## 2.7 Théorème chinois

**Théorème 50.** *Soit $n$ et $m$ des entiers positifs. Soit $\pi_n \colon \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ et $\pi_m \colon \mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ les morphismes d'anneaux quotient. Soit $\pi_n \times \pi_m \colon \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ le morphisme d'anneaux produit.*

*Alors :*

- *On a* $\mathrm{Ker}(\pi_n \times \pi_m) = n\mathbf{Z} \cap m\mathbf{Z} = \mathrm{ppcm}(n, m)\mathbf{Z}$.
- *Supposons en outre $n$ et $m$ premiers entre eux ; alors $\pi_n \times \pi_m$ est surjectif. En particulier le morphisme $\pi_n \times \pi_m$ induit un isomorphisme d'anneaux*

$$\mathbf{Z}/nm\mathbf{Z} \xrightarrow{\sim} \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}.$$

*Démonstration.* Pendant la séance. □

**Théorème 51.** *Soit $A$ un anneau et $\mathcal{I}$, $\mathcal{J}$ deux idéaux de $A$.*

*Soit $\pi_{\mathcal{I}} \colon A \to A/\mathcal{I}$ et $\pi_{\mathcal{J}} \colon A \to A/\mathcal{J}$ les morphismes d'anneaux quotient. Soit $\pi_{\mathcal{I}} \times \pi_{\mathcal{J}} \colon A \to A/\mathcal{I} \times A/\mathcal{J}$ le morphisme d'anneaux produit.*

- *On a* $\mathrm{Ker}(\pi_{\mathcal{I}} \times \pi_{\mathcal{J}}) = \mathcal{I} \cap \mathcal{J}$.
- *Supposons en outre $\mathcal{I} + \mathcal{J} = A$. Alors $\mathcal{I} \cap \mathcal{J} = \mathcal{I} \cdot \mathcal{J}$ et le morphisme $\pi_{\mathcal{I}} \times \pi_{\mathcal{J}}$ est surjectif. En particulier $\pi_{\mathcal{I}} \times \pi_{\mathcal{J}}$ induit un isomorphisme d'anneaux*

$$A/\mathcal{I} \cdot \mathcal{J} \cong A/\mathcal{I} \times A/\mathcal{J}.$$

*Démonstration.* Pendant la séance. □

On peut généraliser à un nombre fini d'idéaux.

**Théorème 52.** *Soit $A$ un anneau. Soit $n \geqslant 1$ un entier. Soit $(\mathcal{I}_i)_{i=1,\ldots,n}$ une ensemble fini d'idéaux de $A$.*

*Pour $i = 1, \ldots, n$, soit $\pi_i \colon A \to A/\mathcal{I}_i$ le morphisme d'anneaux quotient. Soit*

$$\prod_{i=1}^{n} \pi_i \colon A \to \prod A/\mathcal{I}_i$$

*le morphisme d'anneaux produit.*

- *On a* $\mathrm{Ker}(\prod_{i=1}^{n} \pi_i) = \cap_{i=1}^{n} \mathcal{I}_i$.
- *On suppose en outre que si $i \neq j$, on a $\mathcal{I}_i + \mathcal{J}_j = A$. Alors $\cap_{i=1}^{n} \mathcal{I}_i = \prod_{i=1}^{n} \mathcal{I}_i$ et le morphisme $\prod \pi_i$ est surjectif. En particulier $\prod \pi_i$ induit un isomorphisme d'anneaux*

$$A/\prod_{i=1}^{n} \mathcal{I}_i \cong \prod_{i=1}^{n} A/\mathcal{I}_i.$$

Le démonstration de ce dernier résultat peut se faire par récurrence à partir du résultat pour deux idéaux. Il est utile de noter à ce sujet qu'on vérifie facilement que le « produit d'idéaux est associatif ». Par exemple si $\mathcal{I}_1$, $\mathcal{I}_2$ et $\mathcal{I}_3$ sont des idéaux d'un anneau $A$, on a

$$(\mathcal{I}_1 \cdot \mathcal{I}_2) \cdot \mathcal{I}_3 = \mathcal{I}_1 \cdot (\mathcal{I}_2 \cdot \mathcal{I}_3) = \mathcal{I}_1 \cdot \mathcal{I}_2 \cdot \mathcal{I}_3.$$

*Remarque.* L'hypothèse que les $\mathcal{I}_i$ sont *deux à deux* étrangers est importante, on ne peut pas se contenter de l'hypothèse $\sum_{i=1}^{n} \mathcal{I}_i = A$. On se penchera par exemple sur le cas de $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/r\mathbf{Z}$ pour $(n, m, r) = (6, 10, 15)$.

### 2.8 Diviseurs de zéros, anneaux intègres, corps

**Définition 53.** Soit $A$ un anneau. Un *diviseur de zéro* dans $A$ est un élément $a$ de $A$ tel qu'il existe un élément $b$ *non nul* de $A$ vérifiant $a \times b = 0_A$.

Un diviseur de zéro nul est appelé diviseur de zéro trivial.

*Remarque.* ATTENTION, cette terminologie, bien qu'usuelle, peut être source de confusion. Par exemple, dans $\mathbf{Z}$, n'importe quel entier divise 0, mais seul 0 est un diviseur de zéro...

*Exemple.* Un élément de $A^\times$ n'est jamais diviseur de zéro (y compris si $A$ est l'anneau nul; dans ce cas $0_A$ est inversible mais n'est pas diviseur de zéro).

Les anneaux $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{R}[X]$, $\mathbf{C}[X]$... n'ont pas de diviseurs de zéros non triviaux.

Soit $p$ et $q$ deux nombres premiers et $N := p.q$. Alors $[p]_N$ et $[q]_N$ sont des diviseurs de zéro non triviaux de $\mathbf{Z}/N\mathbf{Z}$

L'anneau nul n'a pas de diviseur de zéro. C'est d'ailleurs le seul anneau vérifiant cette propriété.

*Remarque.* ATTENTION, on peut trouver dans d'autres références une définition de « diviseur de zéro » qui correspond à ce que nous appelons « diviseur de zéro non trivial » dans ce texte. Certains des énoncés s'adaptent en conséquence. Il faut bien penser à vérifier la définition employée dans la référence consultée.

**Définition 54.** Un anneau est dit *intègre* s'il est *non nul* et ne possède pas de diviseurs de zéro non triviaux.

*Remarque.* Ainsi un anneau $A$ est intègre si et seulement si $A$ est non nul et on a la propriété

$$\forall (x, y) \in A^2, \quad x \times y = 0_A \Rightarrow (x = 0_A \text{ ou } y = 0_A).$$

C'est souvent sous cette dernière forme qu'on exploite l'intégrité d'un anneau; la généralisation à un produit de plus de deux éléments est immédiate (ritournelle : « Un produit est nul si et seulement si l'un des facteurs est nuls »).

**Proposition 55.** *Un sous-anneau d'un anneau intègre est encore intègre.*

**Définition 56.** Un *corps* est un anneau $A$ non nul et tel que tout élément non nul est inversible. De manière équivalente, un corps est un anneau $A$ tel que $A^\times = A \setminus \{0_A\}$.

*Exemple.* $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Z}/n\mathbf{Z}$ si $n$ est premier, $\mathbf{K}[X]/P\mathbf{K}[X]$ si $K$ est un corps et si $P \in \mathbf{K}[X]$ est un polynôme irréductible.

*Remarque.* Un corps est un anneau intègre.

**Proposition 57.** *Soit $A$ un anneau. Alors $A$ est un corps si et seulement $A$ possède exactement deux idéaux si et seulement si $\{0_A\} \neq A$ et $A$ et $\{0_A\}$ sont les seuls idéaux de $A$.*

**Théorème 58.** *Soit $A$ un anneau et $\mathcal{I}$ un idéal de $A$.*

*L'idéal $\mathcal{I}$ est premier si et seulement si le quotient $A/\mathcal{I}$ est intègre.*

*L'idéal $\mathcal{I}$ est maximal si et seulement si le quotient $A/\mathcal{I}$ est un corps.*

*Démonstration.* Pendant la séance. □

**Théorème 59.** *Soit $n$ un entier* strictement *positif. Alors $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si $\mathbf{Z}/n\mathbf{Z}$ est intègre si et seulement si $n$ est premier*

*Soit $\mathbf{K}$ un corps et $P \in \mathbf{K}[X]$ un polynôme* non nul. *Alors $\mathbf{K}[X]/P\mathbf{K}[X]$ est un corps si et seulement si $\mathbf{K}[X]/P\mathbf{K}[X]$ est intègre si et seulement si $P$ est irréductible.*

*Remarque.* L'anneau $\mathbf{Z}/0\mathbf{Z}$ est isomorphe à $\mathbf{Z}$, c'est donc un anneau intègre qui n'est pas un corps.

*Démonstration.* Au vu du théorème 58, cela découle aussitôt des propositions 27 et 29. □

**Corollaire 60.** *La caractéristique d'un corps est zéro ou un nombre premier.*

*Remarque.* Un anneau de caractéristique un nombre premier $p$ n'est pas nécessairement un corps. Considérer par exemple $\mathbf{Z}/p\mathbf{Z}[X]$.

## 2.9 Éléments irréductibles d'un anneau intègre

On va généraliser, dans le cadre des anneaux intègres, la notion de nombre premier d'une part, de polynôme irréductible d'autre part. Dans tout ce qui suit, $A$ est un anneau *intègre* fixé.

**Définition 61.** Soit $a$ et $b$ des éléments de $A$. On dit que $a$ divise $b$, ou encore que $b$ est un multiple de $a$, et on note $a|b$, s'il existe $c \in A$ tel que $b = c\,a$.

*Remarque.* Encore une fois, attention à la terminologie ! Tout élément de $A$ divise $0_A$, mais comme $A$ est intègre le seul diviseur de zéro dans $A$ (au sens de la définition 2.10) est $0_A$.

*Remarque.* Soit $a \in A^{\times}$. Alors $a$ divise n'importe quel élément de $A$.

**Lemme 62.** *Soit $a, b \in A$.*

*Alors $a$ divise $b$ si et seulement si on a l'inclusion $b\,A \subset a\,A$.*

*Par ailleurs les propriétés suivantes sont équivalentes :*

1. *$a$ divise $b$ et $b$ divise $a$ ;*
2. *on a $b\,A = a\,A$ ;*
3. *il existe $c \in A^{\times}$ tel que $b = c\,a$ ;*

*4. il existe $c \in A^\times$ tel que $a = c\,b$.*

**Définition 63.** Soit $a, b \in A$. On dit que $a$ et $b$ sont des éléments *associés* si l'une des quatre conditions équivalentes de la proposition précédente est vérifiée.

*Remarque.* Il est à noter que si $a$, $a'$ et $b$ sont des éléments de $A$, avec $a$ et $a'$ d'une part, $b$, $b'$ d'autre part, associés, alors $a$ divise $b$ si et seulement $a'$ divise $b'$.

**Définition 64.** Un élément $a$ de $A$ est dit *irréductible* s'il est *non inversible* et pour tous élément $b, c \in A$ tels que $a = bc$, on a $b \in A^\times$ *ou* $c \in A^\times$.

*Remarque.* Un élément irréductible est nécessairement non nul.

*Exemple.* Les éléments irréductibles de $\mathbf{Z}$ sont les nombres premiers et leurs opposés.

Les éléments irréductibles de $\mathbf{K}[X]$ sont... les polynômes irréductibles (ouf !).

*Remarque.* Soit $a \in A$. Alors $a$ est irréductible si et seulement s'il est non nul, non inversible, et tout élément qui divise $a$ est soit inversible soit associé à $a$.

Par ailleurs $a$ est irréductible si et seulement si tout élément associé à $a$ est irréductible.

**Définition 65.** Deux éléments $a$ et $b$ de $A$ sont dit *premiers entre eux* si les seuls éléments de $A$ qui divisent à la fois $a$ et $b$ sont les inversibles de $A$.

**Proposition 66.** *Soit $a$ un élément irréductible de $A$ et $b \in A$. Alors $a$ et $b$ ne sont* pas *premiers entre eux si et seulement si $a$ divise $b$. En d'autres termes, $a$ et $b$ sont premiers entre eux si et seulement si $a$ ne divise pas $b$.*

*Démonstration.* Pendant la séance. □

**Théorème 67.** *Soit $a$ un élément de $A$. Supposons l'idéal $a \cdot A$ premier et non nul. Alors $a$ est irréductible.*

*Démonstration.* Pendant la séance. □

La réciproque est *fausse* (un élément irréductible n'engendre pas toujours un idéal premier), mais les contre-exemples ne sont pas immédiats. On verra en particulier en TD que dans $\mathbf{Z}[i\sqrt{3}]$, 2 est irréductible mais n'engendre pas un idéal premier.

Nous terminons par quelques considérations spécifiques aux polynômes en une indéterminée sur un corps. Soit $\mathbf{K}$ un corps. On note $\mathrm{Irr}(\mathbf{K}[X])$ l'ensemble des polynômes unitaires irréductibles de $\mathbf{K}[X]$.

**Théorème 68.** *Soit $\mathbf{K}$ un corps. Soit $Q \in \mathbf{K}[X]$ non nul. Il existe une unique famille presque nulle $(\nu_P(Q))_{P \in \mathrm{Irr}(\mathbf{K}[X])}$ d'entiers positifs et un unique $\alpha \in \mathbf{K}^\times$ tel que*

$$Q = \alpha \prod_{P \in \mathrm{Irr}(\mathbf{K}[X])} P^{\nu_P(Q)}.$$

Nous donnerons plus tard une démonstration générale de ce théorème pour tous les anneaux dits principaux. En fait en anticipant sur les notions introduites ultérieurement, on montrera que tout anneau principal est factoriel.

**Définition 69.** Soit $\mathbf{K}$ un corps et $P \in \mathbf{K}[X] \setminus \{0\}$. On dit que $P$ est *sans facteur multiple* si pour tout $Q \in \mathrm{Irr}(\mathbf{K}[X])$ on a $\nu_Q(P) \leqslant 1$.

On vérifie qu'il est équivalent de demander que si $Q \in \mathbf{K}[X]$ est non constant alors $Q^2$ ne divise pas $P$.

**Proposition 70.** *Soit* $\mathbf{K}$ *un corps et* $P \in \mathbf{K}[X]$*. Si* $\mathrm{pgcd}(P, P') = 1$ *alors* $P$ *est sans facteur multiple.*

Attention, la réciproque est fausse en général ! Elle est vraie si $\mathbf{K}$ est de caractéristique zéro, ou plus généralement est un corps dit *parfait* (*cf.* exercices de TD ; un corps fini est parfait ; le corps des fractions rationnelles en une indéterminée sur un corps fini ne l'est pas).

**Définition 71.** Un corps $\mathbf{K}$ est dit *algébriquement clos* si tout élément de $\mathbf{K}[X]$ non constant a au moins une racine dans $\mathbf{K}$.

**Proposition 72.** *Soit* $\mathbf{K}$ *un corps algébriquement clos et* $P \in \mathbf{K}[X] \setminus \{0\}$ *sans facteur multiple. Alors* $P$ *a exactement* $\deg(P)$ *racines dans* $\mathbf{K}$*.*

## 2.10 Notion d'algèbre

**Définition 73.** Soit $A$ un anneau. Une *algèbre sur* $A$ est un couple $(B, \varphi)$ où $B$ est un anneau et $\varphi\colon A \to B$ un morphisme d'anneaux.

Si $\varphi\colon A \to B$ est une $A$-algèbre, on a une loi de composition externe naturelle (« multiplication par un scalaire »)

$$\begin{array}{rcl} A \times B & \longrightarrow & B \\ (a, b) & \longmapsto & a \cdot b := \varphi(a) b \end{array}$$

Elle vérifie les propriétés suivantes :

$$\forall b \in B, \quad 0_A \cdot b = 0_B \ ;$$

$$\forall b \in B, \quad 1_A \cdot b = b \ ;$$

$$\forall a \in A, \quad \forall (b_1, b_2) \in B^2, \quad a \cdot (b_1 + b_2) = a \cdot b_1 + a \cdot b_2 \ ;$$

$$\forall (a_1, a_2) \in A^2, \quad \forall b \in B, \quad a_1 \cdot (a_2 \cdot b) = (a_1 a_2) \cdot b.$$

En particulier si $A$ est un corps, *toute* $A$*-algèbre* $B$ *est naturellement munie d'une structure de* $A$*-espace vectoriel.*

Le produit par un scalaire vérifie aussi des propriétés de compatibilités vis à vis de la multiplication dans $A$

$$\forall (a_1, a_2) \in A^2, \quad \forall (b_1, b_2) \in B^2, \quad (a_1 \cdot b_1)(a_2 \cdot b_2) = (a_1 a_2) \cdot (b_1 b_2).$$

Réciproquement, si $B$ est un anneau muni d'une loi de composition externe

$$\begin{array}{rcl} A \times B & \longrightarrow & B \\ (a, b) & \longmapsto & a \cdot b \end{array}$$

vérifiant les propriétés ci-dessus, $B$ est naturellement muni d'une structure de $A$-algèbre : le morphisme $\varphi$ correspondant est $a \mapsto a \cdot 1_B$

*Exemple.* Tout anneau est muni d'une unique structure de $\mathbf{Z}$-algèbre.

Si $A$ est un sous-anneau de $B$, $B$ est naturellement muni d'une structure de $A$-algèbre.

En particulier, si $A$ est un anneau, $A[X]$ et $A[[X]]$ sont naturellement munis de structures de $A$-algèbres.

Si $A$ est un anneau et $B$ une $A$-algèbre, tout quotient de $B$ par un idéal est naturellement muni d'une structure de $A$-algèbre.

Si $A$ est un anneau, l'anneau nul est naturellement muni d'une structure de $A$-algèbre. $A^E$ est naturellement muni d'une structure de $A$-algèbre (morphisme diagonal)

Un anneau de caractéristique $n$ possède une unique structure de $\mathbf{Z}/n\mathbf{Z}$-algèbre (et plus généralement une unique structure de $\mathbf{Z}/m\mathbf{Z}$-algèbre pour tout multiple $m$ de $n$).

**Définition 74.** Soit $\varphi_B \colon A \to B$ et $\varphi_C \colon A \to C$ des $A$-algèbres. Un morphisme de $A$-algèbres de $B$ vers $C$ est un morphisme d'anneaux $\psi \colon B \to C$ qui vérifie $\psi \circ \varphi_B = \varphi_C$.

La plupart des propriétés et notions relatives aux anneaux et morphismes d'anneaux, correctement adaptés, s'étendent facilement aux $A$-algèbres et à leur morphismes. Par exemple la composée de deux morphismes de $A$-algèbres est un morphisme de $A$-algèbres ; on définit de manière évidente la notion d'isomorphisme de $A$-algèbres, et un morphisme de $A$-algèbres est un isomorphisme si et seulement si c'est une application bijective ; on a une notion de sous-$A$-algèbre d'une $A$-algèbre, etc...

Nous détaillons ci-dessous la situation pour l'algèbre $A[X]$ et pour les quotients de $A$-algèbres, d'une importance fondamentale dans la pratique.

**Théorème 75.** Propriété universelle de l'algèbre des polynômes en une indéterminée

*Soit $A$ un anneau. Soit $\iota \colon A \to A[X]$ le morphisme d'anneaux injectif naturel (qui munit $A$ d'une structure de $A$-algèbres). L'application*

$$\begin{array}{rcl} \mathrm{Hom}_{A-alg}(A[X], B) & \longrightarrow & B \\ \varphi & \longmapsto & \varphi(X) \end{array}$$

*est bijective.*

Slogan : « Se donner un morphisme de $A$-algèbres de la $A$-algèbre $A[X]$ vers une $A$-algèbre $B$, c'est se donner un élément de $B$. »

**Définition 76.** Soit $A$ un anneau et $B$ une $A$-algèbre. Soit $b \in B$. L'unique élément de $\mathrm{Hom}_{A-\mathrm{alg}}(A[X], B)$ qui envoie $X$ sur $b$ est appelé morphisme d'évaluation en $b$, et noté $\mathrm{ev}_b \colon P \mapsto P(b)$. On note $A[b]$ l'image de $A[X]$ par $\mathrm{ev}_b$.

Si $P \in A[X]$, une racine (ou zéro) de $P$ dans $B$ est un élément $b \in B$ tel que $P(b) = 0$.

Le résultat suivant peut de manière savante s'exprimer ainsi : « le quotient d'une $A$-algèbre par un idéal est un quotient dans la catégories des $A$-algèbres ».

**Théorème 77.** *Soit $A$ un anneau.*

*Soit $\iota \colon A \to B$ une $A$-algèbre, $\mathcal{I}$ un idéal de $B$, $\pi \colon B \to B/\mathcal{I}$ le morphisme d'anneaux quotient. On considère sur $B/\mathcal{I}$ la structure de $A$-algèbre donnée par $\pi \circ \iota$. En particulier $\pi$ est un morphisme de $A$-algèbres.*

*Soit $C$ une $A$-algèbre et $\varphi \colon B \to C$ un morphisme de $A$-algèbres dont le noyau contient $\mathcal{I}$.*

*Alors l'unique morphisme d'anneaux $\psi \colon B/\mathcal{I} \to C$ tel que $\psi \circ \pi = \varphi$ est un morphisme de $A$-algèbres.*

En particulier, les théorèmes 48, 49 et 47 restent vrais en remplaçant partout dans les énoncés « anneau » (y compris dans « morphisme d'anneaux ») par « algèbre » (sur un anneau de base fixé).