Chapitre 1

Anneaux

La plupart des démonstrations des résultats enoncés dans ce cours sera faite en classe. Certaines d'entre elles seront laissées aux étudiants sous forme d'exercices.

1. Premières définitions

Définition 1

Une loi de composition interne (l.c.i) sur un ensemble E est une application $(x,y)\mapsto x\star y$ de $E\times E\to E$. Cette loi est dite **associative** si

$$\boxed{(x\star y)\star z = x\star(y\star z) \quad \text{pour tous } x,y,z\in E.}$$

Elle est dite **commutative** si

$$\boxed{x\star y = y\star x \quad \text{pour tous } x,y\in E.}$$

Exemple 1

Dans $\mathbb{N}$, l'addition $+$ et la multiplication $\times$ sont des lois de composition internes. La soustraction est une loi de composition interne sur $\mathbb{Z}$ mais pas sur $\mathbb{N}$.

Exemple 2

Dans $\mathbb{R}$, la loi $\star$ définie par $x\star y = x^2+y^2$ est commutative mais non associative. La loi $*$ définie par $x*y = x$ est associative mais non commutative. La loi $\diamondsuit$ définie par $x\diamondsuit y = -x$ n'est ni commutative ni associative.

Définition 2

Un élément **neutre** pour une l.c.i $\star$ sur E est un élément $e\in E$ vérifiant :

$$\boxed{x\star e = e\star x = x \quad \text{pour tout } x\in E\ .}$$

Lorsqu'il existe, un tel élément est **unique** et s'appelle **l'élément neutre** de la loi $\star$.

Exemple 3

Dans $\mathbb{N}$, les lois + et × ont 0 et 1 comme éléments neutres respectifs. Les trois lois définies sur $\mathbb{R}$ dans l'exemple 2 n'ont pas d'élément neutre .

Définition 3

Soit E un ensemble muni d'une loi $\star$ et admettant un élément neutre e. On dit qu'un élément $x \in E$ est **inversible** s'il existe $x' \in E$ tel que

$$x \star x' = x' \star x = e.$$

Dans ce cas, on dit que x' est un **inverse** de x.

Proposition 1

Soit E ensemble muni d'une loi $\star$ **associative** et admettant un élément neutre e. Alors tout élément inversible admet un **unique** inverse.

Remarque 1

Lorsqu'une loi est notée additivement : + , on notera par 0 son élément neutre. Dans ce cas, l'inverse d'un élément x (lorsqu'il existe) sera noté $-x$ et s'appellera l'opposé de x. Lorsque la loi est notée multiplicativement : ×, on désignera l'élément neutre par 1 et l'inverse de x par x^{-1}.

Définition 4

Un **groupe** est un ensemble G muni d'une l.c.i notée + telle que :

1. la loi + est **associative**
2. la loi + admet un **élément neutre**
3. tout élément de G est **inversible.**

Un tel groupe sera noté $(G,+)$ lorsque l'on veut préciser sa loi +. Si la loi + est commutative, on dit que le groupe est commutatif ou abélien.

Exemple 4

$(\mathbb{Z},+)$ est un groupe. Ce n'est pas le cas de $(\mathbb{Z},\times)$.

Définition 5

Un **anneau** est un ensemble $\mathscr{A}$ muni de deux l.c.i notées + et × telles que :

1. $(\mathscr{A},+)$ est un **groupe abélien**
2. la loi × est **associative** et admet un **élément neutre** appelé **l'unité** de $\mathscr{A}$.
3. la loi × est **distributive** par rapport à la loi + :

$$a \times (b+c) = a \times b + a \times c \quad \text{et} \quad (b+c) \times a = b \times a + c \times a \quad \text{pour tous } a,b,c \in \mathscr{A}.$$

On écrira $(\mathscr{A}, +, \times)$ lorsqu'on veut préciser les lois d'un anneau $\mathscr{A}$.

Remarque 2

Comme mentionné plus haut, avec les notations additives et multiplicatives, l'élément neutre de la loi + sera noté 0 et celui de la loi × sera noté 1. Nous utiliserons également la notation $a \cdot b$ ou ab pour désigner $a \times b$. Parfois, pour éviter les confusions lorsqu'il y a plusieurs anneaux, on notera $0_{\mathscr{A}}$ et $1_{\mathscr{A}}$ les éléments neutres de $\mathscr{A}$. Dans la suite les lois des tous les anneaux seront notées additivement et multiplicativement.

Un anneau $(\mathscr{A}, +, \times)$ dont la deuxième loi × est **commutative** sera dit un **anneau commutatif**.

Exemple 5

1. $\mathscr{A} = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ muni de l'addition et la multiplication ordinaires est un anneau commutatif.
2. On considère l'ensemble $\mathbb{Z}/p\mathbb{Z}$ des classes de congruence modulo p où p est un entier naturel non nul. On rappelle que

$$\mathbb{Z}/p\mathbb{Z} = \left\{ \overline{x} \;/\; x = 0, 1, \cdots, p-1 \right\}$$

   où $\overline{x}$ désigne la classe d'équivalence de x. On définit l'addition et la multiplication dans $\mathbb{Z}/p\mathbb{Z}$ par $\overline{x} + \overline{y} = \overline{z}$ où $z = x + y$ et $\overline{x} \times \overline{y} = \overline{t}$ où $t = xy$. Il n'est pas difficile de vérifier que ces deux lois sont bien définies et que $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un anneau commutatif.
3. $\mathscr{M}_n(\mathbb{R})$ muni de l'addition et produit usuels des matrices est un anneau non commutatif.
4. $\mathbb{K}[X]$ avec $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, est un anneau lorsqu'il est muni de l'addition et multiplication usuelles des polynômes (voir section 3 ci-dessous).
5. Si $\mathscr{A}$ est un anneau commutatif, on considère l'ensemble $\mathscr{A}[X]$ des polynômes à coefficients dans $\mathscr{A}$. On peut vérifier que $\mathscr{A}[X]$ est un anneau commutatif lorsqu'il est muni de l'addition et la multiplication usuelles des polynômes (voir section 3 ci-dessous).
6. Soit $A \subset \mathbb{R}$ et soit $\mathscr{A} = C^0(A)$ l'ensemble des fonctions continues de A dans $\mathbb{R}$, muni de l'addition et multiplication usuelles des fonctions numériques. Il est facile de vérifier qu'il s'agit d'un anneau commutatif ayant pour unité la fonction $x \mapsto 1$.

Remarque 3

Les propriétés suivantes découlent immédiatement de la définition d'un anneau :

1. $0 \cdot a = a \cdot 0 = 0$ pour tout $a \in \mathscr{A}$. (On dit que 0 est absorbant).
2. Si $1 = 0$, alors l'anneau est trivial, i.e $\mathscr{A} = \{0\}$.

3. On définit pour tout $m \in \mathbb{Z}$ et tout $a \in \mathscr{A}$:

$$ma = \begin{cases} \underbrace{a + \cdots + a}_{m-fois} & \text{si } m > 0 \\ 0 & \text{si } m = 0 \\ -\underbrace{(a + \cdots + a)}_{|m|-fois} & \text{si } m < 0. \end{cases}$$

On a $(m+n)a = ma + na$, $m(a+b) = ma + mb$, $m(na) = n(ma) = (mn)a$ pour tous $a, b \in \mathscr{A}$ et $m, n \in \mathbb{Z}$.

4. On définit pour tout $m \in \mathbb{N}$ et tout $a \in \mathscr{A}$:

$$a^m = \begin{cases} \underbrace{a \times \cdots \times a}_{m-fois} & \text{si } m \neq 0 \\ 1 & \text{si } m = 0. \end{cases}$$

On a $a^{m+n} = a^m a^n$, $(a^m)^n = (a^n)^m = a^{mn}$ pour tous $a \in \mathscr{A}$ et $m, n \in \mathbb{N}$.

Nous avons la formule très utile suivante :

Proposition 2. (Formule du Binôme)

Dans un anneau $\mathscr{A}$, si $a, b \in \mathscr{A}$ **commutent**, i.e $ab = ba$, alors on a

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

Définition 6

Dans un anneau $\mathscr{A}$, un élément $a \in \mathscr{A}$ est dit **inversible** s'il existe $b \in \mathscr{A}$ tel que

$$\boxed{ab = ba = 1.}$$

Dans ce cas b est **unique**, on l'appelle **l'inverse** de a et on le note a^{-1}.

Nous avons la propriété suivante concernant les éléments inversibles :

Proposition 3

L'ensemble $\mathscr{A}^*$ constitué des éléments inversibles de $\mathscr{A}$ muni de la loi $\times$ est un groupe avec la formule

$$\boxed{(ab)^{-1} = b^{-1}a^{-1}.}$$

Exemple 6

1. Les élément inversibles de $\mathbb{Z}$ sont -1 et 1.
2. Les élément inversibles de $\mathbb{Z}/3\mathbb{Z}$ sont $\overline{1}$ et $\overline{2}$.
3. Les élément inversibles de $\mathbb{R}[X]$ sont les polynômes constants non nuls. Les éléments inversibles de $\mathbb{Z}[X]$ sont les polynômes constants -1 et 1.

Définition 7

Un **corps** est un anneau non trivial (contient au moins deux éléments) dans lequel tout élément **non nul** est **inversible**. Autrement dit, un corps est un anneau $\mathscr{A}$ tel que $\mathscr{A} \setminus \{0\} = \mathscr{A}^*$.

Exemple 7

1. $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ est un corps. $\mathbb{K}[X]$ n'est pas un corps.
2. L'anneau $\mathbb{Z}/3\mathbb{Z}$ vu plus haut est un corps. Plus généralement (voir proposition 4 ci-dessous) si p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps.

Définition 8

Un anneau **intègre** est un anneau dans lequel la propriété suivante est vérifiée :

$$ab = 0 \implies a = 0 \text{ ou } b = 0.$$

Remarque 4

1. Dans un anneau intègre $\mathscr{A}$, il n'y a pas de diviseur de 0. On dit qu'un élément $a \in \mathscr{A} \setminus \{0\}$ est un diviseur de 0 s'il existe $b \in \mathscr{A} \setminus \{0\}$ tel que $ab = 0$ ou $ba = 0$.
2. Un corps est clairement un anneau intègre.

Nous avons la propriété suivante concernant l'anneau $\mathbb{Z}/p\mathbb{Z}$:

Proposition 4

Les trois propriétés suivantes sont équivalentes :

1. $\mathbb{Z}/p\mathbb{Z}$ est un corps
2. $\mathbb{Z}/p\mathbb{Z}$ est un anneau intègre
3. p est premier.

Définition 9

Un élément a d'un anneau $\mathscr{A}$ est dit **nilpotent** (resp. **idempotent**) s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$ (resp. si $a^2 = a$).

Exemple 8

1. Dans tout anneau, 0 est toujours nilpotent et idempotent. L'élément 1 est toujours idempotent. Dans un anneau intègre, le seul élément nilpotent est 0, et les seuls éléments idempotents sont 0 et 1.

2. Dans $\mathbb{Z}/4\mathbb{Z}$ le seul élément nilpotent non nul est $\overline{2}$. Dans $\mathbb{Z}/6\mathbb{Z}$, les éléments idempotents sont $\overline{1}$, $\overline{3}$, $\overline{4}$.

2. Anneaux des polynômes

Habituellement les polynômes à coefficients dans les corps des nombres sont vus comme des fonctions polynomiales. Mais si on veut étudier les polynômes à coefficients dans des corps (ou anneaux) plus généraux, cette identification avec des fonctions n'est pas pertinente car deux polynômes distincts pourraient déterminer une même fonction polynomiale. Par exemple, dans $(\mathbb{Z}/2\mathbb{Z})[X]$ les deux polynômes X et X^2 sont clairement distincts (puisque de degrés distincts) et pourtant ils déterminent la même fonction de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}$. C'est pour cela qu'il serait plus judicieux de définir un polynôme par la suite de ses coefficients et non pas par la fonction polynomiale qu'il détermine.

Une suite à support fini dans un anneau commutatif $\mathscr{A}$ est une suite $(a_0,\cdots,a_n,\cdots)$ d'élements de $\mathscr{A}$ telle que tous les termes sont nuls à partir d'un certain rang, i.e il exsite $n_0 \in \mathbb{N}$ tel que $a_n = 0$ pour tout $n \geqslant n_0$. Sur l'ensemble de telles suites on définit une addition et une multplication par

$$(a_0,\cdots,a_n,\cdots)+(b_0,\cdots,b_n,\cdots)=(a_0+b_0,\cdots,a_n+b_n,\cdots)$$

et

$$(a_0,\cdots,a_n,\cdots)\times(b_0,\cdots,b_n,\cdots)=(c_0,\cdots,c_n,\cdots),\quad c_k=\sum_{i+j=k}a_ib_j$$

qui ont pour éléments neutres

$$0=(0,\cdots,0,\cdots)\ \text{ et }\ 1=(1,0,\cdots,0,\cdots).$$

Définition 10

Un polynôme à une indéterminée à coefficients dans $\mathscr{A}$ est une suite d'éléments de $\mathscr{A}$ à support fini. L'ensemble de ces polynômes est noté $\mathscr{A}[X]$. Muni des opérations définies ci-dessus, $\mathscr{A}[X]$ est un anneau commutatif.

Si on pose $X=(0,1,0,\cdots,\cdots)$, alors tout polynôme $P=(a_0,\cdots,a_n,0,\cdots)$ s'écrit

$$P=a_01+a_1X+a_2X^2+\cdots+a_nX^n.$$

On retrouve ainsi l'écriture habituelle des polynômes avec la notation $a_0 = a_01$. Les polynômes de la forme aX^k, $a \in \mathscr{A}$, $k \in \mathbb{N}$, s'appellent des **monômes**. Si P est différent du polynôme nul, on définit le **degré** de P comme étant le plus grand entier $i \in \mathbb{N}$ tel que $a_i \neq 0$. Par convention le degré du polynôme nul est égal à $-\infty$. Le degré d'un polynôme P sera noté $\deg P$.

Remarque 5

Comme nous l'avons déjà signalé plus haut, un polynôme $P = a_0 + \cdots + a_n X^n$ détermine une fonction (dite polynomiale) : $x \mapsto a_0 + \cdots + a_n x^n$ de $\mathscr{A} \to \mathscr{A}$. Par abus de notation cette fonction sera notée aussi P, tout en gardant à l'esprit qu'il ne s'agit pas d'une identification car deux polynômes distincts pourraient donner lieu à la même fonction polynomiale.

Proposition 5

Soient $P, Q \in \mathscr{A}[X]$. Alors on a

$$\boxed{\deg(P+Q) \leqslant \operatorname{Max}\big(\deg P, \deg Q\big).}$$

Si l'anneau $\mathscr{A}$ est intègre, nous avons la proposition suivante :

Proposition 6

Si $\mathscr{A}$ est intègre, alors pour tous $P, Q \in \mathscr{A}[X]$, on a

$$\boxed{\deg(PQ) = \deg P + \deg Q.}$$

Une conséquence directe de la proposition 2 est le corollaire suivant :

Corollaire 1

L'anneau $\mathscr{A}[X]$ est intègre si et seulement si l'anneau $\mathscr{A}$ est intègre.

Définition 11

Soit P un polynôme non nul de degré n, i.e $P = a_0 + \cdots + a_n X^n$ avec $a_n \neq 0$. Le monôme $a_n X^n$ s'appelle monôme **dominant** de P.

Le théorème suivant est l'un des résultats les plus importants dans l'anneau des polynômes :

Théorème 1. (Divsion euclidienne)

Soient $A, B \in \mathscr{A}[X]$ avec $B \neq 0$. On suppose de plus que le coefficient du monôme dominant de B est inversible. Alors il existe un unique couple $(Q, R) \in \mathscr{A}[X] \times \mathscr{A}[X]$ vérifiant

$$\boxed{A = BQ + R \quad \text{et} \quad \deg R < \deg B.}$$

Les polynômes Q et R s'appellent respectivement quotient et reste de la division euclidienne de A par B.

Nous avons le corollaire suivant :

Corollaire 2

Si $\mathscr{K}$ est un corps, alors pour tous $A, B \in \mathscr{K}[X]$ avec $B \neq 0$, il existe un unique couple $(Q,R) \in \mathscr{K}[X] \times \mathscr{K}[X]$ tel que

$$A = BQ + R \quad \text{et} \quad \deg R < \deg B.$$

3. Sous-anneaux, anneaux engendrés

Définition 12

Un **sous-anneau** d'un anneau $(\mathscr{A}, +, \times)$ est un sous-ensemble $\mathscr{A}' \subset \mathscr{A}$ tel que les lois + et × sont aussi des l.c.i sur $\mathscr{A}'$ et $(\mathscr{A}', +, \times)$ est un anneau ayant pour unité $1_{\mathscr{A}}$ (l'unité de $\mathscr{A}$).

Nous avons la caractérisation très pratique suivante :

Proposition 7

Un sous-ensemble $\mathscr{A}'$ d'un anneau $\mathscr{A}$ est un sous-anneau ssi

1. $1_{\mathscr{A}} \in \mathscr{A}'$
2. pour tous $a, b \in \mathscr{A}'$, on a $a - b \in \mathscr{A}'$ et $ab \in \mathscr{A}'$.

Exemple 9

1. $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$ qui est un sous-anneau de $\mathbb{R}$ qui est un sous-anneau de $\mathbb{C}$.
2. Le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$.
3. $\mathbb{R}[X]$ est un sous-anneau de $\mathbb{C}[X]$.

Remarque 6

Il découle directement de la proposition ci-dessus qu'un sous-anneau de $(\mathscr{A}, +, \times)$ est en particulier un **sous-groupe** de $(\mathscr{A}, +)$. On rappelle qu'un sous-groupe d'un groupe $(G, +)$ est un sous-ensemble non vide $G' \subset G$ stable par rapport à la loi + tel que pour tout $x \in G'$, on ait $-x \in G'$.

Un sous-anneau hérite de certaines propriétés de l'anneau dont il est issu :

Proposition 8

Un sous-anneau d'un anneau intègre est un annaeu intègre. Un sous-anneau d'un anneau commutatif est commutatif.

La propriété suivante nous permettra de définir des nouveaux sous-anneaux d'un anneau donné :

Proposition 9

Soit $(\mathscr{A}_i)_{i\in I}$ une famille de sous-anneau d'un anneau $\mathscr{A}$. Alors $\bigcap_{i\in I}\mathscr{A}_i$ est un sous-anneau de $\mathscr{A}$.

Remarque 7

Contrairement à l'intersection, l'union de deux sous-anneaux n'est pas nécessairement un sous-anneau. On peut le vérifier facilement en considérent les sous-anneaux $\mathbb{Z}[\sqrt{2}]$ et $\mathbb{Z}[\sqrt{3}]$ de $\mathbb{R}$ (voir la définition de $\mathbb{Z}[\sqrt{p}]$ dans la remarque 8 ci-dessous.).

La proposition précédente nous permet de définir :

Définition 13

Soit E un sous-ensemble d'un anneau $\mathscr{A}$. L'intersection de tous les sous-anneaux de $\mathscr{A}$ qui contiennent E est un sous-anneau de $\mathscr{A}$ appelé sous-anneau **engendré** par E. Il s'agit du **plus petit** sous-anneau de $\mathscr{A}$ (au sens de l'inclusion) contenant $\mathscr{A}$.

Remarque 8

1. Lorsque $E=\emptyset$ dans la définition précédente, on obtient $\mathscr{A}_0$ le plus petit sous-anneau de $\mathscr{A}$. On l'appelle le sous-anneau premier de $\mathscr{A}$. On peut vérifier facilement que
$$\boxed{\mathscr{A}_0=\{\, m1_{\mathscr{A}} \;/\; m\in\mathbb{Z}\,\}.}$$
Par exemple, le sous-anneau premier de $\mathbb{R}$ est $\mathbb{Z}$ qui est également le sous-anneau premier de $\mathbb{C}$.
2. On peut vérifier que le sous-anneau engendré par un sous-ensemble E est le même que celui engendré par $E\cup\mathscr{A}_0$. C'est pour cela, en analogie avec l'anneau des polynômes, que l'on note le sous-anneau engendré par E par $\mathscr{A}_0[E]$.
3. Le sous-anneau engendré par un singleton $E=\{x\}$, noté $\mathscr{A}_0[x]$ est :
$$\boxed{\mathscr{A}_0[x]=\left\{\, m_0 1_{\mathscr{A}}+m_1x+m_2x^2+\cdots+m_kx^k \;/\; k\in\mathbb{N},\ m_j\in\mathbb{Z},\ j=0,\cdots k\,\right\}.}$$

En particulier, pour $p\in\mathbb{N}$, on obtient $\mathbb{Z}[\sqrt{p}]=\left\{\, a+b\sqrt{p},\ a,b\in\mathbb{Z}\,\right\}$ comme sous-anneau de $\mathbb{R}$ engendré par $E=\{\sqrt{p}\}$. Si $p\in\mathbb{Z}$ avec $p<0$, en posant $\sqrt{p}=i\sqrt{|p|}$, on a $Z[\sqrt{p}]=\left\{\, a+b\sqrt{p},\ a,b\in\mathbb{Z}\,\right\}$ comme sous-anneau de $\mathbb{C}$ engendré par $E=\{\sqrt{p}\}$.

4. Morphismes d'anneaux, anneaux produits

Définition 14

Soient $\mathscr{A}$ et $\mathscr{B}$ deux anneaux. Un **morphisme** (ou homomorphisme) de $\mathscr{A}$ dans $\mathscr{B}$ est une application $\varphi:\mathscr{A}\to\mathscr{B}$ vérifiant :

1. $\varphi(1_{\mathscr{A}})=1_{\mathscr{B}}$.
2. $\varphi(a+b)=\varphi(a)+\varphi(b)$ et $\varphi(ab)=\varphi(a)\varphi(b)$ pour tous $a,b\in\mathscr{A}$.

Un **isomorphisme** est un morphisme bijectif.

Il découle immédiatement de la définition d'un morphisme $\varphi : \mathscr{A} \to \mathscr{B}$ que $\varphi(0_{\mathscr{A}}) = 0_{\mathscr{B}}$, $\varphi(-x) = -\varphi(x)$ et que si x est inversible, alors $\varphi(x)$ est inversible avec $\varphi(x^{-1}) = \big(\varphi(x)\big)^{-1}$.

La proposition suivante nous dit que l'application réciproque d'un morphisme d'anneaux est un morphisme d'anneaux :

Proposition 10

Si $\varphi : \mathscr{A} \to \mathscr{B}$ un isomorphisme, alors $\varphi^{-1} : \mathscr{B} \to \mathscr{A}$ est un isomorphisme de $\mathscr{B}$ dans $\mathscr{A}$.

Exemple 10

1. L'application $\varphi : \mathbb{R}[X] \to \mathbb{R}$ définie par $\varphi(P) = P(0)$ est un morphisme qui n'est pas un isomorphisme.
2. L'application $\varphi : \mathbb{Z}\left[\sqrt{2}\right] \to \mathbb{Z}\left[\sqrt{2}\right]$ définie par $\varphi\left(a + b\sqrt{2}\right) = a - b\sqrt{2}$ est un isomorphisme.
3. Il n'existe pas de morphisme d'anneaux entre $\mathbb{Z}\left[\sqrt{2}\right]$ et $\mathbb{Z}\left[\sqrt{3}\right]$.

Un isomorphisme d'anneaux préserve toutes les propriétés liées aux lois de composition internes d'un anneau :

Proposition 11

Supposons qu'il existe un isomorphisme φ entre deux anneaux $\mathscr{A}$ et $\mathscr{B}$. Alors on a :

1. $\mathscr{A}$ est commutatif $\iff$ $\mathscr{B}$ est commutatif.
2. $\mathscr{A}$ est intègre $\iff$ $\mathscr{B}$ est intgre.
3. Un élément $a \in \mathscr{A}$ est inversible $\iff$ $\varphi(a)$ est inversible.
4. Un élément $a \in \mathscr{A}$ est nilpotent $\iff$ $\varphi(a)$ est nilpotent.
5. Un élément $a \in \mathscr{A}$ est idempotent $\iff$ $\varphi(a)$ est idempotent.

Définition 15

Soit $\varphi : \mathscr{A} \to \mathscr{B}$ un morphisme d'anneaux. On définit le **noyau** de φ, noté $\ker \varphi$, par

$$\ker \varphi = \left\{ x \in \mathscr{A} \;/\; \varphi(x) = 0 \right\}.$$

On définit de même **l'image** de φ, noté $\operatorname{Im} \varphi$, par

$$\operatorname{Im} \varphi = \left\{ \varphi(x) \;/\; x \in \mathscr{A} \right\}.$$

Nous avons la proposition suivante :

Proposition 12

Soit $\varphi : \mathscr{A} \to \mathscr{B}$ un morphisme d'anneaux. Alors on a :

1. $\ker \varphi$ est un sous-groupe de $(\mathscr{A}, +)$.
2. $\mathrm{Im}\, \varphi$ est un sous-anneau de $\mathscr{B}$.
3. φ est injectif si et seulement si $\ker \varphi = \{0\}$.

Soit $\mathscr{A}$ un anneau et soit $\varphi : \mathbb{Z} \to \mathscr{A}$ définie par $\varphi(m) = m1$, $m \in \mathbb{Z}$. (ici $1 = 1_{\mathscr{A}}$). On vérifie facilement que φ est un morphisme d'anneaux et donc $\ker \varphi$ est un sous-groupe de $\mathbb{Z}$ d'après la proposition précédente. Or tous les sous-groupes de $\mathbb{Z}$ sont de la forme $p\mathbb{Z}$ avec $p \in \mathbb{N}$ (à faire en exercices). L'entier p s'appelle la **caractéristique** de l'anneau $\mathscr{A}$. S'il est non nul, il désigne ainsi le plus petit entier $m \in \mathbb{N}^*$ tel que $m1 = 0$. On verra plus loin que dans un anneau intègre, p est nécessairement un nombre premier.

On va introduire maintenant la notion d'anneau produit. Si $(\mathscr{A}_1, +, \times)$ et $(\mathscr{A}_2, +, \times)$ désignent deux anneaux, on définit sur l'ensemble produit $\mathscr{A}_1 \times \mathscr{A}_2$ les deux lois :

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \quad \text{pour tous } (a_1, a_2), (b_1, b_2) \in \mathscr{A}_1 \times \mathscr{A}_2.$$

et

$$(a_1, a_2) \times (b_1, b_2) = (a_1 \times b_1, a_2 \times b_2) \quad \text{pour tous } (a_1, a_2), (b_1, b_2) \in \mathscr{A}_1 \times \mathscr{A}_2.$$

Nous avons alors la proposition :

Proposition 13

Muni des deux lois définies ci-dessus, l'ensemble $\mathscr{A}_1 \times \mathscr{A}_2$ est un anneau ayant pour éléments neutres $0 = (0_{\mathscr{A}_1}, 0_{\mathscr{A}_2})$ et $1 = (1_{\mathscr{A}_1}, 1_{\mathscr{A}_2})$. De plus, on a les propriétés suivantes :

1. $\mathscr{A}_1 \times \mathscr{A}_2$ est commutatif $\iff$ $\mathscr{A}_1$ et $\mathscr{A}_2$ sont commutatifs.
2. Un élément $(a_1, a_2) \in \mathscr{A}_1 \times \mathscr{A}_2$ est inversible $\iff$ a_1 et a_2 sont inversibles.
3. $\mathscr{A}_1 \times \mathscr{A}_2$ n'est jamais intègre même si $\mathscr{A}_1$ et $\mathscr{A}_2$ le sont. (On suppose ici que les anneaux ne sont pas triviaux).

Il est facile de voir que les deux projections canoniques $P_1 : \mathscr{A}_1 \times \mathscr{A}_2 \to \mathscr{A}_1$ et $P_2 : \mathscr{A}_1 \times \mathscr{A}_2 \to \mathscr{A}_2$ définies respectivement par $P_1(a_1, a_2) = a_1$ et $P_2(a_1, a_2) = a_2$ sont des morphismes d'anneaux.

On définit d'une manière similaire l'anneau produit lorsqu'il s'agit d'une famille finie d'anneaux $\mathscr{A}_1, \cdots, \mathscr{A}_n$ et on obtient les mêmes propriétés que celles enoncées ci-dessus.

Chapitre 2

Ideaux

Dans tout ce qui suit, $\mathscr{A}$ désignera un anneau **commutatif non trivial** . Tous les annaux considérés dans ce chapitre seront supposés **commutatifs**.

1. Premières définitions

Définition 16

Soient $a, b \in \mathscr{A}$.

1. On dit que b **divise** a ou que b est un **diviseur** de a s'il existe $c \in \mathscr{A}$ tel que $a = bc$ et on notera dans ce cas $b \mid a$. On dit également que a est un **multiple** de b.
2. On dit que a et b sont **associés** et on notera $a \sim b$ si $a \mid b$ et $b \mid a$.

Il est facile de voir que la relation $a \sim b$ est une relation d'équivalence sur $\mathscr{A}$. Lorsque l'anneau $\mathscr{A}$ est intègre on a la caractérisation suivante :

Proposition 14

si $\mathscr{A}$ est intègre, deux éléments $a, b \in \mathscr{A}$ sont associés si et seulement s'il existe $u \in \mathscr{A}^*$ tel que $a = ub$.

Définition 17

Un **idéal** de $\mathscr{A}$ est un sous-ensemble $\mathscr{I} \subset \mathscr{A}$ vérifiant

1. $(\mathscr{I}, +)$ est un **sous-groupe** de $\mathscr{A}$
2. pour tout $a \in \mathscr{I}$ et tout $x \in \mathscr{A}$ on a $ax \in \mathscr{I}$.

On rappelle qu'un sous-groupe d'un groupe $(G, +)$ est un sous-ensemble non vide $G' \subset G$ vérifiant $a - b \in G'$ pour tous $a, b \in G'$.

Exemple 11

1. Dans un anneau $\mathscr{A}$ il y a au moins deux idéaux : l'idéal trivial $\{0\}$ et $\mathscr{A}$. De plus si $\mathscr{A}$ est un corps, ce sont les seuls idéaux de $\mathscr{A}$ (voir proposition 2 ci dessous)
2. Dans l'anneau $\mathbb{Z}$, les sous-ensembles $p\mathbb{Z} = \{ pk \ : \ k \in \mathbb{Z} \}$ avec $p \in \mathbb{N}$, sont des idéaux. On verra plus loin que ce sont les seuls idéaux de $\mathbb{Z}$.
3. Si $\varphi : \mathscr{A} \to \mathscr{B}$ est un morphisme d'anneaux, alors il est très facile de vérifier que $\ker \varphi$ est un idéal de $\mathscr{A}$.
4. Il découle directement de la définition que pour tout idéal $\mathscr{I}$ de $\mathscr{A}$, on a $0 \in \mathscr{I}$ et que si $1 \in \mathscr{I}$ alors $\mathscr{I} = \mathscr{A}$.

Il est facile de montrer la caractérisation suivante des idéaux :

Proposition 15

Un sous-ensemble non vide $\mathscr{I} \subset \mathscr{A}$ est un idéal si et seulement si

$$a_1x_1 + \cdots a_kx_k \in \mathscr{I} \quad \text{pour tous} \quad a_1, \cdots, a_k \in \mathscr{I} \quad \text{et tous} \quad x_1, \cdots, x_k \in \mathscr{A}.$$

Remarque 9

1. Pour tout élément $a \in \mathscr{A}$ l'ensemble noté $< a >$ défini par $< a > := \{ ax \ : \ x \in \mathscr{A} \}$ est un idéal de $\mathscr{A}$, on l'appelle **l'idéal engendré** par a (voir ci-dessous la notion d'idéal engendré par un sous-ensemble).
2. Il ne faut pas confondre la notion d'idéal de $\mathscr{A}$ et la notion de sous-anneau de $\mathscr{A}$. Les deux notions son différentes : aucune n'implique l'autre. Il est très facile de voir que le seul idéal de $\mathscr{A}$ qui est aussi un sous-anneau de $\mathscr{A}$ est $\mathscr{A}$.

La proposition suivante est très utile dans la pratique ; elle permet de montrer si un anneau est un corps en utilisant ses idéaux.

Proposition 16

$\mathscr{A}$ est un corps si et seulement si les seuls idéaux de $\mathscr{A}$ sont l'idéal trivial $\{0\}$ et $\mathscr{A}$.

Définition 18

Un idéal $\mathscr{I}$ de $\mathscr{A}$ est dit **principal** s'il existe $a \in A$ tel que $\mathscr{I} = < a >$.

Proposition 17

Si $a, b \in \mathscr{A}$, on a :

$$\boxed{< a > \subset < b > \iff a \in < b > \iff b \mid a.}$$

En particulier :

$$\boxed{< a > = < b > \iff a \sim b.}$$

Exemple 12

1. Tous les idéaux de l'anneau $\mathbb{Z}$ sont principaux car tous les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $p\mathbb{Z}$ avec $p \in \mathbb{N}$ (déjà vérifié en exercice). Comme on le verra ci-dessous, l'anneau $\mathbb{R}[X]$ possède également cette propriété.
2. Dans l'anneau $\mathbb{Z}[X]$, l'idéal $\mathscr{I} = \{ 2P + XQ \ : \ P, Q \in \mathbb{Z}[X] \}$ n'est pas principal.

Nous avons la propriété suivante concernant les idéaux de l'anneau $\mathbb{K}[X]$:

Proposition 18

Si $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, tout idéal de l'anneau $\mathbb{K}[X]$ est principal.

2. Opérations sur les idéaux

Dans ce paragraphe on va voir comment les idéaux d'anneaux réagissent avec les opérations algébriques et ensemblistes usuelles. On commence par la somme et l'intersection

Proposition 19

Si $\mathscr{I}$ et $\mathscr{J}$ sont des idéaux de $\mathscr{A}$, alors $\mathscr{I} + \mathscr{J}$ et $\mathscr{I} \cap \mathscr{J}$ sont des idéaux de $\mathscr{A}$.

On rappelle que la somme de deux sous-ensembles E et F de $\mathscr{A}$ est définie par

$$E + F = \{ x + y \ : \ x \in E, \ y \in F \}.$$

Remarque 10

La proposition 6 reste vraie si l'on remplace la somme de deux idéaux par une somme finie d'idéaux et l'intersection de deux idéaux par l'intersection d'une famille quelconque d'idéaux.

La proposition précédente nous permet d'introduire la notion d'idéal engendré par une partie :

Définition 19

Soit E un sous-ensemble de $\mathscr{A}$. L'intersection de tous les idéaux contenant E est un idéal de $\mathscr{A}$ qui s'appelle **l'idéal engendré** par E. C'est le **plus petit idéal** de $\mathscr{A}$ **contenant** E, on le note $<E>$.

La proposition suivante nous dit que $<E>$ est l'ensemble de toutes les combinaisons « linéaires » finies des éléments de E à coefficients dans $\mathscr{A}$:

Proposition 20

Pour tout $E \subset \mathscr{A}$, on a

$$<E>=\left\{ \sum_{k=1}^{n} a_k x_k \ : \ x_1,...,x_n \in E,\ a_1,...,a_n \in \mathscr{A},\ n \in \mathbb{N}^* \right\}.$$

Un cas particulier de la proposition 6 est lorsque $E=\{x\}$. On retrouve ainsi l'idéal principal $<x>$ qui est donc le plus petit idéal de $\mathscr{A}$ contenant x. Lorsque $E=\{x_1,\cdots,x_n\}$ est un ensemble fini on note par abus de notation $<x_1,\cdots,x_n>$ l'idéal engendré par E.

Remarque 11

Si $\mathscr{I}$ et $\mathscr{J}$ sont des idéaux de $\mathscr{A}$, l'ensemble $\mathscr{I} \cup \mathscr{J}$ n'est pas un idéal en général (voir exemple ci-dessous). On peut vérifier néanmoins que l'idéal engendré par $\mathscr{I} \cup \mathscr{J}$ est $\mathscr{I} + \mathscr{J}$.

Exemple 13

Dans $\mathbb{Z}$ l'union des deux idéaux $2\mathbb{Z}$ et $3\mathbb{Z}$ n'est pas un idéal car par exemple $3-2=1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. L'idéal engendré par $2\mathbb{Z} \cup 3\mathbb{Z}$ est $2\mathbb{Z}+3\mathbb{Z}=\mathbb{Z}$.

3. Anneaux quotients

Si $\mathscr{I}$ est un idéal de $\mathscr{A}$, on définit la relation d'équivalence $\mathscr{R}$ sur $\mathscr{A}$ par :

$$x \mathscr{R} y \iff x-y \in \mathscr{I}.$$

Il n'est pas difficile de vérifier qu'il s'agit effectivement d'une relation d'équivalence sur $\mathscr{A}$. La structure d'anneau de $\mathscr{A}$ peut être transposée sur l'ensemble quotient, mais il faudra pour cela vérifier la compatibilité des lois de $\mathscr{A}$ avec la relation d'équivalence. Rappelons que l'ensemble quotient, que l'on notera $\mathscr{A}/\mathscr{I}$, est l'ensemble des classes d'équivalence dont les éléments seront notés $\overline{x}$, $x \in \mathscr{A}$. On définit sur $\mathscr{A}/\mathscr{I}$ les deux lois + et × (avec la notation multiplicative $ab=a \times b$) par

$$\overline{x}+\overline{y}=\overline{x+y} \quad \text{et} \quad \overline{x}\,\overline{y}=\overline{xy}.$$

En utilisant le fait que $\mathscr{I}$ est un idéal, on démontre la proposition suivante

Proposition 21

L'addition et la multiplication définies ci-dessus sur $\mathscr{A}/\mathscr{I}$ sont des l.c.i et $(\mathscr{A}/\mathscr{I},+,\times)$ est un anneau commutatif avec comme éléments neutres $\overline{0}$ pour l'addition et $\overline{1}$ pour la multiplication. De plus la projection canonique $P:\mathscr{A}\to\mathscr{A}/\mathscr{I}$ définie par $P(x)=\overline{x}$ est un morphisme d'anneaux qui est surjectif et dont le noyau est $\mathscr{I}$.

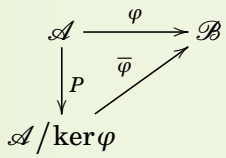
Exemple 14

En prenant $\mathscr{A}=\mathbb{Z}$ et $\mathscr{I}=p\mathbb{Z}$ on retrouve les anneaux des classes de congruence $\mathbb{Z}/pZ$ déjà rencontrés au chaiptre 1.

Nous avons le théorème très important suivant :

Théorème 2. (Théorème de factorisation)

Soit $\varphi:\mathscr{A}\to\mathscr{B}$ un morphisme d'anneaux. Alors il existe un unique morphisme d'anneau $\overline{\varphi}:\mathscr{A}/\ker\varphi\to\mathscr{B}$ qui est injectif et respectant le diagramme commutatif :



En particulier, $\overline{\varphi}:\mathscr{A}/\ker\varphi\to\mathrm{Im}\,\varphi$ est un isomorphisme d'anneaux.

Ce qu'on entend par diagramme commutatif ici est que $\varphi=\overline{\varphi}\circ P$. En particulier, on a $\mathrm{Im}\,\overline{\varphi}=\mathrm{Im}\,\varphi$. Dans la suite on utilisera la notation $\mathscr{A}_1\cong\mathscr{A}_2$ pour exprimer le fait qu'il existe un isomorphisme d'anneaux entre $\mathscr{A}_1$ et $\mathscr{A}_2$. Ainsi d'après le théorème 1 on a $\mathscr{A}/\ker\varphi\cong\mathrm{Im}\,\varphi$.

Exemple 15

1. Soit $\mathscr{A}=\mathbb{R}[X]$ et soit $\varphi:\mathscr{A}\to\mathbb{R}$ définie par $\varphi(P)=P(0)$, i.e φ est la valuation en 0. On a $\ker\varphi=<X>$ et $\mathrm{Im}\,\varphi=\mathbb{R}$. Ainsi on obtient d'après le théorème 1, $\mathbb{R}[X]/<X>\cong\mathbb{R}$. De la même manière, on a plus généralement lorsque $\mathscr{A}$ est un anneau commutatif quelconque, $\mathscr{A}[X]/<X>\cong\mathscr{A}$.
2. Considérons le morphisme $\varphi:\mathbb{Z}[X]\to\mathbb{C}$ défini par $\varphi(P)=P(i)$, où $i=\sqrt{-1}$. On peut montrer que son noyau est engendré par le polynôme X^2+1 (à faire en exercice), i.e $\ker\varphi=<X^2+1>$. Si on note par $\mathbb{Z}[i]$ le sous-anneau de $\mathbb{C}$ engendré par i (voir chapitre 1), on a d'après le théorème 1 :

$$\mathbb{Z}[i]\cong\mathbb{Z}[X]/<X^2+1>.$$

En considérant l'anneau $\mathbb{R}[X]$ au lieu de $\mathbb{Z}[X]$ et en suivant la mème démarche on obtient que

$$\mathbb{C}\cong\mathbb{R}[X]/<X^2+1>.$$

Avant d'énoncer le deuxième théorème sur les morphismes d'anneaux, nous fixons quelques notations et définitions. Si $\mathscr{I}$ et $\mathscr{J}$ sont des idéaux de $\mathscr{A}$ tels que $\mathscr{I} \subset \mathscr{J}$, on définit le morphisme canonique $f : \mathscr{A}/\mathscr{I} \to \mathscr{A}/\mathscr{J}$ par $f(\overline{x}) = \widetilde{x}$, où $\overline{x}$ désigne la classe d'équivalence de x par rapport à $\mathscr{I}$ et $\widetilde{x}$ la classe d'équivalence de x par rapport à $\mathscr{J}$. Il n'est pas difficile de voir que f est bien définie ($f(\overline{x})$ ne dépend pas du représentant de la classe $\overline{x}$).

Nous utiliserons également la notation suivante : si $\mathscr{I}$ est un idéal de $\mathscr{A}$ et $E \subset \mathscr{A}$, on notera :

$$E/\mathscr{I} = P(E)$$

où $P : \mathscr{A} \to \mathscr{A}/\mathscr{I}$ est la projection canonique. On a ainsi

$$E/\mathscr{I} = \{\, \overline{x} \in \mathscr{A}/\mathscr{I} \ : \ x \in E \,\}.$$

Théorème 3. (Théorème d'isomorphisme)

Si $\mathscr{I}$ est un idéal de $\mathscr{A}$, alors les idéaux de $\mathscr{A}/\mathscr{I}$ sont de la forme $\mathscr{J}/\mathscr{I}$, où $\mathscr{J}$ est un idéal de $\mathscr{A}$ tel que $\mathscr{I} \subset \mathscr{J}$. De plus, le morphisme canonique $f : \mathscr{A}/\mathscr{I} \to \mathscr{A}/\mathscr{J}$ est surjectif et induit d'après le théorème 1 un isomortphisme $\overline{f} : (\mathscr{A}/\mathscr{I})/(\mathscr{J}/\mathscr{I}) \to \mathscr{A}/\mathscr{J}$. Ainsi on a

$$\boxed{(\mathscr{A}/\mathscr{I})/(\mathscr{J}/\mathscr{I}) \cong \mathscr{A}/\mathscr{J}.}$$

Exemple 16

1. D'après le théorème 2, si $p \in \mathbb{N}^*$ est un diviseur de $n \in \mathbb{N}^*$, alors on a

$$(\mathbb{Z}/n\mathbb{Z})/(p\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}.$$

2. Considérons l'anneau $\mathscr{K} = \mathbb{R}[X]/< X^2+1 >$. D'après le théorème 2 tous les idéaux de cet anneau sont de la forme $< P > /< X^2+1 >$ avec P un diviseur de X^2+1, mais comme X^2+1 n'a pas de diviseurs dans $\mathbb{R}[X]$ autre que les constantes ou les associés de X^2+1 (prouver le !), on a nécessairement $P \sim (X^2+1)$ ou P est un polynôme constant non nul. Ainsi les seuls idéaux de $\mathscr{K}$ sont l'idéal trivial $\{0\}$ et $\mathscr{K}$, ce qui implique donc que $\mathscr{K}$ est un corps. Ce résultat n'est pas surprenant puisque dans l'exemple 5 ci-dessus on a déjà vu que $\mathscr{K} \cong \mathbb{C}$.

4. Lemme Chinois

Dans ce paragraphe on va étudier l'un des plus vieux théorèmes d'Arithmétique ; il s'agit du « Lemme chinois » qui permet de résoudre des systèmes de congruences. Pour ce faire nous avons besoin de quelques définitions :

Définition 20

Deux idéaux $\mathscr{I}$, $\mathscr{J}$ de $\mathscr{A}$ sont dits **étrangers** (ou étrangers entre eux) si $\mathscr{I} + \mathscr{J} = \mathscr{A}$.

Il découle directement de la définition que deux idéaux $\mathscr{I}$ et $\mathscr{J}$ sont étrangers s'il existe $a \in \mathscr{I}$ et $b \in \mathscr{J}$ tels que $a + b = 1$.

Théorème 4. (Lemme chinois)

Soient $\mathscr{I}_1,\cdots,\mathscr{I}_n$ des idéaux de $\mathscr{A}$ deux à deux étrangers entre eux et soit P_i la projection canonique de A dans $\mathscr{A}/\mathscr{I}_i$, $i=1,\cdots,n$. Alors pour tous $x_1,\cdots,x_n\in\mathscr{A}$, il existe $x\in\mathscr{A}$ tel que

$$P_i(x)=P_i(x_i) \text{ pour tout } i=1,\cdots,n.$$

Par analogie avec l'anneau des entiers $\mathbb{Z}$, le lemme chinois s'écrit : pour tous $x_1,\cdots,x_n\in\mathscr{A}$, il existe $x\in\mathscr{A}$ tel que

$$x\equiv x_i \bmod(\mathscr{I}_i), \text{ pour tout } i=1,\cdots,n.$$

Nous avons le corollaire suivant

Corollaire 3. (Lemme chinois)

Soient $\mathscr{I}_1,\cdots,\mathscr{I}_n$ des idéaux de $\mathscr{A}$ deux à deux étrangers entre eux . Alors on a

$$\mathscr{A}/\mathscr{I}_1\cap\cdots\cap\mathscr{I}_n \cong (A/\mathscr{I}_1)\times\cdots\times(A/\mathscr{I}_n).$$

Exemple 17

Résoudre dans $\mathbb{Z}$ les deux systèmes de congruence :

$$\begin{cases} x\equiv 2 \bmod 5\\ x\equiv 3 \bmod 7\end{cases} \quad ; \quad \begin{cases} x\equiv 2 \bmod 3\\ x\equiv 3 \bmod 5\\ x\equiv 1 \bmod 7.\end{cases}$$

5. Idéaux maximaux, idéaux premiers

Définition 21

Un idéal $\mathscr{M}$ de $\mathscr{A}$ est dit **maximal** s'il est différent de $\mathscr{A}$ et si pour tout idéal $\mathscr{I}$ de $\mathscr{A}$ on a

$$\mathscr{M}\subset\mathscr{I} \Longrightarrow \mathscr{I}=\mathscr{M} \text{ ou } \mathscr{I}=\mathscr{A}.$$

Nous avons la caractérisation très facile suivante :

Proposition 22

Un idéal $\mathscr{M}$ de $\mathscr{A}$ est maximal si et seulement si l'anneau $\mathscr{A}/\mathscr{M}$ est un corps.

Exemple 18

1. Dans $\mathbb{Z}$ les idéaux maximaux sont de la forme $p\mathbb{Z}$ avec p un entier premier.
2. Dans l'anneau $C([0,1])$ l'ensemble $\mathscr{I} = \{ u \in C([0,1]) \ : \ u(0) = 0 \}$ est un idéal maximal.

Remarque 12

Dans la pratique pour savoir si un idéal est maximal on utilise le théorème de factorisation. En effet, supposons qu'il existe un morphisme surjectif $\varphi : \mathscr{A} \to \mathscr{K}$, où $\mathscr{K}$ est un corps. Alors nécessairement $\ker \varphi$ est maximal. Inversement si $\mathscr{I}$ est un idéal maximal, il suffit de prendre φ la projection canonique de $\mathscr{A}$ dans $\mathscr{A}/\mathscr{I}$.

Nous avons la relation suivante entre idéaux maximaux et idéaux étrangers :

Proposition 23

Si $\mathscr{M}_1$ et $\mathscr{M}_2$ sont deux idéaux maximaux de $\mathscr{A}$ alors ils sont étrangers.

Le théorème suivant nous dit que tout idéal propre est inclus dans un idéal maximal.

Théorème 5. (Théorème de Krull)

Si $\mathscr{I}$ est un idéal propre de $\mathscr{A}$, i.e $\mathscr{I} \neq \mathscr{A}$, alors il existe idéal maximal de $\mathscr{A}$ contenant $\mathscr{I}$.

Ce théorème a un interêt plutôt théorique car il ne fournit pas de méthode pour construire l'idéal maximal. Nous avons néanmoins le corollaire suivant :

Corollaire 4

Pour qu'un élément de $\mathscr{A}$ soit inversible il faut et il suffit qu'il n'appartienne à aucun idéal maximal de $\mathscr{A}$.

Nous introduisons maintenant la notion d'idéal premier :

Définition 22

Un idéal $\mathscr{I} \neq \mathscr{A}$ de $\mathscr{A}$ est dit **premier** si :

$$\forall\, x, y \in \mathscr{A},\ xy \in \mathscr{I} \Longrightarrow x \in \mathscr{I} \text{ ou } y \in \mathscr{I}.$$

Exemple 19

1. Dans $\mathbb{Z}$ un idéal (non trivial) est premier si et seulement s'il est de la forme $p\mathbb{Z}$ avec p premier.
2. Dans tout anneau intègre (et commutatif) $\mathscr{A}$, l'idéal trivial $\{0\}$ est premier.

Nous avons la caractérisation suivante :

Proposition 24

Un idéal $\mathscr{I}$ de $\mathscr{A}$ est premier $\iff$ l'anneau $\mathscr{A}/\mathscr{I}$ est intègre.

En particulier, tout idéal maximal est premier.

Exemple 20

1. Soit $\mathscr{A}$ un anneau commutatif et intègre mais qui n'est pas un corps (par exemple $\mathbb{Z}$). Alors l'idéal $\{0\}$ est premier mais non maximal.
2. Dans l'anneau $\mathbb{Z}[X]$, l'idéal $< X >$ est premier puisque $\mathbb{Z}[X]/< X > \cong \mathbb{Z}$ et $\mathbb{Z}$ est intègre. Mais comme $\mathbb{Z}$ n'est pas un corps, alors $< X >$ n'est pas maximal.
3. Si $\varphi : \mathscr{A} \to \mathscr{B}$ est un morphisme d'anneaux avec $\mathscr{B}$ commutatif et intègre, alors $\ker \varphi$ est un idéal premier de $\mathscr{A}$.
4. Si $\varphi : \mathscr{A} \to \mathscr{B}$ est un morphisme d'anneaux, alors pour tout idéal premier $\mathscr{I} \subset \mathscr{B}$, $f^{-1}(\mathscr{I})$ est un idéal premier de $\mathscr{A}$.

Définition 23

Le **radical** d'un idéal $\mathscr{I} \subset \mathscr{A}$ est l'idéal noté $\sqrt{\mathscr{I}}$ défini par

$$\sqrt{\mathscr{I}} = \left\{ x \in \mathscr{A} \ : \ \exists n \in \mathbb{N}^*, \ x^n \in \mathscr{I} \right\}.$$

Le radical de l'idéal trivial $\{0\}$ s'appelle le **nilradical** de $\mathscr{A}$, il est noté $\mathrm{Nil}(\mathscr{A})$.

Il découle directement de cette définition que le nilradical de $\mathscr{A}$ est est l'ensemble de tous les éléments nilpotents de $\mathscr{A}$. Plus généralement, nous avons le théorème suivant :

Proposition 25

Si $\mathscr{I} \neq \mathscr{A}$ est un idéal de $\mathscr{A}$, alors $\sqrt{\mathscr{I}}$ est l'intersection de tous les idéaux premiers contenant $\mathscr{I}$.

Exemple 21

1. Soit $\mathscr{I} = n\mathbb{Z}$, $n \in \mathbb{N}^*$, un idéal de $\mathbb{Z}$. Si on note par p_n le produit de tous les diviseurs premiers de n, on a $\sqrt{\mathscr{I}} = p_n\mathbb{Z}$. En particulier si p est un nombre premier, on a $\sqrt{p^m\mathbb{Z}} = p\mathbb{Z}$.
2. Nous avons $\mathrm{Nil}(\mathbb{Z}) = \{0\}$ et $\mathrm{Nil}(\mathbb{Z}/p\mathbb{Z}) = \{0\}$ si p est premier. Plus généralement, si $\mathscr{A}$ est un anneau commutatif intègre, on a $\mathrm{Nil}(\mathscr{A}) = \{0\}$.
3. Pour tout idéal $\mathscr{I} \subset \mathscr{A}$, on a $\sqrt{\sqrt{\mathscr{I}}} = \sqrt{\mathscr{I}}$.

Chapitre 3

Anneaux particuliers

Dans tout ce qui suit, $\mathscr{A}$ désignera un anneau **commutatif non trivial** . Tous les annaux considérés dans ce chapitre seront supposés **commutatifs**.

1. Divisibilité dans les anneaux

Dans ce paragraphe $\mathscr{A}$ désignera un anneau qui sera supposé **commutatif et intègre.**

Définition 24

On dit qu'un élément $a \in \mathscr{A}$ est **irréductible** si il est non inversible et les seuls diviseurs de a sont les éléments inversibles de $\mathscr{A}$ et les éléments associés à a.

Définition 25

On dit qu'un élément $a \in \mathscr{A} \setminus \{0\}$ est **premier** si il est non inversible et lorsqu'il divise le produit de deux éléments de $\mathscr{A}$ il doit diviser au moins l'un des deux. Autrement dit :

$$\boxed{a \mid bc \implies a \mid b \text{ ou } a \mid c.}$$

Proposition 26

Si $a \in \mathscr{A}$ est premier alors il est irréductible.

La réciproque de la proposition précédente est fausse en général (voir exemple ci-dessous).

Exemple 22

1. Considérons dans l'anneau $\mathbb{Z}\left[\sqrt{-3}\right]$ l'élément 2. On peut montrer que 2 est irréductible mais il n'est pas premier car 2 est un diviseur de 4 et $4 = \left(1+\sqrt{-3}\right)\left(1-\sqrt{-3}\right)$.
2. Dans l'anneau $\mathbb{Z}$, il y a une équivalence entre nombre premier et nombre irréductible. On verra dans la suite que cette propriété est vraie dans d'autres anneaux.

Définition 26

Deux éléments $a, b \in \mathscr{A}$ sont dits **premiers entre eux** si leurs seuls diviseurs communs sont les éléments inversibles de $\mathscr{A}$. On dit qu'ils sont **étrangers** s'il existe $x, y \in \mathscr{A}$ tels que $xa + yb = 1$.

Proposition 27

Si a et b sont étrangers alors ils sont premiers entre eux.

La réciproque de la proposition précédente est fausse comme le montre l'exemple ci-dessous.

Exemple 23

Dans l'anneau $\mathbb{Z}[X]$ les polynômes $P = 3$ et $Q = X$ sont premiers entre eux mais pas étrangers.

2. Anneaux euclidiens

Les anneaux euclidiens sont des anneaux dans lesquels on peut effectuer une sorte de « division euclidienne ».

Définition 27

Un anneau $\mathscr{A}$ est dit **euclidien** s'il est intègre et s'il existe une application $N : \mathscr{A} \setminus \{0\} \to \mathbb{N}$ appelée **stathme** telle que pour tous $a \in \mathscr{A}$ et $b \in \mathscr{A} \setminus \{0\}$, il existe $(q, r) \in \mathscr{A} \times \mathscr{A}$ vérifiant

$$\boxed{a = bq + r \text{ et } N(r) < N(b) \text{ si } r \neq 0.}$$

L'écriture $a = bq + r$ s'appelle division euclidienne de a par b par rapport au stathme N.

Remarque 13

Pour certains auteurs un stathme N doit vérifier la condition $N(a) \leqslant N(ab)$ pour tous $a, b \in \mathscr{A} \setminus \{0\}$. On peut néanmoins démontrer que si un anneau $\mathscr{A}$ est euclidien (au sens de notre définition) on peut toujours trouver un stathme sur $\mathscr{A} \setminus \{0\}$ vérifiant cette condition.

Exemple 24

1. $\mathbb{Z}$ est euclidien de stathme $N(x) = |x|$.
2. $\mathbb{R}[X]$, et plus généralement $\mathbb{K}[X]$ avec $\mathbb{K}$ un corps, est euclidien de stathme $N(P) = \deg P$. (voir proposition 4 ci-dessous)
3. $\mathbb{Z}[i]$ est euclidien de stathme $N(z) = |z|^2$.
4. Tout corps $\mathscr{K}$ est euclidien de sthame n'importe quelle application $N : \mathscr{A} \setminus \{0\} \to \mathbb{N}$.

Proposition 28

L'anneau des polynômes $\mathscr{A}[X]$ est euclidien si et seulement si $\mathscr{A}$ est un corps.

Exemple 25

1. $\mathbb{Z}[X]$ n'est pas euclidien car $\mathbb{Z}$ n'est pas un corps.
2. $(\mathbb{Z}/p\mathbb{Z})[X]$ est euclidien si et seulement si p est premier.

3. Anneaux principaux

Les anneaux principaux (et plus généralement, les anneaux factoriels qu'on découvrira plus tard) sont des anneaux dans lesquels on peut faire de l'Aritmétique d'une façon satisfaisante (comme dans $\mathbb{Z}$).

Définition 28

Un anneau $\mathscr{A}$ est dit principal si il est intègre et tout idéal de $\mathscr{A}$ est principal

Exemple 26

1. $\mathbb{Z}$ est principal.
2. $\mathbb{R}[X]$, et plus généralement $\mathbb{K}[X]$ avec $\mathbb{K}$ un corps, est principal.
3. $\mathbb{Z}[X]$ n'est pas principal car par exemple l'idéal $\mathscr{I} = \left\{ 2P + XQ \ : \ P,Q \in \mathbb{Z}[X] \right\}$ n'est pas principal.

La proposition suivante est très simple à montrer :

Proposition 29

Dans un anneau principal un idéal non nul est premier si et seulement s'il est maximal.

Le lien entre anneau euclidien et principal est donné par la proposition suivante :

Proposition 30

Tout anneau euclidien est principal.

Remarque 14

La réciproque de la proposition précédente est fausse. L'anneau $\mathscr{A} = \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ en est un contre-exemple (voir devoir maison).

Proposition 31. (Lemme d'Euclide)

Dans un anneau principal un élément est premier si et seulement s'il est irréductible.

Nous introduisons la notion de pgcd de deux élément d'un anneau.

Définition 29

Soient a et b deux éléments d'un anneau intègre $\mathscr{A}$. On dit que a et b admettent un **pgcd** (plus grand commun diviseur) s'il existe un diviseur commun d de a et b tel que tout autre diviseur commun de a et b est un diviseur de d. Dans ce cas on dit que d est un pgcd de a et b et on écrit $d = \text{pgcd}(a,b)$.

Remarque 15

Notons qu'un pgcd de deux éléments a et b (lorsqu'il existe) n'est pas unique. Il suffit de prendre un élément associé à ce pgcd pour obtenir un nouveau pgcd. Inversement, tous les pgcd de a et b (lorqu'il en existe) sont associés les uns aux autres.

La proposition suivante nous dit que dans un anneau principal le pgcd de deux éléments existe toujours :

Proposition 32

Soit $\mathscr{A}$ un anneau principal et soient $a,b \in \mathscr{A}$. Alors tout générateur d de l'idéal $< a > + < b >$, i.e $< d > = < a > + < b >$, est un pgcd de a et b.

Remarque 16

Il exsite des anneau dans lesquels certains éléments n'admettent pas de pgcd. Par exemple, dans l'anneau $\mathbb{Z}\left[\sqrt{-5}\right]$ les deux éléments $a = 6$ et $b = 4 + 2i\sqrt{5}$ n'admettent pas de pgcd.

Définition 30

On dit que deux éléments a et b d'un anneau intègre $\mathscr{A}$ sont premiers entre eux si leurs diviseurs communs sont les éléments inversibles de $\mathscr{A}$.

Proposition 33

Dans un anneau principal $\mathscr{A}$, deux éléments $a,b \in \mathscr{A}$ sont premiers entre eux si et seulement si l'un de leurs pgcd est inversible, i.e $\text{pgcd}\,(a,b) \sim 1$.

Comme le pgcd est déterminé aux éléments inversibles près, il suffit qu'un pgcd de a et b dans la proposition précédente soit inversible pour que les autres le soient.

Nous avons le corollaire suivant :

Corollaire 5. (Théorème de Bezout)

Dans un anneau principal $\mathscr{A}$, deux éléments a et b sont premiers entre eux si et seulement s'il existe un couple $(x,y) \in \mathscr{A} \times \mathscr{A}$ tel que

$$ax + by = 1.$$

Ce qui est équivalent aussi à dire que les idéaux $< a >$ et $< b >$ sont étrangers.

Nous avons aussi les deux corollaires suivants :

Corollaire 6. (Lemme de Gauss)

Dans un anneau principal $\mathscr{A}$ si un élément divise le produit de deux éléments et s'il est premier avec l'un des deux, alors il divise l'autre. Plus précisément :

$$a \mid bc \text{ et } \operatorname{pgcd}(a,b) \sim 1 \implies a \mid c.$$

Corollaire 7

Dans un anneau principal $\mathscr{A}$ si deux élément a et b sont premiers entre eux et divisent un élément c, alors leur produit divise c. Plus précisément :

$$a \mid c,\ b \mid c \text{ et } \operatorname{pgcd}(a,b) \sim 1 \implies ab \mid c.$$

Définition 31

Soient a et b deux éléments d'un anneau intègre $\mathscr{A}$. On dit que a et b admettent un **ppcm** (plus petit commun multiple) s'il existe un multiple commun m de a et b tel que tout autre multiple commun de a et b est un multiple de m. Dans ce cas on dit que m est un ppcm de a et b et on écrit $m = \operatorname{ppcm}(a,b)$.

Remarque 17

Comme le pgcd, le ppcm de deux éléments a et b n'est pas unique. Il suffit de prendre un associé à ce ppcm pour obtenir un nouveau ppcm.

La proposition suivante nous dit que dans un anneau principal le ppcm de deux éléments existe toujours :

Proposition 34

Soit $\mathscr{A}$ un anneau principal et soient $a, b \in \mathscr{A}$. Alors tout générateur m de l'idéal $< a > \cap < b >$, i.e $< m > = < a > \cap < b >$, est un ppcm de a et b.

Proposition 35

Soit $\mathscr{A}$ un anneau principal et soient $a, b \in \mathscr{A}$. Alors on a :

$$\text{pgcd}\,(a,b) \times \text{ppcm}\,(a,b) \sim ab.$$

4. Anneaux factoriels

Les anneaux factoriels sont des anneaux dans lesquels le théorème fondamental de l'Arithmétique est valable. Plus précisément, nous avons la définition suivante :

Définition 32

Un anneau $\mathscr{A}$ est dit **factoriel** s'il est intègre et vérifie les deux conditions suivantes :

1. Tout élément $a \in \mathscr{A}$ non nul et non inversible se décompose en produit d'éléments irréductibles , i.e il existe $p_1, \cdots, p_r \in \mathscr{A}$ qui sont irréductibles tels que $a = p_1 \cdots p_r$.
2. La décomposition précédente est unique dans le sens suivant : si $a = p_1 \cdots p_r = q_1 \cdots q_s$ avec $p_1, \cdots, p_r$ et $q_1, \cdots, q_s$ irréductibles, alors $r = s$ et il existe une permutation σ de l'ensemble $\{1, \cdots, r\}$ telle que $p_i \sim q_{\sigma(i)}$ pour tout $i = 1, \cdots, r$.

Nous avons la proposition suivante :

Proposition 36

Tout anneau principal est factoriel.

Remarque 18

La réciproque de la proposition précédente n'est pas vraie en général. En effet, considérons l'anneau $\mathbb{Z}[X]$. Il n'est pas principal (déjà vue !) mais il est factoriel car l'anneau $\mathbb{Z}$ l'est (comme on le verra plus loin, si $\mathscr{A}$ est factoriel, alors $\mathscr{A}[X]$ est factoriel).

Exemple 27

1. L'anneau $\mathbb{Z}\left[\sqrt{-3}\right]$ n'est pas factoriel. Par exemple, 4 possède deux décompositions différentes : $4 = 2 \times 2 = \left(1 + i\sqrt{3}\right)\left(1 - i\sqrt{3}\right)$.

La proposition suivante nous dit que dans un anneau factoriel le pgcd et le ppcm de deux éléments existent toujours :

Proposition 37

Soit $\mathscr{A}$ un anneau factoriel et soient $a,b \in \mathscr{A}$. Alors pgcd (a,b) et ppcm (a,b) exisent et vérifient

$$\text{pgcd}\,(a,b) \times \text{ppcm}\,(a,b) \sim ab.$$

Les deux résultats qui sont lemme d'Euclide et le lemme de Gauss valables dans un anneau principal sont également valables dans un anneau factoriel :

Proposition 38. (Lemme d'Euclide)

Dans un anneau factoriel un élément est premier si et seulement s'il est irréductible.

Proposition 39. (Lemme de Gauss)

Dans un anneau factoriel $\mathscr{A}$ si un élément divise le produit de deux éléments et s'il est premier avec l'un des deux, alors il divise l'autre.

On clôt ce paragraphe par un schéma très utile concernant un anneau $\mathscr{A}$:

$$\mathscr{A} \text{ est euclidien} \implies \mathscr{A} \text{ est principal} \implies \mathscr{A} \text{ est factoriel} \implies \mathscr{A} \text{ est intègre.}$$

5. Corps des fractions d'un anneau

Le corps des fractions d'un anneau est à cet anneau ce que le corps des rationnels $\mathbb{Q}$ est à l'anneau des entiers relatifs $\mathbb{Z}$. Le but est d'inclure $\mathscr{A}$ dans un corps pour que chaque élément non nul soit ainsi inversible.

Soit $\mathscr{A}$ un anneau intègre. On définit sur l'ensemble $\mathscr{A} \times \left(\mathscr{A} \setminus \{0\}\right)$ la relation $\mathscr{R}$:

$$(a,b)\,\mathscr{R}\,(c,d) \iff ad = bc.$$

On vérifie facilement qu'il s'agit d'une relation d'équivalence sur $\mathscr{A} \times \left(\mathscr{A} \setminus \{0\}\right)$. La classe d'équivalence d'un élément $(a,b) \in \mathscr{A} \times \left(\mathscr{A} \setminus \{0\}\right)$ est notée $\dfrac{a}{b}$ (ou parfois a/b). L'ensemble des classes d'équivalence sera noté $\mathscr{K}$, i.e

$$\mathscr{K} = \mathscr{A} \times \left(\mathscr{A} \setminus \{0\}\right)/\mathscr{R}.$$

On définit sur $\mathscr{K}$ les deux lois

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{et} \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}\,.$$

Il n'est pas difficile de vérifier que ce sont bien des lois de composition internes sur $\mathscr{K}$. Elles ont comme éléments neutres : $\dfrac{0}{1}$ (noté 0) pour la loi + (l'addition) et $\dfrac{1}{1}$ (noté 1) pour la loi × (la multiplication). Nous avons la proposition suivante :

Proposition 40

L'ensemble $\mathscr{K}$ muni des deux lois définies ci-dessus est un corps commutatif, on l'appelle le corps des fractions de $\mathscr{A}$. L'inverse d'un élément $\frac{a}{b} \in \mathscr{K} \setminus \{0\}$ est $\frac{b}{a}$. De plus, l'application $i : \mathscr{A} \to \mathscr{K}$ qui à chaque $a \in \mathscr{A}$ associe $i(a) = \frac{a}{1}$ est un morphisme d'anneau qui est injectif.

Grâce à la proposition précédente on identifie l'anneau $\mathscr{A}$ avec le sous-anneau $i(\mathscr{A})$ de $\mathscr{K}$. Ainsi on peut considérer $\mathscr{A}$ comme sous-anneau de $\mathscr{K}$.

Exemple 28

1. Le corps des fractions de $\mathbb{Z}$ est $\mathbb{Q}$.
2. Si $\mathscr{A}$ est un anneau intègre, le corps des fractions de $\mathscr{A}[X]$ est le corps des fractions rationnelles à coefficients dans $\mathscr{A}$ on le note $\mathscr{A}(X)$.

6. Retour sur l'anneau des polynômes

Dans ce paragraphe nous allons voir que l'anneau des plynômes $\mathscr{A}[X]$ est aussi riche que l'anneau $\mathscr{A}$ du point de vue de l'Arithmétique. Nous commençons par quelques définitions.

Soit $\mathscr{A}$ un anneau factoriel et soit $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathscr{A}[X]$. On appelle **contenu** de P, noté $c(P)$, le pgcd de ses coefficients (on définit le pgcd de plusieurs éléments de la même façon que pour deux éléments, son existence étant assuré car on est dans un anneau factoriel). Evidémment, comme le pgcd n'est pas unique, on en choisit un à un élément inversible près. Le contenu d'un polynôme est donc défini à un élément inversible près.

Définition 33

On dit qu'un polynôme $P \in \mathscr{A}[X]$ est **primitif** si son contenu est inversible, i.e $c(P) \sim 1$.

Nous avons la proposition suivante :

Proposition 41

Pour tous $P, Q \in \mathscr{A}[X]$ on a $c(PQ) = c(P)c(Q)$. En particulier si P et Q sont primitifs, alors PQ est primitif.

Soit $\mathscr{A}$ un anneau factoriel et soit $\mathscr{K}$ son corps des fractions. Rappelons que $\mathscr{A}[X]$ est un sous-anneau de $\mathscr{K}$, ce qui implique que $\mathscr{A}[X]$ est un sous-anneau de $\mathscr{K}[X]$. Nous avons le théorème suivant :

Théorème 6

Les polynômes irréductibles de $\mathscr{A}[X]$ sont d'une part les élélements de $\mathscr{A}$ (polynômes de degré 0) qui sont irréductibles dans $\mathscr{A}$. D'autre part, les polynômes de degré au moins 1 qui sont primitifs dans $\mathscr{A}[X]$ et irréductibles dans $\mathscr{K}[X]$.

Le théorème précédent a pour conséquence le théorème très important suivant

Théorème 7. (Théorème de transfert de Gauss)

Si $\mathscr{A}$ est factoriel, alors $\mathscr{A}[X]$ est factoriel.

Exemple 29

1. L'anneau $\mathbb{Z}[X]$ est factoriel.
2. L'anneau $\mathscr{A}[X]$ avec $\mathscr{A} = \mathbb{Z}\left[\sqrt{-3}\right]$ n'est pas factoriel.

Les résultats précédents nous permettent d'étudier les polynômes irréductibles de $\mathbb{Z}[X]$. Pour cela on rappelle quelques notations déjà rencontrés dans les chapitres précédents. Si $p \in \mathbb{N}$, on note par $\overline{a}$ la classe d'un élément $a \in \mathbb{Z}$ dans l'anneau $\mathbb{Z}/p\mathbb{Z}$. Nous avons le théorème suivant

Théorème 8

Soit $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ et soit $p \in \mathbb{N}$ un nombre premier. On suppose que $\overline{a}_n \neq \overline{0}$ dans $\mathbb{Z}/p\mathbb{Z}$ et que le polynôme $\overline{P} = \overline{a}_0 + \overline{a}_1X + \cdots + \overline{a}_nX^n$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Alors P est irréductible dans $\mathbb{Q}[X]$. Si de plus P est primitif, alors il est irréductible dans $\mathbb{Z}[X]$.

On en déduit le corollaire très pratique suivant :

Corollaire 8. (Critère d'Eisenstein)

Soit $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ avec $\deg P \geqslant 1$. On suppose qu'il existe un nombre premier p tel que p divise a_i pour tout $i = 0, \cdots, n-1$, que p ne divise pas a_n et que p^2 ne divise pas a_0. Alors P est irréductible dans $\mathbb{Q}[X]$ et si de plus P est primitif, alors il est irréductible dans $\mathbb{Z}[X]$.

Exemple 30

1. Pour tout entier $n \geqslant 1$, le polynôme $X^n + 2X^{n-1} + \cdots + 2X + 6$ est irréductible dans $\mathbb{Z}[X]$.
2. Soit $a = p_1 \cdots p_r$, où les $p_i \in \mathbb{N}$ sont des nombres premiers deux à deux distincts. Pour tout $n \in \mathbb{N}^*$, le polynôme $P = X^n - a$ est irréductible sur $\mathbb{Z}[X]$

Chapitre 4

Extensions des corps

1. Sous-corps, extensions de corps

Définition 34

Soit $\mathscr{L}$ un corps commutatif. On dit qu'un sous-ensemble $\mathscr{K} \subset \mathscr{L}$ est un sous-corps de $\mathscr{L}$ si $\mathscr{K}$ est un sous-anneau de $\mathscr{L}$ qui est un corps. Ce qui est équivalent à

1. $1 \in \mathscr{K}$ et pour tout $(x,y) \in \mathscr{K}^2$, $x-y \in \mathscr{K}$, $xy \in \mathscr{K}$.
2. Pour tout $x \in \mathscr{K} \setminus \{0\}$, $x^{-1} \in \mathscr{K}$.

Exemple 31

1. $\mathbb{Q}$ est sous-corps de $\mathbb{R}$ qui est un sous-corps de $\mathbb{C}$.
2. $\mathbb{Q}[\sqrt{2}] = \left\{ p + q\sqrt{2} \;/\; (p,q) \in \mathbb{Q}^2 \right\}$ est un sous-corps de $\mathbb{R}$.

Définition 35

Soit K un corps. On appelle caractéristique de $\mathscr{K}$ le plus petit entier $p \in \mathbb{N}^*$ tel que $p1 = 0$, où 1 est l'unité de $\mathscr{K}$ et 0 est le zéro de $\mathscr{K}$. Lorsqu'un tel entier n'existe pas, on dit par convention que la caractéristque de $\mathscr{K}$ est nulle.

La proposition suivante justifie la définition de la caractéristique d'un corps donnée ci-dessus :

Proposition 42

Soit $\mathscr{K}$ un corps. L'application $\varphi : \mathbb{Z} \to \mathscr{K}$ définie, pour tout $m \in \mathbb{Z}$, par $\varphi(m) = m1$, est un morphisme d'anneaux dont le noyau $\ker \varphi$ est un idéal de $\mathbb{Z}$ de la forme $p\mathbb{Z}$, où p est la caractéristuqe de $\mathscr{K}$. De plus, lorsque $p \neq 0$, p est un nombre premier.

Exemple 32

1. Les caratéristiques de $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont nulles.
2. Si p es premier, la caractéristique de $\mathbb{Z}/p\mathbb{Z}$ est p.
3. Si $\mathscr{K}$ est un corps de caractéristique p, alors le corps des fractions rationnelles $\mathscr{K}(X)$

est également de caractéristique p.

Remarque 19

On peut définir la caractéristique d'un anneau commutatif de la même façon que celle d'un corps. La proposition 1 reste valable si l'anneau est intègre.

Dans la proposition 1, lorsque la caractéristique p de $\mathscr{K}$ est non nulle l'image de φ est un sous-corps de $\mathscr{K}$ isomorphe à $\mathbb{Z}/p\mathbb{Z}$ d'après le théorème de factorisation (voir chapitre 1). On l'appelle le sous-corps premier de $\mathscr{K}$ et on peut vérifier facilement que c'est le plus petit sous-corps de $\mathscr{K}$ (il est inclus dans tout sous-corps de $\mathscr{K}$).

Définition 36

Soit $\mathscr{K}$ un corps. On appelle extension de $\mathscr{K}$ tout corps $\mathscr{L}$ tel que $\mathscr{K}$ soit un sous-corps de $\mathscr{L}$.

Si $\mathscr{L}$ est une extension d'un corps $\mathscr{K}$, il est facile de voir que $\mathscr{L}$ est un espace vectoriel sur le corps $\mathscr{K}$. Cela nous permet de justifier la définition suivante :

Définition 37

Soit $\mathscr{L}$ une extension d'un corps $\mathscr{K}$. On appelle degré de $\mathscr{L}$ sur $\mathscr{K}$ la dimension de $\mathscr{L}$ en tant qu'espace vectoriel sur $\mathscr{K}$. Le degré est noté $[\mathscr{L} : \mathscr{K}]$. Lorsque $[\mathscr{L} : \mathscr{K}]$ est finie, on dit que $\mathscr{L}$ est une extension finie de $\mathscr{K}$.

Exemple 33

1. $\mathbb{C}$ est une extension finie de $\mathbb{R}$ avec $[\mathbb{C} : \mathbb{R}] = 2$.
2. $\mathbb{R}$ est une extension de $\mathbb{Q}$ avec $[\mathbb{R} : \mathbb{Q}] = +\infty$ (voir section 2 pour une preuve).

En utilisant le sous-corps premier d'un corps fini on peut démontrer le thérème très important suivant

Théorème 9

Soit $\mathscr{K}$ un corps fini de caractéristique p. Alors le cardinal de $\mathscr{K}$ est donné par

$$\boxed{\text{Card } \mathscr{K} = p^k}$$

où k est le degré de $\mathscr{K}$ en tant qu'extension de son sous-corps premier, i.e $k = [\mathscr{K} : \mathscr{K}_0]$, où $\mathscr{K}_0$ est le sous-corps premier de $\mathscr{K}$.

Corollaire 9

Tout corps fini de cardinal un nombre premier p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Remarque 20

Si p est un nombre premier le corps $\mathbb{Z}/p\mathbb{Z}$ est noté $\mathbb{F}_p$. Le corollaire 1 nous dit qu'à isomorphisme près il n'y a qu'un seul corps de cardinal p premier, c'est le corps $\mathbb{F}_p$. Ce résultat se généralise pour tous les corps finis en remplaçant $\mathbb{Z}/p\mathbb{Z}$ par un quotient convenable de $(\mathbb{Z}/p\mathbb{Z})[X]$.

Pour calculer les degrés des extensions on a besoin de la proposition suivante :

Proposition 43

Soient $\mathcal{K} \subset \mathcal{L} \subset \mathcal{M}$ trois corps tels que $\mathcal{L}$ soit une extention finie de $\mathcal{K}$ et $\mathcal{M}$ une extension finie de $\mathcal{L}$. Si $(e_i)_{i\in I}$ est une base de $\mathcal{L}$ sur $\mathcal{K}$ et $(f_j)_{j\in J}$ est une base de $\mathcal{M}$ sur $\mathcal{L}$, alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathcal{M}$ sur $\mathcal{K}$.

Corollaire 10

Soient $\mathcal{K} \subset \mathcal{L} \subset \mathcal{M}$ trois corps tels que $\mathcal{M}$ soit une extention de $\mathcal{L}$ qui est une extension de $\mathcal{K}$. Alors on a

$$[\mathcal{M} : \mathcal{K}] = [\mathcal{M} : \mathcal{L}][\mathcal{L} : \mathcal{K}]$$

Remarque 21

Dans le corollaire précédent les degrés des différentes extensions peuvent être infinies. En particulier, l'une des conséquences de ce corollaire est que si $\mathcal{M}$ est une extension finie de $\mathcal{K}$, alors toute extension $\mathcal{L}$ de $\mathcal{K}$ telle que $\mathcal{L} \subset \mathcal{M}$ est également une extension finie de $\mathcal{K}$.

2. Extensions algébriques

Définition 38

Soit $\mathcal{L}$ un corps et soit E une partie de $\mathcal{L}$. On appelle corps engendré par E le plus petit sous-corps de $\mathcal{L}$ contenant E. Il est égal à l'intersection de tous les sous-corps de $\mathcal{L}$ qui contiennent E.

On va fixer maintenant quelques notations qui seront très utiles dans la suite. Soit $\mathcal{L}$ un corps et $\mathcal{K}$ un sous-corps de $\mathcal{L}$. Si $\alpha \in \mathcal{L}$, on notera par $\mathcal{K}[\alpha]$ le sous-anneau de $\mathcal{L}$ engendré par $\mathcal{K} \cup \{\alpha\}$. Il est facile de voir que l'on a

$$\mathcal{K}[\alpha] = \left\{ k_0 + k_1\alpha + \cdots + k_n\alpha^n \;/\; k_1, \cdots, k_n \in \mathcal{K},\ n \in \mathbb{N}^* \right\} = \left\{ P(\alpha) \;/\; P \in \mathcal{K}[X] \right\}.$$

De même, on notera par $\mathcal{K}(\alpha)$ le sous-corps de $\mathcal{L}$ engendré par $\mathcal{K} \cup \{\alpha\}$. On peut vérifier facilement que

$$\mathcal{K}(\alpha) = \left\{ R(\alpha) \;/\; R = \frac{P}{Q} \in \mathcal{K}(X), \text{ avec } Q(\alpha) \neq 0 \right\},$$

où $\mathcal{K}(X)$ désigne le corps des fractions de $\mathcal{K}[X]$ (voir chapitre 3). Ainsi on peut observer que l'on a $\mathcal{K}[\alpha] \subset \mathcal{K}(\alpha)$ avec égalité si et seulement si $\mathcal{K}[\alpha]$ est un corps. On pourra remarquer également que lorsque $\alpha \in \mathcal{K}$, on a $\mathcal{K}[\alpha] = \mathcal{K}(\alpha) = \mathcal{K}$.

Définition 39

Soit $\mathcal{L}$ un corps et $\mathcal{K} \subset \mathcal{L}$ un sous-corps de $\mathcal{L}$. On dit qu'un élément $\alpha \in \mathcal{L}$ est algébrique sur $\mathcal{K}$ s'il existe $P \in \mathcal{K}[X] \setminus \{0\}$ tel que $P(\alpha) = 0$. Un élément qui n'est pas algébrique sur $\mathcal{K}$ est dit transcendant sur $\mathcal{K}$.

Exemple 34

1. Dans $\mathcal{L} = \mathbb{R}$, $\alpha = \sqrt{2}$ est algébrique sur $\mathcal{K} = \mathbb{Q}$.
2. Dans $\mathcal{L} = \mathbb{R}$, $\alpha = \sum_{n=1}^{\infty} 10^{-n!}$ est transcendant sur $\mathcal{K} = \mathbb{Q}$ (nombre de Liouville).
3. Dans $\mathcal{L} = \mathbb{R}$, les nombres π et e sont transcendants sur $\mathbb{Q}$ (résultat difficile à montrer : théorème d'Hermite-Lindemann).
4. Si $\mathcal{K}$ est un sous-corps de $\mathcal{L}$, tout élément $\alpha \in \mathcal{K}$ est algébrique sur $\mathcal{K}$.

Remarque 22

Dans le corps $\mathbb{R}$, ce que l'on appelle nombres algébriques sont les nombres réels qui sont algébriques sur $\mathbb{Q}$. Les nombres transcendants sont les nombres qui ne sont pas algébriques.

Proposition 44

Soit $\mathcal{L}$ un corps et $\mathcal{K} \subset \mathcal{L}$ un sous-corps de $\mathcal{L}$. Si $\alpha \in \mathcal{L}$ est algébrique sur $\mathcal{K}$, alors l'ensemble

$$\mathcal{I} = \{ P \in \mathcal{K}[X] \;/\; P(\alpha) = 0 \}$$

est un idéal non nul de $\mathcal{K}[X]$. De plus, il existe un unique polynôme unitaire $P \in \mathcal{K}[X]$ tel que

$$\mathcal{I} = < P > .$$

Le polynôme P s'appelle le polynôme minimal de α et son degré s'appelle le degré de α.

Remarque 23

On peut vérifier immédiatement dans la proposition précédente que le polynôme minimal P est irréductible (ce qui est équivalent à dire que l'idéal $\mathcal{I} = < P >$ est maximal).

Nous avons la caractérisation suivante des éléments algébriques d'un corps :

Théorème 10

Soit $\mathscr{K}$ un sous-corps d'un corps $\mathscr{L}$ et soit $\alpha \in \mathscr{L}$. Alors les propriétés suivantes sont équivalentes :

1. α est algébrique sur $\mathscr{K}$
2. $\mathscr{K}[\alpha] = \mathscr{K}(\alpha)$
3. $\mathscr{K}[\alpha]$ est un corps
4. $[\mathscr{K}(\alpha) : \mathscr{K}] < +\infty$

Lorsque l'une de ces propriétés est vérifiée on a $[\mathscr{K}(\alpha) : \mathscr{K}] = \deg P$, où P est le polynôme minimal de α.

Exemple 35

1. Dans $\mathbb{R}$, $\alpha = \sqrt{2}$ est algébrique de degré 2. Plus généralement, $\alpha = 2^{1/n}$, avec $n \in \mathbb{N}^*$, est algébrique de degré n.
2. Dans $\mathbb{R}$, $\alpha = \sqrt{2} + \sqrt{3}$ est algébrique de degré 4.
3. Dans $\mathbb{C}$, $\alpha = i$ est algébrique sur $\mathbb{R}$ de degré 2.
4. Si $\mathscr{K}$ est un sous-corps de $\mathscr{L}$, tout élément $\alpha \in \mathscr{K}$ est algébrique sur $\mathscr{K}$ de degré 1.

Remarque 24

Si $\alpha \in \mathscr{L}$ est algébrique sur $\mathscr{K}$, alors on a $\mathscr{K}[\alpha] \cong \mathscr{K}[X]/< P >$, où P est le polynôme minimal de α.

Définition 40

On dit qu'un corps $\mathscr{L}$ est une extension algébrique d'un corps $\mathscr{K}$ si tout élément de $\mathscr{L}$ est algébrique sur $\mathscr{K}$.

D'après la définition prédénte toute extension finie d'un corps est une extension algébrique. mais la réciproque est fausse (voir exemple ci-dessous). Nous avons le théorème très important suivant :

Théorème 11

Soit $\mathscr{L}$ une extension d'un corps $\mathscr{K}$ et soit $\mathscr{M}$ l'ensemble des éléments de $\mathscr{L}$ qui sont algébriques sur $\mathscr{K}$. Alors nous avons les deux propriétés suivantes :

1. $\mathscr{M}$ est un sous-corps de $\mathscr{L}$ contenant $\mathscr{K}$. En particulier, $\mathscr{M}$ est une extension algébrique de $\mathscr{K}$.
2. Tout élément de $\mathscr{L}$ qui est algébrique sur $\mathscr{M}$ est dans $\mathscr{M}$. On dit que $\mathscr{M}$ est la clôture algébrique de $\mathscr{K}$ dans $\mathscr{L}$.

Exemple 36

L'ensemble des nombres réels algébriques sur $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$. En particuler, la somme, le produit et le rapport (lorsqu'il est bien défini) de deux nombres algébriques est algébrique. Notons ici que le corps des nombres algébriques est une extension algébrique non finie de $\mathbb{Q}$ (il existe des nombres algébriques de degré aussi grand que l'on veut : prendre par exemple $\alpha = 2^{1/n},\ n \in \mathbb{N}^*$).

3. Corps de rupture

Définition 41

Soit $\mathcal{K}$ un corps et $P \in \mathcal{K}[X]$ un polynôme irréductible. On dit qu'une extension $\mathcal{L}$ de $\mathcal{K}$ est un corps de rupture pour P sur $\mathcal{K}$ s'il existe une racine $\alpha \in \mathcal{K}$ de P telle que $\mathcal{K}[\alpha] = \mathcal{L}$.

Dans la définition précédente il est claire que α est algébrique sur $\mathcal{K}$.

Exemple 37

1. Pour tout $n \in \mathbb{N}^*,\ \mathcal{K}[2^{1/n}]$ est un corps de rupture de $P = X^n - 2$ sur $\mathbb{Q}$.
2. $\mathbb{C}$ et $\mathbb{Q}[i]$ sont les corps de rupture de $P = X^2 + 1$ sur $\mathbb{R}$ et $\mathbb{Q}$ respectivement.

Théorème 12

Soit $\mathcal{K}$ un corps et $P \in \mathcal{K}[X]$ un polynôme irréductible. Alors il existe un corps de rupture $\mathcal{L}$ de P sur $\mathcal{K}$ qui est unique à $\mathcal{K}$-isomorphisme près, i.e si $\mathcal{L}'$ est un autre corps de rupture de P sur $\mathcal{K}$, alors il existe un isomorphisme de $\mathcal{L}$ dans $\mathcal{L}'$ dont la restriction à $\mathcal{K}$ soit égale à l'identité de $\mathcal{K}$.