Master 1 Mathématiques 2017–2018

TD d'Algèbre

Maxime ACHAB

maxime.achab@univ-rouen.fr

Université de Rouen

Laboratoire de Mathématiques Raphaël Salem,

Avenue de l'Université, BP.12,

F76801 Saint-Étienne-du-Rouvray.

Rédigé avec LaTeX

par Hicham AMARIR

le 15 septembre 2026

Table des matières

Algèbre. Fiche n°1. Généralités sur les anneaux.

Mémento :

Rappel :

Attention : on rencontre à propos des anneaux de multiples différences de terminologie ; le parti pris adopté ici est celui de ***définitions minimalistes****.*

Définition 1.1 : (*Anneau*)

Soient A un ensemble, $+$ et $\cdot$ deux LCI sur A.

$(A,+,\cdot)$ est un ***anneau*** si $(A,+)$ est un groupe abélien (d'élément neutre noté 0_A, ou 0), et la multiplication est associative et distributive par rapport à l'addition.

Il est dit : ***commutatif*** si $\forall (x,y) \in A,\ xy = yx$, ***unitaire*** si la multiplication admet un élément neutre 1_A, ***intègre*** s'il n'admet pas de ***diviseurs de zéro***, c'est-à-dire si $xy = 0 \implies (x = 0 \text{ ou } y = 0)$.

Définition 1.2 : (*Éléments inversibles*)

Soit A un anneau unitaire non nul.

Les ***éléments inversibles***, ou ***unités***, de A constituent un groupe multiplicatif.

NB : $(xy)^{-1} = y^{-1}x^{-1}$.

Définition 1.3 : (*Sous-anneau*)

Soit A un anneau et B une partie de A.

B est un ***sous-anneau*** de A si B est non vide et stable par soustraction et multiplication.

Définition 1.4 : (*Morphisme d'anneaux*)

Soient A et A' deux anneaux.

Une application $f : A \to A'$ est un ***morphisme d'anneaux*** si pour tous $x, y \in A$, on a $f(x+y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$.

Définition 1.5 : (*Corps*)

Soit K un ensemble muni de deux LCI $+$ et $\cdot$.

K est un ***corps*** si $(K,+,\cdot)$ est un anneau unitaire tel que $1_K \neq 0_K$ et où tout élément $x \neq 0$ est inversible.

K privé de 0, noté K^*, est alors un groupe multiplicatif.

Définition 1.6 : (*Morphisme de corps*)

Soient K et K' deux corps.

Une application $f : K \to K'$ est un ***morphisme de corps*** si pour tous $x, y \in K$, $f(x+y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$, et si $f(1_K) = 1_{K'}$.

Définition 1.7 : (*Idéal I d'un anneau A*)

Soit A un anneau.

Un ***idéal à gauche*** de A est un sous-groupe additif I de A (partie non vide, stable par soustraction) telle que $A \cdot I \subset I$ (pour tout $a \in A$, pour tout $x \in I$, $a \cdot x \in I$) ; définition analogue pour un ***idéal à droite***.

Un idéal à gauche ou à droite est un sous-anneau mais la réciproque est fausse.

Un idéal à gauche qui est aussi un idéal à droite est appelé ***idéal bilatère***.

Toute intersection d'idéaux à gauche est un idéal à gauche.

La somme $\sum I_\lambda$ d'une famille (I_λ) d'idéaux à gauche est l'idéal à gauche engendré par la réunion des I_λ ; c'est l'ensemble des sommes finies du type $x_i + x_j + \ldots$, où $x_k \in I_k$ pour tout k.

Le produit $I \cdot J$ de deux idéaux bilatères I et J est l'idéal bilatère égal à l'ensemble des sommes finies $x_1 \cdot y_1 + \ldots + x_n \cdot y_n$, où $x_i \in I$ et $y_i \in J$ pour tout i ; on définit de manière analogue le produit d'un nombre fini d'idéaux bilatères.

Définition 1.8 : (*Anneau quotient A/I*)

Soit A un anneau et I un idéal de A.

Si I est un ***idéal bilatère*** de l'anneau A, alors A/I est un anneau.

Propriété 1.9 : (*Premier théorème d'isomorphisme*)

Soient A et A' deux anneaux et $f : A \to A'$ un morphisme d'anneaux.

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

Définition 1.10 : (*Idéal à gauche principal*)

Soit A un anneau et $a \in A$.

Un ***idéal à gauche principal*** est un idéal à gauche engendré par un élément $a \in A$, c'est-à-dire de la forme $I = A \cdot a = \{x \cdot a \mid x \in A\}$.

Définition 1.11 : (*Idéal premier*)

Soit A un anneau.

Un ***idéal premier*** est un idéal bilatère I tel que pour tous $x, y \in A$, $xy \in I \implies (x \in I \text{ ou } y \in I)$.

Définition 1.12 : (*Idéal à gauche maximal*)

Soit A un anneau.

Un ***idéal à gauche maximal*** est un idéal à gauche $M \neq A$ tel que les seuls idéaux à gauche le contenant soient A et lui-même.

Définition 1.13 : (*Ensembles inductifs*)

Soit E un ensemble muni d'une relation binaire $\leq$ réflexive, antisymétrique et transitive (ensemble ordonné).

E est dit ***inductif*** si toute partie de E totalement ordonnée est majorée.

Rappel :

Axiome du choix *: La théorie des ensembles est basée sur les axiomes de ZERMELO (1871-1953), FRAENKEL (1891-1965) et SKOLEM (1887-1963) ; c'est le* ***système ZF*** *(voir par exemple Jean-Louis Krivine, Théorie des ensembles, Cassini, Paris, 1998, ISBN 2-84225-014-1, ou Jean Dieudonné, Abrégé d'histoire des mathématiques, Hermann, Paris, 1986, ISBN 2 7056 6024 0). On obtient le* ***système ZFC*** *(ou ZF+AC) en rajoutant à ZF l'****axiome du choix****, lequel stipule en gros que l'on peut effectuer une infinité de choix, ce qui signifie que pour toute famille non vide $(I \neq \emptyset)$ $(E_i)_{i \in I}$ d'ensembles E_i non vides, on a le droit d'écrire "soit, pour tout $i \in I$, un élément $x_i \in E_i$" ; ou encore : pour toute famille non vide $(E_i)_{i \in I}$ d'ensembles non vides, le produit*

cartésien $\prod_{i\in I} E_i$ est non vide. On se place généralement dans le système ZFC. Par exemple, on a besoin de ZFC pour pouvoir affirmer que tout espace vectoriel admet une base.

Théorème 1.14 : (*Théorème de ZORN (théorie des ensembles)*)

Dans le système ZFC tout ensemble inductif non vide possède un ***élément maximal***.

Remarque :

On montre en fait que dans le système ZF, l'axiome du choix équivaut à l'affirmation "tout ensemble inductif non vide admet un élément maximal" ; autrement dit : Zorn équivaut à l'axiome du choix. Le résultat suivant découle de façon élémentaire du théorème de Zorn.

Théorème 1.15 : (*Théorème de Krull*)

Soit A un anneau unitaire.

Tout idéal à gauche $I \neq A$ d'un anneau unitaire A est contenu dans un ***idéal à gauche maximal*** M.

Rappel :

CAS DES ANNEAUX COMMUTATIFS UNITAIRES INTÈGRES : *anneau factoriel, anneau principal, anneau euclidien.*

On se place à présent dans un ***anneau commutatif unitaire intègre*** A.

On note $(a) = A\cdot a = a\cdot A$ l'idéal engendré par $a \in A$.

Définition 1.16 : (*Divisibilité, élément premier, élément irréductible*)

Soient deux éléments a et b de A.

① On dit que a ***divise*** b s'il existe $c \in A$ tel que $b = a\cdot c$.

On a : a divise $b \iff (b)\subset(a)$; $(a)=(b) \iff \exists u \in A$ inversible, $b = a\cdot u$.

② a est dit ***premier*** si l'idéal (a) est premier.

③ a est dit ***irréductible*** s'il est non inversible et si : $a = b\cdot c \implies$ (b inversible ou c inversible).

Propriété 1.17 : (*Lien entre élément premier et élément irréductible*)

Soit a un élément non nul de A.

Si a est premier alors a est irréductible.

Définition 1.18 : (*Anneau factoriel*)

Un ***anneau factoriel*** est un anneau commutatif unitaire intègre où tout élément $x \neq 0$ se décompose en produit d'un élément inversible et de facteurs irréductibles, de façon unique à l'ordre près des facteurs et à la multiplication près par un élément inversible.

Définition 1.19 : (*Anneau principal*)

Un ***anneau principal*** est un anneau commutatif unitaire intègre dont tout idéal est principal, c'est-à-dire de la forme $(a) = A\cdot a$.

Définition 1.20 : (*Anneau euclidien*)

Un ***anneau euclidien*** est un anneau commutatif unitaire intègre A tel qu'il existe une application $d : A \setminus \{0\} \to \mathbb{N}$, appelée ***stathme euclidien***, vérifiant :

- ⊛ $\forall x, y \in A \setminus \{0\}$, x divise $y \implies d(x) \leqslant d(y)$;
- ⊛ $\forall a, b \in A \setminus \{0\}$, $\exists q, r \in A$, $r = 0$ ou $d(r) < d(b)$, $a = b \cdot q + r$.

Propriété 1.21 : (*Hiérarchie des anneaux*)

Tout anneau euclidien est principal, et tout anneau principal est factoriel :

$$\text{EUCLIDIEN} \implies \text{PRINCIPAL} \implies \text{FACTORIEL}$$

Remarque :

CONTRE-EXEMPLES AUX RÉCIPROQUES

1. Un ***anneau principal non euclidien*** :

$\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] = \left\{a + b\frac{1+i\sqrt{19}}{2} \;\middle|\; a \in \mathbb{Z}, b \in \mathbb{Z}\right\}$

(voir Tauvel, Mathématiques générales pour l'agrégation, Masson 1992, ISBN 2-225-82733-8, pages 154-156).

2. Un ***anneau factoriel non principal*** : $K[X, Y]$, où K est un corps commutatif.

Démonstration.

Soit K un corps commutatif. Alors, $K[X]$ est un anneau factoriel (car il est principal) ; donc, $K[X][Y]$ est aussi factoriel ; autrement dit, $K[X, Y]$ est factoriel.

On raisonne par l'absurde, en supposant cet anneau principal ; soit l'idéal $I = (X)+(Y) = \{X \cdot P + Y \cdot Q \mid P \in K[X, Y], Q \in K[X, Y]\}$, égal en fait à l'ensemble des polynômes de terme constant nul ; d'après l'hypothèse faite, il existe $S \in K[X, Y]$ tel que $I = (S) = \{S \cdot P \mid P \in K[X, Y]\}$; or, $X \in I$; donc il existe $P \in K[X, Y]$ tel que $X = S \cdot P$; ainsi, S divise X ; de même, S divise Y ; donc S divise $\text{PGCD}(X, Y) = 1$; S est égal à une constante non nulle C ; donc $I = (C) = K[X, Y]$; comme I ne contient pas les polynômes constants, on a la contradiction cherchée.

Exercice 1.

On se place dans l'anneau $\mathcal{M}_2(\mathbb{Z})$ des matrices de format 2×2 et à coefficients entiers.

① Cet anneau est-il intègre ?

② Trouver ses éléments inversibles.

③ Soient $k \in \mathbb{Z}$, $h \in \mathbb{Z}$, I l'ensemble des matrices de la forme $M = \begin{pmatrix} 0 & 0 \\ k & h \end{pmatrix}$ et J l'ensemble des matrices de la forme $M = \begin{pmatrix} 0 & k \\ 0 & h \end{pmatrix}$.

I et J sont-ils des idéaux ?

Exercice 2.

Soit i le nombre complexe usuel et $j = \exp\left(\frac{2i\pi}{3}\right)$. On définit :

$$\mathbb{Z}[i] = \left\{x + iy \,\middle|\, x \in \mathbb{Z},\ y \in \mathbb{Z}\right\};$$
$$\mathbb{Z}[j] = \left\{x + jy \,\middle|\, x \in \mathbb{Z},\ y \in \mathbb{Z}\right\};$$
$$\mathbb{Z}[\sqrt{2}] = \left\{x + y\sqrt{2} \,\middle|\, x \in \mathbb{Z},\ y \in \mathbb{Z}\right\}.$$

① Montrer que ce sont des anneaux pour les lois usuelles (traiter seulement le cas de $\mathbb{Z}[j]$) ;

dans ce cas, $\mathbb{Z}[i]$ est appelé l'anneau des **entiers de Gauss**.

② Déterminer les éléments inversibles (ou **unités**) des anneaux $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$.

Indication : si z est inversible, considérer son module $|z|$.

③ Soit $z = x + y\sqrt{2}$ une unité de l'anneau $\mathbb{Z}[\sqrt{2}]$.

ⓐ Montrer que $x^2 - 2y^2 = \pm 1$ (cas particulier de l'**équation de Pell** $x^2 - ay^2 = b$, où a et b sont deux entiers donnés et où x et y sont deux inconnues entières).

ⓑ On s'intéresse à l'équation de Pell $x^2 - 2y^2 = 1$; montrer que x est impair ($x = 2k+1$) et que y est pair $\left(y = 2h\right)$; avec ces notations montrer que $h^2 = k(k+1)/2$

ⓒ En déduire une méthode de construction des solutions.

ⓓ Construire deux éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ autres que $z = \pm 1$.

Exercice 3.

(Rappel : groupe quotient)

Soit $(G, \cdot)$ un groupe et H un sous-groupe.

On note G/H l'ensemble des classes à gauche $xH = \{xh \mid h \in H\}$.

① Établir l'équivalence des propriétés suivantes :

ⓐ $\forall x,\ xH \subset Hx$

ⓑ $\forall x,\ Hx \subset xH$

ⓒ $\forall x,\ xH = Hx$

ⓓ $\forall x,\ xHx^{-1} = H$

ⓔ $\forall x,\ xHx^{-1} \subset H.$

On dit que H est un ***sous-groupe distingué*** s'il vérifie l'une de ces assertions, dont (v) est la plus utilisée.

② Montrer que si H est distingué alors G/H est un groupe.

Exercice 4.

① Soit I un idéal bilatère d'un anneau A. Montrer que A/I est un anneau.

② Montrer qu'un idéal est bilatère si et seulement s'il est le noyau d'un morphisme d'anneaux.

③ Soit $\phi : A \to A'$ un morphisme d'anneaux, I un idéal bilatère de A et $s : A \to A/I$ la surjection canonique ; montrer qu'il existe un morphisme d'anneaux $\psi : A/I \to A'$ tel que $\phi = \psi \circ s$ si et seulement si $I \subset \mathrm{Ker}\left(\phi\right)$ ("factorisation de ϕ par passage au quotient").

④ Montrer que, pour tout morphisme d'anneaux $f : A \to A'$: $\mathrm{Im}\left(f\right) \approx A/\mathrm{Ker}\left(f\right)$.

Exercice 5.

(Notion de corps de rupture)

Dans l'anneau $\mathbb{R}[X]$, soit $I = \left(X^2+1\right)$ et $J = \left(X^2+X+1\right)$ les idéaux respectivement engendrés par X^2+1 et X^2+X+1.

① Déterminer les morphismes d'anneaux $f : \mathbb{R}[X] \to \mathbb{C}$ tels que $f(r) = r \ \forall r \in \mathbb{R}$ et $I \subset \mathrm{Ker}\left(f\right)$.

② En déduire l'isomorphisme de corps $\mathbb{C} \approx \mathbb{R}[X]/\left(X^2+1\right)$.

On dit alors que $\mathbb{C}$ est un ***corps de rupture*** du polynôme X^2+1 irréductible dans $\mathbb{R}[X]$.

③ Montrer de même que $\mathbb{C}$ est un corps de rupture de X^2+X+1.

④ Essayer d'appliquer la méthode des questions ① et ② au polynôme X^2+X.

Exercice 6.

Montrer que tout anneau unitaire intègre fini non nul est un corps.

Exercice 7.

① Quels sont les sous-groupes de $(\mathbb{Z},+)$? Démontrer ce résultat.

② En déduire que $\mathbb{Z}$ est un anneau principal.

③ Quels sont les sous-groupes additifs de $\mathbb{R}$?

④ $\mathbb{R}$ est-il un anneau principal ?

Exercice 8.

① I étant un idéal bilatère d'un anneau A, vérifier que I est premier si et seulement si A/I est intègre.

② Soit M un idéal d'un anneau A **commutatif unitaire**.

Montrer que : M maximal $\iff$ A/M est un corps.

Indication.

pour "$\Rightarrow$" : soit $\overline{x} \in A/M$ avec $\overline{x} \neq \overline{0}$; alors $M + A \cdot x$ est un idéal ;

pour "$\Leftarrow$" : soit I un idéal contenant strictement M ; prendre $x \in I \setminus M$.

Exercice 9.

On se place encore dans un anneau A **commutatif unitaire**.

① Montrer que tout idéal maximal est premier.

② Trouver deux contre-exemples à la réciproque : dans $\mathbb{Z}$ puis dans $\mathbb{Z}^2$.

③ Pseudo-réciproque : montrer que si A est principal alors tout idéal premier non nul, différent de A, est maximal.

Exercice 10.

(PGCD et PPCM)

On se place dans un anneau A **commutatif unitaire intègre**. On note (a) l'idéal engendré par un élément a. Soit $(a_i)_{i\in I}$ une famille d'éléments de A. Si un élément d est tel que (d) soit la borne supérieure, pour la relation d'inclusion, des (a_i), on dit que d est un PGCD des a_i (plus grand commun diviseur). Si un élément m est tel que (m) soit la borne inférieure des (a_i) on dit que m est un PPCM des a_i (plus petit commun multiple).

① Montrer que dans un anneau factoriel toute famille finie admet un PGCD et un PPCM.

② Soit $I_1, \ldots, I_n$ des idéaux de $\mathbb{Z}$.

Déterminer $I_1 + \ldots + I_n$ et $I_1 \cap \ldots \cap I_n$.

Exercice 11.

Dans cet exercice on demande de ne pas utiliser le "théorème chinois".

① Montrer que les anneaux $\mathbb{Z}/24\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ ne sont pas isomorphes.

② Au moyen d'un morphisme adéquat $\phi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ établir l'isomorphisme $\mathbb{Z}/12\mathbb{Z} \approx \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

③ Résoudre dans $\mathbb{Z}$ les deux systèmes de congruences : $x \equiv 4$ (modulo 7) et $x \equiv 9$ (modulo 11) ; $x \equiv 3$ (modulo 4) et $x \equiv 4$ (modulo 6).

Exercice 12.

(Anneau non factoriel)

Montrer que $\mathbb{Z} + i\sqrt{5}\,\mathbb{Z}$ est un anneau non factoriel.

Indication : considérer le produit $3.3 = \left(2 + i\sqrt{5}\right) \cdot \left(2 - i\sqrt{5}\right)$ *; vérifier que les facteurs en jeu sont irréductibles.*

Exercice 13.

On se place dans un anneau A **commutatif unitaire intègre**. On rappelle qu'un idéal I est dit ***premier*** si $xy \in I \implies \left(x \in I \text{ ou } y \in I\right)$, et qu'un élément a est dit ***irréductible*** s'il est non inversible et si $a = bc$ implique que l'un des deux facteurs est inversible ; un élément a est dit ***premier*** s'il engendre un idéal (a) premier.

Soit a un élément non nul de A.

① Montrer que : a premier et non inversible $\implies$ a irréductible.

② Trouver un contre-exemple à la réciproque.

③ Pseudo-réciproque : établir la réciproque lorsque A est factoriel.

Exercice 14.

(Théorème chinois)

(utilisé dans l'antiquité par les astronomes chinois, en termes de congruences, pour prévoir les concomitances de certains événements périodiques).

① Soit A un anneau **unitaire** et I et J deux idéaux **bilatères** tels que $I + J = A$.

Montrer que $A/(I \cap J) \approx (A/I) \times (A/J)$. *Indication : considérer le morphisme qui à* $x \in A$ *associe le couple* $\left(\overline{x}, \overline{x}\right) = (x + I, x + J)$.

② Soit A un anneau **unitaire** et $I_1, \ldots, I_n$ des idéaux bilatères tels que $i \neq j \implies I_i + I_j = A$.

Montrer que $A/(I_1 \cap \ldots \cap I_n) \approx (A/I_1) \times \ldots \times (A/I_n)$.

③ Exprimer ce résultat dans $\mathbb{Z}$ en termes de congruences.

④ Question annexe. On se place dans les conditions de la question 2, et l'on suppose de plus que A est commutatif.

Établir par récurrence sur $n \geq 2$ l'égalité suivante : $I_1 \cap \ldots \cap I_n = I_1 \cdot I_2 \cdot \ldots \cdot I_n$.

Exercice 15.

(Le système de cryptage RSA)

Le système de cryptage RSA avec clé publique a été mis au point en 1978 par Rivest, Shamir et Adleman. Il est encore utilisé aujourd'hui, notamment sur Internet.

① Le destinataire d'un message choisit deux entiers p et q premiers, très grands, qu'il ne communique à personne. Il calcule $n = pq$ et le met dans le domaine public ; en principe retrouver p et q à partir de n demande un temps de calcul rédhibitoire (théorie de la complexité algorithmique).

② Il choisit ensuite un entier positif e premier avec $(p-1)(q-1)$ (c'est-à-dire tel que $\text{PGCD}\left[e,(p-1)(q-1)\right] = 1$), qu'il rend aussi public. Il calcule $d = e^{-1}$ modulo $(p-1)(q-1)$, qu'il garde secret ; ainsi : $de \equiv 1$ modulo $(p-1)(q-1)$.

③ L'expéditeur connaît n et e, qui sont accessibles à tout le monde, et veut envoyer un message M ; il doit s'arranger pour que M, écrit sous forme binaire, soit un nombre entier M compris entre 0 et $n-1$ (par exemple l'écriture 1101 de M signifie que $M = 2^3 + 2^2 + 0 + 1 = 13$). L'expéditeur envoie le message crypté $C \equiv M^e$ (modulo n).

④ Le destinataire, qui est seul à connaître d, calcule $R \equiv C^d$ (modulo n).

Démontrer qu'il décrypte ainsi, dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, le message envoyé M.

Exercice 16.

Soit F un sous-espace vectoriel d'un espace vectoriel E.

Dans l'anneau $\mathcal{L}(E)$ des endomorphismes de E on considère l'ensemble I des endomorphismes tels que $\text{Im}(f) \subset F$.

Montrer que I est un idéal à droite principal de $\mathcal{L}(E)$.

Exercice 17.

(Radical d'un idéal)

Soit une famille $(I_\lambda)_{\lambda\in\Lambda}$ d'idéaux à gauche d'un anneau A.

La ***somme*** $\sum I_\lambda$ des I_λ est l'idéal à gauche engendré par la réunion des I_λ ; c'est aussi l'ensemble des sommes finies $\sum x_\lambda$ où $x_\lambda \in I_\lambda$ pour tout λ ; l'***idéal à gauche engendré*** par une famille $(a_\lambda)_{\lambda\in\Lambda}$ d'éléments de A est $\sum A \cdot a_\lambda$.

Le ***radical*** d'un idéal I d'un anneau **commutatif** A est $\sqrt{I} = \left\{x \in A \mid \exists n \in \mathbb{N},\ x^n \in I\right\}$.

① On se place dans un anneau commutatif A. Soit I et J deux idéaux de A.

Montrer que : $\sqrt{I}$ est un idéal ; $\sqrt{I\cap J} = \sqrt{I}\cap\sqrt{J} = \sqrt{IJ}$.

② Déterminer $\sqrt{12\mathbb{Z}}$ et $\sqrt{72\mathbb{Z}}$ dans $\mathbb{Z}$.

③ Dans $\mathbb{Z}$, quel est l'idéal engendré par $\{4,9\}$?

④ Dans $\mathbb{Z}$, déterminer $(a)\cap(b)$ et $(a)+(b)$ pour tous $a, b \in \mathbb{Z}$.

⑤ Déterminer $I+J$, $I\cap J$, IJ, $\sqrt{I}$ et $\sqrt{J}$ dans les cas suivants :

ⓐ $A = \mathbb{Z}$, $I = 8\mathbb{Z}$, $J = 12\mathbb{Z}$;

ⓑ $A = \mathbb{Z}[X]$, $I = (X-1)$ (idéal engendré par $X-1$), $J = (X)$;

ⓒ $A = \mathbb{Z}[X]$, $I = \left(X^2+1\right)$, $J = (X+2)$.

Exercice 18.

(Anneaux noethériens)

Un idéal à gauche I d'un anneau A est dit ***de type fini*** s'il est engendré par une partie finie $\{a_1, \ldots, a_n\}$ de A, ce qui signifie :

$I = A \cdot a_1 + \ldots + A \cdot a_n = \{x_1 a_1 + \ldots + x_n a_n \mid x_1 \in A, \ldots, x_n \in A\}$.

Un anneau est dit ***noethérien à gauche*** s'il vérifie l'une des trois conditions :

① toute suite croissante d'idéaux à gauche est stationnaire ;

② tout idéal à gauche est de type fini ;

③ toute famille non vide d'idéaux à gauche distincts de A contient un élément maximal.

Établir l'équivalence de ces trois propriétés, par exemple avec le raisonnement suivant ① $\Longrightarrow$ ② $\Longrightarrow$ ③ $\Longrightarrow$ ①.

Pour ② $\Longrightarrow$ ③ on pourra utiliser le théorème de Zorn.

Algèbre. Corrigé de la fiche n^{o}1. Généralités sur les anneaux.

Mémento :

Remarque :

Si $d \geqslant 2$ est un entier sans facteurs carrés > 1 alors $\sqrt{d}$ est irrationnel.

Si $D \geqslant 2$ est un entier comportant des facteurs carrés > 1 alors $\sqrt{D}$ est soit entier, cas sans intérêt et qu'on peut exclure, soit irrationnel et de la forme $\sqrt{D} = e\sqrt{d}$, avec e entier et $d \neq 1$ entier sans facteurs carrés > 1 ; la **convention** $\sqrt{-1} = i$ donne un sens à $\sqrt{D}$ pour tout $D \in \mathbb{Z}$; exemples de décompositions $\sqrt{D} = e\sqrt{d}$: $\sqrt{12} = 2\sqrt{3}$; $\sqrt{-12} = 2\sqrt{-3} = 2i\sqrt{3}$. Avec ces notations on a l'égalité de corps : $\left\{a + b\sqrt{D} \mid a \in \mathbb{Q}, b \in \mathbb{Q}\right\} = \left\{a + b\sqrt{d} \;\middle|\; a \in \mathbb{Q}, b \in \mathbb{Q}\right\}$.

Définition 2.1 : (*Corps quadratique de nombres*)

C'est un corps de la forme $\mathbb{Q}\left(\sqrt{d}\right) = \left\{a + b\sqrt{d} \;\middle|\; a \in \mathbb{Q}, b \in \mathbb{Q}\right\}$ où $d \in \mathbb{Z}$ est un entier différent de 1 et dont la décomposition ne comporte aucun facteur carré $n^2 > 1$; $\mathbb{Q}\left(\sqrt{d}\right)$ est un ***corps quadratique réel*** si $d > 0$, un ***corps quadratique imaginaire*** si $d < 0$. C'est un $\mathbb{Q}$-espace vectoriel de dimension 2, admettant pour base $\left(1, \sqrt{d}\right)$.

Définition 2.2 : (*Conjugaison et norme*)

Avec ces notations, on appelle ***conjugué*** de $x = a + b\sqrt{d}$ le nombre $x^* = a - b\sqrt{d}$, et ***norme*** de $x = a + b\sqrt{d}$ la quantité $N(x) = a^2 - db^2$, laquelle est un nombre rationnel de signe quelconque (ne pas confondre avec la notion du même nom utilisée dans les espaces vectoriels normés).

Propriété 2.3 : (*Propriétés de la conjugaison et de la norme*)

Pour tous $x, y \in \mathbb{Q}\left(\sqrt{d}\right)$, on a :

- $(x+y)^* = x^* + y^*$;
- $(xy)^* = x^* y^*$;
- $N(x) = xx^*$;
- $N(xy) = N(x)\,N(y)$.

Définition 2.4 : (*Anneau des entiers d'un corps quadratique*)

Un élément $x \in \mathbb{Q}\left(\sqrt{d}\right)$ est un ***entier du corps quadratique*** s'il est racine d'un polynôme $P(X) \in \mathbb{Z}[X]$ **unitaire** du second degré, c'est-à-dire s'il existe $k, h \in \mathbb{Z}$ tels que $x^2 + kx + h = 0$.

Théorème 2.5 : (*Théorème de structure*)

(sera démontré en cours)

Si d est un entier différent de 1 et sans facteurs carrés $n^2 > 1$ alors l'***anneau des entiers du corps quadratique*** $\mathbb{Q}\left(\sqrt{d}\right) = \mathbb{Q} + \mathbb{Q}\sqrt{d}$ est :

- $\mathbb{Z}\left[\sqrt{d}\right] = \left\{a + b\sqrt{d} \;\middle|\; a \in \mathbb{Z}, b \in \mathbb{Z}\right\}$ si $d \equiv$ (2 ou 3) modulo 4 ;

⊛ $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a+b\frac{1+\sqrt{d}}{2} \;\middle|\; a\in\mathbb{Z}, b\in\mathbb{Z}\right\}$ si $d\equiv 1$ modulo 4.

Les questions de savoir lesquels de ces anneaux sont euclidiens, ou factoriels, sont difficiles :

Théorème 2.6 : (*Théorème*)

Si $d\in\mathbb{Z}\setminus\{1\}$ est un entier sans facteurs carrés (>1), alors l'anneau des entiers du corps quadratique $\mathbb{Q}\left(\sqrt{d}\right)$ est euclidien si et seulement si

$$d\in\{-1,-2,-3,-7,-11,2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73\}.$$

Théorème 2.7 : (*Théorème*)

Pour un entier $d<0$ sans facteurs carrés >1, l'anneau des entiers du corps quadratique imaginaire $\mathbb{Q}\left(\sqrt{d}\right)$ est factoriel si et seulement si

$$d\in\{-1,-2,-3,-7,-11,-19,-43,-67,-163\}.$$

(la question de savoir quels corps quadratiques réels $\mathbb{Q}\left(\sqrt{d}\right)$, exactement, ont des anneaux factoriels d'entiers, est encore ouverte).

Exercice 1.
(théorème de Lagrange)

Soit H un sous-groupe d'un groupe $(G,\cdot)$. Soit $x,y\in G$. Montrer que les deux classes à gauche xH et yH sont soit disjointes soit confondues. L'ordre d'un groupe fini désigne son cardinal. Montrer que l'ordre de tout sous-groupe d'un groupe fini G divise celui de G. En déduire que si $(G,\cdot)$ est un groupe d'ordre n et d'élément neutre e alors $x^n=e$ pour tout $x\in G$.

Exercice 2.
(Fermat, Euler)

Soit un entier $n\geqslant 1$. On note $\phi(n)$ le nombre d'entiers m compris entre 1 et n tels que $\mathrm{PGCD}(n,m)=1$; par exemple, $\phi(1)=1$, $\phi(2)=1$, $\phi(3)=2$, $\phi(4)=2$, $\phi(5)=4$ et $\phi(6)=2$; ϕ est la ***fonction indicatrice d'Euler***.

① On suppose dans cette question que $n\geqslant 2$. Soit l'anneau $\mathbb{Z}/n\mathbb{Z}=\{\overline{0},\ldots,\overline{n-1}\}$. On rappelle que pour tous $k,h\in\mathbb{Z}$, $\overline{k}=\overline{h}$ signifie que n divise $k-h$. Soit $m\in\mathbb{Z}$; établir l'équivalence des trois propriétés :

- ⓐ $\mathrm{PGCD}(n,m)=1$;
- ⓑ $\overline{m}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$;
- ⓒ $\overline{m}$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z},+)$.

② Établir le **théorème d'Euler** suivant : pour tout $k\in\mathbb{Z}$ premier avec n, $k^{\phi(n)}\equiv 1$ modulo n (distinguer deux cas : $n=1$; $n\geqslant 2$) ;

③ En déduire le "petit théorème de Fermat" :

- ⓐ si $p\geqslant 1$ est premier alors, pour tout $k\in\mathbb{Z}$, $k^p\equiv k$ modulo p ;
- ⓑ si $p\geqslant 1$ est premier alors, pour tout $k\in\mathbb{Z}$ non multiple de p, $k^{p-1}\equiv 1$ modulo p.

Exercice 3.

(fonction indicatrice d'Euler)

On rappelle que, pour tout entier $n \geqslant 1$, $\phi(n)$ est le nombre d'éléments de $\{1,\dots,n-1\}$ premiers avec n (PGCD = 1).

① Pour p premier, déterminer $\phi(p)$ puis $\phi(p^k)$ pour tout $k \in \mathbb{N}$.

② On considère la décomposition en facteurs premiers d'un entier $n \geqslant 2$: $n = p_1^{a_1} \cdots p_l^{a_l}$ (p_i premiers, $\geqslant 2$, distincts ; $a_i \geqslant 1$).

ⓐ Montrer que si $f : A \to A'$ est un morphisme surjectif (ou épimorphisme) d'anneaux et si A et A' sont unitaires alors $f(1_A) = 1_{A'}$.

ⓑ Justifier l'existence d'un isomorphisme d'anneaux

$$f \,:\, \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_l^{a_l}\mathbb{Z}$$

qui vérifiera nécessairement $f(1) = 1$ d'après (a).

(c) En déduire que $\phi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_l}\right)$.

Exercice 4.

(théorème de Wilson)

① Soit $(G,\cdot)$ un groupe abélien fini d'élément neutre e. Montrer que le produit de tous ses éléments est égal au produit des éléments dont le carré vaut e.

② Soit un entier premier $p \geqslant 2$. On désigne par $\overline{k} = k + p\mathbb{Z}$ la classe de $k \in \mathbb{Z}$ selon l'idéal $p\mathbb{Z}$. Rappeler la structure de $\mathbb{Z}/p\mathbb{Z} = \{\overline{0},\dots,\overline{p-1}\}$, démontrer que le produit de ses éléments non nuls vaut $\overline{-1}$.

③ Établir le théorème de Wilson, valable pour tout entier $p \geqslant 1$:

$$p \text{ premier} \quad \Longleftrightarrow \quad p \text{ divise } 1 + (p-1)!$$

Exercice 5.

On pose $\mathbb{Q}(\sqrt{3}) = \mathbb{Q} + \mathbb{Q}\sqrt{3} = \{a + b\sqrt{3} \mid a \in \mathbb{Q}, b \in \mathbb{Q}\}$.

① Montrer que $\mathbb{Q}(\sqrt{3})$ est un corps (corps quadratique de nombres).

② Le nombre $x = \frac{1+\sqrt{3}}{2}$ est-il un **entier du corps quadratique** $\mathbb{Q}(\sqrt{3})$, c'est-à-dire est-il racine d'un polynôme unitaire du second degré $P(X) \in \mathbb{Z}[X]$?

③ $\mathbb{Z} + \mathbb{Z}x$ est-il un anneau ?

Exercice 6.

On considère le corps quadratique $\mathbb{Q}(\sqrt{5}) = \mathbb{Q} + \mathbb{Q}\sqrt{5}$.

① Le nombre $x = \frac{1+\sqrt{5}}{2}$ est-il un entier du corps quadratique $\mathbb{Q}(\sqrt{5})$?

② $\mathbb{Z} + \mathbb{Z}x$ est-il un anneau ?

Exercice 7.

Expliciter, au moyen du "théorème de structure", les anneaux d'entiers des corps quadratiques suivants : $\mathbb{Q}\left(\sqrt{3}\right)$, $\mathbb{Q}\left(\sqrt{5}\right)$, $\mathbb{Q}\left(\sqrt{-1}\right)$, $\mathbb{Q}\left(\sqrt{-3}\right)$.

Exercice 8.

HYPOTHÈSE : $d \in \mathbb{Z}$ est un **entier différent de** 1 **et sans facteurs carrés** > 1 (d n'est divisible par aucun carré n^2 d'entier $n \geqslant 2$) ; désignant par $\sqrt{-1}$ le nombre complexe i on peut parler de $\sqrt{d}$, qui sera un réel irrationnel si $d > 0$ et un imaginaire pur si $d < 0$; dans tous les cas la famille $\left(1, \sqrt{d}\right)$ sera libre dans le $\mathbb{Q}$-espace vectoriel $\mathbb{C}$. On dira que $x \in \mathbb{Q}\left(\sqrt{d}\right) = \mathbb{Q} + \mathbb{Q}\sqrt{d}$ est un ***entier du corps quadratique*** $\mathbb{Q}\left(\sqrt{d}\right)$ s'il est racine d'un polynôme unitaire du second degré $P(X) \in \mathbb{Z}[X]$.

① Expliquer brièvement pourquoi $\mathbb{Z} + \mathbb{Z}\sqrt{d}$ est un anneau et vérifier l'inclusion stricte $\mathbb{Z} + \mathbb{Z}\sqrt{d} \subsetneq \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}$.

② Trouver une condition nécessaire et suffisante, portant sur d, pour que $\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}$ soit un anneau.

③ Trouver une condition nécessaire et suffisante, portant sur d, pour que $\frac{1+\sqrt{d}}{2}$ soit un entier du corps quadratique $\mathbb{Q}\left(\sqrt{d}\right)$.

④ Pour chaque élément $x = a + b\sqrt{d}$ de $\mathbb{Q}\left(\sqrt{d}\right)$, où a et b sont des rationnels, on définit la ***norme de x*** par $N(x) = a^2 - db^2$. Établir l'équivalence :

$$x \text{ est un entier du corps quadratique } \mathbb{Q}\left(\sqrt{d}\right) \iff a \in \frac{1}{2}\mathbb{Z} \text{ et } N(x) \in \mathbb{Z}.$$

⑤ Soit x un entier de $\mathbb{Q}\left(\sqrt{d}\right)$. Montrer que x est inversible dans l'anneau des entiers quadratiques de $\mathbb{Q}\left(\sqrt{d}\right)$ si et seulement si $N(x) = \pm 1$.

Exercice 9.

($\mathbb{Z}[i]$ est euclidien)

Rappeler ce qu'est la norme $N(z)$ d'un élément z de $\mathbb{Q}(i)$. Montrer que pour tout $z \in \mathbb{Q}(i)$ il existe un $y \in \mathbb{Z}[i]$ tel que $N\left(z - y\right) \leqslant \frac{1}{2}$.

Soit $u, v \in \mathbb{Z}[i]$, avec $v \neq 0$; montrer qu'il existe $q \in \mathbb{Z}[i]$ tel que $N\left(u - vq\right) \leqslant \frac{1}{2}N(v)$. En déduire que $\mathbb{Z}[i]$ est euclidien.

Algèbre. Fiche n°3. Extensions de corps, corps finis.

Mémento :

POINTS DE REPÈRE

Définition 3.1 : (*Corps*)

Un ***corps*** est un anneau unitaire K tel que $1_K \neq 0_K$ et où tout $x \neq 0$ est inversible.

Un ***sous-corps*** K' d'un corps K est un sous-anneau (partie non vide stable par soustraction et multiplication) stable par inversion ($\forall x \in K' \setminus \{0\}$, $x^{-1} \in K'$).

Exemples de corps : $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$ (corps des quaternions) ; les $\mathbb{Z}/p\mathbb{Z}$, pour p premier $\geqslant 2$.

Le cardinal de tout corps fini est de la forme $q = p^s$, avec p premier $\geqslant 2$ et s entier $\geqslant 1$; pour chacun de ces nombres $q = p^s$ il existe à isomorphisme près un seul corps de cardinal q, noté $CG(q)$ (corps de Galois), ou $GF(q)$ (Galois field), ou encore $\mathbb{F}_q$.

Définition 3.2 : (*Caractéristique d'un corps*)

La ***caractéristique*** d'un corps est soit 0 soit un nombre premier $p \geqslant 2$.

La caractéristique d'un anneau unitaire est 0 si les sommes finies $1, 1+1, 1+1+1, \ldots$ ne donnent jamais 0, ou alors n si n est le plus petit entier $m \geqslant 1$ tel que $1 + \ldots + 1$, m fois, vaille 0.

Exercice : la caractéristique d'un anneau A unitaire intègre est soit 0 soit un entier premier $p \geqslant 1$ ($p = 1$ signifie que $1 = 0$ et donc que $A = \{0\}$, cas sans intérêt) ; d'où le résultat annoncé, puisque dans un corps on a $1 \neq 0$.

Définition 3.3 : (*Morphisme de corps*)

$f : K \to K'$ est un ***morphisme de corps*** si f respecte l'addition et la multiplication et si $f(1_K) = 1_{K'}$.

Tout morphisme de corps est injectif.

Définition 3.4 : (*Extension*)

L est une ***extension*** du corps K si K est un sous-corps de L ($K \subset L$). Par abus de langage on parlera aussi de l'extension $K \subset L$.

Propriété 3.5 : (*Pour toute extension, L est un K-espace vectoriel*)

Pour toute extension $K \subset L$, L est un ***K-espace vectoriel***.

La multiplication externe qui à $\alpha \in K$ et à $x \in L$ associe $\alpha x \in L$ découle de la multiplication interne de L ; les axiomes de K-espace vectoriel sont vérifiés.

Définition 3.6 : (*Degré d'une extension*)

Le ***degré*** d'une extension $K \subset L$ est la dimension $\dim_K(L)$ du K-espace vectoriel L.

Définition 3.7 : (*Extension de degré fini*)

Une extension $K \subset L$ telle que $\dim_K(L) < \infty$ est dite de ***degré fini***, ou encore, par abus de langage, ***finie***; on note alors : $[L : K] = \dim_K(L)$.

Définition 3.8 : (*Corps de nombres*)

Un ***corps de nombres*** est une extension de $\mathbb{Q}$ dans $\mathbb{C}$ ($\mathbb{Q} \subset L \subset \mathbb{C}$), de degré fini $[L : \mathbb{Q}]$.

Propriété 3.9 : (*Formule des degrés*)

Pour des extensions de degrés finis $K \subset L \subset M$:

$$[M : K] = [M : L] \cdot [L : K]$$

Définition 3.10 : (*Élément algébrique, élément transcendant*)

Soit $K \subset L$ une extension. Un élément $x \in L$ est dit ***algébrique*** (sur K) s'il existe un polynôme non nul $P(X) \in K[X]$ tel que $P(x) = 0$; sinon il est dit ***transcendant***.

Définition 3.11 : (*Extension algébrique*)

Une ***extension algébrique*** est une extension $K \subset L$ telle que tout $x \in L$ soit algébrique (sur K).

Définition 3.12 : (*Nombre algébrique*)

Un ***nombre algébrique*** est un nombre complexe z algébrique sur $\mathbb{Q}$, c'est-à-dire qui est racine d'un polynôme non nul $P(X) \in \mathbb{Q}[X]$ ou encore, ce qui revient au même, racine d'un polynôme non nul $P(X) \in \mathbb{Z}[X]$; un nombre non algébrique est dit transcendant.

Définition 3.13 : (*Corps algébriquement clos*)

Un corps est dit ***algébriquement clos*** si tout polynôme de degré $\geqslant 1$ admet une racine.

Théorème 3.14 : (*Théorème fondamental (d'Alembert-Gauss)*)

$\mathbb{C}$ est algébriquement clos.

Définition 3.15 : (*Clôture algébrique d'un corps K*)

La ***clôture algébrique*** d'un corps K est une extension algébrique algébriquement close.

Théorème 3.16 : (*Théorème fondamental (Steinitz)*)

Tout corps commutatif K admet une clôture algébrique commutative, unique à un K-isomorphisme près.

Théorème 3.17 : (*Théorème de Frobenius*)

Les seules extensions de degré fini $\mathbb{R} \subset L$ contenant $\mathbb{R}$ dans leur centre ($rx = xr$ pour tout $r \in \mathbb{R}$ et tout $x \in L$) sont : $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{H}$.

Théorème 3.18 : (*Théorème de l'élément primitif (cas particulier de Q)*)

Soit K un corps intermédiaire entre $\mathbb{Q}$ et $\mathbb{C}$ ($\mathbb{Q} \subset K \subset \mathbb{C}$), de degré fini sur $\mathbb{Q}$.

Alors il existe $\alpha \in \mathbb{C}$ tel que $K = \mathbb{Q}(\alpha)$ (le plus petit corps contenant $\mathbb{Q}$ et α).

Théorème 3.19 : (*Théorème de Wedderburn*)

Tout corps fini est commutatif.

Définition 3.20 : (*Résidus quadratiques modulo p premier*)

Soit un entier premier $p \geqslant 3$. Un entier $n \in \mathbb{Z}$ non multiple de p est un ***résidu quadratique*** modulo p s'il existe $x \in \mathbb{Z}$ tel que $n \equiv x^2$ modulo p, ou encore, ce qui revient au même, s'il existe $x \in \{1, 2, \ldots, p-1\}$ tel que $n \equiv x^2$ modulo p.

Définition 3.21 : (*Symbole de Legendre*)

Soit p premier $\geqslant 3$ et $n \in \mathbb{Z}$. Le ***symbole de Legendre*** $\left(\frac{n}{p}\right)$ est défini par :

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divise } n \\ 1 & \text{si } n \text{ est un résidu quadratique modulo } p \\ -1 & \text{dans les autres cas} \end{cases}$$

Propriété 3.22 : (*Propriétés du symbole de Legendre*)

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \text{ modulo } p \quad ; \quad \left(\frac{m \cdot n}{p}\right) = \left(\frac{m}{p}\right) \cdot \left(\frac{n}{p}\right)$$

Théorème 3.23 : (*Loi de réciprocité quadratique*)

Pour $p \geqslant 3$, $q \geqslant 3$, premiers, distincts :

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Définition 3.24 : (*Corps finis*)

Tout ***corps fini*** est de la forme suivante, où $p \geqslant 2$ est premier, s entier $\geqslant 1$, $q = p^s$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$: $\mathbb{F}_q = \mathbb{F}_p[X]/(P(X))$, $P(X)$ étant un polynôme irréductible de degré s de $\mathbb{F}_p[X]$ et $(P(X))$ désignant l'idéal, maximal, engendré par $P(X)$: $(P(X)) = \{P(X) \cdot Q(X) \mid Q(X) \in \mathbb{F}_p[X]\}$.

Propriété 3.25 : (*Caractéristique et cardinal des corps finis*)

Si $p \geqslant 2$ est premier et $q = p^s$ avec $s \in \mathbb{N}^*$: $\mathbb{F}_q$ est de cardinal q et de caractéristique p.

Si l'on note $\alpha = \overline{X}$ la classe de X et $1 = \overline{1}$ la classe de 1, $\mathbb{F}_q$ sera égal au $\mathbb{F}_p$-espace vectoriel de base $\left(1, \alpha, \alpha^2, \ldots, \alpha^{s-1}\right)$; ses éléments u seront, indistinctement, des polynômes (modulo $P(X)$) ou encore des s-uplets appartenant à $\mathbb{F}_p = \left(\mathbb{Z}/p\mathbb{Z}\right)^s$:

$$u = u_0 + u_1\alpha + u_2\alpha^2 + \ldots + u_{s-1}\alpha^{s-1} = (u_0, u_1, \ldots, u_{s-1})$$

Propriété 3.26 : (*Structure du corps de Galois*)

Le corps de Galois $\mathbb{F}_q$, où $q = p^s$, est égal au $\mathbb{F}_p$-espace vectoriel $(\mathbb{F}_p)^s$, de dimension s, muni d'une multiplication définie via un polynôme irréductible.

Remarque :

(sur les corps finis $\mathbb{F}_q$)

Les corps finis constituent le soubassement de la théorie du codage algébrique, théorie née il y a 50 ans de la nécessité pour les sondes spatiales de transmettre leurs données par numérisation des signaux, la méthode analogique étant inopérante du fait de l'importance des perturbations électromagnétiques ("bruit"). C'est grâce au codage algébrique qu'est devenue possible, depuis peu, la télévision numérique terrestre (TNT).

Un signal sera un mot $m = (m_0, m_1, \ldots, m_{n-1})$ appartenant à un certain K^n, où K est un corps fini $\mathbb{F}_q$, avec $q = p^s$, p premier $\geqslant 2$, $s \geqslant 1$; le cadre le plus simple est celui où $q = p = 2$. On peut écrire que m est le polynôme $m = m_0 + m_1 X + m_2 X^2 + \ldots + m_{n-1} X^{n-1}$ appartenant au K-espace vectoriel $K_{n-1}[X]$ des polynômes à coefficients dans K et de degré $\leqslant n-1$; cependant, pour obtenir des propriétés intéressantes, on doit pouvoir considérer le produit de deux mots ; dans ce cas, pour ne pas dépasser le degré $n-1$, on définit le mot m par $m = m_0 + m_1 x + m_2 x^2 + \ldots + m_{n-1} x^{n-1}$, élément de l'anneau quotient $\mathbb{F}_q[X]/(X^n - 1)$, x étant la classe de X selon l'idéal engendré par le polynôme $X^n - 1$; ainsi aura-t-on $x^n = 1, x^{n+1} = x$, etc. Un code linéaire est un sous-espace vectoriel de $K^n = (\mathbb{F}_q)^n$. Un code linéaire est dit cyclique s'il est stable par permutation circulaire de $m_0, \ldots, m_{n-1}$; ce sera un sous-anneau de $\mathbb{F}_q[X]/(X^n - 1)$. La distance de Hamming entre deux mots $m = (m_0, \ldots, m_{n-1})$ et $m' = (m'_0, \ldots, m'_{n-1})$ est le nombre d'indices i tels que $m_i \neq m'_i$.

L'objectif de la théorie du codage algébrique est la mise au point d'un sous-espace de $(\mathbb{F}_q)^n$ tel que la distance minimale entre deux mots distincts soit $\geqslant d$, d étant un paramètre aussi grand que possible, garanti par des théorèmes, appelé la distance construite du code ; généralement le signal reçu r sera assez proche du signal envoyé m et assez éloigné de tous les autres signaux autorisés m' ; r sera décodé systématiquement en le signal possible le plus proche, conformément au principe du maximum de vraisemblance, ce qui donnera m. De la sorte la réception du signal sera impeccable et le bruit aura complètement disparu.

Exercice 1.

Soient $K \subset L \subset M$ des extensions de degrés finis de corps. Établir la formule :

$$[M : K] = [M : L] \cdot [L : K]$$

Exercice 2.

(polynôme minimal d'un élément algébrique)

Soit K un corps commutatif, $K \subset L$ une extension, et $a \in L$ un élément algébrique sur K.

On appelle ***polynôme minimal*** de a le polynôme (non nul) unitaire $M(X) = Min_K(a)(X) \in K[X]$, de degré n minimal, tel que $M(a) = 0$. On note $K(a)$ le plus petit corps contenant K et a. On veut démontrer que $[K(a) : K] = n$.

① Montrer que $M(X)$ est irréductible dans $K[X]$.

② Montrer que pour tout $P(X) \in K[X]$: $P(a) = 0 \iff M(X)$ divise $P(X)$.

③ Expliquer pourquoi la famille $\mathcal{B} = (1, a, a^2, \ldots, a^{n-1})$ est libre dans le K-espace vectoriel L. On notera $Vect(\mathcal{B})$ le sous-espace vectoriel de L qu'elle engendre. On pose $K[a] = \{P(a) \ / \ P(X) \in K[X]\}$.

④ Montrer que $Vect(\mathcal{B}) = K[a]$.

⑤ On remarque que $K[a]$ est un sous-anneau du corps $K(a)$. Expliquer pourquoi, pour avoir l'égalité, il suffira de montrer que $K[a]$ est un sous-corps de $K(a)$.

⑥ Soit $P(X) \in K[X]$ tel que $P(a) \neq 0$. Justifier l'existence de $U(X), V(X) \in K[X]$ tels que $M \cdot U + P \cdot V = 1$. En déduire que $(P(a))^{-1} \in K[a]$.

⑦ Conclure.

Exercice 3.
(calculs de degrés d'extensions)

Si F est une famille de nombres complexes, on notera $\mathbb{Q}(F)$ le plus petit sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$ et F.

① Calculer $\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]$ puis $\left[\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right):\mathbb{Q}\right]$.

② Montrer que $\left[\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right):\mathbb{Q}\right] = 4$.

③ Que représente $\sqrt{2}+\sqrt{3}$ pour l'extension $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$?

Exercice 4.
Démontrer que toute extension de degré fini est algébrique.

Exercice 5.
Démontrer que l'ensemble des nombres algébriques est un corps.

Indication : soit a et b deux nombres algébriques ; considérer l'extension $\mathbb{Q} \subset \mathbb{Q}(a,b)$.

Exercice 6.
(morphisme de Frobenius)

① Soit $p \geqslant 2$ un entier premier et k un entier tel que $1 \leqslant k \leqslant p-1$. Montrer que p divise le coefficient binomial $\binom{p}{k}$.

② Soit a et b deux éléments d'un anneau unitaire A, de caractéristique p premier, commutant entre eux ($ab = ba$). Montrer que $(a+b)^p = a^p + b^p$.

③ Soit K un corps commutatif de caractéristique non nulle p. Rappeler pourquoi p est premier $\geqslant 2$. Montrer que l'application $\phi : K \to K$ définie par $\phi(x) = x^p$ est un morphisme de corps (morphisme de Frobenius).

④ Soit $p \geqslant 2$ un entier premier, s un entier $\geqslant 1$, $q = p^s$ et $\mathbb{F}_q$ le corps de Galois à q éléments. Montrer que chaque élément x de $\mathbb{F}_q$ possède une unique racine p-ième $\sqrt[p]{x}$, et que $\sqrt[p]{x+y} = \sqrt[p]{x} + \sqrt[p]{y}$.

Exercice 7.
(une représentation du corps $\mathbb{F}_8$)

① Trouver les 5 polynômes irréductibles de $\mathbb{F}_2[X]$ de degrés $\leqslant 3$; procéder de proche en proche, en éliminant les produits de polynômes irréductibles déjà trouvés. Vérifier en particulier que le polynôme $X^3 + X^2 + 1$ est irréductible.

② On cherche une représentation explicite du corps de Galois $CG\left(2^3\right) = \mathbb{F}_8 = \mathbb{F}_2[X] / \left(X^3 + X^2 + 1\right)$, en posant $\alpha = \overline{X} =$ classe de X dans ce quotient. Un élément de $\mathbb{F}_8$ sera ainsi une expression polynomiale en α, de degré $\leqslant 2$. On assimilera $m = (m_0, m_1, m_2) \in \{0,1\}^3$ à $m_0 + m_1\alpha + m_2\alpha^2$. Calculer les puissances successives de α et expliciter ainsi $\mathbb{F}_8$.

③ Sous ces conventions, calculer le produit des deux éléments $(0,1,1)$ et $(1,1,1)$, ainsi que leurs inverses.

Exercice 8.

(résidus quadratiques)

Pour chaque entier premier $p \geqslant 3$ on considère le corps $\mathbb{F}_p = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}\}$ (le cas $p = 2$ ne présente ici aucun intérêt) ; remarquant que p est nécessairement impair, on posera $p = 2p' + 1$. On rappelle que l'ensemble $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ est un groupe multiplicatif. On pose $\left(\mathbb{F}_p^*\right)^2 = \left\{u^2 \ / \ u \in \mathbb{F}_p^*\right\}$ (ensemble des carrés des éléments non nuls de $\mathbb{F}_p$).

① Déterminer $\left(\mathbb{F}_3^*\right)^2$, $\left(\mathbb{F}_5^*\right)^2$ et $\left(\mathbb{F}_7^*\right)^2$.

② Montrer que $\left(\mathbb{F}_p^*\right)^2$ est de cardinal $p' = (p-1)/2$; on vérifiera que les éléments $\overline{1}^2, \overline{2}^2, \ldots, \overline{p'}^2$ sont tous distincts, puis on considérera $\overline{p'+1}^2, \overline{p'+2}^2, \ldots, \overline{2p'}^2$.

③ Soit le polynôme $P(X) = X^{p'} - 1$ appartenant à $\mathbb{F}_p[X]$, anneau euclidien car le corps $\mathbb{F}_p$ est commutatif. Montrer que ses seules racines sont les éléments de $\left(\mathbb{F}_p^*\right)^2$.

④ Démontrer le résultat suivant, quels que soient l'entier premier $p = 2p' + 1 \geqslant 3$ et l'entier $n \in \mathbb{Z}$ non multiple de p :

- ⊛ $n^{p'} \equiv \pm 1$ (modulo p)
- ⊛ $n^{p'} \equiv 1$ (modulo p) $\iff$ n est un résidu quadratique modulo p.

⑤ On définit le **symbole de Legendre** : $\left(\frac{n}{p}\right) = 1$ si n est un résidu quadratique modulo $p = 2p' + 1 \geqslant 3$ premier, $\left(\frac{n}{p}\right) = -1$ sinon. Montrer que pour tout $n \in \mathbb{Z}$ non multiple de p : $\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}}$ modulo p.

Exercice 9.

(racines carrées de -1 dans $\mathbb{F}_p$)

On suppose connu ici le **théorème de Wilson** (voir TD2, exercice 4) :

$$\text{pour tout entier } p \geqslant 1,\ p \text{ premier} \iff p \text{ divise } 1 + (p-1)!.$$

Soit désormais $p \geqslant 5$ un entier premier tel que $p \equiv 1$ modulo 4, c'est-à-dire de la forme $p = 4k + 1$.

① Montrer que -1 est un résidu quadratique modulo p.

② Vérifier que dans $\mathbb{F}_p$: $(p-1)! = 1 \cdot 2 \ldots (2k-1) \cdot (2k) \cdot (-2k) \cdot (-(2k-1)) \ldots (-1)$.

③ En déduire les racines carrées de -1 dans $\mathbb{F}_p$.

Exercice 10.

On suppose connue la **loi de réciprocité quadratique** :

$$\text{pour } p \geqslant 3 \text{ et } q \geqslant 3 \text{ premiers, distincts, } \left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

On se propose de résoudre l'équation d'inconnue $x \in \mathbb{Z}$: $x^2 \equiv 62$ (modulo 209). On remarque que $209 = 11 \cdot 19$.

① Montrer que l'équation équivaut au système :

$$\begin{cases} x^2 \equiv 62 \text{ modulo } 11 \\ x^2 \equiv 62 \text{ modulo } 19 \end{cases}$$

② Justifier les égalités : $\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right)$; $\left(\frac{4}{7}\right) = 1$.

③ Conclure.

Exercice 11.
(calculs de symboles de Legendre)

① On considère les nombres premiers 257 et 65537. Calculer $\left(\frac{11}{257}\right)$ puis $\left(\frac{3}{65537}\right)$ à l'aide de la loi de réciprocité quadratique.

② Calculer $\left(\frac{3}{p}\right)$ pour tout entier premier $p \geqslant 5$.

Exercice 12.
(version calculatoire du théorème chinois)

On va démontrer que si $m_1 \geqslant 2, \ldots, m_n \geqslant 2$, sont des entiers premiers entre eux deux à deux, alors tout système de congruences

$$\begin{cases} x \equiv r_1 \text{ modulo } m_1 \\ x \equiv r_2 \text{ modulo } m_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv r_n \text{ modulo } m_n \end{cases}$$

où $r_1, r_2, \ldots, r_n$ sont des entiers relatifs arbitraires donnés, admet une solution, qu'on explicitera, et que cette solution est unique modulo $m = m_1 \cdot m_2 \ldots m_n$.

Pour simplifier la rédaction on va se borner au cas $n = 3$: $m = m_1 \cdot m_2 \cdot m_3$.

① On pose $m_i' = \frac{m}{m_i}$. Montrer que m_i' est inversible dans l'anneau $\mathbb{Z}/m_i\mathbb{Z}$. On considère désormais m_i'' tel que $m_i' \cdot m_i'' = 1$ dans $\mathbb{Z}/m_i\mathbb{Z}$. Rappeler comment obtenir m_i''.

② Soit $x = r_1 \cdot m_1' \cdot m_1'' + r_2 \cdot m_2' \cdot m_2'' + r_3 \cdot m_3' \cdot m_3''$. Montrer que x est solution du système (pour $n = 3$).

③ Montrer que la solution est unique modulo m.

Exercice 13.
(théorème chinois et résidus quadratiques)

On veut résoudre l'équation $(\mathcal{E})$: $x^2 \equiv 7$ (modulo 1739), d'inconnue $x \in \mathbb{Z}$. On remarque que $1739 = 37 \cdot 47$.

① Montrer que $(\mathcal{E})$ équivaut au système

$$(\mathcal{S}) : \begin{cases} x^2 \equiv 7 \text{ modulo } 37 \\ x^2 \equiv 7 \text{ modulo } 47 \end{cases}$$

② Vérifier au moyen des symboles de Legendre $\left(\frac{7}{37}\right)$ et $\left(\frac{7}{47}\right)$ que chacune de ces deux équations, prise isolément, admet des solutions.

③ Au moyen de l'algorithme d'Euclide trouver deux entiers u et v tels que $37u + 47v = 1 = \text{PGCD}(37, 47)$. *Résultat :* $14 \cdot 37 - 11 \cdot 47 = 1$.

④ Résoudre alors le système $(\mathcal{S})$ au moyen du théorème chinois (exercice 12).

Résultat : l'ensemble des solutions de $(\mathcal{E})$ *est* $\{675, 453, 1286, 1064\} + 1739\mathbb{Z}$.

Algèbre. Corrigé de la fiche n^{o}3. Extensions de corps, corps finis.