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
$$a \perp (b \star c) = (a \perp b) \star (a \perp c)$$

Remarque. Les abus d'écriture traditionnels sont essentiellement de la même nature que ceux pratiqués pour les groupes (lesquels ont été rappelés dans la première partie). Ainsi, bien que cela soit en toute rigueur abusif, on écrira ou on dira le plus souvent « soit A un anneau… » plutôt que « soit $(A, \star, \perp)$ un anneau… » lorsque les lois mises en jeu sont clairement indiquées par le contexte [6] ; si on pratique cet abus, il est en général implicite que les notations pour les lois de A sont la notation additive pour la première loi et la notation multiplicative pour la seconde (*cf.* la remarque suivante)

Remarque. Les usages en termes de notations sont que la première loi d'un anneau est quasi-systématiquement notée additivement, et la seconde loi est très souvent notée multiplicativement. L'élément neutre de la première loi est ainsi noté 0 et l'élément neutre de la seconde loi 1. L'élément neutre de la seconde loi est souvent appelé l'*élément unité* (voire l'*unité*) de l'anneau, mais attention le terme *unité* désigne n'importe quel élément inversible

6. Si A est un anneau, le cas de l'ensemble $A^{\mathbf{N}}$, qui porte, comme on le verra, au moins deux structures naturelles différentes d'anneau, montre que ce n'est pas toujours le cas

de l'anneau. Pour des raisons pédagogiques, il peut être utile d'écrire plutôt 0_A et 1_A, où A est l'anneau considéré.

Exemple. Il y a déjà tous les exemples déjà évoqués ci-dessus.

Voici un autre exemple sans doute moins connu. Soit $A = \{a\}$ un ensemble réduit à un élément, muni des lois de composition interne $\star$ et $\perp$ définies par les deux relations $a \star a = a$ et $a \perp a = a$. On montre que $(A, \star, \perp)$ est bien un anneau, et qu'on a dans A l'égalité $1_A = 0_A$. Un tel anneau est appelé ***l'anneau nul***. L'article défini est justifié par le fait qu'on peut montrer que tout anneau dont l'ensemble sous-jacent est réduit à un élément est isomorphe à A (*cf.* si nécessaire un peu plus loin pour la notion d'isomorphisme d'anneaux)

On montre par ailleurs que pour un anneau $(A, \star, \perp)$ quelconque, le fait d'être (isomorphe à) l'anneau nul est équivalent à l'égalité $0_A = 1_A$

Remarque. Ce qu'on a défini ici comme étant un « anneau » sera pour d'autres auteurs un « anneau commutatif avec unité ». Dans ce cours, le terme « anneau » est donc synonyme d'« anneau commutatif avec unité ». On peut notamment [7] relâcher la définition en ne demandant pas que la seconde loi, notée $\perp$ dans la définition, soit commutative (anneaux non commutatifs) [8] et/ou en ne demandant pas qu'elle admette un élément neutre (anneaux sans élément unité). Attention, la première loi, notée $\star$ dans la définition, est *toujours* commutative, même pour un anneau dit « non commutatif ». La théorie des anneaux non commutatifs est assez différente de celles des anneaux commutatifs. Contentons nous ici de donner un exemple d'anneau non commutatif (mais avec unité) : le triplet $(M_n(\mathbf{K}), +, \times)$ où $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$, $M_n(\mathbf{K})$ est l'ensemble des matrices carrées de taille n (avec $n \geqslant 2$) à coefficients dans $\mathbf{K}$, $+$ est l'addition matricielle et $\times$ la multiplication matricielle.

Remarque. Les règles de priorité d'écriture sont les mêmes que celles appliquées traditionnellement sur $\mathbf{Z}$, à savoir : la deuxième loi est prioritaire sur la première. Ainsi, si $(A, +, \times)$ est un anneau, l'écriture $a \times b + c$ signifie $(a \times b) + c$ (ou $(a\, b) + c$ en pure notation multiplicative) et désigne donc un élément a priori différent de $a \times (b + c)$.

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.

Remarque. Soit $(A, +, \times)$ un anneau. Pour tout élément a de A et pour n entier *naturel* il est alors possible, et la démarche est strictement similaire à celle de la définition 9, de définir la *puissance itérée n-ème de A*, noté a^n. On a alors les mêmes règles de calcul de puissances que pour les lois de groupes, en se limitant toutefois aux exposants positifs.

Il y a bien sûr aussi une notion de « puissance itérée » pour la première loi (qui appraît notamment dans la proposition 2 ci-dessous). Rappelons que vu la notation adoptée pour

7. C'est utile dans certains contextes qui dépassent le cadre de ce cours.
8. Il faut alors demander la distributivité « à droite et à gauche »

la première loi, à savoir la notation additive, on parlera ici plutôt de « somme itérée » ; on se reportera à la section 2.1.3 pour une petite subtilité à ce sujet.

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

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

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

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

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

Démonstration. Soit $x \in A$. On a, en utilisant la distributivité :

$$x \times 0_A = x \times (0_A + 0_A) = x \times 0_A + x \times 0_A.$$

En ajoutant $-(x \times 0_A)$ à chaque membre, on obtient $x \times 0_A = 0_A$.

Les démonstrations des autres propriétés sont d'un niveau de difficulté similaire et laissées à titre d'exercice. La dernière propriété N'EST PAS une conséquence directe de l'associativité de la loi $\times$. On pourra à ce sujet se reporter à la section 2.1.3 □

Remarque. Si $(a_i)_{i \in I}$ est une famille d'éléments d'un anneau A indexée par un ensemble fini I, on peut donner un sens (conforme à l'intuition) aux expressions $\sum_{i \in I} a_i$ et $\prod_{i \in I} a_i$; notons que si I est l'ensemble vide, on a $\sum_{i \in I} a_i = 0$ et $\prod_{i \in I} a_i = 1$.

Les règles de calculs algébriques classiques bien connues sur les sommes et produits finis de nombres complexes s'étendent (avec des démonstrations strictement similaires). Ainsi on a la formule de « distributivité généralisée » suivant : si $(a_i)_{i \in I}$ (resp. $(b_j)_{j \in J}$) est une famille d'éléments de A indexée par un ensemble fini I (resp. J), on a

$$(\sum_{i \in I} a_i)(\sum_{j \in J} b_j) = \sum_{(i,j) \in I \times J} a_i b_j.$$

Proposition 3. FORMULE DU BINÔME DE NEWTON *Soit A un anneau, x et y des éléments de A. On a alors, pour tout $n \in \mathbf{N}$,*

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

Démonstration. Par récurrence en utililisant la formule de Pascal pour les coefficients binomiaux ; en d'autres termes, strictement similaire à celle a priori déjà vue dans le cas $A = \mathbf{C}$. N'hésitez pas à essayer de réécrire la démonstration si besoin. □

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

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

Démonstration. Strictement similaire à celle a priori déjà vue dans le cas $A = \mathbf{C}$. □

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.

Exemple. Soit A un anneau. On montre que l'ensemble $\{n \cdot 1_A\}_{n \in \mathbf{Z}}$ est un sous-anneau de A.

Exemple. Soit n un entier non nul. Considérons la chaîne d'inclusions

$$\mathbf{Z} \subset \mathbf{Z}[1/n] \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C} \subset \mathbf{C}[X]$$

Alors toute inclusion $A \subset B$ extraite de cette chaîne (par exemple $\mathbf{Z}[1/n] \subset \mathbf{R}$) fait de A un sous-anneau de B.

Exemple. Soit I un intervalle ouvert de $\mathbf{R}$. L'ensemble $\mathbf{R}^I$ des applications de I dans $\mathbf{R}$ est naturellement muni d'une structure d'anneau (*cf.* plus loin si nécessaire). On montre que l'ensemble des fonctions continues (resp. dérivables, resp. $\mathcal{C}^n$ ($n \geqslant 1$ un entier), resp. $\mathcal{C}^\infty$ est un sous-anneau de $\mathbf{R}^I$.

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.*

Remarque. L'un des principaux intérêts de la notion de sous-anneau est semblable à celui pour les groupes décrit dans la remarque suivant la proposition 8 du chapitre 1 : pour montrer qu'un triplet $(A, +\times)$ est un anneau, il est souvent plus commode, quand c'est possible, de montrer que A s'identifie à un sous-anneau d'un anneau « connu » plutôt que d'appliquer directement la définition 1.

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.*

Démonstration. Exercice de TD n°1.2 □

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

Démonstration. Existence Soit E l'ensemble des sous-anneaux de A qui contiennent S, et $B := \cap_{C \in E} C$. En particulier, B est une intersection de sous-anneaux de A, donc, d'après la proposition 7, B est un sous-anneau de A. En outre, par construction, B contient S et tout sous-anneau de A contenant S, c'est-à-dire tout élément de E, contient B.

Unicité Soient B_1 et B_2 deux sous-anneaux de A vérifiant les propriétés de l'énoncé. En particulier B_1 et B_2 contiennent S. Comme B_1 vérifie la seconde propriété et B_2 est un sous-anneau de A qui contient S, on a $B_1 \subset B_2$. En permutant les rôles de B_1 et B_2, on a également $B_2 \subset B_1$. Donc $B_1 = B_2$. □

Remarque. L'énoncé ci-dessus est encore valide si on remplace *minimum* par *minimal*; *cf.* l'énoncé correspondant ci-dessous pour les idéaux.

Exemple. Soit A un anneau. Le sous-anneau de A engendré par $\{0_A\}$ est $\{n \cdot 1_A\}_{n \in \mathbf{Z}}$. Ce sous-anneau est également le sous-anneau de A engendré par $\{1_A\}$ ou par $\{0_A, 1_A\}$, voire par $\varnothing$. Insistons au passage sur le fait que $\{0_A, 1_A\}$ n'est pas en général un sous-anneau de A.

Remarque. La démonstration de l'énoncé ci-dessus donne en un sens une description du sous-anneau engendré par une partie, mais comme on peut s'y attendre une telle description n'est en général d'aucune utilité dans la pratique, et on peut se demander s'il existe des descriptions plus explicites du sous-anneau engendré par une partie. On se reportera à l'exercice de TD n°2.1 pour le cas d'un sous-anneau engendré par un seul élément.

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 $ab \in A^\times$. 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 ».

Démonstration. On peut le faire « à la main ». Une démonstration un peu plus jolie consiste à identifier $A^\times$ à un sous-ensemble du groupe $\mathfrak{S}_A$ des bijections de A sur A via l'application $a \in A^\times \mapsto (x \mapsto a.x)$ (dont on montre qu'elle est bien définie et injective). On montre ensuite que la loi de groupe sur $\mathfrak{S}_A$, c'est-à-dire la composition des bijections, induit la multiplication sur $A^\times$, puis que $A^\times$ est un sous-groupe de $\mathfrak{S}_A$. On n'hésitera pas à essayer de rédiger les détails des arguments. □

Exemples. $\mathbf{Z}^\times = \{1, -1\}$, $\mathbf{R}^\times = \mathbf{R} \setminus \{0\}$, $\mathbf{R}[X]^\times = \mathbf{R}^\times$ (ensemble des polynômes constants non nuls). Plus généralement si A est un anneau intègre $A[X]^\times = A^\times$ (*cf.* si nécessaire plus loin pour les notions d'anneau intègre et de polynômes à coefficients dans un anneau quelconque ; attention, si A n'est pas intègre on a toujours l'inclusion $A^\times \subset A[X]^\times$ mais l'inclusion est stricte en général, *cf.* l'exercice de TD n°1.10.8)

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
$$\forall (x, y) \in A^2, \quad \varphi(xy) = \varphi(x)\varphi(y).$$
- On a $\varphi(1_A) = 1_B$.

Remarque. La dernière condition est essentiellement là pour « éviter » les morphismes inintéressants du type $x \mapsto 0_B$.

Notons qu'étant donné deux anneaux, il n'existe pas nécessairement de morphisme d'anneaux de l'un sur l'autre (contrairement à ce qui se passe pour les morphismes de groupes). On peut montrer par exemple :

- Si A est un anneau non nul, il n'existe aucun morphisme de l'anneau nul vers A

- Il n'existe aucun morphisme d'anneaux de $\mathbf{Q}$ vers $\mathbf{Z}$, plus généralement aucun morphisme d'anneaux d'un corps vers $\mathbf{Z}$.

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.

Démonstration. Exercice de TD n°1.4 ; à savoir faire *absolument* □

Exemples. Si A est un anneau et B est un sous-anneau de A, l'application injective $B \to A$ déduite de l'inclusion de B dans A est un morphisme d'anneaux.
La conjugaison complexe sur $\mathbf{C}$ est un morphisme d'anneaux.
Soit A et B des anneaux. L'application de projection $A \times B \to A$ qui à $(a, b) \in A \times B$ associe a est un morphisme d'anneaux.
Soit A un anneau. L'application identique $\mathrm{Id}_A \colon A \to A$ est un morphisme d'anneau
Exemple important : soit A un anneau et $a \in A$. L'application $A[X] \to A$ qui à $P \in A[X]$ associe $P(a)$ est un morphisme d'anneaux, appelé le morphisme d'évaluation en a.

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,

$$\mathrm{Ker}(\varphi) = \varphi^{-1}(0_B) = \{a \in A, \varphi(a) = 0_B\}$$

Exemples. (exercice) On reprend les exemples de morphismes d'anneaux et on essaie de décrire le noyau le plus explicitement possible ; le seul cas délicat est le morphisme d'évaluation $A[X] \to A$, $P \mapsto P(a)$; on pourra supposer que $A = \mathbf{Q}$ (ou $\mathbf{R}$, ou $\mathbf{C}$) et penser à utiliser la division euclidienne.

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

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

est un morphisme de groupes.

Démonstration. Exercice de TD n°1.4 □

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 $n \cdot 1_A$.*

Démonstration. Soit $\varphi : \mathbf{Z} \to A$ un morphisme d'anneaux. Comme φ est un morphisme de groupes, pour tout $n \in \mathbf{Z}$, on a Pour tout $n \in \mathbf{Z}$, $\varphi(n) = \varphi(n \cdot 1_{\mathbf{Z}}) = n \cdot \varphi(1_{\mathbf{Z}})$ Comme φ est un morphisme d'anneaux, on a $\varphi(1_{\mathbf{Z}}) = 1_A$. Ainsi $\varphi = \varphi_A$, ce qui démontre l'énoncé d'unicité. Il reste à montrer que φ_A est bien un morphisme d'anneaux. Faites le. □

Définition 16. Soit A et B des anneaux. Un *isomorphisme d'anneaux* entre A et B est un morphisme d'anneaux $\varphi : A \to B$ tel qu'il existe un morphisme d'anneaux $\psi : B \to A$ 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.*

Démonstration. Exercice de TD n°1.4 □

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 :

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

Exemples. Soit A un anneau. Alors on montre que $\{0_A\}$ et A sont des idéaux de A. Par ailleurs, pour tout $a \in A$, soit $a \cdot A := \{ab\}_{b \in A}$. Alors $a \cdot A$ est un idéal de A

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 $\mathcal{I} \cap A^\times \neq \varnothing$*

Démonstration. Exercice de TD n°1.2 □

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 $\mathcal{J} \mapsto \pi^{-1}(\mathcal{J})$.*

Démonstration. Exercice de TD n°1.4 ; à savoir faire absolument □

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 $\mathcal{A}$.

Démonstration. Exercice de TD n°1.2, à savoir faire absolument au moins dans le cas d'une famille de deux idéaux. □

Remarque. **Attention !** Si $\mathcal{I}$ est un idéal d'un anneau A, on a toujours $\mathcal{I}+\mathcal{I}=\mathcal{I}$ mais l'égalité $\mathcal{I}+\mathcal{I}=2\mathcal{I}$ est *fausse* en général. Notons également que l'égalité $2\mathbf{Z}+3\mathbf{Z}=5\mathbf{Z}$ est *fausse*.

Remarque. **Attention !** La notation $\prod_{e\in E}\mathcal{I}_e$ peut aussi désigner le produit cartésien de la famille d'idéaux $(\mathcal{I}_e)_{e\in E}$, qui est un idéal de l'anneau produit A^E (alors que l'idéal produit de la famille d'idéaux $(\mathcal{I}_e)_{e\in E}$ est un idéal de A). Le contexte permet en général de lever l'ambiguité. Au niveau de ce cours, par ailleurs, les deux notions joueront un rôle assez limité.

Remarque. On montre que la réunion de deux idéaux n'est pas en général un idéal ; cf l'exercice de TD n° 1.2.

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

$$S \cdot A + T \cdot A = (S \cup T) \cdot A$$

$$(S \cdot A)(T \cdot A) = (S \cdot T) \cdot A \quad \text{où} \quad S \cdot T = \{st\}_{s \in S, t \in T}$$

Démonstration. Soit $\mathfrak{I}(S)$ l'ensemble des idéaux de A contenant S. Rappelons le sens de minimal et minimum dans ce contexte. Un élément $\mathcal{I}$ de $\mathfrak{I}(S)$ est un élément *minimal* de $\mathfrak{I}(S)$ (au sens de l'inclusion) s'il vérifie la propriété suivante : si $\mathcal{J} \in \mathfrak{I}(S)$ vérifie $\mathcal{J} \subset \mathcal{I}$, alors $\mathcal{J} = \mathcal{I}$. C'est un élément *minimum* de $\mathfrak{I}(S)$ (au sens de l'inclusion) s'il vérifie la propriété suivante : pour tout $\mathcal{J} \in \mathfrak{I}(S)$, on a $\mathcal{I} \subset \mathcal{J}$. Ainsi minimum entraîne minimal, mais la réciproque n'est pas vraie en général [9]

Pour montrer l'unicité d'un élément minimal de $\mathfrak{I}(S)$: si $\mathcal{I}$ et $\mathcal{J}$ sont deux tels éléments, on considère $\mathcal{I} \cap \mathcal{J}$.

Pour montrer l'existence d'un élément minimal de $\mathfrak{I}(S)$, on montre l'existence d'un élément minimum, en considérant $\mathcal{I} := \cap_{\mathcal{J} \in \mathfrak{I}(S)} \mathcal{J}$. Ceci termine l'esquisse de la démonstration de la partie 1 de l'énoncé.

Les démonstrations des parties 2 et 3 illustrent la stratégie générale pour montrer qu'une partie $\mathcal{E}$ d'un anneau A est bien l'idéal engendré par une partie S de A : on montre d'une part que tout idéal de A contenant S contient $\mathcal{E}$, d'autre part que $\mathcal{E}$ est un idéal de A qui contient S.

Considérons l'énoncé de la partie 2. Soit $\mathcal{E}$ la partie de A définie par le membre de droite de l'égalité de l'énoncé. Soit $\mathcal{I}$ un idéal contenant S. On montre le résultat suivant : pour toute partie finie T de S et toute famille $(a_t) \in A^T$ d'éléments de A indexée par T, alors $\sum_{t \in T} a_t t$ est dans $\mathcal{I}$. Ceci se fait par récurrence sur le cardinal de T. Ainsi tout idéal contenant S contient $\mathcal{E}$. Donc l'idéal de A engendré par S contient $\mathcal{E}$.

Il reste à montrer que $\mathcal{E}$ est un idéal de A qui contient S. Soit $s \in S$. Par définition de $\mathcal{E}$, $s = 1_A \cdot s$ est un élément de $\mathcal{E}$. Ceci montre l'inclusion $S \subset \mathcal{E}$. Soit b_1 et b_2 des éléments de $\mathcal{E}$. Grâce à la définition de $\mathcal{E}$, on peut trouver un ensemble fini $T \subset S$ et des familles $(a_{1,t}), (a_{2,t}) \in A^T$ telles que

$$b_1 = \sum_{t \in T} a_{1,t}\, t, \quad \text{et} \quad b_2 = \sum_{t \in T} a_{2,t}\, t$$

On a alors

$$b_1 + b_2 = \sum_{t \in T} (a_{1,t} + a_{2,t})\, t$$

9. On peut noter en outre qu'en général, dans un ensemble muni d'un ordre partiel, même s'il existe un unique élément minimal, cet élément n'est pas forcément un minimum

$$-b_1 = \sum_{t\in T}(-a_{1,t})\,t$$

et pour tout $a \in A$

$$a\,b_1 = \sum_{t\in T}(a\,a_{1,t})\,t$$

De ces relations, on déduit facilement que $\mathcal{E}$ est un idéal de A. Ceci termine l'esquisse de la démonstration de la partie 2 de l'énoncé.

Passons à l'énoncé de la partie 3. en nous concentrant sur la démonstration de l'égalité

$$S \cdot A + T \cdot A = (S \cup T) \cdot A$$

(la stratégie est la même pour l'autre égalité). Il suffit de montrer que $S \cdot A + T \cdot A$ est un idéal de A qui contient $S \cup T$, et que tout idéal de A contenant $S \cup T$ contient $S \cdot A + T \cdot A$. Comme $S \cdot A$ et $T \cdot A$ sont des idéaux de A, $S \cdot A + T \cdot A$ est également un idéal de A, qui contient d'ailleurs $S \cdot A$ et $T \cdot A$, et donc qui contient S et T. Soit $\mathcal{I}$ un idéal de A contenant $S \cup T$. Comme $\mathcal{I}$ contient S, $\mathcal{I}$ contient $S \cdot A$ Comme $\mathcal{I}$ contient T, $\mathcal{I}$ contient $T \cdot A$. Et de manière générale, on montre que si un idéal de A contient deux idéaux $\mathcal{I}_1$ et $\mathcal{I}_2$ de A, alors il contient la somme $\mathcal{I}_1 + \mathcal{I}_2$. Ainsi $\mathcal{I}$ contient $S \cdot A + T \cdot A$. Ceci termine l'esquisse de la démonstration de la partie 3 de l'énoncé.

□

Exemples. Soit A un anneau, $a \in A$ et $S = \{a\}$. Alors l'idéal $S \cdot A$ est noté $a \cdot A$, voire $\langle a \rangle$, et on a $a \cdot A = \{a\,b\}_{b\in A}$ (cet exemple a déjà été rencontré précédemment).

Si n est un entier strictement positif et $a_1, \ldots, a_n$ sont n éléments de A, on peut noter $\langle a_1, \ldots, a_n \rangle$ l'idéal de A engendré par $\{a_1, \ldots, a_n\}$. Notons que l'on a l'égalité

$$\langle a_1, \ldots, a_n \rangle = a_1 \cdot A + \cdots + a_n \cdot A.$$

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.

Remarque. Si A est un anneau, l'idéal A n'est donc *pas* un idéal premier de A. Ce n'est pas non plus un idéal maximal 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.*

Démonstration. Un idéal maximal est par définition propre. Ainsi $\mathcal{I}$ est un idéal propre de A. Soit $x, y \in A$ tels que $xy \in \mathcal{I}$ et $x \notin \mathcal{I}$. Il s'agit de montrer que $y \in \mathcal{I}$. Comme $x \notin \mathcal{I}$, l'idéal engendré par $\mathcal{I}$ et x contient strictement $\mathcal{I}$. Comme $\mathcal{I}$ est maximal, l'idéal engendré par $\mathcal{I}$ et x est A, en particulier cet idéal contient 1. Donc il existe $z \in \mathcal{I}$ et $w \in A$ tel que $z + wx = 1$. En multipliant par y, on trouve $yz + wxy = y$. Comme $xy \in \mathcal{I}$ et $z \in \mathcal{I}$, on en déduit qu'on a $y \in \mathcal{I}$ □

Exemples. L'idéal $\{0\}$ est un idéal premier de $\mathbf{Z}$ (intégrité de $\mathbf{Z}$), mais ce n'est pas un idéal maximal de $\mathbf{Z}$. En effet, si n est un entier distinct de 0, 1 et -1, on montre que l'idéal $n\mathbf{Z}$ est propre et contient strictement $\{0\}$.

L'idéal $X\mathbf{Z}[X]$ est un idéal premier non nul de $\mathbf{Z}[X]$, mais ce n'est pas un idéal maximal de $\mathbf{Z}[X]$. En effet, on montre que l'idéal $\langle 2, X\rangle$ est propre et contient strictement $\langle X\rangle$).

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.*

Remarque. Sans hypothèses supplémentaires, on ne peut pas remplacer *premier* par *maximal*. On pourra considérer par exemple le morphisme d'inclusion $\mathbf{Z} \to \mathbf{Q}$.

Démonstration. Exercice de TD n°1.4. □

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.*

Démonstration. L'unicité dans l'assertion 1 découlera de l'assertion 2 (dont la démonstration n'utilise pas l'assertion 1). Montrons l'existence dans l'assertion 1. Elle est vraie si $\mathcal{I} = \{0\}$ en prenant $n = 0$. Supposons à présent $\mathcal{I} \neq \{0\}$. Donc $\mathcal{I}$ possède un élément $m \neq 0$. Quitte à changer m en $-m$, on peut supposer que $m \in \mathbf{N} \setminus \{0\}$. Ainsi $\mathcal{I} \cap \mathbf{N} \setminus \{0\}$ est une partie non vide de $\mathbf{N} \setminus \{0\}$, qui possède donc un plus petit élément n. Comme $n \in \mathcal{I}$, $\mathcal{I}$ contient l'idéal engendré par n, à savoir $n\mathbf{Z}$. Reste à montrer l'inclusion $\mathcal{I} \subset n\mathbf{Z}$. Soit $z \in \mathcal{I}$ et $z = nq + r$ la division euclidienne de z par n (rappelons que n est non nul). En particulier on a $0 \leqslant r < n$. Comme $z \in \mathcal{I}$ et $n \in \mathcal{I}$, on a $r = z - nq \in \mathcal{I}$. Comme on a $0 \leqslant r < n = \mathrm{Min}(\mathcal{I} \cap \mathbf{N} \setminus \{0\})$, on en déduit que $r = 0$. Ainsi $z \in n\mathbf{Z}$.

Montrons l'assertion 2. Supposons $n\mathbf{Z} \subset m\mathbf{Z}$. En particulier $n \in m\mathbf{Z}$, donc n est un multiple de m. Réciproquement, supposons que n est un multiple de m, en d'autres termes que $n \in m\mathbf{Z}$. Alors l'idéal $m\mathbf{Z}$ contient l'idéal de $\mathbf{Z}$ engendré par $\mathbf{Z}$, à savoir $n\mathbf{Z}$.

Passons aux assertions 3 et 4. Soit n un nombre premier. Montrons que $n\mathbf{Z}$ est un idéal maximal de $\mathbf{Z}$. Comme n est premier, 1 n'est pas un multiple de n, et donc $n\mathbf{Z}$ est un idéal propre de $\mathbf{Z}$. Soit $\mathcal{I}$ un idéal de $\mathbf{Z}$ contenant $n\mathbf{Z}$ et $m \in \mathbf{N}$ tel que $\mathcal{I} = m\mathbf{Z}$. D'après l'assertion 2, m divise n. Comme n est premier, on a $m = 1$ ou $m = n$, donc $m\mathbf{Z} = \mathbf{Z}$ ou $m\mathbf{Z} = n\mathbf{Z}$. Ainsi $n\mathbf{Z}$ est bien maximal.

Si $n = 0$, l'idéal $n\mathbf{Z} = \{0\}$ est bien premier (intégrité de $\mathbf{Z}$) Il est par ailleurs strictement contenu dans $2\mathbf{Z}$, lui-même idéal propre de $\mathbf{Z}$. Ainsi l'idéal $\{0\}$ est premier et non maximal.

Soit $n \in \mathbf{N}$ non nul et non premier. Si $n = 1$, l'idéal $n\mathbf{Z} = \mathbf{Z}$ n'est pas premier. Sinon, on peut écrire $n = m_1 m_2$ avec $1 < m_1 < n$ et $1 < m_2 < n$. En particulier n ne peut diviser ni m_1, ni m_2. Ainsi on a $m_1 \notin n\mathbf{Z}$, $m_2 \notin n\mathbf{Z}$ tandis que $m_1 m_2 = n \in n\mathbf{Z}$. Donc l'idéal $n\mathbf{Z}$ n'est pas premier.

□

Remarque. Ainsi tout idéal de $\mathbf{Z}$ est engendré par un élément. Par ailleurs tout idéal premier de $\mathbf{Z}$ est soit nul, soit maximal.

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 $\mathrm{Ker}(\varphi_A) = n\mathbf{Z}$.

Exemples. On montre que l'anneau $\mathbf{Z}$ est de caractéristique nulle, tout comme $\mathbf{R}$, $\mathbf{Q}$, $\mathbf{R}[X]\ldots$

Soit $n \in \mathbf{N}$. Alors on montre que l'anneau quotient $\mathbf{Z}/n\mathbf{Z}$ est de caractéristique n.

On montre que l'anneau $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ est de caractéristique 4.

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.*

Démonstration. Assez similaire à celle de la proposition 28. On verra à la fin du cours un énoncé beaucoup plus général qui englobe les propositions 30 et 28 □

Remarque. Ainsi tout idéal de $\mathbf{K}[X]$ est engendré par un élément. Par ailleurs tout idéal premier de $\mathbf{K}[X]$ est soit nul, soit maximal.

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.*

Démonstration. Exercice de TD n°1.3 □

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*

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

Démonstration. Exercice de TD n°1.3 □

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

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

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.

Démonstration. Exercice de TD n°2.2 □

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.

Démonstration. Exercice de TD n°1.1 □

Remarque. C'est un cas particulier d'anneau produit : en posant, pour tout $e \in E$, $A_e = A$, on montre que l'application

$$\begin{array}{ccc} A^E & \longrightarrow & \prod_{e\in E} A_e \\ \varphi & \longmapsto & (\varphi(e))_{e\in E} \end{array}$$

est un isomorphisme d'anneaux.

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*

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

Démonstration. Exercice de TD n°1.5 □

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.*

Démonstration. (esquisse pour le degré d'un produit) La relation est claire si $P = 0$ ou $Q = 0$ Sinon, on peut écrire $P = a_{\deg(P)} X^{\deg(P)} + \sum_{i \leqslant \deg(P)-1} a_i X^i$, et $Q = b_{\deg(Q)} X^{\deg(Q)} + \sum_{i \leqslant \deg(Q)-1} b_i X^i$ où les a_i et b_i sont des éléments de A et $a_{\deg(P)}$ et $b_{\deg(Q)}$ sont non nuls, et on voit alors qu'on peut écrire, pour certains $c_i \in A$,

$$PQ = a_{\deg(P)} b_{\deg(Q)} X^{\deg(P)+\deg(Q)} + \sum_{i \leqslant \deg(P)+\deg(Q)-1} c_i X^i.$$

Ainsi $\deg(PQ) \leqslant \deg(P) + \deg(Q)$ avec égalité si et seulement si le produit des coefficients dominants de P et Q est non nul. □

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.*

Démonstration. (brève esquisse) On pourra démontrer puis utiliser le résultat suivant : soit $n \in \mathbf{N}$ et $P \in A[[X]]$; alors on a $\nu(P) = n$ si et seulement si il existe $\alpha \in A \setminus 0$ et $Q \in A[[X]]$ tel que $P = X^n(\alpha + XQ)$ □

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* $\deg(R) < \deg(P_2)$.

Remarque. Notons que P_2 étant non nul, la condition $\deg(R) < \deg(Q)$ est toujours vérifiée si R est nul

Démonstration. Unicité Si (Q_1, R_1) et (Q_2, R_2) sont deux couples vérifiant les propriétés de l'énoncé, on peut écrire $P_2(Q_1 - Q_2) = R_1 - R_2$. Comme $\deg(R_1) < \deg(P_2)$ et $\deg(R_2) < \deg(P_2)$, on a $\deg(R_1 - R_2) < \deg(P_2)$ Par ailleurs, comme P_2 est de coefficient dominant inversible, on a

$$\deg(P_2) + \deg(Q_1 - Q_2) = \deg(P_2(Q_1 - Q_2)) < \deg(P_2)$$

Cette inégalité ne peut être valide que si $Q_1 - Q_2 = 0$. Comme $P_2(Q_1 - Q_2) = R_1 - R_2$, on en tire aussitôt $R_1 = R_2$.

Existence On fixe $P_2 \in A[X]$ vérifiant les hypothèses de l'énoncé et on considère l'hypothèse de récurrence $\mathcal{H}_n$ suivante (pour $n \in \mathbf{N}$) : pour tout polynôme P de $A[X]$ de degré inférieur ou égal à n, il existe un couple (Q, R) tel que $P = QP_2 + R$, avec $\deg(R) < \deg(P_2)$

Soit $n \in \mathbf{N}$ tel que $n < \deg(P_2)$ Alors $\mathcal{H}_n$ est vraie (prendre $Q = 0$, $R = P$)

Soit $n \geqslant \deg(P_2)$ tel que $\mathcal{H}_{n-1}$ est vraie. Soit $P \in A[X]$ de degré n et coefficient dominant a. Soit b le coefficient dominant de P_2 ; par hypothèse $b \in A^\times$. Soit $\tilde{P} := P - a\,b^{-1}\,X^{n-\deg(P_2)}P_2$. Alors on vérifie qu'on a $\deg(\tilde{P}) < \deg(P)$ (on a « tué » le terme de plus haut degré de P). Soit (Q, R) un couple convenable pour $\tilde{P}$. Alors $(Q + a\,b^{-1}\,X^{n-\deg(P_2)}, R)$ est un couple convenable pour P.

On pourra remarquer que l'argument précédent est à la base du calcul effectif de la division euclidienne d'un polynôme par un autre, en « posant » la division. □

Remarque. L'hypothèse sur le coefficient dominant est *fondamentale* ; par exemple, dans $\mathbf{Z}[X]$, la division euclidienne de X par $2X$ n'existe pas. Si $A = \mathbf{K}$ est un corps, l'hypothèse sur le coefficient dominant est toujours vérifiée ; il découle alors de la proposition 40 que tout idéal de $\mathbf{K}[X]$ est engendré par un élément. On peut souligner qu'il n'est pas vrai que tout idéal de $\mathbf{Z}[X]$ est engendré par un élément : on montre par exemple que l'idéal $\langle 2, X\rangle$ ne vérifie pas cette propriété.

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*

Démonstration. Supposons que $X - a$ divise P. Il existe donc $Q \in A[X]$ tel que $P = (X - a)Q$ Appliquons le morphisme d'évaluation ev_a : on obtient $\mathrm{ev}_a(P) = \mathrm{ev}_a(X - a)\,\mathrm{ev}_a(Q)$ Or $\mathrm{ev}_a(X - a) = a - a = 0$. Donc $P(a) = \mathrm{ev}_a(P) = 0$.

Supposons que $P(a) = 0$. Le polynôme $X - a$ étant unitaire, il existe d'après la proposition 40 des polynômes $Q, R \in A[X]$ tels que $P = Q.(X - a) + R$ et $\deg(R) < \deg(X - a) = 1$. La dernière condition signifie que $R \in A$ (en particulier $\mathrm{ev}_a(R) = R$. Appliquant le morphisme d'évaluation ev_a à la relation $P = Q.(X - a) + R$, on obtient $\mathrm{ev}_a(P) = \mathrm{ev}_a(X - a)\,\mathrm{ev}_a(Q) + \mathrm{ev}_a(R)$ soit $\mathrm{ev}_a(P) = R$. Par hypothèse $\mathrm{ev}_a(P) = 0$, donc $R = 0$ et $P = (X - a)Q$. Donc $X - a$ 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.*

Remarque. Si A n'est pas intègre, même un polynôme unitaire peut avoir une *infinité* de racines dans A (*cf.* l'exemple de $\mathbf{K}[X]/X^2$ dans le chapitre 3 ci-dessous)

Démonstration. Soit n un entier strictement positif et $a_1, \ldots, a_n$ des racines (deux à deux distinctes) de P dans A. D'après la proposition précédente, il existe $Q_1 \in A[X]$ tel que $P = Q(X - a_1)$. En particulier on a $0 = P(a_2) = Q_2(a_2)(a_2 - a_1)$. Comme $a_2 \neq a_1$ et A est intègre, on en déduit qu'on a $Q_2(a_2) = 0$ Toujours d'après la proposition précédente, il existe $Q_2 \in A[X]$ tel que $Q_1 = Q_2(X - a_2)$. Par une récurrence finie, on montre qu'il existe $Q \in A[X]$ tel que $P = Q(X - a_1)(X - a_2)\ldots(X - a_n)$. On applique alors la proposition 37 (NB : comme les polynômes $X - a_i$ sont unitaires, on n'a pas besoin de l'intégrité de A pour cette partie de l'argument) pour obtenir $\deg(P) = \deg(Q) + n$. Comme P est non nul, Q est non nul et donc $\deg(Q) \in \mathbf{N}$. Finalement on obtient $\deg(P) \geqslant n$ ce qui montre le résultat voulu. □

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*

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

est bijective

Remarque. Pour $B = A$, l'image réciproque de (Id_A, a) par l'application de l'énoncé est le morphisme d'évaluation en a.

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.

Démonstration. (esquisse) Soit $(\psi, b) \in \mathrm{Hom}_{\mathrm{anneaux}}(A, B) \times B$. Soit

$$\theta(\psi, b)\colon \begin{array}{rcl} A[X] & \longrightarrow & B \\ \sum_{n\in\mathbf{N}} a_n X^n & \longmapsto & \sum_{n\in\mathbf{N}} \psi(a_n) b^n \end{array}$$

On montre que $\theta(\psi, b)$ est un morphisme d'anneaux. Par ailleurs on montre que $(\psi, b) \mapsto \theta(\psi, b)$ est l'application réciproque de l'application de l'énoncé. □

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 $\iota : A \to A[X_1, \ldots, X_N]$ 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

Démonstration. Cela peut se démontrer de proche en proche en utilisant la propriété universelle de l'anneau de polynômes en une indéterminée et l'identification $A[X_1, \ldots, X_N] = A[X_1, \ldots, X_{N-1}][X_N]$.

On peut aussi en donner une démonstration directe formellement très similaire à la démonstration de la propriété universelle de l'anneau de polynômes en une indéterminée.

Les détails sont laissés aux personnes intéressées. □

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.

Remarque. Avec les notations ci-dessus, si $A = B$, pour $\mathbf{a} \in A^N$, le morphisme $\varphi \in \mathrm{Hom}_{\text{anneaux}}(A[X_1, \ldots, X_N], B)$ correspondant à $(\mathrm{Id}_A, \mathbf{a})$ est le morphisme d'évaluation en $\mathbf{a}$, noté $\mathrm{ev}_{\mathbf{a}}$ ou $P \mapsto P(\mathbf{a})$.

Remarque. Soit A un anneau *intègre* et $N \geqslant 1$ un entier. On a vu en exemple du cours (*cf.* aussi l'exercice de TD n°1.5.8) que $A[X]^\times$ est l'ensemble des polynômes constants inversibles dans A. De proche en proche, on en déduit que $A[X_1, \ldots, X_N]^\times$ est l'ensemble des polynômes constants inversibles dans A.

Exemple. Soit $\mathbf{K}$ un corps. On considère l'anneau $\mathbf{K}[X, Y]$ des polynômes en deux indéterminées à coefficients dans $\mathbf{K}$. En se rappelant que $\mathbf{K}[X, Y]$ est isomorphe à $(\mathbf{K}[X])[Y]$ (respectivement $(\mathbf{K}[Y])[X]$), on peut voir un élément de $\mathbf{K}[X, Y]$ comme un polynôme en une variable Y (respectivement X) à coefficients dans $\mathbf{K}[X]$ (respectivement $\mathbf{K}[Y]$) et ceci est souvent utile pour raisonner dans $\mathbf{K}[X, Y]$. Notamment, pour tout élément P de $\mathbf{K}[X, Y]$, on peut définit $\deg_Y(P)$ (respectivement $\deg_X(P)$) comme le degré de P vu comme polynôme en une variable à coefficients dans $\mathbf{K}[X]$ (respectivement $\mathbf{K}[Y]$). Par exemple, si $P = 1 + X^2Y + Y^3$, on a $\deg_X(P) = 2$ et $\deg_Y(P) = 3$. La proposition 37 s'applique (noter que $\mathbf{K}[X]$ et $\mathbf{K}[Y]$ sont intègres).

Montrons que les éléments X et Y de $\mathbf{K}[X, Y]$ sont premiers entre eux, c'est à dire : tout élément P qui divise X et Y est nécessairement un élément de $\mathbf{K}[X, Y]^\times = \mathbf{K}^\times$. Supposons l'existence de $Q \in \mathbf{K}[X, Y]$ tel que $X = PQ$. On en déduit $0 = \deg_Y(X) = \deg_Y(P) + \deg_Y(Q)$, donc nécessairement $\deg_Y(P) = 0$. De même, si P divise Y, on doit avoir $\deg_X(P) = 0$. Au final, si P divise X et Y, on doit avoir $\deg_X(P) = \deg_Y(P) = 0$, soit $P \in \mathbf{K}$. Comme P divise X et Y, il ne peut pas être nul, donc finalement $P \in \mathbf{K}^\times$. Donc X et Y sont premiers entre eux.

Montrons qu'en dépit de cela, l'idéal $\langle X, Y \rangle$ engendré par X et Y n'est pas égal à $\mathbf{K}[X, Y]$. C'est une différence fondamentale avec la situation sur $\mathbf{Z}$ ou sur $\mathbf{K}[X]$: le théorème de Bézout n'est pas vrai sur $\mathbf{K}[X, Y]$. L'égalité $\langle X, Y \rangle = \mathbf{K}[X, Y]$ entraîne en effet l'existence de $P, Q \in \mathbf{K}[X, Y]$ tels que $P.X + Q.Y = 1$. Évaluons cette dernière égalité en $(0, 0)$. On obtient $0 = 1$, contradiction.

À titre d'exercice, montrez que l'idéal $\langle X, Y \rangle$ est en fait le noyau du morphisme d'évaluation $P \mapsto P(0, 0)$ et que ce n'est pas un idéal engendré par un élément.

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.

Exemple. Soit A et B des anneaux, et $\mathcal{I}$ l'idéal $A \times \{0_B\}$ de l'anneau produit $A \times B$. Alors la projection $A \times B \to B$, $(a, b) \mapsto b$ est un morphisme surjectif de noyau $\mathcal{I}$. Donc le quotient $(A \times B)/\mathcal{I}$ s'identifie à B, et le morphisme quotient s'identifie à la projection $A \times B \to B$.

Exemples. 1) *(Une construction des quotients de* $\mathbf{Z}$*)* Soit N un entier strictement positif. Pour tout entier $a \in \mathbf{Z}$, soit $r_N(a)$ le reste de la division euclidienne de a par N. Soit $\mathcal{Q}$ l'anneau dont l'ensemble sous jacent est l'ensemble $\{0, 1, \ldots, N-1\}$ des entiers compris entre 0 et $N-1$, muni des lois $\oplus$ et $\otimes$ suivantes : si $a_1, a_2 \in \mathcal{Q}$, on pose $a_1 \oplus a_2 := r_N(a_1 + a_2)$ et $a_1 \otimes a_2 := r_N(a_1 \times a_2)$. On vérifie que $(\mathcal{Q}, \oplus, \otimes)$ est bien un anneau et que l'application $\mathbf{Z} \to \mathcal{Q}$ qui à $a \in \mathbf{Z}$ associe $r_N(a) \in \mathcal{Q}$ est un morphisme surjectif de noyau $N\mathbf{Z}$. Ainsi l'anneau $\mathcal{Q}$ est isomorphe à $\mathbf{Z}/N\mathbf{Z}$. En particulier $\mathbf{Z}/N\mathbf{Z}$ est fini de cardinal N.

2) *(Une construction des quotients d'un anneau de polynômes sur un corps)* Soit $\mathbf{K}$ un corps et $P \in \mathbf{K}[X]$ un polynôme non nul. Pour tout polynôme $A \in \mathbf{K}[X]$, soit $r_P(A)$ le reste de la division euclidienne de A par P. Soit $\mathcal{Q}$ l'anneau dont l'ensemble sous jacent est l'ensemble $\mathbf{K}[X]_{\deg < \deg(P)}$ des polynômes de degré strictement inférieur à $\deg(P)$, muni des lois $\oplus$ et $\otimes$ suivantes : si $A_1, A_2 \in \mathcal{Q}$, on pose $A_1 \oplus A_2 := r_P(A_1 + A_2)$ et $A_1 \otimes A_2 := r_P(A_1 \times A_2)$. On vérifie que $(\mathcal{Q}, \oplus, \otimes)$ est bien un anneau et que l'application $\mathbf{K}[X] \to \mathcal{Q}$ qui à $A \in \mathbf{K}[X]$ associe $r_P(A) \in \mathcal{Q}$ est un morphisme surjectif de noyau $P\mathbf{K}[X]$. Ainsi l'anneau $\mathcal{Q}$ est isomorphe à $\mathbf{K}[X]/P\mathbf{K}[X]$.

3) *(Une généralisation englobant les deux exemples précédents)* Soit A un anneau et $\mathcal{I}$ un idéal de A. Pour $x, y \in A$, la notation $x = y \pmod{\mathcal{I}}$ signifie $x - y \in \mathcal{I}$.

Supposons qu'on ait identifié dans A un « système de représentants modulo $\mathcal{I}$ », c'est à dire une partie S de A et une application $r\colon A \to S$ telle que

1. pour tout $a \in A$, $r(a) = a \pmod{\mathcal{I}}$;
2. pour tous $s_1, s_2 \in S$, on a $s_1 = s_2 \pmod{\mathcal{I}} \Leftrightarrow s_1 = s_2$.

Soit $\mathcal{Q}$ l'anneau dont l'ensemble sous jacent est S muni des lois $\oplus$ et $\otimes$ suivantes : si $s_1, s_2 \in \mathcal{Q}$, on pose $s_1 \oplus s_2 := r(s_1 + s_2)$ et $s_1 \otimes s_2 := r(s_1 \times s_2)$. On vérifie que $(\mathcal{Q}, \oplus, \otimes)$ est bien un anneau et que l'application $A \to \mathcal{Q}$ qui à $x \in A$ associe $r(x) \in \mathcal{Q}$ est un morphisme surjectif de noyau $\mathcal{I}$. Ainsi l'anneau $\mathcal{Q}$ est isomorphe à $A/\mathcal{I}$.

Pour peu que S et $r\colon A \to S$ soit suffisamment « effectifs », ceci peut fournir un moyen pratique de calculer dans $A/\mathcal{I}$. **Attention cependant** à la confusion fréquente signalée dans la remarque ci-dessous.

Remarque. ***L'une des confusions les plus fréquentes dans la manipulation des quotients*** est indéniablement la suivante : en reprenant les notations précédentes, penser (consciemment ou non) que puisque $S \subset A$ peut être identifié à l'ensemble sous-jacent de l'anneau $A/\mathcal{I}$, l'anneau quotient $A/\mathcal{I}$« = » S peut être vu comme un sous-anneau de A ; c'est rarement le cas, et basiquement c'est du au fait que les lois $\oplus$ et $\otimes$ définie sur S ne coincident pas avec les lois sur S induites par celles de A (pour lesquelles S n'est d'ailleurs en général pas stable).

Par exemple, si N est un entier strictement positif, $\mathbf{Z}/N\mathbf{Z}$ ne peut pas être un sous-anneau de $\mathbf{Z}$. Penser que si c'était le cas, on aurait $1_{\mathbf{Z}/N\mathbf{Z}} = 1_{\mathbf{Z}}$ et, comme $N \cdot 1_{\mathbf{Z}/N\mathbf{Z}} = 0_{\mathbf{Z}/N\mathbf{Z}} = 0_{\mathbf{Z}}$, on aurait $N \cdot 1_{\mathbf{Z}} = 0_{\mathbf{Z}}$. Parmi les manifestations classique de cette confusion : écrire, pour $x, y \in \mathbf{Z}/N\mathbf{Z}$, des choses du genre $x \leqslant y$ (ça n'a pas de sens).

Remarque. À propos des notations des éléments des anneaux quotients. Il n'y a pas réellement de notation standardisée. La notation la plus courante consiste certainement à noter un élément d'un quotient $A/\mathcal{I}$ « comme si » c'était un élément de A (plus précisément, π étant le morphisme quotient, on identifie $x \in A/\mathcal{I}$ à $a \in A$ tel que $x = \pi(a)$) et à se rappeler que l'on calcule en fait dans $A/\mathcal{I}$ et non dans A. C'est très pratique pour alléger l'écriture mais du point de vue pédagogique cela crée assez facilement de graves confusions quand on manque d'expérience dans la manipulation des quotients (*cf.* en particulier la remarque précédente).

Au moins lorsque plusieurs quotients sont en jeu, ce qui arrive fréquemment (*cf.* le théorème chinois ci-dessous), il est prudent de distinguer clairement les morphismes quotients et les éléments des différents quotients. Pour ce faire, on pourra noter par exemple $a \pmod I$ (un peu lourd) ou $[a]_{\mathcal{I}}$ l'image de a par le morphisme quotient $A \to A/\mathcal{I}$. Si $n \in \mathbf{Z}$ et $\mathcal{I} = n\mathbf{Z}$, j'écrirai $[a]_n$ pour $[a]_{n\mathbf{Z}}$. On écrira alors par exemple $[3]_4 + [2]_4 = [1]_4$.

En liaison avec les exemples ci-dessus, soulignons que dans certains cas, d'autres représentations intéressantes des éléments du quotient peuvent exister ; *cf.* notamment le cas de $\mathbf{K}[X]/P\mathbf{K}[X]$ discuté un peu plus tard.

Remarque. D'après les propositions 20 et 27, si $\pi\colon A \to A/\mathcal{I}$ est le morphisme quotient, $\mathcal{J} \mapsto \pi(\mathcal{J})$ est une bijection naturelle de l'ensemble des idéaux de A contenant $\mathcal{I}$ sur l'ensemble des idéaux de $A/\mathcal{I}$, qui induit une bijection de l'ensemble des idéaux premiers de A contenant $\mathcal{I}$ sur l'ensemble des idéaux premiers de $A/\mathcal{I}$.

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 $x - y \in \mathcal{I}$.

Démonstration. Démonstration de l'existence On prend pour ensemble sous-jacent à B l'ensemble quotient de A pour la relation d'équivalence $\mathcal{R}_{\mathcal{I}}$ sur A définie par

$$\forall x \in A, \quad \forall y \in A, \quad x \,\mathcal{R}_{\mathcal{I}}\, y \Longleftrightarrow x = y \pmod{\mathcal{I}}.$$

Soit alors $\pi\colon \begin{array}{ccc} A & \longrightarrow & B \\ x & \longmapsto & \overline{x} \end{array}$ l'application qui à $x \in A$ associe sa $\mathcal{R}_{\mathcal{I}}$-classe d'équivalence. Pour $x, y \in A$, on pose $\overline{x} + \overline{y} := \overline{x + y}$ et $\overline{x} \times \overline{y} := \overline{x \times y}$.

On vérifie que ceci est bien défini, qu'on obtient ainsi deux lois de composition interne sur B qui en font un anneau, d'éléments neutres $\overline{0_A}$ pour la première loi et $\overline{1_A}$ pour la seconde lois, et que π est un morphisme d'anneaux surjectif de noyau $\mathcal{I}$. Le plus laborieux dans ce qui précède est certainement la première étape, c'est à dire vérifier que les définitions du paragraphe précédent sont valides. Les étapes suivantes en sont une conséquence quasi-immédiate si l'on comprend bien ce qu'il y a à démontrer. Noter que pour la première étape, il s'agit de montrer que pour tous $x, y, x', y' \in A$ tels que $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, on a $\overline{x + y} = \overline{x' + y'}$ et une propriété analogue pour la multiplication.

L'unicité découlera de la démonstration du théorème suivant. □

Remarque. Avec les notations ci-dessus, le fait que π soit bien défini et soit un morphisme d'anneaux se traduit concrètement par la compatibilité des congruences modulo $\mathcal{I}$ à l'addition et à la multiplication : si $x = y \pmod{\mathcal{I}}$ et $z = t \pmod{\mathcal{I}}$ alors $x + z = y + t \pmod{\mathcal{I}}$ et $xz = yt \pmod{\mathcal{I}}$.

La notion d'anneau quotient n'est en un certain sens rien d'autre qu'une « incarnation abstraite » du calcul modulaire (ou calcul des congruences).

Remarque. Il y a deux raisons pour lesquelles je ne développe pas plus en détail la démonstration de l'existence. Premièrement, et à l'instar d'autres démonstrations de résultats de ce chapitre, c'est typiquement le genre d'exercice de manipulation des définitions que vous devriez être capable de faire en autonomie. Deuxièmement, l'auteur de ces lignes est intimement convaincu que la connaissance de la construction « abstraite » de l'anneau quotient n'est strictement d'aucune utilité pour manipuler des quotients dans la pratique, et peut même avoir tendance à obscurcir considérablement l'appréhension de la notion de quotient ; cette remarque ne se limite pas à la notion de quotient d'anneaux et fait écho à la remarque qui suit l'énoncé du théorème 22 du chapitre 1 du cours.

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 $\mathrm{Ker}(\varphi) = \mathcal{I}$.*

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 $\psi \in \mathrm{Hom}(A/\mathcal{I}, B)$ associe $\psi \circ \pi \in \mathrm{Hom}(A, B)$ permet d'identifier $\mathrm{Hom}(A/\mathcal{I}, B)$ et $\{\varphi \in \mathrm{Hom}(A, B), \quad \mathcal{I} \subset \mathrm{Ker}(\varphi)\}$.

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 $\mathcal{I}$.

Démonstration. On va démontrer le théorème 47 en remplaçant $\pi\colon A \to A/\mathcal{I}$ par n'importe quel morphisme d'anneaux $\pi\colon A \to C$ surjectif de noyau $\mathcal{I}$. Ceci montrera l'unicité dans le théorème 46 ainsi que le théorème 47.

Choisissons une section ensembliste $s\colon C \to A$ de π, c'est-à-dire une application $C \to A$ telle que $\pi \circ s = \mathrm{Id}_C$.

Attention, il n'est pas possible en général de prendre pour s un morphisme d'anneaux.

Remarque pour les puristes : on utilise l'axiome du choix ; en fait et plus précisément, l'existence d'une section ensembliste pour toute application surjective est une des formes sous lesquelles on peut énoncer l'axiome du choix.

Supposons l'existence de ψ comme dans l'énoncé. On a alors

$$\varphi \circ s = \psi \circ \pi \circ s = \psi$$

d'où l'unicité d'un tel morphisme ψ (oui, en dépit du choix arbitraire de s).

Montrons à présent que $\psi := \varphi \circ s$ est bien un morphisme d'anneaux.

Soit $c, c' \in C$. Alors $s(c + c')$ et $s(c) + s(c')$ ont même image par π, à savoir $c + c'$. Donc $s(c + c') - (s(c) + s(c')) \in \mathcal{I}$.

Comme $\mathcal{I} \subset \mathrm{Ker}(\varphi)$, on a bien $\varphi(s(c+c')) = \varphi(s(c)+s(c'))$. Comme φ est un morphisme d'anneaux, on en déduit

$$\varphi(s(c + c')) = \varphi(s(c)) + \varphi(s(c'))$$

d'où

$$\psi(c+c') = \psi(c) + \psi(c').$$

De même $s(cc')$ et $s(c)s(c')$ ont même image par π, à savoir cc'. Donc $s(cc') - s(c)s(c') \in \mathcal{I}$. On en déduit $\varphi(s(cc'))) = \varphi(s(c)s(c'))$.

Enfin $s(1_C)$ et 1_A ont même image par π, à savoir 1_B. Donc $\varphi s(1_C) = \varphi(1_A) = 1_B$, donc $\psi(1_C) = 1_B$.

Montrons que $\varphi \circ s \circ \pi = \varphi$. Soit $a \in A$. Alors $\pi \circ s \circ \pi(a) = \pi(a)$, donc $s \circ \pi(a) - a \in \mathrm{Ker}(\pi)$. On en déduit $\varphi(s \circ \pi(a)) = \varphi(a)$.

Si φ est surjective, comme $\psi\pi = \varphi$, ψ est également surjective.

Si ψ est surjective, comme $\psi\pi = \varphi$ et π est surjective, ψ est également surjective.

On a $\mathrm{Ker}(\psi) = \pi(\mathrm{Ker}(\varphi))$, donc ψ est injective si et seulement si $\pi(\mathrm{Ker}(\varphi) = \{0\}$ si et seulement si $\mathrm{Ker}(\varphi)$ est contenu dans $\mathrm{Ker}(\pi)$. Comme $\mathrm{Ker}(\pi) = \mathcal{I}$ et $\mathcal{I}$ est contenu dans $\mathrm{Ker}(\varphi)$, on obtient le résultat. □

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 $A/\mathrm{Ker}(\varphi)$ sur l'anneau $\mathrm{Im}(\varphi)$. En particulier, si φ est surjectif, φ induit un isomorphisme de $A/\mathrm{Ker}(\varphi)$ sur B. De manière générale, l'anneau quotient $A/\mathrm{Ker}(\varphi)$ 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 $(A/\mathcal{I})[X]/\pi_{\mathcal{I},X}(\mathcal{J})$.*

Remarque. Si $\varphi\colon A \to B$ est un morphisme d'anneaux non surjectif, on peut toujours se ramener au cas surjectif en remplaçant B par le sous-anneau $\mathrm{Im}(\varphi)$.

Remarque. On reprend les notations de l'énoncé. La définition du morphisme $\pi_{\mathcal{I},X}$ utilise la propriété universelle de l'anneau de polynômes en une indéterminée. Concrètement, le morphisme $\pi_{\mathcal{I},X}$ s'obtient en réduisant modulo $\mathcal{I}$ les coefficients d'un polynôme à coefficients dans A. Plus précisément, si $\pi_{\mathcal{I}}\colon A \to A/\mathcal{I}$ est le morphisme quotient et $P = \sum_{n=0}^{+\infty} a_n X^n \in A[X]$, alors $\pi_{\mathcal{I},X}(P) = \sum_{n=0}^{+\infty} \pi_{\mathcal{I}}(a_n) X^n \in (A/I)[X]$

Démonstration. 1(a) découle aussitôt du théorème 47. 1(b) et 1(c) découlent de 1(a) en calculant les noyaux des compositions de morphismes considérées (calcul laissé à titre d'exercice).

Montrons l'assertion 2. La remarque précédente montre que le morphisme $\pi_{\mathcal{I},X}$ est surjectif. L'assertion 2 découlera alors de 1(c) une fois montré l'égalité $\mathrm{Ker}(\pi_{\mathcal{I},X}) = \mathcal{I} \cdot A[X]$. Soit $\mathcal{I}[X] \subset A[X]$ l'ensemble des polynômes à coefficients dans $\mathcal{I}$. On vérifie que $\mathcal{I}[X]$ est un idéal de $A[X]$ contenant $\mathcal{I}$, et que tout idéal de $A[X]$ contenant $\mathcal{I}$ contient $\mathcal{I}[X]$. Ainsi $\mathcal{I} \cdot A[X] = \mathcal{I}[X]$. Le fait que $\mathrm{Ker}(\pi_{\mathcal{I},X}) = \mathcal{I}[X]$ découle alors aussitôt de la remaque précédente. □

Exemple. Soit $\pi\colon \mathbf{Z}[X] \to \mathbf{C}$ l'unique morphisme d'anneaux qui envoie X sur i. L'image de π est l'anneau des entiers de Gauss $A = \mathbf{Z}[i]$, qui contient $\mathbf{Z}$ comme sous-anneau. Soit p un nombre premier. On s'intéresse à la question suivante : l'idéal $p \cdot A$ est-il un idéal premier de A ? On verra plus tard que dans le cas de l'anneau $\mathbf{Z}[i]$ cette question est équivalente à demander si p est un élément irréductible de $\mathbf{Z}[i]$.

On va répondre à cette question en calculant le quotient $A/p.A$ sous une autre forme, en utilisant notamment le théorème précédent.

Tout d'abord, montrons que le noyau de π est l'idéal $(X^2+1) \cdot \mathbf{Z}[X]$.

On a $\pi(X^2+1) = i^2 + 1 = 0$ donc $X^2 + 1 \in \mathrm{Ker}(\pi)$. Comme $\mathrm{Ker}(\pi)$ est un idéal, $\mathrm{Ker}(\pi)$ contient nécessairement l'idéal engendré par X^2+1, soit $(X^2+1) \cdot \mathbf{Z}[X]$.

Montrons l'inclusion réciproque $\mathrm{Ker}(\pi) \subset (X^2+1) \cdot \mathbf{Z}[X]$. Soit $P \in \mathrm{Ker}(\pi)$. Le polynôme X^2+1 étant **UNITAIRE**, on peut appliquer le théorème de division euclidienne et on obtient l'existence de $Q, R \in \mathbf{Z}[X]$, avec $\deg(R) < \deg(X^2+1) = 2$, tels que $P = (X^2+1).Q + R$. En appliquant à cette égalité le morphisme d'évaluation en i, on obtient $0 = 0.Q(i) + R(i)$, soit $R(i) = 0$. Comme $\deg(R) < 2$, il existe $a, b \in \mathbf{Z}$ tels que $R = aX + b$. Ainsi $ai + b = 0$. Par identification des parties réelle et imaginaire, on obtient $a = b = 0$, soit $R = 0$ et $P = (X^2+1).Q$ ce qui conclut.

Noter que $p \cdot A$ est l'image par π de l'idéal $\mathcal{I} = p\mathbf{Z}[X]$. Une application du 1(c) du théorème 48 montre alors que la composition de π avec le morphisme quotient $A \to A/p \cdot A$ induit un isomorphisme $A/p \cdot A \xrightarrow{\sim} \mathbf{Z}[X]/\langle p, X^2+1\rangle$.

Maintenant, si on note $n \mapsto [n]_p$ le morphisme quotient $\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$, le 2 du théorème 48 montre que $\mathbf{Z}[X]/\langle p, X^2+1\rangle$ est lui-même isomorphe à $(\mathbf{Z}/p\mathbf{Z})[X]/\langle X^2 + [1]_p\rangle$. Ainsi, en utilisant le théorème 58, $p \cdot A$ est un idéal premier de A si et seulement si $A/p \cdot A$ est

intègre si et seulement si $(\mathbf{Z}/p\mathbf{Z})[X]/\langle X^2+[1]_p\rangle$ est intègre si et seulement si $\langle X^2+[1]_p\rangle$ est un idéal premier de $(\mathbf{Z}/p\mathbf{Z})[X]$.

Comme p est premier, $\mathbf{Z}/p\mathbf{Z}$ est un corps. Ainsi $\langle X^2+[1]_p\rangle$ est un idéal premier de $(\mathbf{Z}/p\mathbf{Z})[X]$ si et seulement si $X^2+[1]_p$ est irréductible, et comme ce polynôme est de degré 2, cela équivaut à la condition que $X^2+[1]_p$ n'a pas de racine.

En résumé : $p\cdot\mathbf{Z}[i]$ est un idéal premier de $\mathbf{Z}[i]$ si et seulement si -1 n'est pas un carré modulo p. On (re)verra un peu plus tard comment cette dernière condition s'exprime explicitement en termes de congruences.

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*

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

Démonstration. Par définition du quotient, le noyau de π_n (respectivement π_m) est $n\mathbf{Z}$ (respectivement $m\mathbf{Z}$). Par ailleurs, par définition du morphisme produit, on a $\mathrm{Ker}(\pi_n\times\pi_m)=\mathrm{Ker}(\pi_n)\cap\mathrm{Ker}(\pi_m)$.

Montrons, pour mémoire, l'égalité $n\mathbf{Z}\cap m\mathbf{Z}=\mathrm{ppcm}(n,m)\mathbf{Z}$. Soit $d\in\mathbf{N}$ tel que $n\mathbf{Z}\cap m\mathbf{Z}=d\mathbf{Z}$. En particulier $d\in n\mathbf{Z}$ et $d\in m\mathbf{Z}$, donc d est un multiple de n et de m. Par ailleurs, si e est un multiple de n et de m, on a $e\in n\mathbf{Z}\cap m\mathbf{Z}$, donc $e\in d\mathbf{Z}$, donc e est un multiple de d. Ceci montre bien que $d=\mathrm{ppcm}(m,n)$.

Pour la seconde partie, notons que comme n et m sont premiers entre eux, on a $\mathrm{ppcm}(m,n)=mn$. Ainsi le théorème de factorisation et la première partie donneront le résultat une fois montrée la surjectivité de $\pi_n\times\pi_m$.

Soit $(x,y)\in\mathbf{Z}^2$. Il s'agit de montrer qu'il existe $z\in\mathbf{Z}$ tel que

$$z=x\pmod n,\quad z=y\pmod m.$$

Comme n et m sont premiers entre eux, il existe $(u,v)\in\mathbf{Z}^2$ tel que $un+vm=1$ (théorème de Bezout dans $\mathbf{Z}$). L'entier $z=yun+xvm$ convient. □

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*

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

Démonstration. On raisonne similairement au cas $A = \mathbf{Z}$ (théorème précédent). Ce qui ne s'obtient pas directement par extension de la démonstration du théorème précédent : si $\mathcal{I} + \mathcal{J} = A$, alors $\mathcal{I} \cap \mathcal{J} = \mathcal{I} \cdot \mathcal{J}$ et le morphisme $\pi_{\mathcal{I}} \times \pi_{\mathcal{J}}$ est surjectif.

Montrons le. Par définition du produit d'idéaux, l'inclusion $\mathcal{I} \cdot \mathcal{J} \subset \mathcal{I} \cap \mathcal{J}$ est toujours vraie. Montrons l'inclusion réciproque. Par hypothèse, il existe $(a, b) \in \mathcal{I} \times \mathcal{J}$ tel que $a+b = 1$ Soit alors $z \in \mathcal{I} \cap \mathcal{J}$. Alors $z = za + zb$. Comme $z \in \mathcal{J}$ et $a \in \mathcal{I}$, on a $za \in \mathcal{I} \cdot \mathcal{J}$. Comme $z \in \mathcal{I}$ et $b \in \mathcal{J}$, on a $zb \in \mathcal{I} \cdot \mathcal{J}$. Ainsi $z = za + zb \in \mathcal{I} \cdot \mathcal{J}$.

Passons à la surjectivité du morphisme $\pi_{\mathcal{I}} \times \pi_{\mathcal{J}}$. Il faut montrer : soit $(x, y) \in A^2$; alors il existe $z \in A$ tel que $z = x \pmod{\mathcal{I}}$ et $z = y \pmod{\mathcal{J}}$. Soit $(a, b) \in \mathcal{I} \times \mathcal{J}$ tel que $a + b = 1$. Alors $z := ay + bx$ convient. En effet comme $a + b = 1$ et $b \in \mathcal{J}$, on a $a = 1 \pmod{\mathcal{J}}$ donc $ay = y \pmod{\mathcal{J}}$. Comme $b \in \mathcal{J}$, on a par ailleurs $bx = 0 \pmod{\mathcal{J}}$. Donc $z = ay + bx = y + 0 \pmod{\mathcal{J}}$. De même, on montre $z = x \pmod{\mathcal{I}}$. □

Remarque. Si $\mathcal{I} + \mathcal{J} = A$, on dit que les idéaux $\mathcal{I}$ et $\mathcal{J}$ sont étrangers (ou comaximaux, ou premiers entre eux). Dans le cas où A est principal (c'est-à-dire A est intègre, et tout idéal de A est engendré par un élément), l'hypothèse que les idéaux sont étrangers est équivalente à l'hypothèse que les générateurs des idéaux sont premiers entre eux.

Pour mémoire, si $\mathbf{K}$ est un corps, les éléments X et Y de $A = \mathbf{K}[X, Y]$ sont premiers entre eux, mais les idéaux $\mathcal{I} = \langle X \rangle$ et $\mathcal{J} = \langle Y \rangle$, dont la somme est $\langle X, Y \rangle$, ne sont pas étrangers. Exercice : montrer que dans ce cas ni $A/\mathcal{I} \cdot \mathcal{J}$ ni $A/\mathcal{I} \cap \mathcal{J}$ ne sont isomorphes à $(A/\mathcal{I}) \times (A/\mathcal{J})$ (on pourra consulter l'indication de la correction de l'exercice 1.8 du CC1 de 2018-2019).

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 $(\mathcal{I}_i)_{i=1,\ldots,n}$ un 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

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

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

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

Remarque. L'hypothèse que les idéaux $\mathcal{I}_i$ de l'énoncé 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 $(n, m, r) = (6, 10, 15)$ et on montrera que ce produit n'est pas isomorphe à $\mathbf{Z}/nmr\mathbf{Z}$.

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.

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 53. 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 nul »).

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

Démonstration. L'anneau A est non nul si et seulement si l'idéal nul est un idéal propre. Ainsi vu la définition d'un idéal premier, cette proposition n'est qu'une reformulation de la remarque précédente. □

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

Démonstration. Soit A un anneau. La propriété

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

est évidemment encore vraie sur tout sous-anneau de A.

Il suffit donc de montrer qu'un sous-anneau d'un anneau non nul est non nul. Ceci vient du fait qu'un anneau et ses sous-anneaux ont les mêmes 0 et 1, et qu'un anneau nul est caractérisé par l'égalité $1 = 0$. □

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*.

Exemple. $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Z}/n\mathbf{Z}$ si n est premier, $\mathbf{K}[X]/P\mathbf{K}[X]$ si $\mathbf{K}$ est un corps et si $P \in \mathbf{K}[X]$ est un polynôme irréductible. $\mathbf{Q}$ est un sous-corps de $\mathbf{R}$; $\mathbf{Z}$ est un sous-anneau de $\mathbf{C}$ mais ce n'est pas un sous-corps de $\mathbf{C}$

Remarque. Un corps est un anneau intègre.

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.

Démonstration. Exercice □

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. Soit $\pi\colon A \to A/\mathcal{I}$ le morphisme quotient.

Supposons l'idéal $\mathcal{I}$ premier. En particulier il est propre et le quotient $A/\mathcal{I}$ est distinct de l'anneau nul. Soit $x, y \in A/\mathcal{I}$ tel que $xy = 0$. Soit $x', y' \in A$ tels que $x = \pi(x')$ et $y = \pi(y')$. Alors $xy = \pi(x')\pi(y') = \pi(x'y')$ car π est un morphisme d'anneaux. Comme $xy = 0$, on en déduit $x'y' \in \mathrm{Ker}(\pi) = \mathcal{I}$. Comme $\mathcal{I}$ est premier, soit $x' \in \mathcal{I}$, soit $y' \in \mathcal{I}$. Donc soit $x = \pi(x') = 0$, soit $y = \pi(y') = 0$. Donc $A/\mathcal{I}$ est intègre.

Supposons le quotient $A/\mathcal{I}$ intègre. En particulier, il est distinct de l'anneau nul et l'idéal $\mathcal{I}$ est propre. Soit $x, y \in A$ tels que $xy \in \mathcal{I}$. Donc $\pi(xy) = 0$ et comme π est un morphisme d'anneaux, on a $\pi(x)\pi(y) = 0$. Comme $A/\mathcal{I}$ est intègre, on a soit $\pi(x) = 0$, soit $\pi(y) = 0$, donc soit $x \in \mathcal{I}$, soit $y \in \mathcal{I}$. Donc $\mathcal{I}$ est un idéal premier.

Supposons l'idéal $\mathcal{I}$ maximal. En particulier il est propre et le quotient $A/\mathcal{I}$ est distinct de l'anneau nul. Soit $x \in A/\mathcal{I}$ tel que $x \neq 0$. Soit $x' \in A$ tel que $x = \pi(x')$. Comme x est non nul, on a $x' \notin \mathcal{I}$. Comme $\mathcal{I}$ est maximal, l'idéal engendré par $\mathcal{I}$ et x' est A, donc il existe $y \in \mathcal{I}$ et $u \in A$ tel que $y + ux' = 1$. Ainsi, comme π est un morphisme d'anneaux, on a $1 = \pi(y + ux') = \pi(y) + \pi(u)\pi(x')$ or $\pi(y) = 0$ donc $\pi(u)\pi(x') = 1$. Donc x est inversible. Ainsi $A/\mathcal{I}$ est un corps.

Supposons que $A/\mathcal{I}$ est un corps. En particulier, $A/\mathcal{I}$ n'est pas l'anneau nul donc $\mathcal{I}$ est un idéal propre. Soit $\mathcal{J}$ un idéal de A tel que $\mathcal{I} \subset \mathcal{J}$. Alors, comme π est surjectif, $\pi(\mathcal{J})$ est un idéal de $A/\mathcal{I}$. Comme $A/\mathcal{I}$ est un corps, d'après la proposition 57, on a $\pi(\mathcal{J}) = A/\mathcal{I}$ ou $\pi(\mathcal{J}) = \{0\}$. Comme $\mathcal{J}$ contient $\mathcal{I} = \mathrm{Ker}(\pi)$, on a $\pi^{-1}(\pi(\mathcal{J})) = \mathcal{J}$ (*cf.* proposition 20). Ainsi $\mathcal{J} = \mathcal{I}$ ou $\mathcal{J} = A$. □

Remarque. On retrouve en particulier qu'un anneau est intègre si et seulement si son idéal nul est premier et est un corps si et seulement si son idéal nul est maximal.

Remarque. Version condensée de l'argument pour un corps : d'après la proposition 20, l'ensemble des idéaux de $A/\mathcal{I}$ est en bijection avec l'ensemble des idéaux de A contenant $\mathcal{I}$. Ainsi, d'après la proposition 57, $A/\mathcal{I}$ est un corps si et seulement si $\mathcal{I}$ est contenu dans exactement deux idéaux de A. Cette dernière propriété caractérise les idéaux maximaux de A.

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 28 et 30. □

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 52) 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 $a = c\,b$.*

Démonstration. La première propriété se démontre exactement comme dans le cas particulier $A = \mathbf{Z}$. L'équivalence 1. $\Leftrightarrow$ 2. en découle aussitôt. L'équivalence 3. $\Leftrightarrow$ 4. est facile et laissée au lecteur. Compte tenu de cette dernière équivalence, on en déduit alors 3. $\Rightarrow$ 1..

Il reste à montrer 1. $\Rightarrow$ 3.. Si $b = 0$, on a $a = 0$ et 3. est vraie avec $c = 1$. Supposons $b \neq 0$. Par hypothèse, il existe $c \in A$ tel que $b = c\,a$ et $d \in A$ tel que $a = d\,b$. En particulier on a $b = c\,d\,b$ soit $b\,(1 - c\,d) = 0$. Comme A est supposé intègre et b est non nul, on en déduit $c\,d = 1$. En particulier $c \in A^\times$. □

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 ».

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. Si a divise b, a est un diviseur commun de a et b qui est non inversible (car a est irréductible), donc a et b ne sont pas premiers entre eux.

Si a et b ne sont pas premier entre eux, il existe un diviseur commun c de a et b qui n'est pas inversible. Comme a est irréductible, c et a sont associés. Donc, comme c divise b, a divise également b. □

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

Démonstration. Comme l'idéal $a \cdot A$ est premier, il est propre, donc a est non inversible.

Soit $b, c \in A$ tels que $a = bc$. En particulier $bc \in a \cdot A$. Comme $a \cdot A$ est premier, on a $b \in a \cdot A$ ou $c \in a \cdot A$. Supposons par exemple $b \in a \cdot A$. Donc a divise b. Par ailleurs b divise a, donc a et b sont associés. Ainsi il existe $\alpha \in A^\times$ tel que $a = a\alpha c$. Comme $a \cdot A$ est non nul, a est non nul, et comme A est intègre, on a donc $\alpha c = 1$. Donc c est inversible. De même, si $c \in a \cdot A$, on trouve par symétrie $b \in A^\times$.

Ainsi a est bien un élément irréductible de A. □

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 $\nu_Q(P) \leqslant 1$.

Remarque. On montre 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.*

Démonstration. Montrons la contraposée. Supposons qu'il existe $Q \in \mathbf{K}[X]$ irréductible et $R \in \mathbf{K}[X]$ tels que $P = Q^2 R$. En dérivant, on trouve $P' = 2QQ'R + Q^2R' = Q\,(2Q'R + QR')$. Ainsi Q est un facteur irréductible commun à P et P', et P et P' ne sont pas premiers entre eux. □

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

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

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

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 $\varphi_B \colon A \to B$ 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

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

est bijective.

Démonstration. Ceci découle de la propriété universelle de l'anneau des polynômes en une indéterminée (théorème 44). En reprenant les notations de ce théorème, pour tout $(\psi, b) \in \mathrm{Hom}_{\text{anneaux}}(A, B) \times B$, le morphisme $\varphi \in \mathrm{Hom}_{\text{anneaux}}(A[X], B)$ correspondant est par définition un morphisme de A-algèbres si et seulement si le morphisme ψ coïncide avec la structure de A-algèbres $A \to B$ sur B. □

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).

Démonstration. On pourra s'aider d'un petit diagramme pour appréhender la démonstration.

Notons $\theta\colon A \to C$ la structure de A-algèbre sur C. Le fait que φ soit un morphisme de A-algèbres se traduit par l'égalité de morphismes $\varphi \circ \iota = \theta$.

Par ailleurs, montrer que ψ est un morphisme de A-algèbres revient à montrer l'égalité $\psi \circ \pi \circ \iota = \theta$. Comme $\psi \circ \pi = \varphi$, c'est immédiat. □

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 :
$$A[b] = \{\sum_{i \in \mathbf{N}} a_i \cdot b^i\}_{(a_i) \in A^{(\mathbf{N})}}.$$