ANNEAUX ET CORPS

I. INTRODUCTION

① DÉFINITION PREMIÈRE

L'ensemble $\mathbb{Z}$ et ses deux lois + et **.** bénéficient d'une structure très riche permettant de « faire de l'arithmétique ».
Cherchons si d'autres ensembles munis de deux lois permettent le même travail.

Munissons pour cela un ensemble A de deux lois + et **.** en leur donnant, dans un premier temps, un certain nombre des propriétés de $\mathbb{Z}$:

1.1.1. $(A, +, .)$ est un **anneau** si :
- *(i)* $(A, +)$ groupe commutatif
- *(ii)* la loi **.** est associative
- *(iii)* la loi **.** est distributive à gauche et à droite par rapport à +.

2. $(A, +, .)$ est dit **unitaire** si la loi **.** admet un neutre.

3. $(A, +, .)$ est dit **commutatif** si la loi **.** est commutative.

☝ Si l'ensemble A est muni de deux lois notées autrement que + et **.**, bien distinguer la loi de groupe de l'autre.

☝ Ne pas confondre les deux neutres :
- 0 pour la loi + (la confusion avec le zéro d'un autre anneau n'étant pas gênante)
- 1 pour la loi **.** (ou 1_A si il y a possibilité de confondre avec l'unité d'un autre anneau).

☝ Ne pas confondre les symétriques d'un élément a :
- $-a$ pour la loi + (appelé **opposé** de a), dont l'existence et l'unicité sont assurées par *(i)*
- a^{-1} pour la loi **.** (appelé **inverse** de a), dont rien n'assure l'existence !

☝ $b + (-a)$ se note $b - a$, mais attention, $(A, -)$ n'est pas un groupe ($-$ n'est pas associative !).

✋ Attention à bien distinguer le produit interne ab, avec $a, b \in A$, et le produit externe na, avec $n \in \mathbb{Z}$ et $a \in A$, qui désigne $a + ... + a$ (ou $-a - ... - a$ selon le signe de n) avec n termes.

QUELQUES PRÉCAUTIONS :

Le fait que les axiomes de **1.1.1.** soient vérifiés par de nombreux ensembles justifie la définition d'une nouvelle structure.
Cependant, les anneaux non unitaires représentent des cas rares et quasi pathologiques. Certains manuels définissent même un anneau comme étant nécessairement unitaire, les non-unitaires étant alors nommés **pseudo-anneaux**.
De plus, les anneaux non commutatifs, s'ils se rencontrent plus régulièrement que les non unitaires (anneaux de matrices, de fonctions), ne permettent pas de définir efficacement la notion élémentaire de division.
Enfin, tout singleton $\{a\}$ peut être muni d'une structure d'anneau avec les lois : $a + a = a$ et $a.a = a$. Son unique élément joue le rôle du zéro et de l'unité. On l'appelle **anneau nul**. Il ne présente pas grand intérêt, et surtout il ne permet pas non plus de définir les notions que nous allons étudier.
C'est pourquoi, sauf mention du contraire, nous choisirons de ne parler que des anneaux non nuls commutatifs unitaires (nous préciserons « quelconque » pour désigner un anneau non nécessairement de cette forme).

② RÈGLES DE CALCUL

2.1. $\forall\, n, m \in \mathbb{Z}\ ;\ \forall\, a, b \in A\ ;\ (na).(mb) = (nm)(a.b)$.

2.2. FORMULE DU BINÔME DE NEWTON :

Si $ab = ba$, on a : $(a + b)^n = \sum_{k=0}^{n} C_n^k\, a^{n-k} b^k$

🕮 Même structure que la formule de Leibniz donnant la dérivée $n^{\text{ème}}$ d'un produit de deux fonctions.

2.3. FACTORISATION :

Si $ab = ba$, on a : $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1})$.
En particulier : $a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + ... + a + 1)$.

③ SOUS-ANNEAU

3.1. A' **sous-anneau** de A si :
- *(i)* $(A', +) < (A, +)$
- *(ii)* A' stable par **.**
- *(iii)* $1_A \in A'$.

☝ La notion de sous-anneau est beaucoup moins utilisée que la notion de sous-groupe.

☝ Remarquons que les seuls sous-anneaux de $\mathbb{Z}$ sont $\{0\}$ et $\mathbb{Z}$.
Les autres sous-groupes, les $n\mathbb{Z}$ pour $n \notin \{0, 1\}$, ne sont pas des sous-anneaux à cause du *(iii)*.

🕮 Certains manuels n'imposent pas la condition d'unitarité *(iii)*.
En définissant les sous-anneaux avec seulement *(i)* et *(ii)*, on a quelques comportements surprenants :
- A peut être unitaire sans que A' le soit :
  les $n\mathbb{Z}$, qui deviennent alors tous des sous-anneaux de $\mathbb{Z}$, sont non unitaires pour $n \notin \{0, 1\}$.
- A et A' peuvent être unitaires sans avoir le même élément unité :
  . les sous-anneaux de $\mathbb{Z}/6\mathbb{Z}$ sont $\{\overline{0}, \overline{2}, \overline{4}\}$, d'unité $\overline{4}$, et $\{\overline{0}, \overline{3}\}$, d'unité $\overline{3}$.
  . $A \times A$, d'unité $(1, 1)$, a pour sous-anneau $A \times \{0\}$, d'unité $(1, 0)$.

④ MORPHISME

4.1. Soit A et B des anneaux.
Une application $\varphi : A \to B$ est un **morphisme d'anneaux** si :
- *(i)* $\varphi(x + y) = \varphi(x) + \varphi(y)$
- *(ii)* $\varphi(x.y) = \varphi(x).\varphi(y)$
- *(iii)* $\varphi(1_A) = 1_B$.

4.2.1. $\varphi(0_A) = 0_B$.
2. $\varphi(-a) = -\varphi(a)$.
3. a inversible $\Rightarrow \varphi(a)$ inversible.
Et : $\varphi(a^{-1}) = \varphi(a)^{-1}$.

☝ Bien comprendre pourquoi $\varphi(0_A) = 0_B$ est une conséquence de **4.1.** *(i)*,
et pourquoi $\varphi(1_A) = 1_B$ n'est pas une conséquence de *(ii)* (c'est bien un axiome).
Citons par exemple l'application : $A \to A \times A$
$a \mapsto (a, 0)$ qui vérifie *(i)* et *(ii)* sans vérifier *(iii)*.

4.3. L'image d'un sous-anneau par un morphisme est un sous-anneau.

⑤ CARACTÉRISTIQUE

5.1. Le morphisme d'anneaux : $\mathbb{Z} \to A$
$n \mapsto n.1_A$ a un noyau de la forme $k\mathbb{Z}$.
L'entier positif k est appelé **caractéristique** de A.

☝ A est de caractéristique nulle $\Leftrightarrow \forall\, n \in \mathbb{N}^* ;\ n.1_A \neq 0$.
Sinon, A est de caractéristique $inf\{n \in \mathbb{N}^* ;\ n.1_A = 0\}$ (c'est alors l'ordre additif de 1_A).

☝ Tout sous-anneau de A a la même caractéristique que A.

5.2. A de caractéristique $k \Rightarrow \forall\, a \in A ;\ ka = \underbrace{a + \ldots + a}_{k \text{ termes}} = 0$.

☝ $\mathbb{Z}/k\mathbb{Z}$ est de caractéristique k car : $k.1 \equiv k \equiv 0\ [k]$.
Mais attention à ne pas confondre caractéristique et cardinal :
$(\mathbb{Z}/k\mathbb{Z}) \times (\mathbb{Z}/k\mathbb{Z})$ est de cardinal k^2 mais de caractéristique k.
Cependant, si A est de cardinal fini, sa caractéristique est non nulle et divise $Card(A)$ (le montrer avec **5.1.**).
On en déduit que : A de caractéristique nulle $\Rightarrow A$ de cardinal infini.
Mais réciproque fausse : $\mathbb{F}_p[X]$ est infini mais de caractéristique p.

☝ A de caractéristique p premier $\Rightarrow (a + b)^p = a^p + b^p$, pour tous a et b de A (le montrer avec **5.2.**).

II. THÉORIE DE LA DIVISIBILITÉ

Nous allons voir que les axiomes de **I** ① **1.1.**, s'ils permettent de retrouver un grand nombre de notions bien connues chez les entiers, ne suffisent pas pour travailler entièrement comme dans $\mathbb{Z}$.
Le triplet $(\mathbb{Z}, +, .)$ possède en effet d'autres propriétés, qui seront nécessaires à l'ensemble A pour y « faire de l'arithmétique ».
Redécouvrons progressivement toutes les notions attachées à l'étude de la structure d'anneau, en privilégiant, dans un premier temps, le rôle de l'élément (et non celui des idéaux, voir § **III**) :

① INVERSIBILITÉ

La loi **.** ne munit pas A d'une structure de groupe. En particulier, tout élément n'admet pas nécessairement un inverse.

☝ Il va donc falloir perdre les habitudes acquises avec les groupes notés multiplicativement $(G, .)$, dans lesquels tout élément a admettait un symétrique a^{-1}.

1.1.1. Si un élément admet un inverse, alors il est dit **inversible**.
2. L'ensemble $\mathcal{U}(A)$ des inversibles de A, muni de **.**, est un groupe.

☝ Notons que cette notion n'a aucun sens dans un anneau non unitaire.

✋ Dans certains manuels, les inversibles sont nommés **unités**, à ne pas confondre avec l'élément unité 1.

☝ Dans les anciens manuels, $\mathcal{U}(A)$ est souvent noté A^*.
Mais attention, de plus en plus, $\mathcal{U}(A)$ est noté $A^\times$, et A^* désigne alors $A - \{0\}$ (qui n'est lui qu'un monoïde).

② RÉGULARITÉ ET INTÉGRITÉ

● *a)* La simplification d'un terme ne pose aucun problème.
$(A, +)$ étant un groupe, tout a de A est simplifiable car opposable (*i.e.* symétrisable pour +) :
$x + a = y + a \Rightarrow x + a - a = y + a - a \Rightarrow x = y$, pour tous x et y de A.

● *b)* Pour la loi **.**, la simplification d'un facteur n'est pas aussi simple.

2.1. Un élément a simplifiable pour la multiplication est dit **régulier**.

◆ Le raisonnement du *a)* reste valable pour les éléments inversibles (*i.e.* symétrisables pour **.**) :
$ax = ay \Rightarrow a^{-1}ax = a^{-1}ay \Rightarrow x = y$.
Donc, tout élément inversible est régulier.
Notons que la réciproque est fausse : s'il peut arriver que les éléments réguliers soient exactement les inversibles (par exemple dans $\mathcal{F}(\mathbb{R}, \mathbb{R})$ avec les fonctions ne s'annulant pas), ce n'est en général pas le cas (par exemple dans $\mathbb{Z}$, tout élément non nul, et donc pas nécessairement inversible, est régulier).

◆ Pour les non inversibles, évacuons le cas particulier de zéro dont nous n'avons pas encore étudié le comportement avec **.** :
si 0 est neutre pour + ($\forall\ a \in A\ ;\ 0 + a = a$), la distributivité lui fait suivre avec **.** une règle en quelque sorte contraire.
$\forall\ a \in A\ ;\ 0.a = 0$: on dit que 0 est **absorbant**.

◆ Pour un élément a non inversible non nul, il faut perdre ses réflexes de simplification et passer par :
$ax = ay \Leftrightarrow a(x - y) = 0$.
Deux cas se présentent :
• $x - y = 0$, et alors : $x = y$, donc a est régulier.
• $x - y \neq 0$, et alors : $x \neq y$, donc a est non régulier.
Exemples : Dans $\mathbb{Z}/6\mathbb{Z}$, comme : $\bar{2}.\bar{3} = \bar{0}$, on a : $\bar{2}.\bar{3} = \bar{2}.\bar{0}$, avec $\bar{3} \neq \bar{0}$. Donc $\bar{2}$ n'est pas régulier.
Dans $\mathbb{Z}\times\mathbb{Z}$, on a : $(0, 1).(1, 0) = (0, 0)$ (généralisable à tout produit d'anneaux non nuls).
Dans $\mathcal{M}_2(\mathbb{R})$, on a : $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

2.2. Un élément a non nul est dit **diviseur de zéro** si : $\exists\ b \neq 0\ ;\ ab = 0$.

⚠ On ne confondra pas avec le fait trivial que tout élément non nul divise l'élément 0 ! Puisque $a\times 0 = 0$!!

2.3.1. Un élément d'un anneau est :
• soit nul
• soit régulier (éventuellement inversible) caractérisé par : $(ax = 0 \Rightarrow x = 0)$
• soit diviseur de zéro.

2. Un anneau est dit **intègre** si il est sans diviseur de zéro.

Nous avons donc défini un anneau dans lequel on peut simplifier tranquillement par tout élément non nul, comme dans $\mathbb{Z}$.

☝ Les trois exemples fournissent les cas classiques d'anneaux non intègres, le troisième étant de plus non commutatif.

2.4. A intègre $\Rightarrow$ la caractéristique de A est 0 ou un nombre premier.

☝ $\mathbb{Z}/n\mathbb{Z}$ intègre $\Leftrightarrow$ n premier.

☝ Réciproque fausse : $(\mathbb{Z}/p\mathbb{Z})\times(\mathbb{Z}/p\mathbb{Z})$, avec p premier, est de caractéristique p mais non intègre.

③ DIVISION

● *a)* Dans un groupe, on peut toujours obtenir un élément a en multipliant à droite (ou à gauche) un élément b :
il existe un et un seul élément q tel que $bq = a$ (c'est $b^{-1}a$), et un et un seul élément q' tel que $q'b = a$ (c'est ab^{-1}).
De plus, si le groupe est commutatif, on a : $q = q'$.
Dans un anneau, le fait que tout élément ne soit pas inversible rend la situation exceptionnelle :

3.1. b **divise** a (on note : $b \mid a$) si : $\exists\ q \in A\ ;\ a = bq$.
b est **diviseur** de a et a est **multiple** de b.
q est appelé **quotient** de a par b.

☝ L'ensemble des multiples de a se note aA.
Et on a : $b \mid a \Leftrightarrow aA \subset bA$ (attention à l'inversion).

☝ Si l'anneau n'est pas commutatif, on est obligé de définir une **division à droite** et une **division à gauche**.

☝ Remarquons qu'en plus du problème d'existence peut se poser celui de l'unicité.
✍ Dans $\mathbb{Z}/6\mathbb{Z}$, $\bar{2}$ et $\bar{5}$ sont deux quotients de $\bar{4}$ par $\bar{2}$ (car $\bar{2}\times\bar{2} = \bar{4}$ et $\bar{2}\times\bar{5} = \bar{10} = \bar{4}$).

Mais il est facile de voir que :

3.2. Dans un anneau intègre, le quotient, s'il existe, est unique. On le note alors $a : b$ ou a/b.

● *b)* Notre modèle $\mathbb{Z}$ est sur ce plan en difficulté puisque le quotient peut ne pas exister : la division de 3 par 2 est impossible.
Cependant (et c'est un bon exemple de la puissance de l'utilisation conjointe des deux lois + et **.**), pour tout $b \neq 0$, nous pouvons toujours écrire a sous la forme $bq + r$ avec $|r| < |b|$, à défaut de $r = 0$.

3.3.1. Dans un anneau intègre A, toute application $\varphi : A^* \to \mathbb{N}$ telle que :
• $_{(i)}$ b diviseur strict de $a \Rightarrow \varphi(b) < \varphi(a)$
• $_{(ii)}$ $\forall\ a \in A\ ;\ \forall\ b \in A^*\ ;\ \exists\ (q, r) \in A^2\ ;\ a = bq + r$, avec $r = 0$ ou $\varphi(r) < \varphi(b)$
est appelée **stathme** (ou **algorithme**) **euclidien** sur A.

2. Un anneau admettant un stathme est appelé **anneau euclidien**.

3. Trouver un tel couple (q, r) s'appelle effectuer une **division euclidienne** (ou **division avec reste**) de a par b.

🕮 L'axiome $_{(i)}$ ne présente pas un grand intérêt pratique (il est même souvent absent des définitions d'anneau euclidien).
Nous avons choisi de le faire figurer car il permet en particulier de démontrer qu'un anneau euclidien est factoriel (par une jolie récurrence sur l'ensemble des $\varphi(a)$, $a \in A$). Pour information, $_{(i)}$ permet également de munir les anneaux euclidiens d'algorithmes de construction d'éléments irréductibles.

🕮 Dans $\mathbb{Z}$, on remarque que, si b ne divise pas a (donc $r \neq 0$), deux couples (q, r) vérifient l'égalité $a = bq + r$.
Pour l'un, on a : $0 < r < |b|$, et pour l'autre, on a : $-|b| < r < 0$.
Nécessairement, l'un de ces deux restes vérifie : $|r| \leq \frac{|b|}{2}$ $_{(*)}$.
On peut montrer que : $_{(*)} \Leftrightarrow \varphi(r) < \varphi(b)$, où $\varphi : \mathbb{Z}^* \to \mathbb{N}$
$x \mapsto$ le nombre de chiffres de x écrit en base 2.
On obtient un nouveau stathme euclidien sur $\mathbb{Z}$!
Cette nouvelle division euclidienne sur $\mathbb{Z}$ s'appelle le **division de plus petit reste** ou **division centrée**.
Remarquons que, là encore, il n'y a pas unicité du couple (q, r) :
$27 = 6\times 4 + 3$ et $27 = 6\times 5 - 3$ sont deux divisions centrées de 27 par 6.
Il est même possible de construire sur $\mathbb{Z}$ d'autres divisions euclidiennes (plus anecdotiques !).
Éviter donc de parler de la division euclidienne d'un anneau, il peut y en avoir plusieurs.

④ ASSOCIATION

4.1.1. Deux éléments a et a' ont les mêmes multiples ($aA = a'A$) $\Leftrightarrow a \mid a'$ et $a' \mid a$.
On dit alors que a et a' sont **associés** (on note : $a \sim a'$).
C'est une relation d'équivalence.

2. CARACTÉRISATION DANS UN ANNEAU INTÈGRE :
a et a' associés $\Leftrightarrow \exists\, u$ inversible ; $a' = ua$.

☝ 0 n'a que 0 pour associé.

☝ 1 est associé à tous les inversibles.
D'où le nom d'**unités** donné parfois aux inversibles, 1 ne jouant pas, dans de nombreux cas, un rôle spécifique par rapport à ses associés.

☝ Dans $\mathbb{Z}$, l'association correspond à l'opposition.

⑤ IRRÉDUCTIBILITÉ

Tout élément non nul possède au moins pour diviseurs tous ses associés et tous les inversibles.
Si il est inversible, ses associés coïncident trivialement avec les inversibles, et de plus, il n'a pas d'autres diviseurs.
La même situation pour un non inversible est exceptionnelle :

5.1.1. Un élément non inversible ayant exactement ses associés et les inversibles pour diviseurs est dit **irréductible**.

2. CARACTÉRISATION DANS UN ANNEAU INTÈGRE :
p est irréductible $\Leftrightarrow (p = ab \Rightarrow a$ ou b est inversible).

⑥ FACTORISABILITÉ

On a reconnu qu'un élément irréductible d'un anneau correspond à un nombre premier (ou à son opposé) dans $\mathbb{Z}$.
Or, une des propriétés les plus importantes de $\mathbb{Z}$ (à tel point qu'on la nomme souvent **théorème fondamental de l'arithmétique**) est que tout entier ≥ 2 se décompose en produit de nombres premiers.
Cette décomposition est unique à ceci près qu'on peut remplacer un nombre pair de facteurs par leurs opposés.
Quant au fait qu'on puisse changer l'ordre des facteurs, c'est évident puisque **.** est commutative dans $\mathbb{Z}$.
De plus, au signe près, on peut généraliser aux entiers ≤ -2.
C'est malheureusement une propriété dont un anneau, même intègre, ne peut être muni par les axiomes de **1.1.**
D'où la définition :

6.1. Un anneau intègre est dit **factoriel** si :
- *(i)* tout élément non nul et non inversible se décompose en produit fini d'éléments irréductibles
- *(ii)* cette décomposition est unique au remplacement près d'un certain nombre de facteurs par des associés.

☝ Remarquons que les éléments non nuls et non inversibles d'un anneau correspondent aux relatifs à valeur absolue ≥ 2.

✋ Si on travaille dans un anneau non commutatif, il faut ajouter que la décomposition est unique à l'ordre près des facteurs.

6.2.1. On appelle **valuation** de p dans la décomposition primaire de a, et on note $\nu_p(a)$, le plus grand entier n tel que : $p^n \mid a$.

2. Dans un anneau factoriel, la division se traduit par : $a \mid b \Leftrightarrow (\forall\, p$ irréductible ; $\nu_p(a) \leq \nu_p(b))$.

⑦ PRIMALITÉ

La primalité d'un entier $p \geq 2$ est généralement définie par :
- *(i)* les seuls diviseurs positifs de p sont 1 et p,
en quoi on reconnaît la définition d'un élément irréductible : primalité et irréductibilité coïncident dans $\mathbb{Z}$.

Une des premières propriétés énoncées sur les nombres premiers est :
- *(ii)* $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$,
connue sous le nom de théorème de Gauss.

En fait, on démontre facilement que, dans $\mathbb{Z}$, c'est une propriété caractéristique.
Mais c'est faux en théorie générale des anneaux.
Nous avons donc affaire à deux notions distinctes : l'irréductibilité, toujours définie par *(i)*, et la primalité, en fait définie par *(ii)*.

7.1. Un élément p, non nul et non inversible, est dit **premier** s'il vérifie la propriété de Gauss : $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$.

On a quand même :

7.2.1. Si A est intègre :
p premier $\Rightarrow p$ irréductible.

2. Si A est factoriel :
p premier $\Leftrightarrow p$ irréductible.

☝ La décomposition en facteurs irréductibles des anneaux factoriels est souvent (et légitimement d'après **7.2.2.**) appelée décomposition en facteurs premiers, ou **décomposition primaire**.

⑧ PGCD, PPCM

Comme dans $\mathbb{Z}$, $Div(a, b)$, l'ensemble des diviseurs communs à a et b, est quasi-ordonné pour la relation "divise" : c'est une relation d'ordre « à l'association près », ou plus précisément, c'est une relation d'ordre sur l'ensemble-quotient $Div(a, b)/\sim$.
Les éléments de la classe maximale de $Div(a, b)/\sim$ pour l'ordre « divise » sont appelés **plus grands diviseurs communs** à a et b.
Les éléments de la classe minimale de $Div(a, b)/\sim$ pour l'ordre « divise » sont appelés **plus petits multiples communs** à a et b.

8.1.1. δ est un **plus grand diviseur commun** à a et b si : ($\delta \in Div(a, b)$, et : $\forall\, d \in Div(a, b)$; d divise δ).
On le note $pgcd(a, b)$ ou $a \wedge b$.

2. μ est un **plus petit multiple commun** à a et b si : ($\mu \in Mult(a, b)$, et : $\forall\, m \in Mult(a, b)$; μ divise m).
On le note $ppcm(a, b)$ ou $a \vee b$.

✋ Si a et b admettent δ pour *pgcd*, alors tous les associés de δ sont aussi des *pgcd* de a et b.
On note abusivement : $\delta = a \wedge b$ (au lieu de $\delta \sim a \wedge b$) bien qu'il n'y ait donc pas unicité (même chose avec un *ppcm*).

☝ On définit les *pgcd* et *ppcm* de plus de deux éléments de manière similaire :
($\delta \in Div(a_1, \ldots, a_n)$, et : $\forall\, d \in Div(a_1, \ldots, a_n)$; d divise δ)
ou par associativité : $a_1 \wedge \ldots \wedge a_n = (a_1 \wedge \ldots \wedge a_{n-1}) \wedge a_n$.
Même chose avec $a_1 \vee \ldots \vee a_n$.

✋ Le parallèle avec $\mathbb{Z}$ ne peut aller jusqu'à la définition des *pgcd* comme étant générateurs de $aA + bA$, puisque rien n'affirme que $aA + bA$ est un ensemble de multiples.
☞ Nous verrons au **III** ③ que cette seconde définition sera possible dans les anneaux principaux.
Nous avions vu que définir les *pgcd* comme en **8.1.1.** avait comme inconvénient de ne pas en assurer l'existence !
Mais si l'inconvénient pouvait être levé dans $\mathbb{Z}$ par la construction d'entiers adéquats par l'algorithme d'Euclide, ce ne sera pas toujours possible dans un anneau quelconque : deux éléments peuvent n'avoir ni *pgcd*, ni *ppcm* !

8.2. Dans A intègre, pour tout c non nul, et sous condition d'existence des *pgcd* :
$\delta = a \wedge b \Leftrightarrow c\delta = (ca) \wedge (cb)$.

☝ En fait, seule l'existence de $(ca) \wedge (cb)$ doit être supposée pour démontrer $\Rightarrow$.

8.3. Si A est factoriel :
$a \wedge b$ et $a \vee b$ existent toujours et s'obtiennent à partir des décompositions primaires de a et b.
Si $a = \prod p_i^{\alpha_i}$ et $b = \prod p_i^{\beta_i}$ (avec les α_i et les β_i éventuellement nuls pour que les deux décompositions comportent les mêmes irréductibles), alors :
- $a \wedge b = \prod p_i^{\inf(\alpha_i, \beta_i)}$
- $a \vee b = \prod p_i^{\sup(\alpha_i, \beta_i)}$

Si l'on est assuré de son existence (ce qui n'est pas un mince progrès par rapport aux intègres), on n'obtient pas une méthode très efficace de recherche du *pgcd*, la décomposition n'étant pas toujours aisée à trouver.
Les anneaux euclidiens permettent une méthode bien plus rapide avec le fameux…

8.4. ALGORITHME D'EUCLIDE
Si A est euclidien, muni d'un stathme φ, alors $a \wedge b$ s'obtient par divisions euclidiennes successives.
On construit une suite $(r_n)_{n \in \mathbf{N}}$ avec : • $r_0 = a$ et $r_1 = b$
• la récurrence : $r_{i-1} = r_i q_{i+1} + r_{i+1}$, avec $r_{i+1} = 0$ ou $\varphi(r_{i+1}) < \varphi(r_i)$.
Alors : $\exists\, k$; $r_k \neq 0$ et $r_{k+1} = 0$,
et : $r_k = a \wedge b$.

✋ Il est à noter que le stathme joue un rôle essentiel dans la bonne marche de l'algorithme :
φ étant à valeurs dans $\mathbb{N}$, $(r_n)_{n \in \mathbf{N}}$ est une suite d'entiers positifs strictement décroissante, donc constante nulle à partir d'un certain rang.
De plus, tout repose sur le fait que, si $\alpha = \beta\lambda + \rho$ avec $\rho = 0$ ou $\varphi(\rho) < \varphi(\beta)$, alors : $Div(\alpha, \beta) = Div(\beta, \rho)$.
On a donc : $Div(a, b) = Div(b, r_1) = Div(r_1, r_2) = \ldots = Div(r_n, r_{n+1} = 0) = Div(r_n)$.

🕮 Algorithme récursif :
Si $b = 0$, alors : $a \wedge b = a$,
sinon : $a = bq + r$, avec $r = 0$ ou $\varphi(r) < \varphi(b)$.
Si $r = 0$, alors : $a \wedge b = b$,
sinon : $a \wedge b = b \wedge r$.

⑨ ÉLÉMENTS ÉTRANGERS

On sait qu'un inversible divise tout élément non nul.
Donc, pour tous a et b non nuls, $Div(a, b)$ contient l'ensemble des inversibles.

9.1. Si les inversibles sont les seuls diviseurs communs à a et b, ou encore si 1 est *pgcd* de a et b,
a et b sont dits alors **premiers entre eux** ou **étrangers**.

☝ On note abusivement $a \wedge b = 1$, mais tous les inversibles sont alors aussi *pgcd* de a et b.

☝ On étend la définition à une famille finie : les a_i sont **premiers entre eux dans leur ensemble** si $a_1 \wedge \ldots \wedge a_n = 1$.
On ne confondra pas avec des éléments premiers entre eux deux à deux.

9.2. THÉORÈME DE GAUSS :
Si A est intègre, on a : $\begin{cases} a \wedge b = 1 \\ a \mid bc \end{cases} \Rightarrow a \mid c$.

III. IDÉAL

① QUOTIENTAGE

● *a)* RAPPELS SUR LES QUOTIENTAGES DE GROUPES :
Étant donnés un groupe G et une relation d'équivalence $\mathcal{R}$, l'ensemble-quotient $G/\mathcal{R}$ peut être muni d'une structure de groupe en cohérence avec la loi de G (*i.e.* telle que la composée des classes $\bar{x}.\bar{y}$ soit naturellement la classe des composés $\bar{x}\bar{y}$) si et seulement si $\mathcal{R}$ est compatible à droite et à gauche avec $.$ (*i.e.* $x \,\mathcal{R}\, y \Rightarrow xz \,\mathcal{R}\, yz$ et $zx \,\mathcal{R}\, zy$).
De plus, à toute relation d'équivalence $\mathcal{R}$ compatible à droite et à gauche correspond un unique sous-groupe H tel que :
$x \,\mathcal{R}\, y \Leftrightarrow x^{-1}y \in H$.
Ce sous-groupe H est la classe $\bar{e}$ du neutre de G et le groupe $G/\mathcal{R}$ peut se noter G/H.

Étant donné un sous-groupe H, la compatibilité à droite et à gauche de sa relation associée (qui permet la structure de groupe) se traduit par : $\forall\, x \in G\ ;\ xH = Hx$. On dit que H est **distingué**.

● *b)* On sait que les seuls sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ et qu'ils sont évidemment distingués.
Or, les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ peuvent être muni d'une structure d'anneau avec la loi **.** définie par : $an\mathbb{Z} \,.\, bn\mathbb{Z} = abn\mathbb{Z}$.
On s'aperçoit que la vérification de la distributivité de **.** par rapport à + utilise une propriété bien connue :
tout élément multiplié par un multiple de a devient à son tour multiple de a.
C'est justement cette propriété, de pouvoir « absorber » tout élément, qui va permettre de généraliser :

● *c)* Soit un anneau A et une relation d'équivalence $\mathcal{R}$ sur A.
On sait déjà que $\mathcal{R}$ est associée à un sous-groupe I de $(A, +)$.
$(A, +)$ étant commutatif, I est nécessairement distingué.
Donc, on est assuré de pouvoir munir $A/\mathcal{R}$ d'une structure de groupe telle que : $\bar{x} + \bar{y} = \overline{x + y}$.
On montre de plus que :

1.1.1. Le groupe $(A/\mathcal{R}, +)$ est muni d'une structure d'anneau cohérente avec **.** (c'est-à-dire telle que : $\bar{a}.\bar{b} = \overline{ab}$)
$\Leftrightarrow$ le sous-groupe $(I, +)$ associé à $\mathcal{R}$ vérifie : $\forall\, a \in A\ ;\ \forall\, h \in I\ ;\ ah \in I$.
2. I est alors appelé **idéal** de A.
3. $A/\mathcal{R}$ est appelé **anneau-quotient** et on le note A/I.

☝ Tout ensemble de multiples aA est un idéal.
La réciproque est fausse, mais elle serait si pratique qu'on va définir des anneaux dans lesquels ce sera vrai (voir **3.3.**).

✋ À cause de la condition d'unitarité, un idéal n'est pas nécessairement un sous-anneau.

📖 Dans un anneau non commutatif, on définit :
- I est un **idéal à gauche** si : $\forall\, a \in A\ ;\ \forall\, h \in I\ ;\ ah \in I$.
- I est un **idéal à droite** si : $\forall\, a \in A\ ;\ \forall\, h \in I\ ;\ ha \in I$.
- I est un **idéal bilatère** si I est idéal à gauche et à droite.

aA n'est alors qu'idéal à gauche.

② GÉNÉRALITÉS

2.1. Soit $\varphi : A \to B$ un morphisme d'anneaux.
1. L'image d'un idéal de A est un idéal de $\varphi(A)$.
2. L'image réciproque d'un idéal de B est un idéal de A.
En particulier : $Ker(\varphi)$ est un idéal de A.

2.2.1. Une intersection d'idéaux est un idéal.
2. Une somme finie d'idéaux est un idéal.

2.3. CARACTÉRISATION :
I idéal de $A \Leftrightarrow \exists\, \varphi$ morphisme partant de A ; $I = Ker(\varphi)$.

③ PRINCIPALITÉ

● *a)* GÉNÉRATION :
Par analogie avec la génération de groupes :

3.1. Soit $B \subset A$.
L'intersection de tous les idéaux de A contenant B est un idéal.
On l'appelle **idéal de** A **engendré** par B, on le note $< B >$.

☝ $< B >$ est l'ensemble des combinaisons A-linéaires finies d'éléments de B :
$< B > = \{\sum \lambda_i b_i\ ;\ \lambda_i \in A\ ;\ b_i \in B\}$ (attention, c'est la loi +).

● *b)* IDÉAL PRINCIPAL :
Par analogie avec les groupes cycliques :

3.2. I est dit **principal** si I est engendré par un élément a.
I est alors l'ensemble aA des multiples de a.

☝ On le note parfois (a) ou $< a >$.

● *c)* ANNEAU PRINCIPAL :

3.3. Un anneau intègre est dit **anneau principal** si tout idéal est principal.

📖 Si tout idéal est engendré par un nombre fini d'éléments, l'anneau est dit **noethérien**.

Les anneaux principaux autorisent de nouvelles propriétés pour les *pgcd* et *ppcm* :

3.4. Si A est principal :
1. $a \wedge b$ et $a \vee b$ sont générateurs d'idéaux : $< a \wedge b > = aA + bA$.
$< a \vee b > = aA \cap bA$.
2. $a \wedge b = \delta \Rightarrow \exists\, u, v \in A\ ;\ au + bv = \delta$.
3. THÉORÈME DE BÉZOUT :
$a \wedge b = 1 \Leftrightarrow \exists\, u, v \in A\ ;\ au + bv = 1$.

✋ Ne pas dire les mais des **coefficients de Bézout** :

si (u_o, v_o) sont des coefficients de Bézout, l'ensemble des coefficients de Bézout est $\{(u_o - k\frac{b}{\delta},\ v_o + k\frac{a}{\delta})\ ;\ k \in A\}$.

④ PRIMALITÉ

Nous avons vu que l'intégrité est une qualité d'anneau sans laquelle se posent beaucoup de problèmes.
Or, même si A l'est, A/I peut ne pas être intègre : c'est en fait I qui va décider de l'intégrité de A/I :

4.1. A/I est intègre $\Leftrightarrow (xy \in I \Rightarrow x \in I \text{ ou } y \in I)$.
On dit alors que I est **premier**.

✍ $6\mathbb{Z}$ n'est pas premier car : 2×3 est dans $6\mathbb{Z}$ alors que ni 2, ni 3 ne le sont.

☝ Si A est principal :
pA idéal premier $\Leftrightarrow$ p premier.

IV. COMPARAISON DES DIFFÉRENTS TYPES D'ANNEAUX

① LIENS

1.1. A euclidien $\Rightarrow$ A principal $\Rightarrow$ A factoriel $\Rightarrow$ A intègre.

☝ Les euclidiens, principaux et factoriels sont intègres par définition.

✋ Attention, les implications de **1.1.** sont strictes :

- un anneau peut être intègre non factoriel (c'est le cas de $\mathbb{Z}[\sqrt{-5}] = \{x + iy\sqrt{5} \, ; \, x, y \in \mathbb{Z}\}$)
- un anneau peut être factoriel non principal (c'est le cas de $\mathbb{Z}[X]$, ensemble des polynômes à coefficients entiers)
- un anneau peut être principal non euclidien (c'est le cas de $\mathbb{R}[X, Y]/(X^2 + Y^2 + 1)$ et de $\mathbb{Q}[\sqrt{-19}] = \{x + iy\sqrt{19} \, ; \, x, y \in \mathbb{Q}\}$)

② TABLEAU COMPARATIF

<table>
<tr><th></th><th colspan="5">Anneau non nul, commutatif unitaire</th></tr>
<tr><th></th><th></th><th colspan="4">Anneau intègre</th></tr>
<tr><th></th><th></th><th></th><th colspan="3">Anneau factoriel</th></tr>
<tr><th></th><th></th><th></th><th></th><th colspan="2">Anneau principal</th></tr>
<tr><th></th><th></th><th></th><th></th><th></th><th>Anneau euclidien</th></tr>
<tr><td>Définition</td><td></td><td>◆ Sans diviseur de 0</td><td>◆ Intégrité + existence et unicité d'une décomposition primaire pour tout élément non nul et non inversible</td><td>◆ Intégrité + principalité de tout idéal (engendré par un élément, de la forme aA).</td><td>◆ Intégrité + stathme euclidien.</td></tr>
<tr><td>Simplification</td><td>◆ Non en général.
◆ Sauf pour les éléments dits réguliers.
◆ $xa = xb \Leftrightarrow x(a - b) = 0$, puis on discute.</td><td colspan="4">◆ Toujours possible
(tout élément non nul est régulier)</td></tr>
<tr><td rowspan="3">Division</td><td colspan="5">◆ La division n'est pas toujours possible</td></tr>
<tr><td>◆ Si la division est possible, il peut y avoir plusieurs quotients</td><td colspan="4">◆ Si la division est possible, le quotient est unique</td></tr>
<tr><td colspan="5">◆ Division euclidienne (toujours possible)</td></tr>
<tr><td rowspan="3">Irréductibilité et primalité</td><td colspan="5">◆ p irréductible si il n'a pas d'autres diviseurs que ses associés et les inversibles
◆ p premier si : $p \mid ab \Rightarrow p \mid a$ ou b</td></tr>
<tr><td colspan="2"></td><td colspan="3">◆ p irréductible $\Leftrightarrow (p = ab \Rightarrow a$ ou b inversible)</td></tr>
<tr><td colspan="2"></td><td>◆ p premier $\Rightarrow p$ irréductible</td><td colspan="2">◆ p premier $\Leftrightarrow p$ irréductible</td></tr>
<tr><td rowspan="4">pgcd et ppcm</td><td colspan="5">◆ Un plus grand diviseur commun est un élément de $Div(a, b)$ divisible par tout élément de $Div(a, b)$.
◆ Un plus petit multiple commun est un élément de $Mult(a, b)$ diviseur de tout élément de $Mult(a, b)$.</td></tr>
<tr><td colspan="2">◆ a et b peuvent n'avoir ni $pgcd$, ni $ppcm$</td><td colspan="3">◆ $a \wedge b$ et $a \vee b$ existent toujours et s'obtiennent par les décompositions primaires de a et b</td></tr>
<tr><td colspan="3"></td><td colspan="2">◆ $a \wedge b$ engendre $aA + bA$
(et donc : $\exists \, u, v \, ; \, au + bv = a \wedge b$)
◆ $a \vee b$ engendre $aA \cap bA$</td></tr>
<tr><td colspan="4"></td><td>◆ Algorithme d'Euclide pour le $pgcd$</td></tr>
<tr><td rowspan="4">Éléments étrangers</td><td colspan="5">◆ a et b étrangers si les seuls diviseurs communs sont les inversibles (càd : $a \wedge b = 1$)</td></tr>
<tr><td colspan="2"></td><td colspan="3">◆ Gauss : $a \wedge b = 1$ et $a \mid bc \Rightarrow a \mid c$</td></tr>
<tr><td colspan="3"></td><td colspan="2">◆ Bézout : $a \wedge b = 1 \Leftrightarrow \exists \, u, v \, ; \, au + bv = 1$</td></tr>
<tr><td colspan="4"></td><td>◆ L'algorithme d'Euclide permet de trouver des coefficients de Bézout</td></tr>
</table>

V. CORPS

① DÉFINITION ET PROPRIÉTÉS

1.1. Un anneau unitaire, non nécessairement commutatif, est appelé un **corps** si tous ses éléments non nuls sont inversibles.

☝ Il est équivalent de dire que l'ensemble des éléments non nuls forment, pour **.**, un groupe.
Pour un corps K, on a : $\mathcal{U}(K) = K - \{0\}$, et donc possibilité de confondre les notations K^* et $K^\times$.

✍ Exemples classiques :
- les corps habituels $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
- les $\mathbb{Z}/p\mathbb{Z}$, avec p premier (notés $\mathbb{F}_p$, de l'anglais *field* utilisé pour désigner des corps)
  Rappelons que : $\mathbb{Z}/n\mathbb{Z}$ corps $\Leftrightarrow$ $\mathbb{Z}/n\mathbb{Z}$ intègre $\Leftrightarrow$ n premier.
- le corps $\mathscr{C}$ des nombres constructibles, réels qui sont coordonnée, dans (O, I, J) orthonormé, d'un point constructible à la règle et au compas par un nombre fini d'étapes à partir de O et I (voir sujet d'étude du chapitre 7).
- les corps de fractions rationnelles $\mathbb{R}(X)$ et $\mathbb{C}(X)$.
- le corps $\mathbb{H}$ des quaternions d'Hamilton, non commutatif (voir chapitre 2).

☝ La convention faite au début du chapitre sur la commutativité implicite de nos anneaux s'étend désormais aux corps.

1.2. Tout corps est un anneau intègre.

☝ On en déduit que la caractéristique d'un corps est 0 ou un nombre premier.

☝ Si la réciproque est bien sûr fausse (avec $\mathbb{Z}$), elle est vraie pour un anneau fini.

1.3. CARACTÉRISATION PAR LES IDÉAUX :
Un anneau est un corps $\Leftrightarrow$ il est **simple** (*i.e.* ses seuls idéaux sont $\{0\}$ et lui-même).

✋ Le sens $\Leftarrow$ peut être faux si l'anneau n'est pas commutatif.
C'est le cas des anneaux $\mathscr{M}_n(\mathbb{R})$, qui sont simples sans être des corps (voir **VI** ③ **3.1.**).

☝ Comme prolongement de **III** ④ **4.1.**, on a :
A/I est un corps $\Leftrightarrow$ I n'est inclus dans aucun autre idéal que A et lui-même.
On dit alors que I est **maximal**.

1.4. CORPS DES FRACTIONS D'UN ANNEAU INTÈGRE :
Soit A un anneau intègre.
On définit sur $A\times A^*$ la relation d'équivalence : $(a, b)\ \mathcal{R}\ (a', b') \Leftrightarrow ab' = a'b$.
La classe de (a, b) est notée $\frac{a}{b}$.
On munit $(A\times A^*)/\mathcal{R}$ des lois : $\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + ba'}{bb'}$ et $\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$.
C'est un corps, appelé **corps des fractions** de A, noté $Frac(A)$.

☝ L'injection : $A \to Frac(A)$
$a \mapsto \frac{a}{1}$ permet d'identifier A à un sous-anneau de $Frac(A)$.

☝ $Frac(A)$ est le plus petit corps contenant A.
Mais on ne parle pas de corps engendré par une partie. Au besoin, on fabriquera le corps des fractions de l'idéal engendré.

② SOUS-CORPS

2.1. Soit un corps K.
Toute partie k de K ayant une structure de corps est appelée **sous-corps** de K.
K est dit **sur-corps** de k.

☝ Toute intersection de sous-corps est un sous-corps.

2.2.1. Un corps est dit **premier** s'il n'a d'autre sous-corps que lui-même.
2. $\mathbb{Q}$ et les $\mathbb{Z}/p\mathbb{Z}$ sont premiers.

2.3.1. L'intersection $P(K)$ de tous les sous-corps de K est premier : on l'appelle **le sous-corps premier** de K.
2. Si K est de caractéristique nulle : $P(K) \approx \mathbb{Q}$.
Si K est de caractéristique p premier : $P(K) \approx \mathbb{Z}/p\mathbb{Z}$.

☝ On en déduit que tout corps fini de cardinal p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

☝ Que K soit commutatif ou non, $P(K)$ l'est toujours.

③ EXTENSION

3.1. Soit un corps K.
Tout corps L, tel qu'il existe un homomorphisme de d'anneaux $\varphi : K \to L$, est appelé **extension** de K.

✋ Si tout sur-corps K de k en est une extension (avec l'injection canonique : $k \to K$), la réciproque est fausse, mais on se permettra l'identification : L extension de $K \Leftrightarrow K$ sous-corps de L.

☝ $P(K)$ est une extension de K.
On en déduit que tout corps de caractéristique nulle est une extension de $\mathbb{Q}$.
De même, tout corps de caractéristique p premier est une extension de $\mathbb{Z}/p\mathbb{Z}$.

3.2. Soit L une extension de K.
Muni de + et de la loi externe $K\times L \to L$
$(\lambda, x) \mapsto \varphi(\lambda).x$, L est un K-espace vectoriel.
La dimension de L comme K-espace vectoriel est appelée **degré** de l'extension, on la note $[L : K]$.

☝ Muni de ses trois lois, L est une K-algèbre.

✍ $[\mathbb{C} : \mathbb{R}] = 2$.
Mais : $[\mathbb{R} : \mathbb{Q}] = \infty$, car $\mathbb{Q}$ est dénombrable et $\mathbb{R}$ ne l'est pas.

3.3. Soit K_3 une extension de K_2 et K_2 une extension de K_1.
Alors K_3 est une extension de K_1 et :
$[K_3 : K_1] = [K_3 : K_2].[K_2 : K_1]$.

☝ Toute suite de corps $(K_1, \ldots, K_n)$ finie et croissante (pour $\subset$) est appelée **tour d'extensions**.
Si de plus : $\forall\ i$; $[K_i : K_{i-1}] = 2$, on l'appelle **tour d'extensions quadratiques**.

④ CORPS FINIS

4.1. Soit K un corps fini.
1. Sa caractéristique est un nombre premier p.
2. Son sous-corps premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
3. Son cardinal est de la forme p^n.

☞ Nous démontrerons dans le chapitre 6 (**VII** ② **2.2.**) le...

4.2. THÉORÈME DE WEDDERBURN :
Tout corps fini est commutatif.

☝ Rappelons deux résultats vus dans le cours sur les groupes :
- Si K est commutatif, tout sous-groupe fini de $(K^*, .)$ est cyclique.
- Si K est fini, $(K^*, .)$ est cyclique (conséquence directe du précédent et de Wedderburn).

VI. Exercices

On travaille a priori dans un anneau A non nul, commutatif et unitaire.

① REMISE À NIVEAU

1.1. Soit deux anneaux A et B et une application $\varphi : A \to B$ vérifiant : • *(i)* $\varphi(x + y) = \varphi(x) + \varphi(y)$
• *(ii)* $\varphi(x.y) = \varphi(x).\varphi(y)$.

Voici trois démonstrations de : $\varphi(1_A) = 1_B$.
Démonstration 1 :
Étant donné un inversible u de A : $\varphi(1_A) = \varphi(u.u^{-1}) = \varphi(u)\varphi(u^{-1}) = \varphi(u)\varphi(u)^{-1} = 1_B$.
Démonstration 2 :
$\varphi(1_A) = \varphi(1_A.1_A) = \varphi(1_A).\varphi(1_A)$.
En simplifiant par $\varphi(1_A)$, on obtient : $\varphi(1_A) = 1_B$.
Démonstration 3 :
Pour tout a de A : $\varphi(a) = \varphi(1_A.a) = \varphi(1_A)\varphi(a)$.
Par conséquent, $\varphi(1_A)$ est neutre pour la loi $.$ de B, donc c'est 1_B.
Ces trois démonstrations sont bien sûr fausses, puisqu'on a vu en **I** ④ **4.1.** que « $\varphi(1_A) = 1_B$ » est indépendant de *(i)* et *(ii)*.
a) Trouver l'erreur dans chacune d'elle.
b) Trouver celle que l'on peut adapter pour démontrer : $\varphi(0_A) = 0_B$.

1.2. *a)* Montrer que $\{0\}$, muni de $+$ et $.$ définies par : $0 + 0 = 0$ et $0.0 = 0$, est un anneau unitaire.
b) Montrer que si $0_A = 1_A$, alors A est l'anneau nul.

1.3. X étant un ensemble infini, on munit $\mathcal{P}(X)$ de la loi Δ définie par : $A\Delta B = (A \cup B) - (A \cap B)$ (**différence symétrique**).
Montrer que $(\mathcal{P}(X), \Delta, \cap)$ est un anneau, et que, bien qu'infini, il est de caractéristique 2.

1.4. Montrer que $\mathbb{Z}$ est le seul sous-anneau de $\mathbb{Q}$ qui ne soit pas dense dans $\mathbb{Q}$.
(On pourra utiliser le fait qu'un sous-groupe de $(\mathbb{Q}, +)$ est soit dense, soit de la forme $x\mathbb{Z}$ avec $x \in \mathbb{Q}^+$.)

1.5. Soit un groupe commutatif G.
Montrer que $(End(G), +, \circ)$ est un anneau. Est-il unitaire ? intègre ?

1.6. Montrer que si un idéal I contient 1_A, alors : $I = A$.
En déduire que si un idéal I contient un inversible, alors : $I = A$.

1.7. On définit sur $\mathbb{R}$ les lois : $x \oplus y = x + y + 1$, et : $x \otimes y = x + y - xy$.
Montrer que $(\mathbb{R}, \oplus, \otimes)$ est un corps commutatif.

② LES CLASSIQUES À CONNAÎTRE

2.1. Soit A non nécessairement commutatif.
Montrer que : $(1 - ab)$ inversible $\Rightarrow (1 - ba)$ inversible.
(On pourra procéder par analyse-synthèse, en tentant d'exprimer l'inverse de $(1 - ba)$, supposé inversible, en fonction de l'inverse de $(1 - ab)$, quitte à se placer momentanément dans un espace dans lequel $(1 - ba)^{-1}$ est la somme d'une série !)

2.2. Éléments nilpotents

A est ici un anneau non nécessairement commutatif.

On dit que x est **nilpotent** s'il existe $n \in \mathbb{N}^*$ tel que : $x^n = 0$. L'**indice de nilpotence** de x est l'entier k tel que : $x^k = 0$ et $x^{k-1} \neq 0$.

1. Quels sont les éléments nilpotents d'un anneau intègre ?

2. Montrer que : xy nilpotent $\Rightarrow yx$ nilpotent.

3. Soit x et y nilpotents et commutant.

Montrer que $(x + y)$ et xy sont aussi nilpotents.

4. Montrer que : x nilpotent $\Rightarrow (1 - x)$ inversible.

5. On appelle **nilradical** de A anneau commutatif l'ensemble $Nil(A)$ formé de des éléments nilpotents de A.

Montrer que $Nil(A)$ est un idéal de A.

6. Endomorphismes nilpotents :

Soit u endomorphisme de l'anneau $(\mathcal{L}(E), +, \circ)$, où E de dimension finie.

a) Quelles sont les valeurs propres de u, s'il est nilpotent ?

b) Montrer que : u nilpotent $\Leftrightarrow u^{\dim(E)} = 0$.

(1ère méthode : montrer qu'on peut trouver une famille $(x, u(x), u^2(x), \ldots, u^{p-1}(x))$***, où*** p ***indice de nilpotence, est libre.***

2ème méthode : appliquer le théorème de Cayley-Hamilton.)

c) En déduire que l'ensemble des endomorphismes nilpotents est un fermé.

d) Montrer que : u nilpotent $\Rightarrow$ il existe une base dans laquelle la matrice de u est triangulaire de diagonale nulle.

2.3. Radical d'un idéal

On appelle **radical** d'un idéal I l'ensemble $\sqrt{I} = \{x \in A \,;\, \exists\, n \in \mathbb{N}^* \,;\, x^n \in I\}$.

a) Montrer que $\sqrt{I}$ est un idéal de A.

b) Déterminer le radical d'un idéal $n\mathbb{Z}$ de $\mathbb{Z}$.

(Après avoir étudié les cas $n = 0$ ***et*** $n = 1$***, on montrera que le radical de*** $n\mathbb{Z}$ ***est*** $p_1 \ldots p_k\mathbb{Z}$ ***si la décomposition primaire de*** n ***est*** $p_1^{\alpha_1} \ldots p_k^{\alpha_k}$***.)***

c) Déterminer le radical de $\{0_A\}$.

d) Montrer que, si I et J sont des idéaux tels que : $I \subset J$, on a : $\sqrt{I} \subset \sqrt{J}$.

En déduire que $\sqrt{\sqrt{I}} = \sqrt{I}$.

e) Montrer que, si I et J sont des idéaux, on a :

$$\sqrt{I} \cap \sqrt{J} = \sqrt{I \cap J} \,;\, \sqrt{I} + \sqrt{J} \subset \sqrt{I + J} \,;\, \sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}.$$

2.4. Anneaux de Boole

On appelle **anneau de Boole** un anneau A dont tout élément est idempotent ($\forall\, x \in A \,;\, x^2 = x$).

a) De l'idempotence de $(x + x)$, déduire que A est de caractéristique 2.

b) De l'idempotence de $(x + y)$, déduire que A est commutatif.

c) Montrer que pour tout x, y de A : $xy(x + y) = 0$.

Montrer que, si A est intègre, il a au plus 2 éléments.

☝ L'anneau à deux éléments n'est autre que le corps $\mathbb{F}_2$.

On note parfois ses éléments en utilisant les *booléens* `faux` (pour 0) et `vrai` (pour 1). L'addition est alors la conjonction (`and`) et la multiplication est la disjonction exclusive (`xor`).

d) Montrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau de Boole.

2.5. Soit $\alpha \in \mathbb{Q}^{+}{}^*$ tel que $\sqrt{\alpha} \notin \mathbb{Q}$.

On pose $\mathbb{Q}(\sqrt{\alpha}) = \{x + y\sqrt{\alpha} \,;\, x, y \in \mathbb{Q}\}$.

a) Montrer que $\mathbb{Q}(\sqrt{\alpha})$, muni des lois usuelles, est un corps.

b) Montrer que $\mathbb{Q}^2$ et $\mathbb{Q}(\sqrt{\alpha})$ ne sont pas isomorphes.

c) Montrer que $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$ ne sont pas isomorphes.

(On pourra étudier ce que deviendrait la relation $(\sqrt{2})^2 - 2 = 0$***, transportée dans*** $\mathbb{Q}(\sqrt{3})$ ***par un éventuel isomorphisme.)***

③ AUTRES EXERCICES

3.1. Anneau simple qui n'est pas un corps

Soit I un idéal bilatère non nul de l'anneau $\mathcal{M}_2(\mathbb{R})$ et posons $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$ un élément non nul de I.

a) Montrer que : $a \neq 0 \Rightarrow I = A$.

(Utiliser la première question de l'exercice 1.6.***)***

b) Montrer qu'on peut se ramener au *a)* si b, c ou d est non nul.

c) Montrer que $\mathcal{M}_2(\mathbb{R})$ n'est pas un corps.

3.2. L'anneau $\mathcal{C}^\infty(\mathbb{R})$

Soit l'anneau $\mathcal{C}^\infty(\mathbb{R})$ des fonctions de classe C^∞ de $\mathbb{R}$ dans lui-même.

a) Montrer que l'ensemble des fonctions nulles en 0 est un idéal maximal.

b) Montrer que $\{f \in \mathcal{C}^\infty(\mathbb{R}) \,;\, \forall\, k \in \mathbb{N}^* \,;\, f^{(k)}(0) = 0\}$ est un idéal premier.

VII. Sujet d'étude

ANNEAUX D'ENTIERS QUADRATIQUES

1. Soit $\mathbb{Z}[\sqrt{-5}] = \{a + ib\sqrt{5};\ a, b \in \mathbb{Z}\}$.

On pose N : $\mathbb{Z}[\sqrt{-5}] \to \mathbb{N}$

$z = a + ib\sqrt{5} \mapsto |z|^2 = (a + ib\sqrt{5})(a - ib\sqrt{5}) = a^2 + 5b^2$.

a) Pourquoi $\mathbb{Z}[\sqrt{-5}]$ est-il intègre ?

b) Montrer que $\mathcal{U}(\mathbb{Z}[\sqrt{-5}]) = \{1, -1\}$.

(Montrer que pour tout z inversible, on a $N(z) = 1$.)

c) Montrer que les nombres 2, 3, $(1 + i\sqrt{5})$ et $(1 - i\sqrt{5})$ sont irréductibles.

d) En déduire que $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel.

e) Montrer que 2, bien qu'irréductible, n'est pas premier.

f) Montrer que $2(1 + i\sqrt{5})$ et $(1 + i\sqrt{5})(1 - i\sqrt{5})$ n'ont pas de *pgcd* dans $\mathbb{Z}[\sqrt{-5}]$.

2. Soit $\mathbb{Z}[i] = \{a + ib;\ a, b \in \mathbb{Z}\}$, appelé **anneau des entiers de Gauss**.

On pose $N : \mathbb{Z}[i] \to \mathbb{N}$

$z \mapsto |z|^2$.

a) Pourquoi $\mathbb{Z}[i]$ est-il intègre ?

b) Montrer que $\mathcal{U}(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

(Montrer que pour tout z inversible, on a $N(z) = 1$.)

c) α) Montrer que, pour p entier premier : p irréductible dans $\mathbb{Z}[i] \Leftrightarrow p$ n'est pas de la forme $N(z)$.

β) Soit z non associé, dans $\mathbb{Z}[i]$, à un entier.

Montrer que : z irréductible dans $\mathbb{Z}[i] \Leftrightarrow N(z)$ premier dans $\mathbb{Z}$.

γ) En déduire les irréductibles de $\mathbb{Z}[i]$.

d) Montrer que $\mathbb{Z}[i]$ est euclidien.

(Former le quotient complexe de z par z', en déduire le quotient euclidien dans $\mathbb{Z}[i]$. Le stathme est N.)

3. Soit $\mathbb{Z}[j] = \{a + jb;\ a, b \in \mathbb{Z}\}$, où $j = \frac{1}{2} + i\frac{\sqrt{3}}{2}$.

On pose N : $\mathbb{Z}[j] \to \mathbb{N}$

$z = a + jb \mapsto (a + jb)(a + j^2 b) = a^2 - ab + b^2$.

a) Montrer que N est une norme algébrique :

- *(i)* Pour tout z : $N(z) \geq 0$.
- *(ii)* $N(z) = 0 \Rightarrow z = 0$.
- *(iii)* Pour tous z et z' : $N(zz') = N(z)N(z')$.

b) Quels sont les inversibles de $\mathbb{Z}[j]$?

c) Montrer que $\mathbb{Z}[j]$ est euclidien de stathme N.

Bibliographie

Carrega	*Théorie des corps*	Hermann	Cours sur les corps en vue de l'étude détaillée des constructions à la règle et au compas, applications aux problèmes de géométrie grecs.
Demazure	*Cours d'algèbre*	Cassini	Cours sur les anneaux de l'Ecole Polytechnique. Très complet et agréable à lire.
Francinou, Gianella	*Exercices de mathématiques pour l'agrégation*	Masson	Cours succinct sur les anneaux et les corps, des exercices très variés, certains traitant d'anneaux et corps théoriques, d'autres étudiant des exemples classiques. Nilradical, anneaux de Boole, entiers de Gauss, corps finis, points constructibles à la règle et au compas.
Gourdon	*Algèbre*	Ellipses	Théorie succincte , radical, anneau de Boole, entiers de Gauss.
Hauchecorne	*Les contre-exemples en mathématiques*	Ellipses	Pas de cours mais l'essentiel des exemples illustrant les implications strictes.
Lafon	*Algèbre*	Hermann	Résumé de cours sur les anneaux et les corps, exercices variés et intéressants, $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$, anneau de Boole, corps des quaternions
Mazet	*Algèbre et géométrie pour le CAPES et l'agrégation*	Ellipses	Pas d'exercices, mais un cours très complet, pédagogiques, avec beaucoup d'exemples et de contre-exemples permettant une bonne culture.
Merlin	*Méthodix – Algèbre*	Ellipses	Pour les matrices nilpotentes
Monnier	*Algèbre - Tome 1*	Dunod	Exercices nombreux et variés, peu de classiques, corrections rapides.
Naudin, Quitté	*Algorithmique algébrique*	Masson	Cours complet sur les anneaux, peu de choses sur les corps. Anneaux d'entiers quadratiques,