2 Notions de base de théorie des anneaux

2.1 Définition, notations et abus d'écriture, règles de calcul

2.1.1 Définition d'un anneau (commutatif, unitaire)

Considérons les ensembles suivants : $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{R}[X]$ (anneau des polynômes en une indéterminée à coefficients dans $\mathbf{R}$), $\mathbf{Z}[1/n]$ (n étant un entier non nul fixé, cette notation désigne l'ensemble des rationnels qui peuvent être représentés par une fraction dont le dénominateur est une puissance de n). Vous savez bien que ces ensembles (ainsi que d'autres que vous pouvez sans doute imaginer) sont naturellement munis d'un couple de lois de composition interne $(+, \times)$ appelées respectivement addition et multiplication, qui jouissent d'un certain nombre de propriétés communes permettant de calculer avec.

Ces ensembles (munis de l'addition et de la multuplication) sont des exemples d'anneaux. Plus généralement, un anneau sera un ensemble muni d'un couple de lois de composition interne qui possèdent (au moins pour partie) les mêmes propriétés que celles de l'addition et de la multiplication dans les exemples précédents.

Définition 1. Un anneau est un triplet $(A, \star, \perp)$ où A est un ensemble (appelé *ensemble sous-jacent* de l'anneau) et $\star$ et $\perp$ sont deux lois de composition interne sur A, lesquelles vérifient les propriétés suivantes :

1. $(A, \star)$ est un groupe *commutatif*;
2. la loi $\perp$ possède un élément neutre, est associative et commutative ;
3. la loi $\perp$ est *distributive* par rapport à la loi $\star$; ceci signifie que pour tout triplet (a, b, c) d'éléments de A, on a
$$a \perp (b \star c) = (a \perp b) \star (a \perp c)$$

2.1.2 Règles de calcul dans un anneau

Il peut être utile de relire la section 1.4 consacrée aux usages en matière de notations en théorie des groupes.

Proposition 2. *Soit $(A, +, \times)$ un anneau. On a alors les propriétés suivantes :*

$$\forall x \in A, \quad x \times 0_A = 0_A \times x = 0_A$$

$$\forall (x, y) \in A^2, \quad x \times (-y) = (-x) \times y = -(x \times y)$$

$$\forall (x, y) \in A^2, \quad (-x) \times (-y) = x \times y$$

$$\forall (x, y) \in A^2, \forall m \in \mathbf{Z}, \quad x \times (m \cdot y) = (m \cdot x) \times y = m \cdot (x \times y)$$

Proposition 3. Formule du binôme de Newton *Soit A un anneau, x et y des éléments de A. On a alors, pour tout $n \in \mathbf{N}$,*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^k \, y^{n-k}.$$

Proposition 4. *Soit A un anneau, x et y des éléments de A. On a alors, pour tout $n \in \mathbf{N}$,*

$$x^n - y^n = (x-y)(\sum_{k=0}^{n-1} x^k \, y^{n-1-k}).$$

2.1.3 Une particularité de l'anneau $(\mathbf{Z}, +, \times)$ et une petite subtilité concernant les sommes itérées dans un anneau

Nous disons ici quelque mots d'un point un peu subtil dont la compréhension, il faut bien le dire, n'est pas vraiment facilitée par les usages traditionnels en matière de notation. Soit $n \in \mathbf{Z}$. Alors pour tout élément x de $\mathbf{Z}$, les écritures $n\,x$ et $n \cdot x$ ont un sens et désignent a priori deux éléments différents, à savoir respectivement le produit de n par x et la « somme itérée n-ème » de x. Bien évidemment, et c'est heureux, ces deux éléments coïncident.

Conservons à présent notre $n \in \mathbf{Z}$ et considérons un élément x d'un anneau $(A, +, \times)$ quelconque. Alors l'expression $n \cdot x$ a toujours un sens, à savoir la « somme itérée n-ème » de x. Mais il n'est plus question en général de l'interpéter comme une multiplication, et il faudrait *a priori* éviter de l'écrire $n\,x$ (même si dans la pratique on ne s'en prive pas, y compris dans les présentes notes de cours...). Ce n'est même pas que l'égalité

$$n\,x = n \times x$$

soit fausse, c'est que son second membre n'a pas de sens en général, car $\times$ est par définition une application $A \times A \to A$, et le couple (n, x) ne fait a priori pas partie du domaine de définition de cette application. En particulier, l'égalité

$$n\,1_A = n$$

n'a pas non plus de sens en général. Une exception importante se produit lorsque A contient $\mathbf{Z}$ comme sous-anneau (*cf.* plus loin pour la définition précise d'un sous-anneau),

par exemple $A = \mathbf{Q}$ ou $A = \mathbf{R}[X]$. Dans ce cas les égalités ci-dessus ont un sens et elles sont vraies (heureusement, d'ailleurs...). Notamment 1_A n'est autre que le 1 « traditionnel ».

Mais il existe des anneaux très intéressants, tels que les anneaux $\mathbf{Z}/N\mathbf{Z}$, qui ne contiennent pas $\mathbf{Z}$ comme sous-anneau et pour lesquels il faut faire un peu attention.

2.2 Sous-anneaux d'un anneau

Définition 5. Soit A un anneau. Un *sous-anneau* de A est une partie B de A vérifiant les propriétés suivantes :

- B est un sous-groupe de $(A, +)$
- pour tout $(x, y) \in B^2$, $x \times y$ est dans B
- 1_A est dans B.

De façon similaire à ce qui se passe pour les groupes, les lois de composition interne sur un anneau induisent des lois de composition interne sur chacun de ses sous-anneaux. On montre alors, a priori sans trop de difficultés, le résultat suivant.

Proposition 6. *Un sous-anneau d'un anneau est un anneau pour les opérations induites.*

Proposition 7. *Une intersection quelconque de sous-anneaux d'un anneau est un sous-anneau de cet anneau. Plus précisément : soit A un anneau, E un ensemble et $(A_e)_{e\in E}$ une famille de sous-anneaux de A indexée par E. Alors $\cap_{e\in E} A_e$ est un sous-anneau de A.*

Voici une application de la proposition précédente.

Proposition 8. *Soit A un anneau et S une partie de A. Il existe un et un seul sous-anneau B de A qui vérifie les propriétés suivantes :*

1. *B contient S*
2. *B est minimum au sens de l'inclusion pour la propriété précédente : en d'autres termes, si C est un sous-anneau de A qui contient S, alors C contient B.*

Ce sous-anneau B est appelé le sous-anneau de C engendré par S

2.3 Le groupe des éléments inversibles d'un anneau

Définition 9. Soit A un anneau. Un élément $a \in A$ est dit *inversible* s'il admet un symétrique pour la seconde loi, c'est-à-dire qu'il existe $b \in A$ vérifiant $a \times b = 1_A$.

L'ensemble des éléments inversibles de l'anneau A est noté $A^\times$.

Théorème 10. *Soit A un anneau. Alors l'ensemble $A^\times$ est stable par la loi $\times$. En d'autres termes, pour tous $a, b \in A^\times$, on a $a\,b \in A^\times$. Ainsi la loi $\times$ induit une loi de composition interne sur $A^\times$. Muni de cette loi, $A^\times$ est un groupe commutatif.*

De manière un peu plus informelle, cet théorème dit : « l'ensemble des éléments inversibles d'un anneau est un groupe pour la multiplication ».

2.4 Morphismes d'anneaux, noyau et image d'un morphisme d'anneaux ; idéaux d'un anneau

Définition 11. Soit A et B des anneaux. Un morphisme d'anneaux est une application $\varphi : A \to B$ vérifiant les propriétés suivantes :

- φ est un morphisme de groupes de $(A, +)$ vers $(B, +)$; pour mémoire cela signifie qu'on a
$$\forall (x, y) \in A^2, \quad \varphi(x + y) = \varphi(x) + \varphi(y).$$
- On a
$$\forall (x, y) \in A^2, \quad \varphi(x\,y) = \varphi(x)\varphi(y).$$
- On a $\varphi(1_A) = 1_B$.

Proposition 12. *L'image d'un sous-anneau de l'anneau de départ par un morphisme d'anneaux est un sous-anneau de l'anneau d'arrivée.*

L'image réciproque d'un sous-anneau de l'anneau d'arrivée par un morphisme d'anneaux est un sous-anneau de l'anneau de départ.

Définition 13. Soit A et B des anneaux et $\varphi\colon A \to B$ un morphisme d'anneaux. Le noyau de φ, noté $\mathrm{Ker}(\varphi)$ est le noyau de φ en tant que morphisme de groupes $(A, +) \to (B, +)$. En d'autres termes,
$$\mathrm{Ker}(\varphi) = \varphi^{-1}(0_B) = \{a \in A, \varphi(a) = 0_B\}$$

Proposition 14. *Si φ est un morphisme d'anneaux bijectif, alors l'application réciproque de φ est encore un morphisme d'anneaux.*

La composée de deux morphismes d'anneaux (lorsqu'elle est définie) est un morphisme d'anneaux.

Un morphisme d'anneaux est injectif si et seulement si son noyau est $\{0\}$.

Si $\varphi : A \to B$ est un morphisme d'anneaux, alors pour tout $a \in A$ et tout $n \in \mathbf{Z}$, on a $\varphi(n\,a) = n\,\varphi(a)$ et pour tout $n \in \mathbf{N}$, on a $\varphi\,(a^n) = \varphi(a)^n$.

Soit $\varphi : A \to B$ un morphisme d'anneaux. Alors $\varphi(A^\times) \subset B^\times$ et l'application (co)induite

$$\varphi_{A^\times}^{B^\times} \colon A^\times \to B^\times$$

est un morphisme de groupes.

Théorème 15. *Soit A un anneau. Il existe un unique morphisme d'anneaux de $\mathbf{Z}$ vers A. C'est l'application φ_A qui à $n \in \mathbf{Z}$ associe $n \cdot 1_A$.*

Définition 16. Soit A et B des anneaux. Un *isomorphisme d'anneaux* entre A et B est un morphisme d'anneaux $\varphi \colon A \to B$ tel qu'il existe un morphisme d'anneaux $\psi \colon B \to A$ vérifiant les relations $\varphi \circ \psi = \mathrm{Id}_B$ et $\psi \circ \varphi = \mathrm{Id}_A$.

Deux anneaux sont dits *isomorphes* s'il existe un isomorphisme de l'un sur l'autre.

Proposition 17. *Un morphisme d'anneaux est un isomorphisme si et seulement si c'est une application bijective.*

En théorie des groupes, le noyau d'un morphisme de groupes est un sous-groupe du groupe de départ. Ceci montre que le noyau d'un morphisme d'anneaux est un sous-groupe du groupe sous-jacent à l'anneau de départ ; cependant ce n'est presque jamais un sous-anneau de l'anneau de départ.

Définition 18. Soit A un anneau. Un *idéal* de A est une partie $\mathcal{I}$ de A qui est un sous-groupe de $(A, +)$ et qui vérifie en outre :

$$\forall a \in A, \forall b \in \mathcal{I}, \quad a \times b \in \mathcal{I}.$$

La proposition suivante, quoique de démonstration aisée, est souvent utile dans la pratique.

Proposition 19. *Soit A un anneau et $\mathcal{I}$ un idéal de A. On a $\mathcal{I} = A$ si et seulement si $1_A \in \mathcal{I}$ si et seulement si $\mathcal{I} \cap A^\times \neq \varnothing$*

Proposition 20. *Le noyau d'un morphisme d'anneaux est un idéal de l'anneau de départ.*

Plus généralement, l'image réciproque d'un idéal de l'anneau d'arrivée par un morphisme d'anneaux est un idéal de l'anneau de départ.

L'image d'un idéal de l'anneu de départ par un morphisme d'anneaux π surjectif *est un idéal de l'anneau d'arrivée. Dans ce cas l'application $\mathcal{I} \to \pi(\mathcal{I})$ est une bijection de l'ensemble des idéaux de l'anneau de départ contenant le noyau sur l'ensemble des idéaux de l'anneau d'arrivée, de réciproque $\mathcal{J} \mapsto \pi^{-1}(\mathcal{J})$.*

Définition 21. Soit A un anneau, $\mathcal{I}$ et $\mathcal{J}$ des idéaux de A.

- La *somme* des idéaux $\mathcal{I}$ et $\mathcal{J}$ est la parties de A notée $\mathcal{I} + \mathcal{J}$ et définie par
$$\mathcal{I} + \mathcal{J} := \{a + b\}_{a \in \mathcal{I}, b \in \mathcal{J}}.$$
- Le produit des idéaux $\mathcal{I}$ et $\mathcal{J}$ est la partie de A notée $\mathcal{I} \cdot \mathcal{J}$ (voire $\mathcal{I}\mathcal{J}$) et définie par
$$\mathcal{I} \cdot \mathcal{J} = \{\sum_{f \in F} a_f b_f\}_{\substack{F \text{ ensemble fini} \\ (a_f, b_f) \in (\mathcal{I} \times \mathcal{J})^F}}$$

Plus généralement, soit E un ensemble et $(\mathcal{I}_e)_{e \in E}$ une famille d'idéaux de A indexée par E.

- La somme de cette famille d'idéaux est la partie de A notée $\sum_{e \in E} \mathcal{I}_e$ et définie comme
$$\sum_{e \in E} \mathcal{I}_e := \{\sum_{e \in E} a_e\}_{\substack{(a_e) \in \prod_{e \in E} \mathcal{I}_e \\ \{e \in E, a_e \neq 0_A\} \text{est fini}}}$$
- On suppose E fini. Le produit de la famille d'idéaux $(\mathcal{I}_e)_{e \in E}$ est la partie de A notée $\prod_{e \in E} \mathcal{I}_e$ et définie comme
$$\prod_{e \in E} \mathcal{I}_e := \{\sum_{f \in F} \prod_{e \in E} a_{e,f}\}_{\substack{F \text{ ensemble fini} \\ (a_{e,f}) \in (\prod_{e \in E} \mathcal{I}_e)^F}}$$

Proposition 22. *Soit A un anneau, E un ensemble et $(\mathcal{I}_e)_{e \in E}$ une famille d'idéaux de A indexée par E.*

Alors l'intersection $\cap_{e\in E}\mathcal{I}_e$, la somme $\sum_{e\in E}\mathcal{I}_e$ et (si E est fini) le produit

$$\prod_{e\in E}\mathcal{I}_e$$

sont des idéaux de $\mathcal{A}$.

Proposition 23. *Soit A un anneau et S une partie de A.*

1. *Il existe un unique idéal de A contenant S et minimal (au sens de l'inclusion) pour cette propriété ; on le note $S\cdot A$ (ou $\langle S\rangle$ lorsque l'anneau A est clairement indiqué par le contexte) L'idéal $S\cdot A$ est minimum (au sens de l'inclusion) parmi les idéaux de A contenant S.*
2. *On a*
$$S\cdot A=\{\sum_{s\in S} a_s\, s\}_{\substack{(a_s)\in A^S\\ \{s\in S, a_s\neq 0_A\}\text{est fini}}}.$$
En d'autres termes $S\cdot A$ est l'ensemble des « combinaisons linéaires à coefficients dans A des éléments de S ».
3. *Si T est une autre partie de A, on a*
$$S\cdot A+T\cdot A=(S\cup T)\cdot A$$
$$(S\cdot A)(T\cdot A)=(S\cdot T)\cdot A \quad \text{où} \quad S\cdot T=\{st\}_{s\in S,t\in T}$$

Définition 24. Soit A un anneau. Un idéal $\mathcal{I}$ de A est un *idéal premier* si c'est un idéal *propre* de A (c'est à dire $\mathcal{I}\neq A$) et il vérifie la propriété suivante : pour tous $x,y\in A$ tels que $xy\in\mathcal{I}$, alors $x\in\mathcal{I}$ ou $y\in\mathcal{I}$.

Un idéal $\mathcal{I}$ de A est *idéal maximal* si c'est un idéal propre de A et tout idéal $\mathcal{J}$ de A contenant $\mathcal{I}$ est soit égal à $\mathcal{I}$, soit égal à A. En d'autres termes, un idéal maximal de A est un élément maximal pour l'inclusion de l'ensemble des idéaux propres de A.

Proposition 25. *Soit A un anneau et $\mathcal{I}$ un idéal maximal de A. Alors $\mathcal{I}$ est un idéal premier de A.*

Théorème 26. (admis) *Soit A un anneau. Tout idéal propre de A est inclus dans un idéal maximal de A. En particulier tout anneau non nul possède au moins un idéal premier.*

Proposition 27. *L'image réciproque d'un idéal premier de l'anneau d'arrivée par un morphisme d'anneaux est un idéal premier de l'anneau de départ.*

Proposition 28.
1. *Soit $\mathcal{I}$ un idéal de $\mathbf{Z}$. Alors il existe un unique $n \in \mathbf{N}$ tel que $\mathcal{I} = n\mathbf{Z}$.*
2. *Soit $n, m \in \mathbf{Z}$. On a $n\mathbf{Z} \subset m\mathbf{Z}$ si et seulement si m divise n. En particulier on a $n\mathbf{Z} = m\mathbf{Z}$ si et seulement si $|n| = |m|$.*
3. *Un idéal de $\mathbf{Z}$ est premier si et seulement s'il est nul ou il est engendré par un nombre premier.*
4. *Un idéal de $\mathbf{Z}$ est maximal si et seulement s'il est engendré par un nombre premier.*

Définition 29. Soit A un anneau et $\varphi_A \colon \mathbf{Z} \to A$ l'unique morphisme d'anneaux de $\mathbf{Z}$ vers A (*cf.* théorème 15). On appelle *caractéristique de A*, et on note $car(A)$, l'unique entier positif $n \in \mathbf{N}$ tel que $\mathrm{Ker}(\varphi_A) = n\mathbf{Z}$.

L'exercice de TD n°2.9 propose de démontrer quelques propriétés de la caractéristique d'un anneau.

Soit $\mathbf{K}$ un corps (prenez $\mathbf{K} = \mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$ si vous ne savez pas ce qu'est un corps). **Pour mémoire**, un polynôme $P \in \mathbf{K}[X]$ est *irréductible* si et seulement s'il est non constant (de manière équivalente, non nul et non inversible) et toute factorisation $P = QR$, avec $Q, R \in \mathbf{K}[X]$, entraîne que soit Q, soit R est constant.

Proposition 30. *Soit $\mathbf{K}$ un corps.*
1. *Soit $\mathcal{I}$ un idéal de $\mathbf{K}[X]$. Alors il existe $P \in \mathbf{K}[X]$ tel que $\mathcal{I} = P\mathbf{K}[X]$.*
2. *Soit $P, Q \in \mathbf{K}[X]$. On a $P\mathbf{K}[X] \subset Q\mathbf{K}[X]$ si et seulement si Q divise P. En particulier on a $Q\mathbf{K}[X] = P\mathbf{K}[X]$ si et seulement s'il existe $\alpha \in \mathbf{K}^\times$ tel que $P = \alpha\, Q$.*

3. *Un idéal de* $\mathbf{K}[X]$ *est premier si et seulement s'il est nul ou il est engendré par un polynôme irréductible.*
4. *Un idéal de* $\mathbf{K}[X]$ *est maximal si et seulement s'il est engendré par un polynôme irréductible.*

2.5 Produits d'anneaux, anneaux de polynômes et de séries formelles à coefficients dans un anneau (Construire des anneaux à partir d'autres anneaux, partie 1)

Proposition 31. *Soit* E *un ensemble et* $(A_e)_{e\in E}$ *une famille d'anneaux indexées par* E. *On définit sur le produit cartésien* $\prod_{e\in E} A_e$ *deux lois de compositions internes* $+$ *et* $\times$ *comme suit : soit* $(a_e)_{e\in E}$ *et* $(b_e)_{e\in E}$ *deux élément de* $\prod_{e\in E} A_e$ *; on pose*

$$(a_e)_{e\in E} + (b_e)_{e\in E} = (a_e + b_e)_{e\in E}$$

et

$$(a_e)_{e\in E}(b_e)_{e\in E} = (a_e b_e)_{e\in E}.$$

Ces lois de composition internes sont bien définies et font de $\prod_{e\in E} A_e$ *un anneau.*

Proposition 32. *Le groupe des inversibles d'un anneau produit est le groupe produit des groupes des inversibles des composantes. Plus précisément, en reprenant les notations de la proposition 31, on a*

$$(\prod_{e\in E} A_e)^\times = \prod A_e^\times.$$

Proposition 33. *On reprend les notations de la proposition 31. Soit* $f \in E$. *Alors*

$$\pi_f : \begin{array}{ccc} \prod_{e\in E} A_e & \longrightarrow & A_f \\ (a_e) & \longmapsto & a_f \end{array}$$

est un morphisme d'anneaux.

Soit B un anneau. L'application

$$\begin{array}{rcl} \mathrm{Hom}_{\text{anneaux}}(B, \prod_{e\in E} A_e) & \longrightarrow & \prod_{e\in E} \mathrm{Hom}_{\text{anneaux}}(B, A_e) \\ \varphi & \longmapsto & (\pi_f \circ \varphi) \end{array}$$

est bijective.

Si $(\varphi_e) \in \prod_{e\in E} \mathrm{Hom}_{\text{anneaux}}(B, A_e)$ on note $\prod_{e\in E} \varphi_e$ l'élément de $\mathrm{Hom}_{\text{anneaux}}(B, \prod_{e\in E} A_e)$ qui lui correspond par la bijection ci-dessus.

Slogan. Se donner un morphisme vers un produit d'anneaux, c'est se donner un morphisme vers chaque composante du produit.

Proposition 34. *Soit E un ensemble et A un anneau. On définit sur l'ensemble A^E des applications de E vers A deux lois de compositions internes $+$ et $\times$ comme suit : soit $\varphi, \psi \in A^E$; $\varphi + \psi$ et $\varphi\psi$ sont définies respectivement par*

$$\forall e \in E, \quad (\varphi + \psi)(e) = \varphi(e) + \psi(e)$$

et

$$\forall e \in E, \quad (\varphi.\psi)(e) = \varphi(e).\psi(e)$$

Ces lois de composition internes sont bien définies et font de A^E un anneau.

L'ensemble des applications d'un ensemble E dans un anneau A est naturellement muni d'une structure d'anneau.

On passe aux anneaux de série formelles et de polynômes. Avant toute chose, il sera utile d'adopter la convention de notation suivante.

Définition. *(somme pseudo-infinie)* Soit A un anneau et $(a_n) \in A^{(\mathbf{N})}$ une suite presque nulle d'élément de A, c'est à dire : l'ensemble $\{n \in \mathbf{N}, \quad a_n \neq 0\}$ est fini.

Soit $N \in \mathbf{N}$ tel que pour tout $n \geqslant N + 1$, on a $a_n = 0$. On pose

$$\sum_{n=0}^{+\infty} a_n := \sum_{n=0}^{N} a_n.$$

On vérifie que cette définition ne dépend pas du choix d'un tel entier N. On note aussi $\sum_{n=0}^{+\infty} a_n = \sum_{n\in\mathbf{N}} a_n$.

Proposition 35. Anneaux de polynômes et de séries formelles en une indéterminée à coefficients dans un anneaux *Soit A un anneau.*

1. *L'ensemble $A^{\mathbf{N}}$ des suites à valeurs dans A, muni de l'addition « terme à terme » induite par celle de A et de la multiplication définie ainsi : soit $\boldsymbol{a} = (a_n) \in A^N$ et $\boldsymbol{b} = (b_n) \in A^{\mathbf{N}}$; alors $\boldsymbol{a} \times \boldsymbol{b}$ est la suite $\boldsymbol{c} = (c_n) \in A^{\mathbf{N}}$ définie par*

$$\forall n \in \mathbf{N}, \quad c_n = \sum_{k=0}^{n} a_k b_{n-k}$$

   est un anneau.
2. *L'ensemble $A^{(\mathbf{N})}$ des suites presque nulles à valeurs dans A, est un sous-anneau de $A^{\mathbf{N}}$. On note X l'élément de $A^{(\mathbf{N})}$ défini par $X(1) = 1$ et pour tout $n \in \mathbf{N} \setminus \{1\}$, $X(n) = 0$.*
3. *Le sous-ensemble de $A^{(\mathbf{N})}$ consitué des suites (a_n) telles que pour tout $n \geqslant 1$, on a $a_n = 0$ est un sous-anneau de $A^{(\mathbf{N})}$, naturellement isomorphe à l'anneau A. Dans la suite, on identifie l'anneau A à ce sous-anneau.*
4. *Pour tout entier naturel $N \in \mathbf{N}$, X^N est l'élément de $A^{(\mathbf{N})}$ qui vaut 1 en N et 0 partout ailleurs.*
5. *Soit $\boldsymbol{a} = (a_n) \in A^{(\mathbf{N})}$. Alors la suite $(a_n X^n)$ est une suite presque nulle d'éléments de $A^{(\mathbf{N})}$ et pour tout $N \in \mathbf{N}$ tel que pour tout $n \geqslant N + 1$, on a $a_n = 0$, on a*

$$\boldsymbol{a} = \sum_{n=0}^{N} a_n X^n = \sum_{n=0}^{+\infty} a_n X^n.$$

Définition. On note désormais $A[[X]]$ l'anneau $A^{\mathbf{N}}$ muni des lois ci-dessus et $A[X]$ le sous-anneau $A^{(\mathbf{N})}$. L'élément X introduit dans la proposition ci-dessus s'appelle l'indéterminée ou la variable. Le choix de la lettre X est essentiellement affaire de convention : tout autre symbole non déjà utilisé dans le contexte où l'on travaille ferait a priori l'affaire.

L'anneau $A[[X]]$ est l'anneau des séries formelles en une indéterminée à coefficients dans A et $A[X]$ est l'anneau des polynômes en une indéterminée à coefficients dans A.

Au vu notamment du dernier résultat de la proposition précédente, pour $\boldsymbol{a} \in A[[X]]$, on notera encore $\boldsymbol{a} := \sum_{n=0}^{+\infty} a_n X^n$ ou encore $\boldsymbol{a} := \sum_{n \in \mathbf{N}} a_n X^n$. Il s'agit bien là d'une nouvelle convention de *notation* : si $\boldsymbol{a} \notin A[X]$, la suite $(a_n X^n)$ n'est pas une suite presque nulle d'éléments de $A^{\mathbf{N}}$. Cette notation ressemble à celle de la somme d'une série en analyse, mais intervient dans un contexte différent. On adopte cette notation car elle est pratique et l'écriture des calculs qui en découle est conforme à l'intuition. On peut par exemple montrer

les égalités

$$X^r \sum_{n\in\mathbf{N}} a_n X^n = \sum_{n\in\mathbf{N}} a_n X^{n+r} = \sum_{n\geqslant r} a_{n-r} X^n.$$

Important : on représente **quasi-systématiquement** les éléments de $A[[X]]$ sous la forme de "sommes infinies" (ou finie dans le cas de $A[X]$) et quasiment jamais sous la forme de suite ; l'utilisation des suites dans la définition n'est là que pour donner une assise formellement rigoureuse à la construction.

Si $\sum_{n\in\mathbf{N}} a_n X^n$ est un élément de $A[[X]]$, la suite (a_n) est alors appelée la suite des coefficients de la série formelle. Une série formelle est nulle si et seulement si ses coefficients sont nuls. Deux séries formelles sont égales si et seulement si elles ont les mêmes coefficients (*i.e.* la même suite de coefficients).

Dans le paragraphe qui précède on peut remplacer « série formelle » par « polynôme ».

On adopte les conventions suivantes :

$$\forall n \in \mathbf{N}\cup\{-\infty\}, \quad -\infty \leqslant n$$

$$\forall n \in \mathbf{N}\cup\{-\infty\}, \quad -\infty + n = -\infty$$

Définition 36. *(Degré d'un polynôme)* Soit A un anneau. Soit $P \in A[X]$ un polynôme, noté $P = \sum_{n=0}^{+\infty} a_n X^n$, où $(a_n) \in A^{(\mathbf{N})}$. Le degré de P note $\deg(P)$, est l'élément de $\mathbf{N}\cup\{-\infty\}$ défini par

$$\deg(P) = \mathrm{Sup}\{n \in \mathbf{N}, \quad a_n \neq 0\}$$

Soit P tel que $\deg(P) \neq -\infty$. Le coefficient dominant de P est l'élément $a_{\deg(P)} \in A$.

Proposition 37. *Soit A un anneau.*

- *Soit $P \in A[X]$. On a $\deg(P) = -\infty$ si et seulement si $P = 0$.*
- *Soit $P, Q \in A[X]$.*
  - *On a $\deg(P+Q) \leqslant \mathrm{Max}(\deg(P), \deg(Q))$ avec égalité si $\deg(P) \neq \deg(Q)$.*
  - *On a*

    $$\deg(PQ) \leqslant \deg(P) + \deg(Q)$$

    avec égalité si le coefficient dominant de P (ou de Q) n'est pas diviseur de zéro (par exemple s'il est inversible, ou s'il est non nul et A est intègre) ou si P ou Q est nul.
- *Si A est un anneau intègre, $A[X]$ est un anneau intègre.*
- *(morphisme d'évaluation) Soit $a \in A$ et $P \in A[X]$, noté $P = \sum_{n=0}^{+\infty} b_n X^n$. Alors $\sum_{n=0}^{+\infty} b_n a^n$ est bien défini comme élément de A : on le note $P(a)$. L'application qui à $P \in A[X]$ associe $P(a) \in A$, notée ev_a, est un morphisme d'anneaux.*

On adopte les conventions suivantes :

$$\forall n \in \mathbf{N} \cup \{+\infty\}, \quad n \leqslant +\infty$$

$$\forall n \in \mathbf{N} \cup \{-\infty\}, \quad +\infty + n = +\infty$$

Définition 38. *(Valuation d'une série formelle)* Soit $P \in A[[X]]$ une série formelle, notée $P = \sum_{n=0}^{+\infty} a_n X^n$, où $(a_n) \in A^{\mathbf{N}}$. La valuation de P notée $\nu(P)$, est l'élément de $\mathbf{N} \cup \{+\infty\}$ défini par

$$\nu(P) = \mathrm{Inf}\{n \in \mathbf{N}, \quad a_n \neq 0\}.$$

Soit P tel que $\nu(P) \neq +\infty$. La *composante angulaire* de P est l'élément $a_{\nu(P)} \in A$.

Proposition 39. *Soit A un anneau.*

- *Soit $P \in A[[X]]$. On a $\nu(P) = +\infty$ si et seulement si $P = 0$.*
- *Soit $P, Q \in A[[X]]$.*
  - *On a $\nu(P+Q) \geqslant \mathrm{Min}(\nu(P), \nu(Q))$ avec égalité si $\nu(P) \neq \nu(Q)$.*
  - *On a*
    $$\nu(PQ) \geqslant \nu(P) + \nu(Q),$$
    avec égalité si la composante angulaire de P (ou de Q) n'est pas diviseur de zéro (par exemple si elle est inversible, ou si elle est non nulle et A est intègre) ou si P ou Q est nul.
- *Si A est un anneau intègre, $A[[X]]$ est un anneau intègre.*

Proposition 40. (Division euclidienne dans un anneau de polynômes à coefficients dans un anneau) *Soit A un anneau. Soit $P_1, P_2 \in A[X]$, P_2* non nul *et de coefficient dominant* ***inversible****. Il existe alors un unique couple (Q, R) tel que $P_1 = QP_2 + R$ et* $\deg(R) < \deg(P_2)$.

Définition 41. Soit A un anneau et P un élément de $A[X]$. Une racine (ou zéro) de P (dans A) est un élément $a \in A$ tel que $P(a) = 0$.

Corollaire 42. *Soit $P \in A[X]$, et $a \in A$. Alors a est une racine de P si et seulement si $X - a$ divise P*

Corollaire 43. *Soit A un anneau **intègre** et $P \in A[X]$ un polynôme non nul. Alors $A[X]$ a au plus* $\deg(P)$ *racines dans A. En particulier, si $A[X]$ a une infinité de racines dans A, alors P est le polynôme nul.*

Voici une propriété très importante des anneaux de polynômes en une indéterminée

Théorème 44. PROPRIÉTÉ UNIVERSELLE DE L'ANNEAUX DES POLYNÔMES EN UNE INDÉTERMINÉE *Soit A un anneau. Soit $\iota\colon A \to A[X]$ le morphisme d'anneaux injectif naturel. Soit B un autre anneau. L'application*

$$\begin{array}{ccc} \mathrm{Hom}_{\text{anneaux}}(A[X], B) & \longrightarrow & \mathrm{Hom}_{\text{anneaux}}(A, B) \times B \\ \varphi & \longmapsto & (\varphi \circ \iota, \varphi(X)) \end{array}$$

est bijective

Slogan. Se donner un morphisme de $A[X]$ vers B, c'est se donner un morphisme de A vers B et un élément de B.

Définition. Avec les mêmes notations que dans le théorème, on pourra noter $\varphi(A)[b]$ ($A[b]$ quand φ est injective et clairement indiquée par le contexte) le sous anneau de B image de $A[X]$ par le morphisme correspondant à $\theta(\varphi, b)$.

Soit $N \geqslant 1$ un entier (qu'on pourra supposer égal à 2 en première lecture pour fixer les idées). Il existe (au moins) deux façons de définir l'anneau des polynômes $A[X_1, \ldots, X_N]$ en N indéterminées à coefficients dans A.

- On itère la construction précédente $A[X_1, X_2] := (A[X_1])[X_2]$, $A[X_1, X_2, X_3] = (A[X_1, X_2])[X_3])$, etc
- on considère l'ensemble $A^{(\mathbf{N}^N)}$ des applications presques nulles de $\mathbf{N}^N$ vers A. L'addition est définie terme à terme. Le produit de $\boldsymbol{a} = (a_{\boldsymbol{n}})$ et $\boldsymbol{b} = b_{\boldsymbol{n}}$ est

$$\forall \boldsymbol{n} \in \mathbf{N}^N, \quad (\boldsymbol{a} \times \boldsymbol{b})_{\boldsymbol{n}} = \sum_{\substack{\boldsymbol{m}, \boldsymbol{k} \in \mathbf{N}^N \\ \boldsymbol{m}+\boldsymbol{k}=\boldsymbol{n}}} a_{\boldsymbol{m}} b_{\boldsymbol{k}}$$

Ces deux constructions conduisent à des anneaux isomorphes (et même à des A-algèbres isomorphes, *cf.* plus loin). Via la seconde construction, l'indéterminée X_i n'est autre que l'élément de $A^{(\mathbf{N}^N)}$ nul en tout élément de $\mathbf{N}^N$ sauf en l'élément $\boldsymbol{n}^{(i)} := (0, \ldots, 0, 1, 0, \ldots, 0)$ (1 est placé au rang i) où il vaut 1_A.

Tout élément de $A[X_1, \ldots, X_N]$ s'écrit alors de manière unique

$$\sum_{\boldsymbol{n} \in \mathbf{N}^N} a_{\boldsymbol{n}} \prod_{i=1}^{N} X_i^{n_i}$$

avec $\boldsymbol{a} = (a_{\boldsymbol{n}}) \in A^{(\mathbf{N}^N)}$.

Une remarque similaire vaut pour les séries formelles en N indéterminées (qui ne seront pas du tout utilisées dans ce cours). On peut même construire des versions avec un nombre infini (dénombrable ou non) d'indéterminées.

D'après la première construction et la proposition 37, on voit que que si A est un anneau intègre, alors $A[X_1, \ldots, X_N]$ est encore un anneau intègre.

Théorème 45. PROPRIÉTÉ UNIVERSELLE DE L'ANNEAU DE POLYNÔMES EN N INDÉTERMINÉES *Soit A un anneau et $N \geqslant 1$ un entier. Soit $\iota \colon A \to A[X_1, \ldots, X_N]$ le morphisme d'anneaux injectif naturel. Soit B un autre anneau. L'application*

$$\begin{array}{rcl} \mathrm{Hom}_{\text{anneaux}}(A[X_1, \ldots, X_N], B) & \longrightarrow & \mathrm{Hom}_{\text{anneaux}}(A, B) \times B^N \\ \varphi & \longmapsto & (\varphi \circ \iota, \varphi(X_1), \ldots, \varphi(X_N)) \end{array}$$

est bijective

Slogan. Se donner un morphisme de $A[X_1, \ldots, X_N]$ vers B, c'est se donner un morphisme de A vers B et N éléments de B.

2.6 Anneaux quotient (Construire des anneaux à partir d'autres anneaux, partie 2)

Théorème 46. *Soit A un anneau, $\mathcal{I}$ un idéal de A. Il existe un anneau B et un morphisme surjectif $\pi \colon A \to B$ de noyau $\mathcal{I}$.*

Le couple (B, π) est unique à isomorphisme unique près, c'est-à-dire : soit (B_i, π_i), $i \in \{1, 2\}$, deux couples où B_i est un anneau commutatif et $\pi_i \colon A \to B_i$ un morphisme surjectif de noyau $\mathcal{I}$. Alors il existe un unique *isomorphisme d'anneaux $\varphi \colon B_1 \to B_2$ tel que $\varphi \circ \pi_1 = \pi_2$.*

L'anneau B de l'énoncé est appelé *anneau quotient* (de A par $\mathcal{I}$) et noté $A/\mathcal{I}$. Le morphisme π est appelé *morphisme quotient*. L'énoncé d'unicité nous permet moralement de parler de « l' » anneau quotient de A par $\mathcal{I}$ et « du » morphisme quotient.

Définition. (déjà utilisée ci-dessus) Soit A un anneau, $\mathcal{I}$ un idéal de A. Pour $(x, y) \in A^2$, la notation $x = y \pmod{\mathcal{I}}$ (ou $x \Leftrightarrow y \pmod{\mathcal{I}}$) se lit « x est congru à y modulo $\mathcal{I}$ », ou « x est égal à y modulo $\mathcal{I}$ » et signifie que $x - y \in \mathcal{I}$.

Théorème 47. Propriété universelle de l'anneau quotient - Théorème de factorisation *Soit A un anneau, $\mathcal{I}$ un idéal de A, $\pi\colon A \to A/\mathcal{I}$ le morphisme quotient.*

Soit B un anneau et $\varphi\colon A \to B$ un morphisme d'anneaux dont le noyau contient $\mathcal{I}$. Alors il existe un unique morphisme d'anneaux $\psi\colon A/\mathcal{I} \to B$ tel que $\psi \circ \pi = \varphi$

En outre :

- *ψ est surjectif si et seulement si φ est surjectif ;*
- *ψ est injectif si et seulement si $\operatorname{Ker}(\varphi) = \mathcal{I}$.*

En particulier, si φ est surjectif de noyau $\mathcal{I}$, il existe un unique isomorphisme d'anneaux $\psi\colon A/\mathcal{I} \xrightarrow{\sim} B$ tel que $\varphi = \psi \circ \pi$.

Ce théorème est un outil de base fondamental pour travailler avec des anneaux quotient, notamment pour constuire des morphismes de source un anneau quotient.

Slogan. Se donner un morphisme d'anneaux de $A/\mathcal{I}$ vers B, c'est se donner un morphisme d'anneaux de A vers B dont le noyau contient $\mathcal{I}$.

De façon un peu moins informelle : A anneau et $\mathcal{I}$ idéal étant fixés (soit $\pi\colon A \to A/\mathcal{I}$ le morphisme quotient), pour tout anneau B, l'application qui à $\psi \in \operatorname{Hom}(A/\mathcal{I}, B)$ associe $\psi \circ \pi \in \operatorname{Hom}(A, B)$ permet d'identifier $\operatorname{Hom}(A/\mathcal{I}, B)$ et $\{\varphi \in \operatorname{Hom}(A, B), \quad \mathcal{I} \subset \operatorname{Ker}(\varphi)\}$.

Slogan. Pour montrer que l'anneau B est isomorphe à l'anneau quotient $A/\mathcal{I}$, il suffit de construire un morphisme surjectif $A \to B$ de noyau $\mathcal{I}$.

Comme corollaire immédiat du théorème précédent, on obtient divers « théorèmes d'isomorphisme ». Basiquement, un théorème d'isomorphisme identifie sous certaines hypothèses deux quotients construits a priori « différemment ».

Théorème 48. Théorèmes d'isomorphisme

1. *Soit $\varphi\colon A \to B$ un morphisme d'anneaux.*
   (a) *Le morphisme φ induit un isomorphisme de $A/\operatorname{Ker}(\varphi)$ sur l'anneau $\operatorname{Im}(\varphi)$. En particulier, si φ est surjectif, φ induit un isomorphisme de $A/\operatorname{Ker}(\varphi)$ sur B. De manière générale, l'anneau quotient $A/\operatorname{Ker}(\varphi)$ est toujours isomorphe à un sous-anneau de B.*

(b) *Supposons φ surjectif. Soit $\mathcal{J}$ un idéal de B. Alors la composition de φ avec le morphisme quotient $B \to B/\mathcal{J}$ induit un isomorphimse de $A/\varphi^{-1}(\mathcal{J})$ sur $B/\mathcal{J}$.*

(c) *Supposons φ surjectif. Soit $\mathcal{I}$ un idéal de A. Alors la composition de φ avec le morphisme quotient $B \to B/\varphi(\mathcal{I})$ induit un isomorphisme de $A/(\mathcal{I}+\mathrm{Ker}(\varphi))$ sur $B/\varphi(\mathcal{I})$.*

2. *Soit $\mathcal{I}$ un idéal de A. On note $\pi_{\mathcal{I},X}\colon A[X] \to (A/\mathcal{I})[X]$ l'unique morphisme qui envoie X sur X et qui induit le morphisme $A \to (A/\mathcal{I})[X]$ donné par la composition des flèches naturelle $A \to A/\mathcal{I} \to (A/\mathcal{I})[X]$. Soit $\mathcal{J}$ un idéal de $A[X]$. Alors la composition du morphisme $\pi_{\mathcal{I},X}$ avec le morphisme quotient $(A/\mathcal{I})[X] \to (A/\mathcal{I})[X]/\pi_{\mathcal{I},X}(\mathcal{J})$ induit un isomorphisme de $A[X]/(\mathcal{I}\cdot A[X]+\mathcal{J})$ sur $(A/\mathcal{I})[X]/\pi_{\mathcal{I},X}(\mathcal{J})$.*

2.7 Théorème chinois

Théorème 49. *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*

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

Théorème 50. *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 le morphisme $\pi_{\mathcal{I}} \times \pi_{\mathcal{J}}$ induit un isomorphisme d'anneaux*

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

On peut généraliser le théorème chinois à un nombre fini d'idéaux.

Théorème 51. *Soit A un anneau. Soit $n \geqslant 1$ un entier. Soit $(\mathcal{I}_i)_{i=1,\dots,n}$ un ensemble fini d'idéaux de A.*

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

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

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 $\mathcal{I}_i + \mathcal{I}_j = A$. 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

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

2.8 Diviseurs de zéros, anneaux intègres, corps

Définition 52. 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.

Définition 53. Un anneau est dit *intègre* s'il est *non nul* et ne possède pas de diviseurs de zéro non triviaux.

Proposition 54. *Soit A un anneau. Alors A est intègre si et seulement si l'idéal nul $\{0_A\}$ est un idéal premier.*

Proposition 55. *Un sous-anneau d'un anneau intègre est encore un anneau 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 $A^\times = A \setminus \{0_A\}$.

Un *sous-corps* d'un corps est un sous-anneau de ce corps qui est également un corps.

Un *morphisme de corps* entre deux corps est un morphisme d'anneaux entre ces deux corps ; un morphisme de corps est aussi appelé une *extension de corps*.

Proposition 57. *Soit A un anneau. Les propriétés suivantes sont équivalentes :*

- *A est un corps ;*
- *A possède exactement deux idéaux ;*
- *$\{0_A\} \neq A$ et A et $\{0_A\}$ sont les seuls idéaux de A ;*
- *$\{0_A\}$ est un idéal maximal de A.*

En particulier si A est un corps, B est un anneau non nul, et $\varphi\colon A \to B$ est un morphisme d'anneaux, φ est injectif et B possède un sous-anneau isomorphe au corps 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.

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.*

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

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 $b = c\,a$.

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.

Slogan. Les propriétés des éléments d'un anneau intègre liées à la notion de divisibilité sont « invariantes par association ».

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* $c \in A^\times$.

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.*

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

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 la terminologie introduite 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 $\nu_Q(P) \leqslant 1$.

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, φ) 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, on a la remarque importante suivante : si A est un corps, *toute A-algèbre B est naturellement munie d'une structure de A-espace vectoriel*. Rappelons qu'en outre si B n'est pas l'anneau nul alors B possède un sous-anneau isomorphe au corps A.

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 φ correspondant est $a \mapsto a \cdot 1_B$

Définition 74. Soit $\varphi_B\colon A \to B$ une A-algèbre. Une sous-A-algèbre de B est un sous-anneau B' de B tel que le morphisme d'anneaux $\iota\colon B' \to B$ se factorise par φ_B, en d'autres termes il existe une structure de A-algèbre $\varphi_{B'}\colon A \to B'$ telle que $\varphi_B = \iota \circ \varphi_{B'}$.

Soit $\varphi_C\colon A \to C$ une autre A-algèbre. 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, sous-anneaux et morphismes d'anneaux, correctement adaptés, s'étendent facilement aux A-algèbres et à leur morphismes et sous-algèbres.. 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.

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

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

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 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 π 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 47, 48 et 46 restent vrais en remplaçant partout dans les énoncés « anneau » (y compris dans « morphisme d'anneaux ») par « algèbre » (sur un anneau de base fixé).

Complément : notion de sous-algèbre

Cette notion est très similaires à la notion de sous-anneau d'un anneau et jouit de propriétés élémentaires analogues. Elle ne figure pas dans le cours (en particulier aucune connaissance à ce sujet n'est exigible lors des examens écrits) pour ne pas alourdir démesurément le chapitre 2, et également car elle intervient dans ce module uniquement dans l'exercice de TD n° 3.15.

On donne juste la définition et quelques énoncés sans preuve. Les démonstrations ne sont *a priori* pas très difficiles (« Il suffit d'écrire »)

- Soit A un anneau et $\iota\colon A \to B$ une A-algèbre ; une *sous-A-algèbre de B* est un sous-anneau C de B tel que $\iota(A) \subset C$. Noter que cette dernière condition entraîne que ι induit par corestriction un morphisme d'anneaux $A \to C$, en d'autre termes une structure de A-algèbre sur C ; on munira systématiquement une sous-algèbre de cette structure induite. *Exemples* : B est une sous-A-algèbre de B ; $\iota(A)$ est une sous-A-algèbre de B.
- Soit A un anneau et $\iota\colon A \to B$ une A-algèbre ; soit $A \times B \to B, \quad (a, b) \mapsto a \cdot b$ la loi de composition externe induite ; soit C un sous-anneau de B ; alors C est une sous-A-algèbre de B si et seulement si pour tout $a \in A$ et tout $c \in C$ on a $a \cdot c \in C$ si et seulement si pour tout $a \in A$ on a $a \cdot 1_B \in C$.
- Soit A un anneau et $\iota\colon A \to B$ une A-algèbre. Une intersection quelconque de sous-A-algèbres de B est une sous-A-algèbre de B.
- Soit A un anneau, $A \to B$ une A-algèbre et $S \subset B$ une partie de B. Il existe une unique sous-A-algèbre de B contenant S et minimale (au sens de l'inclusion) pour cette condition. Elle est également minimum (au sens de l'inclusion) pour cette condition. On l'appelle la *sous-A-algèbre de B engendrée par S*.
- Soit A un anneau, $A \to B$ et $A \to C$ des A-algèbres et $\varphi\colon B \to C$ un morphisme de A-algèbres. Soit D une sous-A-algèbre de B. Alors $\varphi(D)$ est une sous-A-algèbre de C. En particulier $\varphi(B)$ est une sous A-algèbre de C.
- Soit A un anneau, $A \to B$ une A-algèbre et $b \in B$. Soit $\mathrm{ev}_b\colon A[X] \to B$ l'unique morphisme de A-algèbres qui envoie X sur b (*cf.* la définition 76). Alors la sous-A-algèbre de B engendrée par b est $\mathrm{ev}_b(A[X])$ et est notée $A[b]$ (*cf.* l'exercice 2.1). On a la description :
$$A[b] = \{\sum_{i \in \mathbf{N}} a_i \cdot b^i\}_{(a_i) \in A^{(\mathbf{N})}}.$$