alors les idéaux de A/I sont en bijection avec les idéaux de A contenant I via les deux applications, croissantes pour l'inclusion :

$$\begin{array}{cccc} & \{\text{idéaux de } A \text{ contenant } I\} & \overset{1-1}{\longleftrightarrow} & \{\text{idéaux de } A/I\} \\ \psi : & J & \mapsto & \pi(J) \\ \varphi : & \pi^{-1}(J') & \hookleftarrow & J' \end{array}$$

Preuve. $\pi : A \to A/I$ étant un morphisme d'anneaux surjectif, $\pi(J)$ est un idéal de A/I pour tout J idéal de A contenant I. Et pour tout J' idéal de A/I, l'image réciproque $\pi^{-1}(J')$ est bien un idéal de A, qui contient I car $0_{A/I} \in J'$ et $\pi^{-1}(\{0_{A/I}\}) = \mathrm{Ker}(\pi) = I$. Donc les applications ψ et φ sont bien définies.
La croissance de ces applications pour l'inclusion est immédiate. Reste donc à montrer qu'elles sont inverses l'une de l'autre :

- Soit J un idéal de A contenant I. Montrons que $\pi^{-1}(\pi(J)) = J$. L'inclusion $J \subset \pi^{-1}(\pi(J))$ est toujours satisfaite (vérifiez le si besoin), on démontre l'inclusion réciproque. Soit pour cela $x \in \pi^{-1}(\pi(J))$. On a $\pi(x) \in \pi(J)$, de sorte qu'il existe $y \in J$ tel que $\pi(x) = \pi(y)$. Comme π est un morphisme de groupes, on en déduit que $\pi(x - y) = 0_{A/I}$, et donc que $x - y \in \mathrm{Ker}(\pi) = I \subset J$. Ainsi $x \in y + J \subset J$ car $(J, +)$ est un groupe. D'où l'égalité voulue.
- Soit J' un idéal de A/I. Alors $\pi(\pi^{-1}(J')) = J'$ car J' est une application surjective.

Ainsi ψ et φ sont des bijections réciproques l'une de l'autre, et les idéaux de A/I sont bien en bijection avec les idéaux de A contenant I. □

Exemple. Les idéaux de $(\mathbb{Z}/nZ, +, \times)$ sont les $d\mathbb{Z}/n\mathbb{Z}$ où $n\mathbb{Z} \subset d\mathbb{Z}$, c'est-à-dire où d divise n.

Théorème 12 (*Théorème d'isomorphisme*)

Soient A et B deux anneaux et $f : A \to B$ un morphisme d'anneaux. Alors on a un isomorphisme d'anneaux :

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

Preuve. Pour simplifier, on notera dans la suite $\overline{x}$ la classe d'un élément $x \in A$ dans le quotient $A/\mathrm{Ker}(f)$. Considérons pour cela l'application :

$$\begin{array}{cccc} \overline{f} : & A/\mathrm{Ker}(f) & \to & \mathrm{Im}(f) \\ & \overline{x} & \mapsto & f(x) \end{array}$$

Montrons pour commencer que $\overline{f}$ est bien définie, c'est-à-dire que $\overline{f}(\overline{x})$ ne dépend pas du représentant de la classe de x choisi. Soit pour cela $y \in A$ tel que $\overline{x} = \overline{y}$. On a par définition $x - y \in \mathrm{Ker}(f)$, de sorte que :

$$f(x - y) = 0_A \underbrace{\Rightarrow}_{f \text{ morph. d'ann.}} f(x) - f(y) = 0_A \quad \Rightarrow \quad f(x) = f(y).$$

Donc $\overline{f}$ est bien définie. On a pour tout $\overline{x}, \overline{y} \in A/\mathrm{Ker}(f)$:

$$\overline{f}(\overline{x} + \overline{y}) = \overline{f}(\overline{x + y}) = f(x + y) \underbrace{=}_{f \text{ morph. d'ann.}} f(x) + f(y) = \overline{f}(\overline{x}) + \overline{f}(\overline{y}),$$

$$\overline{f}(\overline{x}\times\overline{y}) = \overline{f}(\overline{x\times y}) = f(x\times y) \underbrace{=}_{f \text{ morph. d'ann.}} f(x)\times f(y) = \overline{f}(\overline{x})\times\overline{f}(\overline{y}),$$

$$\overline{f}(\overline{1_A}) = f(1_A) = 1_B.$$

$\overline{f}$ est donc un morphisme d'anneaux, surjectif de façon immédiate. Et pour tout $\overline{x}\in\mathrm{Ker}(\overline{f})$, on a :

$$\overline{f}(\overline{x}) = f(x) = 0_B \quad\Rightarrow\quad x = x - 0_A \in \mathrm{Ker}(f) \quad\Rightarrow\quad \overline{x} = \overline{0_A}.$$

$\overline{f}$ est donc un isomorphisme d'anneaux de $A/\mathrm{Ker}(f)$ sur $\mathrm{Im}(f)$. □

1.5 Idéaux premiers, idéaux maximaux

Définition.

Soit A un anneau, I un idéal de A. I est dit *premier* si :

(i) I est un idéal propre, c'est-à-dire $I\subsetneq A$,

(ii) $\forall x,y\in A,\ x\times y\in I \Rightarrow x\in I$ ou $y\in I$.

Remarque. A est intègre $\Leftrightarrow \{0_A\}$ est un idéal premier.

Théorème 13

Soit I un idéal propre de A. Alors :

$$I \text{ est un idéal premier} \quad\Leftrightarrow\quad A/I \text{ est intègre.}$$

Preuve.

$\Rightarrow$ Comme I premier, I est propre et A/I n'est pas réduit à $\{0_{A/I}\}$. De plus, soient $\overline{a},\overline{b}$ des éléments de A/I. On a :

$$0_{A/I} = \overline{a}\times\overline{b} = \overline{a\times b} \quad\Rightarrow\quad a\times b\in I \underset{I \text{ premier}}{\Rightarrow} a\in I \text{ ou } b\in I \quad\Rightarrow\quad \overline{a}=0_{A/I} \text{ ou } \overline{b}=0_{A/I}$$

Donc A/I est bien intègre.

$\Leftarrow$ Supposons que A/I est intègre. En particulier $A/I\neq\{0_{A/I}\}$ et donc I est propre. Soient $a,b\in A$. On a :

$$a\times b\in I \quad\Rightarrow\quad \overline{a}\times\overline{b} = \overline{a\times b} = 0_{A/I} \underset{A/I \text{ intègre}}{\Rightarrow} \overline{a}=0_{A/I} \text{ ou } \overline{b}=0_{A/I} \quad\Rightarrow\quad a\in I \text{ ou } b\in I$$

Donc l'idéal I est premier.

□

Exercice. Montrer que les idéaux premiers de $\mathbb{Z}$ sont $\{0\}$ ou $p\mathbb{Z}$ avec p premier.

Définition.

Un idéal I d'un anneau A est dit *maximal* si :

(i) I est propre, c'est-à-dire $I\subsetneq A$,

(ii) I est maximal pour l'inclusion : pour tout idéal J de A, $I\subseteq J\subseteq A \quad\Rightarrow\quad J=I$ ou $J=A$.

Théorème 14

Soit I un idéal de A. On a l'équivalence :

$$I \text{ maximal} \quad\Leftrightarrow\quad A/I \text{ est un corps.}$$

Preuve.

⇒ Supposons I maximal. Il est en particulier propre, de sorte que A/I n'est pas réduit à $\{0_{A/I}\}$. Soit $\overline{a}$ un élément non nul de A/I. Montrons que $\overline{a}$ est inversible. Considérons pour cela l'idéal $J = I + \langle a \rangle$ de A. Cet idéal contient I, et est distinct de I car $a \in J \setminus I$ (puisque $\overline{a} \neq 0_{A/I}$). Comme I est un idéal maximal, on a donc :

$$J = A \quad \Rightarrow \quad 1_A \in J = I + \langle a \rangle.$$

Ainsi, il existe $i \in I$ et $b \in A$ tel que :

$$1_A = i + a \times b \quad \Rightarrow \quad \overline{1_A} = \overline{i + a \times b} = \underbrace{\overline{i}}_{=0_{A/I}} + \overline{a \times b} = \overline{a} \times \overline{b}.$$

$\overline{a}$ est donc inversible, et A/I est bien un corps.

⇐ Supposons que A/I soit un corps, et considérons J un idéal contenant strictement I. Montrons que $J = A$. Soit $a \in J \setminus I$. On a $\overline{a} \neq 0_{A/I}$, et puisque A/I est un corps, il existe $\overline{b} \in A/I$ tel que :

$$\overline{a \times b} = \overline{a} \times \overline{b} = \overline{1_A} \quad \Rightarrow \quad 1_A - a \times b \in I.$$

Il existe donc $i \in I$ tel que :

$$1_A = \underbrace{a}_{\in J} \times b + \underbrace{i}_{\in I \subset J} \in J.$$

Ainsi $J \cap \mathscr{U}(A) \neq \emptyset$, et on a bien $J = A$.

□

Corollaire 15

Tout idéal maximal est premier.

Preuve. Si I est un idéal maximal, alors A/I est un corps. En particulier, A/I est intègre, ce qui implique que I est premier. □

Remarque. La réciproque est fausse : par exemple $\{0\}$ est un idéal premier de $\mathbb{Z}$ car $\mathbb{Z}$ est intègre, mais il n'est pas maximal car par exemple $\{0\} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$.

Exercice. Montrer que les idéaux maximaux de $\mathbb{Z}$ sont exactement les idéaux $p\mathbb{Z}$ avec p premier.
En déduire les équivalences suivantes pour $n \geq 2$:

$$(\mathbb{Z}/n\mathbb{Z}, +, \times) \text{ est un corps} \quad \Leftrightarrow \quad (\mathbb{Z}/n\mathbb{Z}, +, \times) \text{ est un anneau intègre} \quad \Leftrightarrow \quad n \text{ est premier.}$$

Propriété 16

Soit A un anneau, I un idéal. Les idéaux premiers (resp. maximaux) de A/I sont en bijection avec les idéaux premiers (resp. maximaux) de A contenant I, via les deux applications ψ et φ définies à la Propriété 11.

Preuve. C'est immédiat pour les idéaux maximaux puisque les bijections réciproques ψ et φ sont croissantes pour l'inclusion.

Pour les idéaux premiers, puisque ψ et φ sont des bijections réciproques l'une de l'autre, il suffit de vérifier qu'elles envoient bien par restriction idéaux premiers sur idéaux premiers.

Pour ψ, soit J un idéal premier de A contenant I. Montrons que $\pi(J)$ est un idéal premier de A/I. Comme J est propre, $J \neq A$ et donc $\pi(J) \neq \pi(A) = A/I$ (car ψ injective), de sorte que $\pi(J)$ est propre également. De plus soient $\overline{a}, \overline{b} \in A/I$. On a :

$$\begin{aligned} \overline{a} \times \overline{b} \in \pi(J) \quad &\Rightarrow \quad \overline{a \times b} \in \pi(J) \quad \Rightarrow \quad \exists j \in J,\ \overline{a \times b} = \pi(j) = \overline{j} \\ &\Rightarrow \quad \exists j \in J,\ a \times b \in \underbrace{j}_{\in J} + \underbrace{I}_{\subset J} \subset J \quad \Rightarrow \quad a \times b \in J \\ &\underset{J \text{ premier}}{\Rightarrow} \quad a \in J \text{ ou } b \in J \quad \Rightarrow \quad \overline{a} \in \pi(J) \text{ ou } \overline{b} \in \pi(J). \end{aligned}$$

Donc $\pi(J)$ est premier.

Pour φ, soit J' un idéal premier de A/I. Montrons que $\pi^{-1}(J')$ est un idéal premier de A. De même, comme $J' \neq A/I$, on a $\pi^{-1}(J') \neq A$ (car φ injective), et donc $\pi^{-1}(J')$ est propre. Et pour tout $a, b \in A$, on a :

$$\begin{aligned} a \times b \in \pi^{-1}(J') \quad &\Rightarrow \quad \pi(a) \times \pi(b) = \pi(a \times b) \in J' \quad \underset{J' \text{ premier}}{\Rightarrow} \quad \pi(a) \in J' \text{ ou } \pi(b) \in J' \\ &\Rightarrow \quad a \in \pi^{-1}(J') \text{ ou } b \in \pi^{-1}(J'). \end{aligned}$$

Donc $\pi^{-1}(J')$ est premier. D'où le résultat. □

Signalons enfin le théorème suivant dont la démonstration dépasse le programme de l'agrégation interne (elle résulte du lemme de Zorn).

Théorème 17 (*de Krull* (1899-1971))

Soit I un idéal propre de A. Alors il existe un idéal maximal m de A contenant I.

Prolongement possible.

- Anneaux noethériens (voir par exemple [6], [8] ou encore [1]).

2 Anneaux principaux

2.1 Définition

Définition.

Un anneau A est dit *principal* s'il est intègre et si tout idéal de A est principal.

Exemples.

- $\mathbb{Z}$ est un anneau principal.
- Un corps est un anneau principal.
- Nous verrons que si $\mathbb{K}$ est un corps commutatif, alors $\mathbb{K}[X]$ est un anneau principal.
- Si n n'est pas premier, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre, donc pas principal. Cependant, tous ses idéaux sont principaux.

Exemple. $\mathbb{Z}[X]$ n'est pas un anneau principal. En effet, supposons que l'idéal $\langle 2, X\rangle$ soit principal, de la forme $\langle P\rangle$ avec $P \in \mathbb{Z}[X]$. Alors on aurait :

$$2 \in \langle 2, X\rangle = \langle P\rangle \quad \Rightarrow \quad \exists Q \in \mathbb{Z}[X],\ 2 = PQ,$$

et de même :

$$X \in \langle 2, X\rangle = \langle P\rangle \quad \Rightarrow \quad \exists R \in \mathbb{Z}[X],\ X = PR.$$

De la première égalité, on obtient que P et Q sont constants, et donc que $P = \pm 1$ ou $P = \pm 2$. Et de la deuxième relation, on obtient que $P = \pm 1$. Mais alors on aurait :

$$1 \in \langle P\rangle = \langle 2, X\rangle \quad \Rightarrow \quad \exists U, V \in Z[X],\ 1 = 2U + XV.$$

Ce qui donne en prenant $X = 0$ dans cette relation $1 = 2U(0)$ avec $U(0) \in \mathbb{Z}$. D'où une contradiction.

2.2 Propriétés arithmétiques d'un anneau principal

Divisibilité

Dans cette section, $(A, +, \times)$ désignera un anneau intègre.

Définition.

Soient $a, b \in A$. On dit que a *divise* b (ou que b est un *multiple* de a), et on note $a|b$, si $\langle b\rangle \subset \langle a\rangle$, ce qui équivaut à l'existence d'un élément $c \in A$ tel que $b = a \times c$.

Propriété 18

Soient $x, y_1, \dots, y_n$ des éléments de A.

- x divise $y_1, \dots y_n$ si et seulement si $\langle y_1\rangle + \cdots + \langle y_n\rangle \subset \langle x\rangle$.
- x est un multiple de $y_1, \dots y_n$ si et seulement si $\langle x\rangle \subset \langle y_1\rangle \cap \cdots \cap \langle y_n\rangle$.

Définition.

Deux éléments $a, b \in A$ sont dits *associés dans* A s'il existe $u \in \mathscr{U}(A)$ tel que $a = u \times b$.

Remarque. « être associé » est une relation d'équivalence sur A.

Exemple. Deux entiers $n, m \in \mathbb{Z}$ sont associés si $n = \pm m$.

Propriété 19

Soient $a, b \in A$. On a l'équivalence :

$$a \text{ et } b \text{ sont associés} \quad \Leftrightarrow \quad a|b \text{ et } b|a \quad \Leftrightarrow \quad \langle a\rangle = \langle b\rangle.$$

PGCD, PPCM

Dans toute la suite, A désigne un anneau principal.

Théorème 20

Soient $a, b \in A$.

- Soit $m \in A$ tel que $\langle a\rangle \cap \langle b\rangle = \langle m\rangle$. L'élément m satisfait :
  (i) $a|m$ et $b|m$, i.e. m est un multiple commun de a et de b,
  (ii) $\forall \ell \in A$, $a|\ell$ et $b|\ell \Rightarrow m|\ell$, i.e. m divise tout multiple commun de a et de b.

  De plus si m' satisfait (i) et (ii), alors m' et m sont associés.
- Soit $d \in A$ tel que $\langle a\rangle + \langle b\rangle = \langle d\rangle$. L'élément d satisfait :
  (iii) $d|a$ et $d|b$, i.e. d est un diviseur commun de a et de b,
  (iv) $\forall c \in A$, $c|a$ et $c|b \Rightarrow d|c$, i.e. tout diviseur commun de a et de b divise d.

  De plus si d' satisfait (iii) et (iv), alors d' et d sont associés.

Preuve. Prouvons le premier point (le deuxième point se démontre de manière similaire). Puisque $\langle m\rangle \subset \langle a\rangle \cap \langle b\rangle$, m est bien un multiple commun de a et de b, de sorte qu'on a (i). Soit $\ell \in A$ tel que $a|\ell$ et $b|\ell$. On a :

$$\langle \ell\rangle \subset \langle a\rangle \cap \langle b\rangle = \langle m\rangle.$$

Donc m divise bien ℓ, et (ii) est bien satisfait.

Soit maintenant m' satisfaisant (i) et (ii). On a :

- puisque m satisfait (i) et m' satisfait (ii), $m'|m$.
- inversement, puisque m' satisfait (i) et m satisfait (ii), $m|m'$.

Donc m et m' sont bien associés. □

Définition.

- Un élément m satisfaisant (i) et (ii) est appelé *un plus petit commun multiple* (PPCM) de a et b, et noté $a \vee b$
- Un élément d satisfaisant (iii) et (iv) est appelé *un plus grand commun diviseur* (PGCD) de a et b, et noté $a \wedge b$.

Mise en garde.

Un PGCD et un PPCM de a et b ne sont pas uniques : ils sont uniques à multiplication par un élément inversible de A près. Dans $\mathbb{Z}$, on fait le choix de les prendre dans $\mathbb{N}$ pour les rendre uniques. Dans $\mathbb{K}[X]$, on pourra exiger de les prendre unitaires pour la même raison.

Définition.

On dit que deux éléments a et b de A sont *premiers entre eux* si $a \wedge b = 1_A$ (ou plus précisément $a \wedge b$ est associé à 1_A).

Théorème 21 (*de Bezout* (1730 - 1783))

Soient $a, b \in A$. Les assertions suivantes sont équivalentes :

(i) $a \wedge b = 1_A$ (i.e. a et b sont premiers entre eux),

(ii) $A = \langle a \rangle + \langle b \rangle$,

(iii) $\exists u, v \in A, \quad a \times u + b \times v = 1_A$.

Preuve.

(i) ⇒ (ii) Si $a \wedge b = 1_A$, alors $\langle a \rangle + \langle b \rangle = \langle 1_A \rangle = A$.

(ii) ⇒ (iii) Si $A = \langle a \rangle + \langle b \rangle$, alors 1_A appartient à $\langle a \rangle + \langle b \rangle$, et il existe $u, v \in A$ tels que :

$$1_A = a \times u + b \times v.$$

(iii) ⇒ (i) S'il existe $u, v \in A$ tels que $1_A = a \times u + b \times v$, alors 1_A appartient à $\langle a \rangle + \langle b \rangle$, de sorte que $\langle a \rangle + \langle b \rangle = A = \langle 1_A \rangle$ et que $a \wedge b = 1_A$.

□

Théorème 22 (*de Gauss* (1777 - 1855))

Soient $a, b, c \in A$. Si a divise $b \times c$ et que a est premier avec b, alors a divise c.

Preuve. Comme a est premier avec b, il existe $u, v \in A$ tels que :

$$1_A = a \times u + b \times v.$$

En multipliant par c, on obtient :

$$c = \underbrace{a \times (u \times c)}_{\in \langle a \rangle} + \underbrace{(b \times c)}_{\in \langle a \rangle \text{ car } a | b \times c} \times v \in \langle a \rangle.$$

Donc a divise c. □

Propriété 23

Soient $a, b, c, d \in A \setminus \{0_A\}$.

(1) $d = a \wedge b \quad \Leftrightarrow \quad \exists a', b' \in A, \begin{cases} a = d \times a' \\ b = d \times b' \\ a' \wedge b' = 1_A \end{cases}$.

(2) $d = a \wedge b \quad \Leftrightarrow \quad d \times c = (a \times c) \wedge (b \times c)$.

Preuve.

(1) $\Rightarrow$ Comme $d = a \wedge b$, d divise a et b, et il existe $a', b' \in A$ tels que :

$$a = d \times a' \quad \text{et} \quad b = d \times b'.$$

Montrons que $a' \wedge b' = 1_A$. Puisque $d \in \langle d \rangle = \langle a \rangle + \langle b \rangle$, il existe deux éléments u et v de A tels que :

$$d = a \times u + b \times v = d \times a' \times u + d \times b' \times v.$$

Ce qui donne en simplifiant par $d \neq 0_A$ (possible car A intègre) :

$$1_A = a' \times u + b' \times v.$$

Donc a' et b' sont bien premiers entre eux.

$\Leftarrow$ Supposons qu'il existe des éléments a', b' premiers entre eux, et d tels que :

$$a = d \times a' \quad \text{et} \quad b = d \times b'.$$

d divise donc a et b, de sorte que $\langle a \rangle + \langle b \rangle \subset \langle d \rangle$. Montrons l'inclusion réciproque. Comme $a' \wedge b' = 1_A$, il existe $u, v \in A$ tels que :

$$a' \times u + b' \times v = 1_A \quad \Rightarrow \quad a \times u + b \times v = d \times a' \times u + d \times b' \times v = d \times \underbrace{(a' \times u + b' \times v)}_{1_A} = d.$$

Ainsi d appartient à $\langle a \rangle + \langle b \rangle$, et on a l'inclusion $\langle d \rangle \subset \langle a \rangle + \langle b \rangle$. D'où finalement l'égalité $\langle d \rangle = \langle a \rangle + \langle b \rangle$, et donc que $d = a \wedge b$.

(2) On a avec le point précédent :

$$d = a \wedge b \Leftrightarrow \exists a', b' \in A, \begin{cases} a = d \times a' \\ b = d \times b' \\ a' \wedge b' = 1_A \end{cases} \underset{c \neq 0_A \text{ et } A \text{ intègre}}{\Leftrightarrow} \exists a', b' \in A, \begin{cases} a \times c = (d \times c) \times a' \\ b \times c = (d \times c) \times b' \\ a' \wedge b' = 1_A \end{cases}$$
$$\Leftrightarrow d \times c = (a \times c) \wedge (b \times c).$$

□

Propriété 24

Soient $a, b, c, m \in A \setminus \{0_A\}$.

(1) $a \times b = (a \vee b) \times (a \wedge b)$.

(2) $m = a \vee b \quad \Leftrightarrow \quad m \times c = (a \times c) \vee (b \times c)$.

Preuve.

(1) Notons $d = a \wedge b$, et $a', b' \in A$ tels que $\begin{cases} a = d \times a' \\ b = d \times b' \\ a' \wedge b' = 1_A \end{cases}$, et posons $m = d \times a' \times b'$. Montrons que $m = a \vee b$.

On a :

$$m = d \times a' \times b' = a \times b' = a' \times b.$$

Donc m est un multiple commun de a et de b.

Soit $\ell \in A$ tel que $a|\ell$ et $b|\ell$. Il existe donc $a'', b'' \in A$ tels que :

$$\ell = a \times a'' = a' \times d \times a'' \quad \text{et} \quad \ell = b \times b'' = b' \times d \times b''.$$

D'où l'égalité :

$$a' \times d \times a'' = b' \times d \times b'' \underset{d \neq 0_A \text{ et } A \text{ intègre.}}{\Rightarrow} a' \times a'' = b' \times b''.$$

Ainsi a' divise $b' \times b''$, et comme $a' \wedge b' = 1_A$, le théorème de Gauss assure l'existence d'un élément $c \in A$ tel que

$$b'' = a' \times c \quad \Rightarrow \quad \ell = b' \times d \times b'' = b' \times d \times a' \times c = m \times c.$$

Ainsi m divise ℓ. On a donc bien que $m = d \times a' \times b$ est égal à $a \vee b$, et donc que :

$$a \times b = d \times a' \times b' \times d = m \times d = (a \vee b) \times (a \wedge b).$$

(2) On a à l'aide du point précédent :

$$c \times (a \vee b) \times c \times (a \wedge b) = (a \times c) \times (b \times c) = ((a \times c) \vee (b \times c)) \times ((a \times c) \wedge (b \times c)) \underset{\text{Propriété 23}}{=} ((a \times c) \vee (b \times c)) \times c \times (a \wedge b).$$

Et comme A est intègre, et que $c \times (a \wedge b) \neq 0_A$, on obtient :

$$c \times (a \vee b) = (a \times c) \vee (b \times c).$$

L'équivalence demandée se déduit alors directement de cette égalité.

□

Remarque. On définit aisément par récurrence le PGCD et le PPCM de n éléments.

Décomposition en produit d'irréductibles

Définition.

Soit $p \in A$. On dit que p est *irréductible* si :

(i) $p \notin \mathscr{U}(A)$, (ii) $p = a \times b \quad \Rightarrow \quad a \in \mathscr{U}(A)$ ou $b \in \mathscr{U}(A)$.

Remarques.

- 0_A n'est pas irréductible car $0_A = 0_A \times 0_A$ et que $0_A \notin \mathscr{U}(A)$.
- Dans $\mathbb{Z}$, les éléments irréductibles sont les nombres premiers et leurs opposés.

Propriété 25

Soit $p \in A$. Les assertions suivantes sont équivalentes :

(i) p est irréductible,

(ii) $\langle p \rangle$ est premier et non nul,

(iii) $\langle p \rangle$ est maximal et non nul,

(iv) $\langle p \rangle$ est non nul et $A/\langle p \rangle$ est un corps.

Preuve.

(i) $\Rightarrow$ (iii) Comme p est irréductible, $p \neq 0_A$ et donc $\langle p \rangle$ n'est pas nul. Soit I un idéal contenant $\langle p \rangle$. Comme A est principal, I est de la forme $\langle a \rangle$. On a donc $p \in \langle p \rangle \subset \langle a \rangle$, de sorte qu'il existe $b \in A$ tel que :

$$p = a \times b \quad \underbrace{\Rightarrow}_{p \text{ irréd.}} \quad a \in \mathscr{U}(A) \text{ ou } b \in \mathscr{U}(A).$$

Si $a \in \mathscr{U}(A)$, alors on a $I = \langle a \rangle = A$. Si $b \in \mathscr{U}(A)$, alors p et a sont associés, et on a $\langle p \rangle = \langle a \rangle = I$. Donc $\langle p \rangle$ est bien maximal.

(iii) $\Rightarrow$ (iv) Découle directement du Théorème 14.

(iv) $\Rightarrow$ (ii) Si $A/\langle p \rangle$ est un corps, il est en particulier intègre et donc $\langle p \rangle$ est premier.

(ii) $\Rightarrow$ (i) Comme $\langle p \rangle$ est un idéal premier, il est propre et donc $p \notin \mathscr{U}(A)$. Soient maintenant $a, b \in A$ tels que $p = a \times b$. On a :

$$a \times b \in \langle p \rangle \quad \Rightarrow \quad a \in \langle p \rangle \text{ ou } b \in \langle p \rangle.$$

Supposons par exemple que $a \in \langle p \rangle$. Il existe $u \in A$ tel que $a = p \times u$, ce qui donne donc $p = a \times b = p \times u \times b$. p étant de plus non nul et A étant intègre, cela donne $1_A = u \times b$. Ainsi b appartient à $\mathscr{U}(A)$.

□

Remarque. On a ainsi montré que pour un anneau A principal qui n'est pas un corps, les idéaux premiers sont l'idéal $\{0_A\}$ et les idéaux maximaux $\langle p \rangle$ engendrés par les irréductibles.

Théorème 26 (*Théorème fondamental de l'arithmétique*)

(AF1) Tout élément a non nul de A s'écrit $a = up_1 \dots p_r$ avec $u \in \mathscr{U}(A)$ et $p_1, \dots, p_r$ irréductibles.

(AF2) Cette décomposition est unique, à permutation près et à des inversibles près : si $a = up_1 \dots p_r = vq_1 \dots q_s$, on a $r = s$ et il existe $\sigma \in S_r$ tel que p_i et $q_{\sigma(i)}$ soient associés pour tout i.

Remarque. Un anneau intègre satisfaisant (AF1) et (AF2) est dit *factoriel*. On montre donc ici qu'un anneau principal est factoriel. La réciproque est cependant fausse en général : on peut par exemple montrer que l'anneau $\mathbb{Z}[X]$ est factoriel mais pas principal.

Pour démontrer ce résultat, on aura besoin des résultats suivants.

Propriété 27

Dans un anneau principal A, toute suite croissante d'idéaux pour l'inclusion stationne.

Preuve. Soit (I_n) une suite croissante d'idéaux pour l'inclusion. Montrons que $J = \bigcup I_n$ est un idéal de A :

- Soient $x, y \in J$.Il existe $m, n \in \mathbb{N}$ tels que $x \in I_n$ et $y \in I_m$. Supposons par exemple $m \geq n$, alors on a $x, y \in I_m$ puisque la suite d'idéaux est croissante pour l'inclusion. Comme $(I_m, +)$ est un groupe, on a :

$$x - y \in I_m \subset J.$$

- Soient $x \in J$ et $a \in A$. Il existe $m \in \mathbb{N}$ tel que x appartient à I_m. Et comme I_m est un idéal, on a :

$$a \times x \in I_m \subset J.$$

J est donc un idéal de A qui est principal, il existe donc un élément $a \in A$ tel que $J = \langle a \rangle$. Cet élément a appartient à J, de sorte qu'il existe $m \in \mathbb{N}$ tel que a appartient à I_m. Mais la suite étant croissante, on a aussi $a \in I_n$ pour tout $n \geq m$. Et donc pour tout $n \geq m$, on a :

$$\langle a \rangle \subset I_n \subset J = \langle a \rangle.$$

Ainsi $I_n = \langle a \rangle$ pour tout $n \geq m$, et la suite (I_n) stationne bien. □

Propriété 28

Soit $a \in A$ un élément non nul. Si a n'est pas inversible, il admet au moins un diviseur irréductible.

Preuve. Supposons par l'absurde que a n'admette aucun diviseur irréductible. Dans ce cas, $a_0 = a$ n'est lui même pas irréductible, et il existe a_1 et b_1 des éléments non inversibles tels que $a = a_1 \times b_1$.

Comme a_1 n'est pas irréductible, il existe a_2 et b_2 non inversibles tels que $a_1 = a_2 \times b_2$.

En poursuivant cette construction par récurrence, on obtient une suite (a_n) d'éléments de A tels que pour tout $n \in \mathbb{N}$, a_{n+1} divise a_n, sans être inversible, ni associé à a_n. La suite d'idéaux $(\langle a_n \rangle)$ serait alors strictement croissante dans A principal, ce qui est impossible. D'où le résultat. □

Preuve du Théorème 26.
Démontrons (AF1). Soit a un élément non nul de A. Si a est inversible, c'est terminé. Supposons $a_0 = a$ non inversible, alors a_0 admet un diviseur irréductible p_1, de sorte qu'il existe $a_1 \in A$ tel que $a_0 = a_1 \times p_1$.

Si a_1 est inversible, on a obtenu une factorisation de la forme voulue. Sinon, il admet un diviseur irréductible p_2, et il existe un élément $a_2 \in A$ tel que $a_0 = a_2 \times p_1 \times p_2$.

De même si a_2 est inversible, on obtient une factorisation de la forme voulue. Sinon on poursuit ce procédé jusqu'à avoir une factorisation de la forme voulue, qui s'écrit :

$$a_0 = a_N \times p_1 \times p_2 \times \cdots \times p_N \text{ avec } a_N \text{ inversible et } p_1, \dots p_N \text{ irréductibles.}$$

Un tel rang $N \geq 1$ existe nécessairement. En effet, on aurait sinon une suite (a_n) d'éléments non inversibles et une suite (p_n) d'éléments irréductibles satisfaisant $a_n = a_{n+1}p_{n+1}$, avec donc a_{n+1} divise a_n sans être inversible ni associé à a_n pour tout $n \in \mathbb{N}$. De même que précédemment, la suite d'idéaux $(\langle a_n \rangle)$ serait strictement croissante dans A principal, ce qui est impossible.

Pour (AF2), je vous renvoie par exemple à [3] ou [4].

□

2.3 Cas des anneaux euclidiens

Définition et exemples

Définition.

Soit A un anneau commutatif unitaire et intègre. On dit que A est un *anneau euclidien* s'il existe une application $N : A \setminus \{0_A\} \to \mathbb{N}$, appelée *stathme euclidien*, telle que pour tout $a, b \in A \setminus \{0_A\}$, il existe $q, r \in A$ tels que :

$$a = b \times q + r \quad \text{et} \quad r = 0_A \quad \text{ou} \quad N(r) < N(b).$$

On dit alors qu'on a fait la *division euclidienne* de a par b. Les éléments q et r sont alors appelés *quotient* et *reste* de cette division euclidienne.

Exemples.

- Tout corps est un anneau euclidien, puisque pour tout $x, y \in \mathbb{K}^*$, $x = q \times y + r$ avec $q = x \times y^{-1}$ et $r = 0_{\mathbb{K}}$. Toute application $N : \mathbb{K}^* \to \mathbb{N}$ convient ici.
- L'anneau $\mathbb{Z}$ est euclidien, avec pour stathme euclidien sur $\mathbb{Z}$ l'application $N : \mathbb{Z}^* \to \mathbb{N},\ k \mapsto |k|$.
- Si $\mathbb{K}$ est un corps, l'anneau $\mathbb{K}[X]$ est euclidien avec pour stathme euclidien l'application $N : \mathbb{K}[X]^* \to \mathbb{N},\ P \mapsto \deg(P)$.

Théorème 29

Tout anneau euclidien est principal.

Preuve. Soit A un anneau euclidien. Il est en particulier intègre par définition. Soit I un idéal non nul de A. L'ensemble $\{N(a),\ a \in I \setminus \{0_A\}\}$ est une partie non vide de $\mathbb{N}$. Elle admet donc un plus petit élément $n_0 \in N$. Prenons $x \in I \setminus \{0_A\}$ tel que $N(x) = n_0$. On a $x \in I$, et donc $\langle x \rangle I$. Montrons l'inclusion réciproque. Prenons pour cela $a \in I \setminus \{0_A\}$ et effectuons la division euclidienne de a par x. Il existe $q, r \in A$ tels que :

$$a = x \times q + r \quad \text{avec} \quad r = 0_A \quad \text{ou } N(r) < N(x).$$

Supposons $r \neq 0_A$. On aurait $r = a - x \times q \in I \setminus \{0_A\}$ et $N(r) < N(x)$, ce qui est impossible par définition de x et n_0. Donc $r = 0_A$, et on a $a = x \times q \in \langle x \rangle$. Ainsi $I = \langle x \rangle$ et A est un anneau principal. □

Remarque. Il existe des anneaux principaux qui ne sont pas euclidien. On peut par exemple montrer que $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais n'est pas euclidien (voir à ce sujet [8] ou [9]).

PGCD dans les anneaux euclidiens

Un anneau euclidien étant en particulier principal, deux éléments admettent toujours un pgcd et un ppcm. La structure euclidienne permet de plus de calculer un pgcd, écrire une relation de Bezout, ... de façon algorithmique.

Propriété 30

Soit A un anneau euclidien et $a, b \in A \setminus \{0_A\}$. Soient $q, r \in A$ tels que $a = b \times q + r$. Alors on a :

$$a \wedge b = b \wedge r.$$

Preuve. Il suffit de montrer que les diviseurs communs à a et b sont les mêmes que ceux de b et r.

- Si d divise a et b, alors d divise $a - b \times q = r$. Et donc d divise b et r.
- Si d divise b et r, alors d divise $b \times q + r = a$. Et donc d divise a et b.

□

Algorithme d'Euclide. On dispose de l'algorithme suivant pour le calcul du pgcd de deux nombres.

```
Entrer a >= b
r0 = b
r1 = reste de la division eucl de a par b
Tant que r1 <> 0, faire
      r2 = reste de la division euclidienne de r0 par r1
      r0 = r1
      r1 = r2
Fin du Tant que
Retourner r0
```

Propriété 31

L'algorithme d'Euclide s'arrête au bout d'un nombre fini d'étapes. De plus, $a \wedge b$ est le dernier reste non nul dans l'algorithme d'Euclide.

Preuve. Justifions la terminaison de l'algorithme, c'est-à-dire que l'algorithme s'arrête bien au bout d'un nombre fini d'étapes. Notons pour cela r_n la valeur contenue dans la variable `r1` à la fin de la n-ème itération de la boucle `Tant que`. La suite $(N(r_n))$ est une suite strictement décroissante d'entiers naturels. Elle est donc finie, et il existe bien un entier N pour lequel $r_N = 0$.

Assurons nous à présent de la correction de l'algorithme en justifiant que la valeur renvoyée est bien $a \wedge b$. Toujours avec les mêmes notations, on montre par une récurrence immédiate que :

$$\forall n \in [\![0, N-1]\!], \quad r_n \wedge r_{n+1} = a \wedge b.$$

En particulier, on a :

$$a \wedge b = r_{N-1} \wedge r_N = r_{N-1} \wedge 0 = r_{N-1},$$

et $a \wedge b$ est bien le dernier reste non nul dans l'algorithme d'Euclide qui est justement la valeur renvoyée par l'algorithme. □

Remarque. On peut améliorer l'algorithme pour obtenir également une relation de Bezout. En effet, si on écrit à chaque itération de l'algorithme $r_k = u_k a + v_k b$, avec $u_0 = 1$ et $v_0 = -q_0$, on aura :

$$r_{k+1} = r_{k-1} - q_k r_k = (u_{k-1} - q_k u_k)a + (v_{k-1} - q_k v_k)b.$$

2.4 Théorème des restes chinois

Propriété 32

Soit A un anneau commutatif et unitaire, I et J des idéaux de A tels que $I + J = A$.

L'application Φ associant à la classe $\widehat{x}$ de $x \in A$ modulo $I \cap J$ le couple $(\overline{x}, \overset{\circ}{x})$ des classes de x modulo I et modulo J, est un isomorphisme de l'anneau $A/(I \cap J)$ sur l'anneau $(A/I) \times (A/J)$.

Preuve. On vérifie sans difficulté que l'application $\varphi : x \in A \mapsto (\overline{x}, \overset{\circ}{x}) \in (A/I) \times (A/J)$ est un morphisme d'anneaux. Et on a :

$$x \in \mathrm{Ker}(\varphi) \quad \Leftrightarrow \quad (\overline{x}, \overset{\circ}{x}) = (\overline{0_A}, \overset{\circ}{0_A}) \quad \Leftrightarrow \quad x \in I \cap J.$$

Ainsi $\mathrm{Ker}(f) = I \cap J$ et par le théorème d'isomorphisme, f se « factorise » en un morphisme injectif d'anneaux Φ de $A/I \cap J$ sur $(A/I) \times (A/J)$.

Montrons que Φ est surjectif. Soit pour cela $(\overline{a}, \overset{\circ}{b}) \in (A/I) \times (A/J)$. Comme $I + J = A$, il existe $(u, v) \in I \times J$ tels que $u + v = 1_A$. Posons alors $x = b \times u + a \times v$. On a $\overline{v} = \overline{1_A}$ et donc $\overline{x} = \overline{a} \times \overline{v} = \overline{a}$, et de même $\overset{\circ}{x} = \overset{\circ}{b}$. Ainsi $\Phi(x) = (\overline{a}, \overset{\circ}{b})$, et Φ est bien surjective. □

Comme conséquence directe de ce résultat, on a le

Théorème 33 (*des restes chinois*)

Soient A un anneau principal, $m \in A$ et $n \in A$ premiers entre eux. L'application :

$$\Phi : \begin{array}{ccc} A/\langle m \times n\rangle & \longrightarrow & (A/\langle m\rangle) \times (A/\langle n\rangle) \\ \widehat{x} & \mapsto & (\overline{x}, \overset{\circ}{x}) \end{array}$$

est un isomorphisme d'anneaux.

Preuve. On applique le résultat précédent avec $I = \langle m\rangle$ et $J = \langle n\rangle$, en notant que $I + J = A$ puisque $m \wedge n = 1_A$, et que $I \cap J = \langle m \times n\rangle$ car $m \vee n = m \times n$. □

Remarque. La démonstration de la Proposition 32 nous indique comment expliciter la bijection réciproque de Φ : puisque $m \wedge n = 1_A$, il existe un couple de Bezout $(u, v) \in A^2$ tel que $1_A = m \times u + n \times v$ (qui, rappelons le, peut être obtenu par l'algorithme d'Euclide étendu lorsque A est euclidien). L'isomorphisme réciproque Φ^{-1} est alors donné par :

$$\Phi^{-1} : \begin{array}{ccc} (A/\langle m\rangle) \times (A/\langle n\rangle) & \longrightarrow & A/\langle m \times n\rangle \\ (\overline{a}, \overset{\circ}{b}) & \mapsto & b \times m \times \widehat{u + a} \times n \times v \end{array}.$$

Remarque. Ces résultats se généralisent par récurrence au cas d'un produit de $p \geq 2$ éléments $m_1, \ldots, m_p$ deux à deux premiers entre eux.

3 Exemples fondamentaux d'anneaux principaux

3.1 Anneau $\mathbb{Z}$ des entiers relatifs

On a le résultat suivant, conséquence de tout ce qui a été obtenu précédemment.

Théorème 34

- L'anneau $(\mathbb{Z}, +, \times)$ est euclidien (avec pour stathme euclidien $N : n \in \mathbb{Z}^* \mapsto |n|$), donc principal.
- On a $\mathscr{U}(\mathbb{Z}) = \{-1, 1\}$.
- Les éléments irréductibles de $\mathbb{Z}$ sont les nombres de la forme $\pm p$ avec p premier.
- Les idéaux premiers de $\mathbb{Z}$ sont $\{0\}$ et les $\langle p \rangle$ avec p premier.
- Les idéaux maximaux de $\mathbb{Z}$ sont les $\langle p \rangle$ avec p premier.
- Tout nombre entier $n \geq 2$ admet une décomposition en produit de nombres premiers unique à permutation des facteurs près.

Algorithme de division euclidienne. Voici une méthode naïve de division euclidienne de deux entiers positifs.

```
Entrer a >=0, b>0
q = 0 ; r = a ;
Tant que r>b faire
      r = r-b
      q = q+1
Fin du Tant que
Retourner q et r
```

Le nombre d'itérations est ici de $\lfloor \frac{a}{b} \rfloor$.

Remarque. On dispose de l'algorithme d'Euclide pour le calcul de pgcd. On peut ici majorer le nombre d'étapes N qu'il faut pour trouver le pgcd. Sachant que la suite des restes est strictement décroissante, on trouve que $N \leq b$. On peut faire bien mieux : le Théorème de Lamé montre que N est inférieur ou égal à 5 fois le nombre de décimales de b. Pour plus de détails, le vous renvoie par exemple à mon cours **Algorithmique pour l'agrégation interne**.

Applications possibles.

- Résolution de l'équation diophantienne $ax + by = c$.
- Représentant irréductible d'un rationnel.
- Irrationalité de $\sqrt{2}$ ou plus généralement de $\sqrt{n}$ lorsque n n'est pas le carré d'un entier.

3.2 Étude de l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$

Dans toute la suite, n est un entier supérieur ou égal à 2.

Premières propriétés

Comme conséquence des résultats obtenus précédemment, on a les propriétés suivantes.

Théorème 35

$n\mathbb{Z}$ est un idéal de $\mathbb{Z}$, et on dispose donc de l'anneau quotient $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ commutatif et unitaire.

Théorème 36

On a les équivalence suivantes :

$$\mathbb{Z}/n\mathbb{Z} \text{ est intègre } \Leftrightarrow \mathbb{Z}/n\mathbb{Z} \text{ est un corps } \Leftrightarrow n \text{ est premier.}$$

Théorème des restes chinois

Toujours comme conséquence de l'étude générale faite précédemment, on a le résultat suivant.

Théorème 37 (*des restes chinois* - Version « anneaux quotients »)

Soient $n_1, \dots, n_p$ des entiers deux à deux premiers entre eux, et n leur produit. On a l'isomorphisme d'anneaux :

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_p\mathbb{Z}.$$

Plus précisément, l'application $\Phi : \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_p\mathbb{Z}, x[n] \mapsto (x[n_1], \dots, x[n_p])$ est un isomorphisme d'anneaux.

Ce résultat se reformule comme suit.

Théorème 38 (*des restes chinois* - Version « congruence »)

Soient $n_1, \dots, n_p$ des entiers deux à deux premiers entre eux, et n leur produit. Pour tout entier $m_1, \dots, m_p$, le système de congruences

$$\begin{cases} x = m_1[n_1] \\ \quad \dots \\ x = m_p[n_p] \end{cases} \qquad (*)$$

possède une solution $x \in \mathbb{Z}$, qui est unique modulo n.

Méthode. Résolution d'un système de congruences.

Pour résoudre explicitement un système de congruences, c'est-à-dire en d'autres termes pour expliciter Φ^{-1}, on procèdera comme suit :

- *on commence par poser $N_i = \prod_{j \neq i} n_i$ pour tout $1 \leq i \leq p$, de sorte qu'on a*[a] $N_1 \wedge \cdots \wedge N_p = 1$;
- *par le théorème de Bezout, il existe $(u_1, \dots, u_p) \in \mathbb{Z}^p$ tels que :*

$$u_1N_1 + \cdots + u_pN_p = 1. \qquad (**)$$

  On détermine ces entiers par l'algorithme d'Euclide étendu (en cherchant un couple de Bezout pour (N_1, N_2), puis pour $(N_1 \wedge N_2, N_3)$, puis pour $(N_1 \wedge N_2 \wedge N3, N_4)$, ...) ;
- *Pour tout $i \in [\![1, p]\!]$, on a d'après $(**)$ et par définition des N_i que :*

$$\forall j \in [\![1, p]\!], \quad u_jN_j = \begin{cases} 1\ [n_i] & \text{si } i = j \\ 0\ [n_i] & \text{si } i \neq j \end{cases}.$$

  Une solution du système de congruence $(*)$ est donc $x = m_1u_1N_1 + \cdots + m_pu_pN_p$, qui est unique modulo n.

[a] ces éléments ne pouvant pas tous avoir de facteur premier en commun.

Inversibles de $\mathbb{Z}/n\mathbb{Z}$

Théorème 39

Soit $s \in \mathbb{Z}$. Les propriétés suivantes sont équivalentes :

(i) s est premier avec n,

(ii) $\bar{s}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$,

(iii) $\bar{s}$ est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

En particulier, on a donc $\mathscr{U}(\mathbb{Z}/n\mathbb{Z}) = \{\bar{s},\ s \wedge n = 1\}$.

Preuve.

(i) $\Rightarrow$ (iii) Si $s \wedge n = 1$, il existe un couple de Bezout $(u, v) \in \mathbb{Z}$ tel que :

$$su + nv = 1.$$

Ce qui donne dans $\mathbb{Z}/n\mathbb{Z}$:

$$\overline{su} = \overline{1}.$$

Donc $\overline{s}$ est bien inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

(iii) $\Rightarrow$ (ii) Supposons $\overline{s}$ inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$. Il existe donc $\overline{u}$ un élément de $\mathbb{Z}/n\mathbb{Z}$, dont on peut prendre un représentant $u \in [\![1, n-1]\!]$, tel que :

$$\overline{1} = \overline{su} = \underbrace{\overline{s} + \cdots + \overline{s}}_{u \text{ fois}}.$$

Ainsi le sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ engendré par $\overline{s}$ contient $\overline{1}$, et est donc égal à $\mathbb{Z}/n\mathbb{Z}$ tout entier. Donc $\overline{s}$ est bien un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$.

(ii) $\Rightarrow$ (i) Supposons que $\overline{s}$ soit un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$. Alors $\overline{1}$ appartient au sous-groupe engendré par $\overline{s}$, et il existe $u \in [\![1, n-1]\!]$ tel que :

$$\overline{1} = \underbrace{\overline{s} + \cdots + \overline{s}}_{u \text{ fois}} = \overline{s \times u}.$$

En particulier, n divise $s \times u - 1$ et il existe $k \in \mathbb{Z}$ tel que :

$$su - 1 = nk \quad \Rightarrow \quad su - nk = 1.$$

Ce qui, par le théorème de Bezout, montre que s est premier avec n.

□

Méthode. Calcul de l'inverse d'un élément inversible.

Pour déterminer si un élément $\bar{s}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$, on vérifiera $s \wedge n = 1$. Si c'est le cas, $\bar{s}$ est bien inversible. De plus pour obtenir son inverse, on cherche un couple de Bezout :

$$us + vn = 1$$

Alors $\bar{u}\bar{s} = \bar{1}$ dans $\mathbb{Z}/n\mathbb{Z}$, et $\bar{u}$ est l'inverse de $\bar{s}$ dans $\mathbb{Z}/n\mathbb{Z}$.

Définition.

On appelle *fonction indicatrice d'Euler* et on note $\varphi(n)$ le cardinal de $\mathscr{U}(\mathbb{Z}/n\mathbb{Z})$, c'est-à-dire le nombre d'entiers s tels que $1 \leq s \leq n$ et $s \wedge n = 1$.

Remarque. Si p est premier, on a $\varphi(p) = p - 1$ et $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ pour $\alpha \in \mathbb{N}^*$.

Propriété 40

On a un isomorphisme de groupes $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathscr{U}(\mathbb{Z}/n\mathbb{Z})$. En particulier, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est un groupe abélien, de cardinal $\varphi(n)$.

Preuve. On vérifie facilement que l'application :

$$\Psi : \begin{array}{ccc} (\mathscr{U}(\mathbb{Z}/n\mathbb{Z}), \times) & \to & (\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ) \\ \overline{u} & \mapsto & f_{\overline{u}} : \overline{x} \mapsto \overline{x} \times \overline{u} \end{array}$$

définit un morphisme injectif de groupes entre $\mathscr{U}(\mathbb{Z}/n\mathbb{Z})$ et $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$. Étudions la surjectivité. Pour tout $f \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, $\mathrm{Im}(f) = \mathbb{Z}/n\mathbb{Z}$ et est engendré (comme groupe) par $f(\overline{1})$. Notons cet élément qui est donc inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$. On a pour tout $x \in [\![0, n-1]\!]$:

$$f_{\overline{u}}(\overline{x}) = \overline{u} \times \overline{x} = \underbrace{\overline{u} + \cdots + \overline{u}}_{x \text{ fois}} = \underbrace{f(\overline{1}) + \cdots + f(\overline{1})}_{x \text{ fois}} \underset{\substack{f \text{ morph.} \\ \text{de groupes}}}{=} f(\underbrace{\overline{1} + \cdots + \overline{1}}_{x \text{ fois}}) = f(\overline{x}).$$

Ainsi on a bien $\Psi(\overline{u}) = f$, et Ψ est bien surjective. □

Théorème 41 (*d'Euler* (1707 - 1783))

Si k est un entier premier avec n, alors $k^{\varphi(n)} = 1\,[n]$.

Preuve. C'est une application directe du théorème de Lagrange, puisque $\varphi(n)$ est par définition l'ordre du groupe $\mathscr{U}(\mathbb{Z}/n\mathbb{Z})$. □

Corollaire 42 (*Petit théorème de Fermat* (1601 - 1665))

Soit $p \in \mathbb{N}$ premier. Pour tout $x \in \mathbb{Z}$, on a $x^p = x\,[p]$.

Preuve. En notant que $\varphi(p) = p - 1$, on obtient que $x^{p-1} = 1\,[p]$ pour tout x premier avec p. On obtient donc $x^p = x\,[p]$ pour tout x dans $\mathbb{Z}$, y compris si x est un multiple de p. □

Corollaire 43 (*Théorème de Wilson* (1741 - 1793))

Soit $p \geq 2$. p est un nombre premier si et seulement si $(p-1)! = -1[p]$.

Preuve. Supposons p premier. L'égalité est vérifiée si $p = 2$. Supposons $p \geq 3$. D'après le théorème de Fermat, le polynôme $X^{p-1} - \overline{1}$ admet pour racines $\overline{1}, \ldots, \overline{p-1}$ dans le corps $K = \mathbb{Z}/p\mathbb{Z}$. Il se factorise donc sous la forme :

$$X^{p-1} - \overline{1} = (X - \overline{1})(X - \overline{2}) \ldots (X - \overline{p-1}).$$

L'égalité des termes constants donne :

$$-\overline{1} = (-1)^{p-1}\overline{1} \times \overline{2} \times \cdots \times \overline{p-1} \quad \text{d'où} \quad -1 = (p-1)!\,[p].$$

Réciproquement, si on a $(p-1)! = -1\,[p]$, alors tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible. Donc $\mathbb{Z}/p\mathbb{Z}$ est un corps, et p est premier. □

Propriété 44

- Si m et n sont premiers entre eux, on a $\varphi(mn) = \varphi(m)\varphi(n)$.
- Soit $n \geq 2$, $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ sa décomposition en facteurs premiers. Alors :

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

Preuve. Comme $m \wedge n = 1$, on a par le théorème des restes chinois que :

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Cet isomorphisme d'anneaux induit un isomorphisme de groupes entre $\mathscr{U}(\mathbb{Z}/mn\mathbb{Z})$ et $\mathscr{U}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$. Or on vérifie facilement que si A et B sont des anneaux unitaires, alors $\mathscr{U}(A \times B) = \mathscr{U}(A) \times \mathscr{U}(B)$. Ce qui donne ici :

$$\mathscr{U}(\mathbb{Z}/mn\mathbb{Z}) \simeq \mathscr{U}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = \mathscr{U}(\mathbb{Z}/m\mathbb{Z}) \times \mathscr{U}(\mathbb{Z}/n\mathbb{Z}).$$

D'où en prenant les cardinaux $\varphi(mn) = \varphi(m)\varphi(n)$.

Le deuxième point en découle alors immédiatement :

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \dots \varphi(p_k^{\alpha_k}) = p_1^{\alpha_1 - 1}(p_1 - 1) \dots p_k^{\alpha_k - 1}(p_k - 1) = n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

□

Applications et prolongements.

- Système de chiffrement RSA (voir par exemple [6]).
- Résolution de systèmes de congruences (voir par exemple [6]).
- (Étude de $\mathscr{U}(\mathbb{Z}/n\mathbb{Z})$ (voir par exemple [8]).)
- (Loi de réciprocité quadratique (voir par exemple [6]).)

3.3 Anneau $\mathbb{K}[X]$ des polynômes sur un corps commutatif $\mathbb{K}$

Premières propriétés.

Théorème 45

- Soit $\mathbb{K}$ un corps commutatif. L'anneau $(\mathbb{K}[X], +, \times)$ est euclidien, donc principal.
- On a $\mathscr{U}(\mathbb{K}[X]) = \mathbb{K}^*$.

Mise en garde.

Si $\mathbb{K}$ n'est pas un corps, $\mathbb{K}[X]$ n'est pas principal. On pourra par exemple montrer que $(\mathbb{Z}[X], +, \times)$ n'est pas principal en considérant l'idéal $\langle 2, X \rangle$.

On a en fait le résultat suivant.

Propriété 46

Soit A un anneau. $A[X]$ est principal si et seulement si A est un corps.

Preuve. Si A est un corps, on a vu que $A[X]$ est euclidien, donc principal.

Réciproquement, supposons $A[X]$ principal. C'est en particulier un anneau intègre, donc A l'est aussi. De plus, X est un élément irréductible de $A[X]$[1]. Comme $A[X]$ est principal, $A \simeq A[X]/\langle X \rangle$ est un corps. □

Remarque. On peut cependant montrer que si A est factoriel, alors $A[X]$ est factoriel (voir par exemple [8] à ce sujet).

[1] Si $X = P \times Q$, alors on a par exemple $\deg(P) = 1$ et $\deg(Q) = 0$. Donc P est de la forme aX et $Q = b$ avec $a, b \in A$. Et on a en identifiant les coefficients $1_A = a \times b$, de sorte que $b \in \mathscr{U}(A) \subset \mathscr{U}(A[X])$.

Éléments irréductibles

Propriété 47

- Tout polynôme de degré 1 est irréductible.
- Tout polynôme irréductible de degré > 1 n'a pas de racine dans $\mathbb{K}$.
- Les polynômes irréductibles de degré 2 ou 3 sont exactement ceux qui n'ont pas de racine dans $\mathbb{K}$.

Preuve. Le premier point est immédiat pour des raisons de degrés. Pour le deuxième point, si P est un polynôme de degré > 1 ayant une racine $a \in \mathbb{K}$, alors il existe Q de degré ≥ 1 tel que :

$$P = (X - a) \times Q.$$

Comme $(X - a)$ et Q ne sont pas inversibles, P n'est pas irréductible.

Soit enfin un polynôme P de degré 3 par exemple sans racine dans $\mathbb{K}$, et soient $Q, R \in \mathbb{K}[X]$ tels que $P = Q \times R$. On a $0 \leq \deg(Q) \leq 3$. Si $\deg(Q) = 1$, alors Q, et donc P, admettrait une racine dans $\mathbb{K}$, ce qui contredit l'hypothèse. Si $\deg(Q) = 2$, alors $\deg(R) = 1$ et on aboutit aussi à une contradiction. Donc $\deg(Q) = 0$ ou $\deg(Q) = 3$, de sorte qu'on a $Q \in \mathscr{U}(\mathbb{K}[X])$ ou $R \in \mathscr{U}(\mathbb{K}[X])$. On procède de même pour un polynôme de degré 2. □

Propriété 48

- Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré un.
- Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré un et les polynômes de degré deux de discriminant strictement négatifs.

Preuve. Comme $\mathbb{C}$ est algébriquement clos, tout polynôme non constant est produit de facteurs de degré un. Un tel polynôme n'est irréductible que s'il est de degré un.

Soit $P \in \mathbb{R}[X]$ de degré $n \geq 1$, et décomposons le en produit de facteurs de degré un dans $\mathbb{C}[X]$. Dans cette décomposition, notons que si $z \in \mathbb{C}\backslash\mathbb{R}$ est racine de P de multiplicité $r \geq 1$, alors $\overline{z}$ est aussi racine de P de multiplicité r. En effet, on a :

$$P(z) = P'(z) = \cdots = P^{(r-1)}(z) = 0 \text{ et } P^{(r)}(z) \neq 0,$$

ce qui donne en passant au conjugué (puisque les polynômes $P^{(i)}$ sont à coefficients réels) :

$$P(\bar{z}) = P'(\bar{z}) = \cdots = P^{(r-1)}(\bar{z}) = 0 \text{ et } P^{(r)}(\bar{z}) \neq 0.$$

Ainsi $\bar{z}$ est racine de multiplicité r de P.
En regroupant les termes conjugués, on obtient dans la factorisation de P les polynômes $(X - z)(X - \bar{z}) = X^2 - 2Re(z)X + |z|^2$ de degré deux irréductibles dans $\mathbb{R}[X]$, et les polynômes de degrés un irréductibles aussi dans $\mathbb{R}[X]$. Les polynômes irréductibles de $\mathbb{R}[X]$ sont donc les polynômes de degré un et les polynômes de degré deux à discriminant strictement négatifs. □

Applications et prolongements.

- Critère d'Eisenstein (voir par exemple [6] ou [9]).
- Existence et unicité d'un polynôme minimal pour $u \in \mathscr{L}(E)$ avec $\dim(E) < +\infty$ (voir par exemple [6] ou [9]).
- Théorème des noyaux et théorème de Dunford (voir par exemple [6]).
- Résultant (voir par exemple [6]).
- Anneau des entiers de Gauss (qui fait l'objet du sujet « facile » de cet été - voir par exemple [8], [3] ou [6]).

4 Corps commutatifs

4.1 Définition, exemples

Rappelons la définition d'un corps.

Définition.

Un anneau commutatif $(\mathbb{K}, +, \times)$ est un *corps* si tout élément non nul de $\mathbb{K}$ est inversible. Il est dit *fini* si son cardinal est de plus fini.

Exemples.

- $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.
- $\mathbb{Z}/p\mathbb{Z}$ est un corps fini pour tout p premier.

Définition.

Soit $\mathbb{L}$ un corps et $\mathbb{K} \subset \mathbb{L}$. On dit que $\mathbb{K}$ est un *sous-corps* de $\mathbb{L}$ si la restriction à $\mathbb{K}$ des lois $+$ et $\times$ lui confère une structure de corps. On dit aussi que $\mathbb{L}$ est un *sur-corps* ou une *extension de corps* de $\mathbb{K}$.

Exemple. $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, qui est lui même un sous-corps de $\mathbb{C}$.

Propriété 49

Toute intersection de sous-corps d'un corps $\mathbb{K}$ est un sous-corps de $\mathbb{K}$.

Preuve. Laissée en exercice. □

4.2 Corps des fractions d'un anneau intègre

L'anneau $\mathbb{Z}$ n'est pas un corps, mais on peut toujours regarder ses éléments comme des éléments de $\mathbb{Q}$, qui est un corps, dans lequel tout élément non nul de $\mathbb{Z}$ devient inversible. On montre ici que c'est possible pour tout anneau intègre.

Théorème 50

Soit A un anneau commutatif unitaire et intègre. Alors il existe un corps $\mathbb{F}$ et $\varepsilon : A \to \mathbb{F}$ un morphisme d'anneaux injectif tel que :

$$\forall x \in \mathbb{K},\ \exists (a,s) \in A \times A^*(\text{ ou } A^* = A \setminus \{0_A\}),\ x = \varepsilon(a)\varepsilon(s)^{-1}.$$

Preuve. La construction de $\mathbb{F}$ est la généralisation de la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$.

- **Étape 1. Construction de $\mathbb{F}$.**
  On définit une relation d'équivalence $\mathscr{R}$ sur $A \times A^*$ en posant :
  $$\forall (a,s),(b,t) \in A \times A^*,\ (a,s)\mathscr{R}(b,t) \Leftrightarrow at = bs.$$
  On note $\dfrac{a}{s}$ la classe d'équivalence de (a,s) pour cette relation que l'on appelle *fraction de a par s*. On note $\mathbb{F}$ l'ensemble de ces fractions.
- **Étape 2. Lois de composition interne sur $\mathbb{F}$.**
  On munit $\mathbb{F}$ des lois $+$ et $\times$ suivantes :
  $$\begin{cases} \mathbb{F} \times \mathbb{F} & \longrightarrow \mathbb{F} \\ \left(\dfrac{a}{s}, \dfrac{b}{t}\right) & \mapsto \dfrac{a}{s} + \dfrac{b}{t} := \dfrac{at+bs}{st} \end{cases}.$$

$$\begin{cases} \mathbb{F}\times\mathbb{F} & \longrightarrow \mathbb{F} \\ \left(\frac{a}{s},\frac{b}{t}\right) & \mapsto \frac{a}{s}\times\frac{b}{t} := \frac{ab}{st} \end{cases}.$$

On vérifie que $+$ et $\times$ sont bien définies, c'est-à-dire que ces opérations ne dépendent pas du représentant de la fraction choisie.

- **Étape 3. Structure de corps sur $\mathbb{F}$.**

  On vérifie toutes les propriétés d'un corps. En particulier on montre que :

$$0_{\mathbb{F}} = \frac{0_A}{1_A} = \frac{0_A}{s} \quad 1_{\mathbb{F}} = \frac{1_A}{1_A} = \frac{s}{s}$$

  et que si $x = \frac{a}{s} \neq 0_{\mathbb{F}}$, alors x est inversible et $x^{-1} = \frac{s}{a}$.

- **Étape 3. Morphisme $\varepsilon : A \hookrightarrow \mathbb{F}$.**

  On vérifie que $\varepsilon : \begin{cases} A & \to \mathbb{F} \\ a & \mapsto \frac{a}{1_A} \end{cases}$ est un morphisme d'anneaux injectif, tel que pour tout $x = \frac{a}{s} \in \mathbb{F}$, on ait :

$$x = \varepsilon(a)\varepsilon(s)^{-1}.$$

□

Remarque. Les anneaux A et $\mathrm{Im}(\varepsilon)$ étant isomorphes, on les identifiera dans la suite, si bien qu'on se permettra d'écrire $A \subset Frac(A)$.

Définition.

Le corps $\mathbb{F}$ ainsi construit est appelé le *corps des fractions de* A, et noté $Frac(A)$.

Propriété 51 (Propriété universelle du corps des fractions)

Soit A un anneau commutatif unitaire intègre. Pour tout corps $\mathbb{L}$ et tout homomorphisme injectif $f : A \to \mathbb{L}$, il existe un unique homomorphisme $\tilde{f} : Frac(A) \to \mathbb{L}$ dont la restriction à $A \subset Frac(A)$ soit f.

Exemples.

- $Frac(\mathbb{Z}) = \mathbb{Q}$.
- $Frac(\mathbb{K}[X])$ est appelé le *corps des fractions rationnelles* en l'indéterminée X et notée $K(X)$

Prolongement possible.

- Décomposition en éléments simples (voir par exemple [6] ou [9]).

4.3 Caractéristique d'un corps, sous-corps premier

Propriété 52

Soit A un anneau. Il existe un unique morphisme d'anneaux de $\mathbb{Z}$ dans A : l'application f définie par :

$$\forall n \in \mathbb{Z}, \quad f(n) = \underbrace{1_A + \cdots + 1_A}_{n \text{ fois}} \quad \text{ce qu'on notera plus simplement} \quad n1_A.$$

$\mathrm{Ker}(f)$ étant un idéal de l'anneau principal $\mathbb{Z}$, il est lui même principal. On note $k \in \mathbb{N}$ l'unique entier tel que $\mathrm{Ker}(f) = k\mathbb{Z}$.

Définition.

k est appelé la *caractéristique* de A, et on note $car(A) = k$.

Remarques.

- $car(\mathbb{Z}/n\mathbb{Z}) = n$, $car(\mathbb{R}) = car(\mathbb{Z}) = 0$.
- Un anneau et un quelconque de ses sous-anneaux ont la même caractéristique.
- Dans le cas où $k = car(A) > 0$, on a pour tout $a \in A$:

$$\underbrace{a + \cdots + a}_{n \text{ fois}} = a \times (\underbrace{1_A + \cdots + 1_A}_{n \text{ fois}}) = a \times 0_A = 0_A.$$

Propriété 53

(1) Si A est intègre, alors $car(A) = 0$ ou $car(A)$ est un nombre premier.

(2) Si $car(A) = 0$, alors A est infini.

Preuve.

(1) Si A est intègre, le sous-anneau $\mathrm{Im}(f)$ l'est aussi. Et par le théorème d'isomorphisme, il est isomorphe à $\mathbb{Z}/car(A)\mathbb{Z}$ qui est intègre aussi. Or on sait que c'est le cas si et seulement si $car(A) = 0$ ou $car(A)$ est un nombre premier.

(2) Si $car(A) = 0$, f est injective et $\mathrm{Im}(f) \simeq \mathbb{Z}$. En particulier, $\mathrm{Im}(f)$ est infini, et A (qui contient $\mathrm{Im}(f)$) l'est aussi.

□

Propriété 54 (*Morphisme de Frobenius* (1849 - 1917))

Soit A un anneau de caractéristique $p \in \mathbb{P}$.

- Pour tout $(a, b) \in A^2$, on a :
$$(a + b)^p = a^p + b^p.$$
Autrement dit, l'application $F : \begin{cases} A \to A \\ a \mapsto a^p \end{cases}$ est un morphisme d'anneaux.
- Si A est un corps fini, alors F est bijective.
- Si $A = \mathbb{Z}/p\mathbb{Z}$, alors $F = Id_A$.

Preuve. Par la formule du binôme dans A anneau commutatif, on a pour tout $(a, b) \in A^2$:

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{n-k}.$$

Pour tout $1 \leq k \leq p - 1$, on a $k\binom{p}{k} = p\binom{p-1}{k-1}$ et $k \wedge p = 1$. Par le théorème de Gauss, p divise $\binom{p}{k}$, et donc :

$$(a + b)^p = a^p + \underbrace{\sum_{k=1}^{p-1} \binom{p}{k} a^k b^{n-k}}_{=0_A} + b^p = a^p + b^p.$$

Supposons de plus que A soit un corps fini. $\mathrm{Ker}(F)$ est un idéal propre de A, donc égal à $\{0_A\}$. Ainsi F est injective entre deux ensemble de cardinal fini. C'est donc une bijection.

Si enfin $A = \mathbb{Z}/p\mathbb{Z}$, F est l'identité par le petit théorème de Fermat. □

Définition.

Soit $\mathbb{K}$ un corps. On appelle *sous-corps premier de* $\mathbb{K}$ le sous-corps P engendré par $1_{\mathbb{K}}$, c'est-à-dire l'intersection de tous les sous-corps de $\mathbb{K}$.

Un corps $\mathbb{K}$ est dit *premier* s'il n'a d'autre sous-corps que lui-même, ce qui équivaut à $\mathbb{K} = P$

Propriété 55

Soit $\mathbb{K}$ un corps, et P son sous-corps premier.

(1) Si $car(\mathbb{K}) = 0$, alors $P \simeq \mathbb{Q}$.

(2) Si $car(\mathbb{K}) = p \in \mathbb{P}$, alors $P \simeq \mathbb{Z}/p\mathbb{Z}$.

Preuve.

(1) Supposons que $car(\mathbb{K}) = 0$. Alors $f : \mathbb{Z} \to \mathbb{K}$ est un morphisme d'anneaux injectif. Par la propriété universelle du corps des fractions, f se prolonge de façon unique en un morphisme $\overline{f} : \mathbb{Q} \to \mathbb{K}$, nécessairement injectif puisque $\mathrm{Ker}(\overline{f})$ est un idéal propre de $\mathbb{Q}$. $\overline{f}(\mathbb{Q})$ est donc un sous-corps de $\mathbb{K}$ isomorphe à $\mathbb{Q}$. On a donc $P \subset \overline{f}(\mathbb{Q})$, et même $P = \overline{f}(\mathbb{Q})$ car $\mathbb{Q}$ est premier.

(2) Supposons $car(\mathbb{K}) = p \in \mathbb{P}$. Par le théorème d'isomorphisme, f se factorise en un morphisme injectif $\tilde{f}$ de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathbb{K}$. $\tilde{f}(\mathbb{Z}/p\mathbb{Z})$ est donc un sous-corps de $\mathbb{K}$, de sorte que $P \subset \tilde{f}(\mathbb{Z}/p\mathbb{Z})$, et même $P = \tilde{f}(\mathbb{Z}/p\mathbb{Z})$ car $\mathbb{Z}/p\mathbb{Z}$ est premier.

□

4.4 Éléments algébriques, transcendants

Soit $\mathbb{K}$ un corps, et $\mathbb{L}$ une extension de $\mathbb{K}$.

Propriété 56

Soit $a \in \mathbb{L}$. L'application

$$ev_a : \begin{cases} \mathbb{K}[X] & \to \mathbb{L} \\ P & \mapsto P(a) \end{cases}$$

est un morphisme d'anneaux. On note $I(a) = \mathrm{Ker}(ev_a) = \{P \in \mathbb{K}[X],\ P(a) = 0\}$. Cet idéal est appelé l'*idéal annulateur*.

Définition.

On est dans une et une seule des deux situations suivantes :

- ou bien $I_a \neq \{0_A\}$, et il existe $P \in \mathbb{K}[X]$ tel que $P(a) = 0$. On dit alors que a est un *élément algébrique sur* $\mathbb{K}$.
- ou bien $I(a) = \{0_A\}$, et on dit alors que a est *transcendant sur* $\mathbb{K}$.

Exemples.

- Tout élément a d'un corps $\mathbb{K}$ est algébrique sur $\mathbb{K}$, car racine du polynôme non nul $X - a \in \mathbb{K}[X]$.
- $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ car racine du polynôme non nul $X^2 - 2 \in \mathbb{Q}[X]$.
- e est transcendant (résultat démontré par Hermite en 1873).
- π est transcendant (démontré par Lindemann en 1882).

Définition.

Soit $a \in \mathbb{L}$ un élément algébrique sur $\mathbb{K}$. On note M_a l'unique polynôme unitaire tel que $I(a) = \langle M_a \rangle$. Ce polynôme M_a est appelé le *polynôme minimal de* a.

Propriété 57

Soit $a \in \mathbb{L}$ un élément algébrique sur $\mathbb{K}$.
$P \in \mathbb{K}[X]$ est le polynôme minimal de a si et seulement si P est unitaire, $P(a) = 0$ et P est irréductible dans $\mathbb{K}[X]$.

Preuve. Si $P = M_a$, alors $P(a) = 0$ et P est unitaire. Montrons qu'il est de plus irréductible. Pour cela, il est équivalent de montrer que $I_a = \langle P \rangle$ est un idéal premier. Il est propre car P n'est pas constant ($P(a) = 0$ et $P \neq 0_{\mathbb{K}[X]}$). Et si $R \times S$ appartient à I_a, alors on a :

$$R(a) \times S(a) = 0 \quad \underbrace{\Rightarrow}_{\mathbb{K} \text{ intègre}} \quad R(a) = 0 \text{ ou } S(a) = 0 \quad \Rightarrow \quad R \in I_a \text{ ou } S \in I_a.$$

Réciproquement, supposons que P soit irréductible et unitaire, et admette a pour racine. Alors P appartient à $I_a = \langle M_a \rangle$, et il existe donc $Q \in \mathbb{K}[X]$ tel que $P = Q \times M_a$. Et comme P est irréductible et que $M_a \neq 0_{\mathbb{K}[X]}$ (car $I_a \neq \{0_A\}$ puisque a est algébrique), on a $Q \in \mathscr{U}(\mathbb{K}[X]) = \mathbb{K}^*$. Les polynômes P et M_a étant enfin unitaires tous les deux, on obtient donc que $Q = 1$ et que $P = M_a$. □

Exemple. Le polynôme $P = X^2 - 2$ est unitaire, irréductible sur $\mathbb{Q}$ car de degré 2 sans racine dans $\mathbb{Q}$, et satisfait $P(\sqrt{2}) = 0$. Donc P est le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$.

Propriété 58

Soient $\mathbb{L}$ un corps commutatif, et $\mathbb{K} \subset \mathbb{L}$ un sous corps. Les éléments de $\mathbb{L}$ algébriques sur $\mathbb{K}$ forment un sous-corps de $\mathbb{L}$.

Preuve. Admis. □

Propriété 59

Le corps des nombres complexes algébriques sur $\mathbb{Q}$ est dénombrable.

Preuve. Rappelons que $\mathbb{Q}$ est dénombrable : il est en bijection avec le sous-ensemble de $\mathbb{Z} \times \mathbb{N}^*$ constitué des fractions $\frac{p}{q}$ réduites, où $p \wedge q = 1$. L'ensemble $\mathscr{P}_n$ des polynômes de $\mathbb{Q}[X]$ de degré majoré par n est en bijection avec $\mathbb{Q}^{n+1}$, et donc dénombrable. L'ensemble des polynômes $\mathbb{Q}[X] = \cup \mathscr{P}_n$, réunion dénombrable d'ensembles dénombrables, est dénombrable. Et tout $P \in \mathbb{Q}[X]$ n'a qu'un nombre fini de racines. L'ensemble des nombres algébriques est donc une partie dénombrable de $\mathbb{C}$. □

$\mathbb{C}$ n'étant lui pas dénombrable, on déduit de ce résultat qu'il y a « bien plus » de nombres transcendants que de nombres algébriques. Il est cependant difficile de montrer qu'un nombre est transcendant, ou d'exhiber des nombres transcendants (outre e et π).

Prolongements possibles.

- Nombres transcendants de Liouville (voir [6] ou [3]).
- Degré d'une extension, preuve de la Propriété 58 (voir [3] ou [8]).
- Construction à la règle et au compas (voir [3] ou [8]).

4.5 Racines et extensions de corps

Puisque $\mathbb{K}[X]$ est principal, on a le résultat suivant.

Propriété 60

Soit $P \in \mathbb{K}[X]$ un polynôme non nul. On a l'équivalence entre les propositions suivantes :

(i) Le polynôme P est irréductible,

(ii) L'anneau quotient $\mathbb{K}[X]/\langle P\rangle$ est intègre,

(iii) L'anneau quotient $\mathbb{K}[X]/\langle P\rangle$ est un corps.

Considérons $P = \sum_{k=0}^{n} a_k X^k$ un polynôme irréductible de $\mathbb{K}[X]$ et $\mathbb{L} = \mathbb{K}[X]/\langle P\rangle$. Notons π la projection canonique.

- La restriction de π à $\mathbb{K}$ est un morphisme injectif de corps, permettant d'identifier $\mathbb{K}$ à un sous corps de $\mathbb{L}$, et donc $\mathbb{L}$ à une extension de $\mathbb{K}$. On peut en particulier voir P comme un polynôme à coefficients dans $\mathbb{L}$.
- Soit $x = \pi(X) \in \mathbb{L}$, on a :

$$0 = \pi(P(X)) = \sum_{k=0}^{n} \pi(a_k)\pi(X)^k = \sum_{k=0}^{n} a_k x^k = P(x)$$

  Donc $x \in \mathbb{L}$ est racine de P.

On a donc montré le résultat suivant.

Propriété 61

Soient $P \in \mathbb{K}[X]$ un polynôme irréductible sur $\mathbb{K}$. Alors il existe une extension $\mathbb{L}$ de $\mathbb{K}$ dans laquelle P admet une racine.

Exemple. Construction du corps $\mathbb{C}$ des nombres complexes.
Le polynôme X^2+1 est irréductible sur le corps $\mathbb{R}$. Donc $\mathbb{R}[X]/\langle X^2+1\rangle$ est un corps. Si on note $\mathbb{C}$ ce corps, et i la classe de X dans le quotient, alors on vérifie que :

- $i^2 = -1$,
- tout élément $z \in \mathbb{C}$ s'écrit de manière unique $z = a + ib$,
- on retrouve la somme et le produit usuel des complexes avec les lois quotients.

Corollaire 62

Soit $\mathbb{K}$ un corps, et $P \in \mathbb{K}[X]$ un polynôme non constant.

(1) Il existe une extension $\mathbb{L}$ de $\mathbb{K}$ dans laquelle P admet au moins une racine.

(2) Il existe une extension $\mathbb{M}$ de $\mathbb{K}$ dans laquelle P est scindé.

Preuve.

(1) P étant un polynôme non constant, il admet un diviseur P_0 irréductible dans $\mathbb{K}[X]$. D'après la propriété précédente, il existe une extension $\mathbb{L}$ de $\mathbb{K}$ dans laquelle P_0 admet une racine, et donc a fortiori P aussi.

(2) On procède par récurrence sur le degré de P.

Init. Pour $n = 1$, P est de degré 1 donc scindé dans $\mathbb{K}[X]$.

Hér. Soit $n \geq 1$ et supposons la propriété vrai au rang n. Montrons la au rang $n+1$.

Soit pour cela P de degré $n+1$. Par le point précédent, il existe une extension $\mathbb{L}$ de $\mathbb{K}$ dans laquelle P admet une racine x. Alors P vu comme polynôme de $\mathbb{L}[X]$ se factorise sous la forme :

$$P = (X - x)Q$$

avec $Q \in \mathbb{L}[X]$ de degré n. Par hypothèse de récurrence, il existe donc une extension $\mathbb{M}$ de $\mathbb{L}$ dans laquelle Q est scindé. Ainsi $\mathbb{M}$ est une extension de $\mathbb{K}$ dans laquelle P est scindé. D'où la propriété au rang $n+1$.

On conclut par principe de récurrence.

□

Remarque. On peut montrer que de telles extensions de corps sont uniques à isomorphisme près, appelées respectivement *corps de rupture de P sur $\mathbb{K}$* pour $\mathbb{L}$, et *corps de décomposition de P sur $\mathbb{K}$* pour $\mathbb{M}$ (voir à ce sujet [8] par exemple).

4.6 Cas des corps fini

Théorème 63

Soit $\mathbb{K}$ un corps fini.

(1) $car(\mathbb{K}) = p$ et son sous-corps premier $\mathbb{K}'$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

(2) Le cardinal de $\mathbb{K}$ est égal à p^n où $n = \dim_{\mathbb{Z}/p\mathbb{Z}} \mathbb{K}$

Preuve.

(1) Comme $\mathbb{K}$ est fini et intègre, on a $car(\mathbb{K}) = p$ d'après la Propriété **??**. Et son sous-corps premier $\mathbb{K}'$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

(2) $\mathbb{K}$ est une extension de corps de $\mathbb{Z}/p\mathbb{Z}$, si bien qu'on peut voir $\mathbb{K}$ comme un espace vectoriel sur $\mathbb{Z}/p\mathbb{Z}$, nécessairement de dimension finie puisque $\mathbb{K}$ est fini. Si on note $n = \dim_{\mathbb{Z}/p\mathbb{Z}} \mathbb{K}$, alors $\mathbb{K}$ est isomorphe (en tant qu'espace vectoriel) à $(\mathbb{Z}/p\mathbb{Z})^n$, et est donc de cardinal p^n.

□

Remarque. Il n'existe donc pas de corps à 6 éléments ou à 10 éléments.

Exemple. Construction d'un corps à 4 éléments.
Le polynôme $X^2 + X + \overline{1}$ est irréductible sur $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ car il est de degré 2 sans racine dans $\mathbb{F}_2$. Ainsi $\mathbb{L} = \mathbb{F}_2[X]/\langle X^2+X+\overline{1}\rangle$ est un corps. Si on note j l'image de X dans le quotient, on vérifie que $\mathbb{L} = \{\overline{0}, \overline{1}, j, j^2 = \overline{1}+j\}$ et on peut dresser les tables d'opérations.

$+$	$\overline{0}$	$\overline{1}$	j	$\overline{1}+j$
$\overline{0}$	$\overline{0}$	$\overline{1}$	j	$\overline{1}+j$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{1}+j$	j
j	j	$\overline{1}+j$	$\overline{0}$	$\overline{1}$
$\overline{1}+j$	$\overline{1}+j$	j	$\overline{1}$	$\overline{0}$

$\times$	$\overline{0}$	$\overline{1}$	j	$\overline{1}+j$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	j	$\overline{1}+j$
j	$\overline{0}$	j	$\overline{1}+j$	$\overline{1}$
$\overline{1}+j$	$\overline{0}$	$\overline{1}+j$	$\overline{1}$	j

Remarque. On peut montrer que pour tout $p \in \mathbb{P}$ et $n \in \mathbb{N}^*$, il existe un corps fini à p^n éléments, et qu'un tel corps est unique à isomorphisme près (voir par exemple [8] à ce sujet).

Prolongements possibles.

- Théorème de Wedderburn (voir par exemple [6] ou [7]).
- Cyclicité du groupe $(\mathbb{K}^*, \times)$ lorsque $\mathbb{K}$ est un corps fini (voir par exemple [8]).
- (Existence et unicité d'un corps fini à p^n éléments (voir par exemple [7])).
- (Cyclicité du groupe $(\mathbb{K}^*, \times)$ lorsque $\mathbb{K}$ est un corps fini (voir par exemple [8]).)

References

[1] Calais, J. Éléments de théorie des anneaux. Anneaux commutatifs. Cours et exercices.

[2] Calais, J. Extensions de corps : théorie de Galois. Cours et exercices.

[3] Combes, F. Algèbre et géométrie. Cours et exercices corrigés.

[4] Debeaumarché, G. Manuel de Mathématiques, Volumes 2 et 4, Algèbre et géométrie. Cours et exercices.

[5] Francinou, S., Gianella, H. et Nicolas, S. Exercices de mathématiques, oraux x-ens. Exercices corrigés.

[6] Gourdon, X. Les maths en tête, Algèbre. Résumé de cours et exercices corrigés.

[7] Gozard, I. Théorie de Galois. Cours et exercices.

[8] Perrin, D. Cours d'algèbre. Cours et exercices.

[9] Skandalis, G. Algèbre générale et algèbre linéaire. Cours et exercices corrigés.