Chapitre 1

Introduction

1.1 Notions de structures sur un ensemble

Un ensemble sans structure n'a pas d'intérêt en mathématiques. Il y a bien longtemps, c'est-à-dire avant la formalisation de la théorie des ensembles, on s'est aperçu que les ensembles de nombres que maniaient les mathématiciens possédaient des propriétés particulières.

Ainsi, les entiers naturels sont munis d'une addition, c'est-à-dire une façon d'associer à deux éléments quelconque un troisième, et cette "opération" a des propriétés bien particulière : elle est *associative, commutative, admet un élément neutre* (0).

On dira, après la formalisation intervenue à la fin du siècle dernier (réponse à l'un des problèmes posés par Hilbert), que tout ensemble muni d'une telle structure est un *monoïde commutatif.*

De la même façon, une fois introduits les entiers négatifs, on a remarqué que ceux-ci apparaissaient "naturellement" munis d'une addition commutative, associative, admettant un élément neutre, avec la propriété supplémentaire que *tout élément admet un symétrique* :

$$\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z} \text{ tel que } n + m = m + n = 0.$$

On dit de tout ensemble qui admet une opération possédant ces propriétés qu'il possède une structure de *groupe commutatif* (ou *abélien*).

Autres exemples : dans les années antérieures, vous avez encore appris les notions de *anneaux*, *corps*, *espaces vectoriels*,...et vous verrez les notions de *modules*, *espaces topologiques*, *variétés différentiables*, *analytiques*, etc...

Vue la grande diversité des structures possibles, qui, toutes, à un degré ou à un autre, ne sont que des formalisations ou des généralisations de structures "naturelles", il importe toujours de bien savoir de quoi l'on parle. C'est pourquoi, j'insisterai sur la nécessité de connaître parfaitement les définitions de chacune de ces structures, aussi bien celle déjà vues, que celles que vous allez découvrir.

Dans ce cours, on va s'attacher à étudier deux de ces structures et leurs propriétés : d'une part, les **anneaux** (essentiellement commutatifs), d'autre part, les **modules** sur ces anneaux.

1.2 Notions de relations d'équivalence

1.2.1 Relations

Une structure sur un ensemble peut aussi être d'un autre genre. Ainsi, on peut avoir envie de "mettre en relation" des éléments d'un ensemble (ou plus généralement, des éléments d'un ensemble avec ceux d'un autre ensemble).

Soit A et B deux ensembles, l'ensemble des éléments $(x, y), x \in A, y \in B$, tels que x est en relation avec y ou x et y sont en relation décrit un sous-ensemble G de l'ensemble des couples (x, y), c'est-à-dire $A \times B$. On dit que G est le *graphe* de la relation.

Si l'on note xRy le fait que x soit en relation R avec y, on a : $xRy \Leftrightarrow (x, y) \in G$.

Exemple : Une application $f : A \to B$ est une relation dont le graphe est l'ensemble $\{(x, f(x)) \mid x \in A\}$.

On s'intéresse plus particulièrement au cas où $A = B$. Une telle relation est appelée *relation binaire.* Dans ce cas donc, $G \subseteq A \times A$.

Exemple : L'égalité définit une relation binaire sur un ensemble. Son graphe est alors l'ensemble Δ des couples (x, x) de $A \times A$.

1.2.2 Propriétés des relations binaires

Définition 1.2.1 *Une relation binaire R sur un ensemble E est dite :*
** réflexive si $\forall x \in E$, on a xRx ;*
** symétrique si $xRy \Rightarrow yRx$;*
** antisymétrique si (xRy et yRx) $\Rightarrow x = y$;*
** transitive si (xRy et yRz) $\Rightarrow xRz$.*

Définition 1.2.2 *Une relation d'équivalence sur un ensemble E est une relation binaire réflexive, symétrique et transitive.*

En fait, c'est une relation "minimale" à mettre sur E pour **ranger** sans ambiguïté les éléments de E en sous-ensembles disjoints.

Les sous-ensembles correspondants sont appelés des *classes d'équivalence.* On notera le plus souvent par $\bar{x}$ la classe qui contient x et on dit que x est un *représentant* de x. Notons tout de suite que cette notation est souvent pratique, mais aussi bien malheureuse car elle est insuffisante lorsque l'on doit - cas fréquent - considérer plusieurs relations en même temps. L'ensemble des classes d'équivalence, noté E/R en général, est appelé *ensemble quotient* de E par la relation R.
notons encore qu'il y a une surjection naturelle π de E vers E/R donnée par $\pi(x) = \bar{x}$

Z : *Il* faut faire bien attention au fait que x est un **élément** de E tandis que $\bar{x}$ est un **sous-ensemble** de E ; ainsi $x \in \bar{x}$ et $\bar{x} \subseteq E$!!

Exemples
1) La relation $=$ est une relation d'équivalence sur n'importe quel ensemble. Les classes d'équivalence pour cette relation sont les singletons : $\forall x \in E,\ \bar{x} = \{x\}$. On a bien $E = \coprod_{x \in E} \bar{x}$. On remarque dans ce cas que $\pi : E \to E/R$ est une bijection.
2) $E = \mathbb{Z}$ et soit $\equiv$ la relation de congruence modulo un entier p. Cette relation est une relation d'équivalence.

Soit $n \in \mathbb{Z}$, alors $\bar{n} = \{m \in \mathbb{Z} \mid \exists k \in \mathbb{Z},\ m - n = kp\}$. Il est bien clair, par l'existence de la division euclidienne dans $\mathbb{Z}$, que chaque classe admet un unique représentant dans l'intervalle $\{0, .., p-1\}$. Ce qui signifie que le quotient $\mathbb{Z}/\equiv$ est en bijection avec $\{0, .., p-1\}$. La bijection inverse étant : $\forall n, 0 \leq n < p$, $\bar{n} \to n$.

Remarquons que le quotient sera ici noté plus volontiers $\mathbb{Z}/p\mathbb{Z}$ et nous verrons plus loin qu'il possède une structure d'anneau, et même, si p est premier, de corps.

3) Autres exemples : ($\mathbb{R}$, xRy ssi $x - y = 2k\pi$), soit $f : A \to B$ et xRy ssi $f(x) = f(y)$, ...

1.3 Relations d'ordre

1.3.1 Définitions

Définition 1.3.1 *Une relation d'ordre sur un ensemble E est une relation binaire réflexive, antisymétrique et transitive.*

Au lieu de noter xRy, on notera en général $x < y$ et on dira que x est *inférieur* à y. Mais attention, la relation $x < y$ sur $\mathbb{R}$ **n'** est **pas** une relation d'ordre puisqu'elle n'est ni réflexive, ni antisymétrique ; cependant la relation $\leq$, toujours sur $\mathbb{R}$ est bien une relation d'ordre.

Exemples :

* $\mathbb{N}^*$ avec la relation de division $a \mid b$.

* E étant un ensemble et $\mathcal{P}(E)$ étant l'ensemble des parties de E, la relation d'inclusion $\subseteq$ est une relation d'ordre sur $\mathcal{P}(E)$.

Définition 1.3.2 *Soit $(E, <)$ un ensemble ordonné. On dit que E est totalement ordonné si deux éléments quelconques x et y de E sont comparables par $<$, i.e. $\forall (x, y) \in E \times E,\ x < y$ ou $y < x$.*

S'il existe au moins deux éléments non comparables, on dit que E est *partiellement ordonné.*

Exercice : Dans les exemples précédents, lesquels définissent un ordre total ?

Définition 1.3.3 *Soit $(E, <)$ un ensemble ordonné et F un sous-ensemble de E. On dit que $a \in E$ est un majorant (resp. minorant) de F si, $(\forall x \in F),\ x < a$ (resp. $a < x$). On dira alors que F est majoré (resp. minoré).*

Si, dans E, existe un élément a tel que $(\forall x \in E),\ x < a$ (resp. $a < x$), il est unique et appelé *le plus grand* (resp. *le plus petit*) élément de E.

Exercice : Définir les notions de borne supérieure (inférieure) d'un sous-ensemble majoré (minoré) de E.

Si, dans E, existe un élément a tel que $(x \in E$ et $a < x) \Rightarrow a = x$, (resp. $x \in E$ et $a > x \Rightarrow a = x$), on dit que a est un élément *maximal* (resp. *minimal*) de E.

Remarques : Si E admet un plus grand élément a, alors a est maximal, et c'est bien sûr le seul. La réciproque est cependant fausse (voir exercices).

Définition 1.3.4 *Un ensemble E est dit inductivement ordonné si tout sous-ensemble totalement ordonné admet un majorant.*

Le lemme de Zorn : celui-ci peut être considéré comme un axiome de la théorie des ensembles ou être démontré à partir d'un autre axiome : l'axiome du choix.

Lemme 1.3.1 *Tout ensemble inductivement ordonné non vide admet des éléments maximaux.*

Nous aurons souvent à utiliser ce résultat par la suite, il importe donc de bien le connaître.

Exercices :

1. Y a-t-il des éléments maximaux ou minimaux dans les ensembles ordonnés suivants :

$$(\mathcal{P}(E), \subseteq),\ (\mathcal{P}(E) \setminus \emptyset, \subseteq),\ (\mathcal{P}(E) \setminus (\emptyset, E), \subseteq).$$

2. Dans $\mathbb{N}^* \setminus \{1\}$ ordonné par la division, y a-t-il des éléments maximaux, minimaux ?

Chapitre 2

Généralités sur les anneaux

2.1 Anneaux et corps

2.1.1 Premières définitions

Définition 2.1.1 *Un anneau est un ensemble A muni de deux lois (ou opérations binaires), addition et multiplication, notées $+, \cdot$, telles que $(A, +)$ soit un groupe abélien et $(A, \cdot)$ un monoïde (i.e. $\cdot$ est associative) avec de plus une propriété de distributivité de la multiplication par rapport à l'addition, à gauche et à droite. Si, en outre, $\cdot$ admet un élément neutre, A est dit unitaire ; si $\cdot$ est commutative, A est dit commutatif.*

La distributivité signifie que, pour tout triplet $(a, b, c) \in A^3$, on doit avoir

$$a(b + c) = ab + ac \text{ et } (a + b)c = ab + bc.$$

Premiers exemples : L'anneau trivial réduit à un seul élément :0 avec les $0 + 0 = 0$ et $00 = 0$. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $K[X]$, $K[X_1, .., X_n]$ sont des anneaux commutatifs unitaires, $\mathrm{End}(G)$, où G est un groupe (avec quelles lois ?) est un anneau non comutatif unitaire.

Conséquences immédiates de la définition :

1. $\forall a \in A$, $a0 = 0a = 0$. Il suffit pour cela de faire $a + 0 = a \Rightarrow a(a + 0) = aa$, d'où $aa + a0 = aa = aa + 0$, d'où le résultat par soustraction de aa.

2. Si A n'est pas trivial, alors $1 \neq 0$. En effet, $1 = 0 \Rightarrow a = a1 = a0 = 0$, $\forall a$, d'où $A = \{0\}$. Ainsi, dans la suite, nous supposerons tous les anneaux unitaires et tels que $1 \neq 0$.

3. Pour tous $a, b \in A$, $((-a)b = -(ab) = a(-b)$. On le vérifie par $0 = 0b = (a + (-a))b = ab + (-a)b$, d'où $-(ab) = (-a)b$.

4. Pour tout entier n et tout $a \in A$, on a $n(ab) = (na)b = a(nb)$. En effet : si $n > 0$, $n(ab) = ab + \cdots + ab$ (n fois) $= (a + \cdots + a)b$ (par distributivité), donc $= (na)b$ (ou de même, $= a(nb)$). Si $n < 0$, on utilise le résultat précédent.

Définition 2.1.2 *Un élément $x \in A$ est inversible s'il existe $y \in A$ tel que $xy = yx = 1$. Les éléments inversibles de A forment un groupe.*

Remarque : si $a \in A$ admet un inverse à gauche c, ie $ca = 1$ et un inverse à droite b i.e. $ab = 1$, alors $c = b$.

Exercice : formule du binôme.

Définition 2.1.3 *Un corps est un ensemble K muni de deux lois $+, \cdot$ telles que $(K, +)$ est un groupe abélien, $(K \setminus \{0\}, \cdot)$ est un groupe et la multiplication est distributive par rapport à l'addition.*

Remarque : on constate donc qu'un corps est naturellement un anneau. Lorsque la multiplication n'est pas commutative, on parlera de corps non commutatif ou d'anneau de division.

Lemme 2.1.1 *Si A est un anneau tel que tout élément non nul est inversible, alors A est un corps.*

Preuve : Il suffit de montrer que $(A \setminus \{0\}, \cdot)$ est un groupe ; or la seule propriété qui a priori fait défaut est que tout élément de $A \setminus \{0\}$ admette un inverse à gauche et à droite et c'est précisément notre hypothèse.

Définition 2.1.4 *Un homomorphisme d'anneaux est une application $f : A \to B$ où A, B sont deux anneaux et f vérifie, pour tous $a, b \in A$,*

$$\begin{cases} f(a+b) &= f(a) + f(b) \\ f(a \cdot b) &= f(a) \cdot f(b) \end{cases}$$

et tel que $f(1) = 1$. (Dans ce cas, on dira aussi que f est un homomorphisme d'anneaux unitaires).

On dira encore que le morphisme d'anneaux $f : A \to B$ est un *monomorphisme* si f est injective, un *épimorphisme* si f est surjective, un *isomorphisme* si f est bijective.

Notons tout de suite que la composée de $g \circ f : A \to C$ de deux homomorpshimes d'anneaux $f : A \to B$ et $g : B \to C$ est un homomorphisme d'aneaux, comme il est facile de le vérifier.

Exemples : les injections naturelles $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$ sont des monomorphismes d'anneaux. Pour tout n, l'application $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ qui à un entier k associe sa classe modulo n est un épimorphisme.

Proposition 2.1.1 *Pour tout anneau A, il existe un unique morphisme d'anneaux $\phi : \mathbb{Z} \to A$.*

Preuve : Notons e l'élément neutre pour la multiplication de A. ϕ étant un homomorphisme d'anneaux, on doit avoir $\phi(1) = e$ et, par conséquent, pour tout $n > 0$, $\phi(n) = \phi(1 + \cdots + 1) = \phi(1) + \cdots + \phi(1) = n\phi(1) = n \cdot e$. Et, si $n < 0$, on a $\phi(n) = \phi(-(-n)) = -\phi(-n) = (-n)e = -ne$. L'application est donc bien uniquement définie et est un homomorphisme de groupes additifs. Il reste à voir que $\phi(mn) = \phi(m)\phi(n)$, autrement dit que $(me)(ne) = (mn)e$, ce qui est immédita pour $m, n > 0$ et s'en déduit par la règle 3 ci-dessus pour des entiers négatifs.

Définition 2.1.5 *On appelle caractéristique de l'anneau A le plus petit entier m tel que $me = 0$ où e désigne l'élément neutre de la multiplication de A. Si cela n'est jamais le cas, on dit que A est de caractéristique 0 (certains disent, et ce serait, vue cette définition, plus logique,* caractéristique infinie).

Exemples : $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont de caractéristique 0, alors que $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n.

Proposition 2.1.2 *Si A est de caractéristique 0, alors l'homomorphisme $\phi : \mathbb{Z} \to A$ de la proposition précédente est injectif.*
Si A est de caractéristique finie n, alors il existe un monomorphisme d'anneaux $\mathbb{Z}/n\mathbb{Z} \to A$.

Preuve : Le noyau de l'homomorphisme de groupes additifs ϕ est un sous-groupe additif de $\mathbb{Z}$, donc est de la forme $m\mathbb{Z}$, pour un certain m. On a alors $\phi(m) = me = 0$, donc $n < m$ et ; mieux, $n|m$ (en effet, on peut faire la division de m par n : $m = nq + r$ où $r = 0$ ou $r < n$; mais, $r = m - nq$, d'où $\phi(r) = \phi(m) - \phi(q)\phi(n) = 0$, donc, par minimimalité de n, nécessairement, $r = 0$). Mais, $n \in m\mathbb{Z}$, donc n est un multiple de m, donc $m = n$ et $\ker(\phi) = n\mathbb{Z}$. L'application $\overline{\phi} : \mathbb{Z}/n\mathbb{Z} \to A$ qui à $\overline{x}$ associe $\phi(x)$ est alors bien définie et injective.

Si la caractéristique est 0, alors le noyau est $0\mathbb{Z}$, donc réduit à 0 et l'application ϕ est injective.

2.1.2 Autres définitions

Définition 2.1.6 *Un élément $x \neq 0$ de A est un diviseur de zero s'il existe $y \neq 0$ dans A tel que $xy = 0$.*

Exemple : $\mathbb{Z}/6\mathbb{Z}$ admet 2 et 3 comme diviseurs de zéro ; alors que $\mathbb{Z}$ lui-même n'en possède aucun.

Définition 2.1.7 *Un anneau (commutatif unitaire) qui ne possède aucun diviseur de zéro est dit intègre.*

Un type particulier de diviseur de zéro est donné par les *éléments nilpotents* ; $x \neq 0$ est *nilpotent* s'il existe $n \in \mathbb{N}$ tel que $x^n = 0$.

L'ensemble des éléments nilpotents d'un anneau A s'appelle le *nilradical* de A, on le notera $\mathcal{N}(A)$ (on trouve aussi la notation $\sqrt{A}$).

2.2 Constructions d'anneaux

Définition 2.2.1 *Un sous-ensemble B d'un anneau A est un sous-anneau si B est un sous-groupe de $(A, +)$ tel que, pour tous $x, y \in B$, $xy \in B$, et $1 \in B$.*

Remarque : un sous-anneau est un anneau.

Exemples : 1. ∘ si $f : A \to B$ est un homomorphisme d'anneaux (unitaires !), alors $Im(f)$ est un sous-anneau de B.

2. Le *centre* de A est l'ensemble des $x \in A$ qui commutent avec tout élément de A. Montrer que le centre de A est un sous-anneau de A.

∘ Si B et C sont deux sous-anneaux d'un même anneau A, alors $B \cap C$ est un sous-anneau de A.

∘ L'ensemble des *entiers de Gauss*, c'est-à-dire $\{m + in \mid m, n \in \mathbb{Z}\}$ forme un sous-anneau de $\mathbb{C}$.

Une autre construction intéressante est celle du produit :

Définition 2.2.2 *Etant donnés deux anneaux A et B, l'ensemble des couples $(a, b) \in A \times B$ peut être muni d'une structure d'anneaux par les opérations suivantes :*

$$(a, b) + (a', b') = (a + a', b + b');\ (a, b)(a', b') = (aa', bb');\ \textit{neutre} = (1_A, 1_B).$$

On note $A \times B$ et on l'appelle produit des anneaux A et B.

Remarque : les applications de projection $p_A : A \times B \to A$ et $p_B : A \times B \to B$ sont alors des épimorphismes.

Proposition 2.2.1 *Pour tout anneau A et tout couple de morphismes d'anneaux $\alpha : A \to B$, $\beta : A \to C$, il existe un unique morphisme d'anneaux $\phi : A \to B \times C$ tel que $p_B \circ \phi = \alpha$ et $p_C \circ \phi = \beta$.*

Preuve : On définit ϕ par $\phi(a) = (\alpha(a), \beta(a))$.

Exercice : montrer que l'application $A \to A \times B$ telle que $a \mapsto (a, 0)$ n'est pas un homomorphisme d'anneaux.

Le produit de deux anneaux commutatifs est évidemment commutatif.

Remarque : On peut généraliser à un nombre quelconque d'anneaux. Soit$\{A_i\}_{i\in I}$ une famille d'anneaux. La structure d'anneau sur $A = \prod_i A_i = \{(a_i)_{i\in I} \mid a_i \in A_i\}$ est donnée par l'addition $(a_i) + (b_i) = (a_i + b_i)$ et la multiplication par $(a_i)(b_i) = (a_i b_i)$.

Z! Comme remarqué ci-dessus, l'injection naturelle : $A_i \to A$ définie par $(a_i) \mapsto (0, .., 0, a_i, 0, ..)$ n'est pas un homomorphisme d'anneaux. En effet, l'élément neutre 1 pour la multiplication de A_i ne s'envoie pas sur l'élément neutre du produit qui est $(1, 1, 1, \ldots)$.

Soit X un ensemble quelconque et A un anneau. L'ensemble des applications $X \to A$ est naturellement muni d'une structure d'anneau (unitaire) par les opérations suivantes :

$- >$ la somme $f + g$ est définie comme l'application $f + g : X \to A$ qui à x associe $f(x) + g(x)$;

$- >$ le produit $f \cdot g$ est défini comme l'application qui à x associe $f(x) \cdot g(x)$;

$- >$ l'application qui à tout $x \in X$ associe l'éléménet neutre 1 de A est élément neutre pour cette multiplication.

Il faut vérifier que ces opérations satisfont bien aux axiomes de structure d'anneau. On note A^X l'anneau des fonctions sur X à valeurs dans A. On peut aussi vérifier que, si A est commutatif, A^X l'est. Par ailleurs, il est possible de réaliser A comme sous-anneau de A^X en identifiant $a \in A$ avec la fonction constante $X \to A$, $x \mapsto a$, $\forall x \in X$.

Rappelons aussi que, si G est un groupe abélien, l'ensemble des endomorphismes $\mathrm{End}(G)$ de G, muni des lois $+, \circ$ a une structure d'anneau (non commutatif en général). Montrer que $\mathrm{End}(\mathbb{Z}) \cong \mathbb{Z}$ (attention aux structures des $\mathbb{Z}$ dans cet isomorphisme). Montrer que $\mathrm{End}(\mathbb{Z} \times \mathbb{Z})$ n'est pas commutatif (prendre $f(n, m) = (m, n)$ et $g(n, m) = (n, 0)$ par exemple). On pourrait aussi parler, étant donné un anneau non commutatif A de l'anneau *opposé* A^{op} muni de la multiplication opposée.

2.3 Idéaux d'un anneau

2.3.1 Définitions

Définition 2.3.1 *Un idéal à gauche (resp. à droite, bilatère) $\mathcal{I}$ de A est un sous-groupe de $(A, +)$ tel que : $\forall x \in A$, $x\mathcal{I} \subseteq \mathcal{I}$, ie un sous-groupe tel que $A\mathcal{I} \subseteq \mathcal{I}$ (resp. tel que : $\mathcal{I}A \subseteq \mathcal{I}$, tel que : $A\mathcal{I}A \subseteq \mathcal{I}$).*

Exemples :

* Le sous-ensemble réduit à (0) est un idéal bilatère, de même que l'anneau tout entier.

* Dans l'ensemble des matrices carrées $\mathcal{M}_n(\mathbb{R})$, l'ensemble des matrices dont la première colonne est nulle est un idéal à gauche, l'ensemble des matrices dont la première ligne est nulle est un idéal à droite (vérifier que $\mathcal{M}_n(\mathbb{R})$ est bien un anneau - non commutatif !).

* Soit $a \in A$, alors l'ensemble $Aa = \{xa \mid x \in A\}$ est un idéal à gauche de A (de même, $aA \ldots$, AaA, $\ldots$ sont des idéaux à droite, bilatère).

* Un corps K a exactement deux idéaux : 0 et K.

* Si f est un homomorphisme, alors $\ker(f)$ est un idéal bilatère (le prouver). Et, plus généralement, l'image réciproque d'un idéal est un idéal. **Z !** L'image d'un idéal par un morphisme d'anneau $f : A \to B$ n'est pas, en général, un idéal de l'anneau d'arrivée B (mais est un idéal de l'anneau (? ?) $f(A) \subset B$).

* Si un anneau A n'a que (0) et A comme idéaux, alors A est un corps (en effet, soit $x \neq 0$, $x \in A$, alors, si Ax est un idéal de A, non réduit à 0, donc $Ax = A$. Par conséquent, $1 \in Ax$, autrement dit, il existe y tel que $yx = 1$; donc x est inversible).

* Le nilradical d'un anneau est un idéal (le prouver).

Remarques : Si A est commutatif, tout idéal à gauche ou à droite est bilatère. Dans la suite, nous ne considérerons la plupart du temps que des idéaux bilatères.

Un idéal contenant 1 (ou un élément inversible) est l'anneau tout entier.

Définition 2.3.2 *Un idéal à gauche (resp. à droite, bilatère) est dit principal s'il peut s'écrire Aa (aA, AaA). Un anneau principal est un anneau commutatif intègre dans lequel tout idéal est principal.*

Exemples : Dans $\mathbb{Z}$ ou $K[X]$ tout idéal est principal. Mais dans $K[X, Y]$, (X) est principal, mais pas (X, Y).

2.3.2 Opérations sur les idéaux

Considérons deux idéaux (à gauche, à droite, $\ldots$) $\mathcal{I}$, $\mathcal{J}$. On définit les opérations suivantes :

Définition 2.3.3 *La somme est l'ensemble $\mathcal{I} + \mathcal{J} = \{a + b \mid a \in \mathcal{I} \text{ et } b \in \mathcal{J}\}$, c'est un idéal (à gauche, à droite,bilatère) de A appelé somme des idéaux $\mathcal{I}$ et $\mathcal{J}$.*

*L'ensemble $\mathcal{I}\mathcal{J} = \{$sommes finies de $ab \mid a \in \mathcal{I}$ et $b \in \mathcal{J}\}$ est un idéal de A appelé produit de deux idéaux **bilatères** $\mathcal{I}$ et $\mathcal{J}$.*

Remarquons encore que l'intersection ensembliste $\mathcal{I} \cap \mathcal{J}$ est un idéal de A, appelé intersection des deux idéaux.

Remarques : On montre facilement que $\mathcal{I}\mathcal{J} \subseteq \mathcal{I} \cap \mathcal{J}$.
On pourrait aussi définir le produit d'un idéal à gauche par un idéal à droite, dans cet ordre.

Z : $\mathcal{I} \cup \mathcal{J}$ n'est pas, en général, un idéal de A (en effet : considérons l'anneau $\mathbb{Z}$ et les idéaux $2\mathbb{Z}$ et $3\mathbb{Z}$. La réunion de ces deux idéaux n'est pas $\mathbb{Z}$ tout entier ; or, si $\mathcal{I}$ est un idéal de $\mathbb{Z}$ contenant 2 et 3, alors $\mathcal{I} \ni 3 - 2 = 1$, donc $\mathcal{I} = A$. Par conséquent, $2\mathbb{Z} \cup 3\mathbb{Z}$ ne peut être un idéal). Mais, comme on le verra plus loin $\mathcal{I} \cup \mathcal{J} \subseteq \mathcal{I} + \mathcal{J}$.

2.3.3 Générateurs d'un idéal

Définition 2.3.4 *Si S est une partie de A, l'intersection des idéaux à gauche (resp à droite, bilatère) contenant S est un idéal et on dit que S engendre cet idéal, ou encore que les éléments de S sont les générateurs de cet idéal.*

Exemple : * L'idéal principal (cf. ci-dessus) Aa est l'idéal engendré par a, souvent noté (a).

* Si $S = \{a_1, \ldots, a_n\}$, on notera $(a_1, \ldots, a_n)$ l'idéal engendré par S.

* Dans l'anneau $K[X, Y]$, l'idéal engendré par X et Y est l'ensemble des polynomes dont le terme constant est nul.

Exercices : 1. Montrer que $\mathcal{I} + \mathcal{J}$ est engendré par $\mathcal{I} \cup \mathcal{J}$.

2. Montrer que l'idéal engendré par $a_1, \ldots, a_n$ est l'ensemble des éléments de la forme $b_1a_1 + \cdots + b_na_n$ où les b_i décrivent A.

2.3.4 Idéaux premiers. Idéaux maximaux

On supposera dans ce paragraphe que les anneaux sont tous commutatifs.

Définition 2.3.5 *Un idéal $\mathfrak{p}$ de A est dit premier si $\mathfrak{p} \neq \mathbf{A}$ et si, $(\forall x, y \in A)$, $(xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ où $y \in \mathfrak{p})$.*

Un idéal $\mathfrak{m}$ de A est dit maximal si $\mathfrak{m} \neq A$ et si $(\mathcal{I} \supseteq \mathfrak{m} \Rightarrow \mathcal{I} = \mathfrak{m})$.

2.3.5 Propriétés

Proposition 2.3.1 *Tout idéal $\mathcal{I}$ de A différent de A est contenu dans un idéal maximal.*

Preuve : Considérons l'ensemble $\mathcal{E}$ des idéaux $\mathcal{J}$ de A tq $\mathcal{J} \neq A$ et $\mathcal{I} \subseteq \mathcal{J}$.
On ordonne $\mathcal{E}$ par l'inclusion. On a $\mathcal{I} \in \mathcal{E}$, donc $\mathcal{E} \neq \emptyset$. Montrons que $\mathcal{E}$ est ordonné inductivement.

Soit $\mathcal{F} = \{\mathcal{I}_\alpha\}_{\alpha \in K}$ un sous-ensemble totalement ordonné de $\mathcal{E}$. Il est constitué d'idéaux $\mathcal{I}_\alpha$ tels que, pour tout couple d'indices $(\alpha, \beta) \in K \times K$, on a soit $\mathcal{I}_\alpha \subseteq \mathcal{I}_\beta$, soit $\mathcal{I}_\alpha \supseteq \mathcal{I}_\beta$ et tels que $1 \notin \mathcal{I}_\alpha, 1 \notin \mathcal{I}_\beta, \mathcal{I} \subseteq \mathcal{I}_\alpha, \mathcal{I} \subseteq \mathcal{I}_\beta$.

Soit alors $\mathcal{J} = \bigcup_{\alpha \in K} \mathcal{I}_\alpha$. Alors, $\mathcal{J}$ est un idéal : en effet, si, $x, y \in \mathcal{J}$, alors $\exists \alpha, \beta \in K$ tels que $x \in \mathcal{I}_\alpha,\ y \in \mathcal{I}_\beta$, et comme, par exemple, $\mathcal{I}_\alpha \subseteq \mathcal{I}_\beta$, on en déduit $x - y \in \mathcal{I}_\beta \subseteq \mathcal{J}$; donc $\mathcal{J}$ est un sous-groupe additif. De plus, clairement, pour tout x de A, $x\mathcal{J} \subseteq \mathcal{J}$. En outre, $1 \notin \mathcal{J}$ (sinon il existerait un $\alpha \in K$ tel que $1 \in \mathcal{I}_\alpha$) et $\mathcal{I} \subseteq \mathcal{J}$.

Donc, $\mathcal{J} \in \mathcal{E}$ et est un majorant de $\mathcal{F}$ et, par conséquent, $\mathcal{E}$ satisfait aux hypothèses du lemme de Zorn, donc admet un élément maximal :

$$ie : \exists \mathfrak{m} \in \mathcal{E} \text{ tel que } (\mathcal{K} \in \mathcal{E} \text{ et } \mathfrak{m} \subseteq \mathcal{K} \Rightarrow \mathfrak{m} = \mathcal{K}).$$

Evidemment, cela implique que $\mathfrak{m}$ est un idéal maximal : en effet, si $\mathcal{L}$ est un idéal propre de A tq. $\mathcal{L} \supseteq \mathfrak{m}$, alors $\mathcal{L} \supset \mathcal{I}$, donc $\mathcal{L} \in \mathcal{E}$ et, par maximalité, $\mathcal{L} = \mathfrak{m}$.

Corollaire 2.3.1 *Tout élément non inversible de A est contenu dans un idéal maximal.*

Définition 2.3.6 *Si un anneau A ne possède qu'un seul idéal maximal, on dira qu'il est local (on écrira souvent $(A, \mathfrak{m})$ pour préciser le nom de l'idéal maximal).*

Si A possède un nombre fini, > 1, d'idéaux maximaux, on dira qu'il est semi-local.

2.4 Anneaux quotients

Soit A un anneau et $\mathcal{I}$ un idéal **bilatère**. Prenons sur A la relation R définie par $xRy \Leftrightarrow x - y \in \mathcal{I}$. On vérifie facilement que R est une relation d'équivalence sur A ; on peut donc en prendre l'ensemble quotient A/R (cf. TD préliminaire), que nous écrirons ici $A/\mathcal{I}$.

Parlant ici d'anneaux, il est naturel de vouloir munir $A/\mathcal{I}$ d'une structure d'anneau, autrement dit de définir deux opérations sur $A/\mathcal{I}$ ayant les propriétés voulues.

Définissons tout d'abord une addition, i.e. une application :

$$\begin{array}{rccc} + : & A/\mathcal{I} \times A/\mathcal{I} & \to & A/\mathcal{I} \\ & (\bar{x}, \bar{y}) & \mapsto & \bar{x} + \bar{y} \end{array}$$

avec les propriétés adéquates. Pour cela, on a envie de poser : $\bar{x} + \bar{y} = \overline{x + y}$.

Nous avons ainsi défini une relation, il faut encore vérifier que c'est une application : c'est-à-dire qu'à un couple (x, y) n'est associé qu'une seule image. Or, x et y ne sont que des représentants de $\bar{x}$ et $\bar{y}$; quelle image est définie à partir de deux autres représentants x' et y' ? Plus précisément, a-t-on $x' \bar{+} y' = x \bar{+} y$?

Clairement, $(x'+y')-(x+y) = (x'-x)+(y'-y) \in \mathcal{I}$, leurs classes d'équivalence coïncident donc bien, par conséquent, on peut bien définir l'addition comme ci-dessus. On remarque aussi tout de suite qu'avec cette définition, la surjection canonique π (cf. 0.2.) est un homomorphisme de groupes.

On procède de même pour la multiplication ; on définit $\bar{x} \cdot \bar{y} = \overline{x \cdot y}$. A nouveau, il faut vérifier que c'est légitime, à savoir, il faut vérifier que si x' et y' sont d'autres représentants de $\bar{x}$ et $\bar{y}$ respectivement, alors $\overline{x' \cdot y'} = \overline{x \cdot y}$.

Or, $x' \cdot y' - x \cdot y = x'y' - x'y + x'y - xy = x'(y' - y) + (x' - x)y$ qui, parce que $\mathcal{I}$ est un idéal **bilatère**, appartient bien à $\mathcal{I}$.

Comme pour l'addition, cette définition fait que π vérifie $\pi(x \cdot y) = \pi(x) \cdot \pi(y)$.

De plus, $\pi(1) = \bar{1}$, d'où, $\forall \bar{x} \in A/\mathcal{I}$:

$$\pi(1) \cdot \bar{x} = \pi(1 \cdot x) = \pi(x) = \pi(x \cdot 1) = \bar{x} \cdot \pi(1),$$

donc $\pi(1)$ est élément neutre de $A/\mathcal{I}$).

Par conséquent, l'application $\pi : A \to A/\mathcal{I}$ est un homomorphisme d'anneaux.

Notation On note souvent $x + \mathcal{I}$ la classe de x *modulo* $\mathcal{I}$, au lieu de $\bar{x}$.

Proposition 2.4.1 *Soit $g : A \to B$ un homomorphisme d'anneaux et $\mathcal{I} \subseteq A$ un idéal bilatère tel que $\mathcal{I} \subseteq \ker(g)$, alors il existe un unique homomorphisme d'anneaux $\tilde{g}$ de $A/\mathcal{I}$ vers B tel que $g = \tilde{g} \circ \pi$.*

Preuve : Il suffit de vérifier qu'il est bien légitime de poser $\tilde{g}(x + \mathcal{I}) = g(x)$. Pour cela, il suffit de voir que :

$$x \sim x' \Rightarrow g(x') = g(x).$$

L'unicité résulte immédiatement de cette définition.

Proposition 2.4.2 *Il y a une correspondance biunivoque entre les idéaux de A contenant $\mathcal{I}$ et les idéaux de $A/\mathcal{I}$. De plus, cette bijection respecte l'inclusion.*

Preuve : Soit $\mathcal{J}$ un idéal de $A/\mathcal{I}$, il est immédiat que $\pi^{-1}(\mathcal{J})$ est un idéal de A.

De même, étant donné un idéal $\mathcal{I}'$ de A contenant $\mathcal{I}$, $\pi(\mathcal{I}'$ est clairement un idéal de $A/\mathcal{I}$. Reste donc à montrer que $\pi^{-1}(\pi(\mathcal{I}')) = \mathcal{I}'$ et $\pi(\pi^{-1}(\mathcal{J})) = \mathcal{J}$. Ce qu'on vérifie facilement.
En effet : pour des raisons ensemblistes, on sait a priori que $\pi^{-1}(\pi(\mathcal{I}')) \supseteq \mathcal{I}'$ et $\pi(\pi^{-1}(\mathcal{J})) = \mathcal{J}$; il n'y a donc que $\pi^{-1}(\pi(\mathcal{I}')) \subseteq \mathcal{I}'$ à prouver. Or, $x \in \pi^{-1}(\pi(\mathcal{I}')) \Rightarrow \pi(x) \in \pi(\mathcal{I}')$, donc $\exists y \in \mathcal{I}'$ tel que $x \sim y$, i.e. $x - y \in \mathcal{I}$, d'où $x \in y + \mathcal{I} \subseteq \mathcal{I}' + \mathcal{I} = \mathcal{I}'$ puisque $\mathcal{I} \subseteq \mathcal{I}'$.
Encore pour raisons ensemblistes, $\mathcal{J}' \subseteq \mathcal{J} \Rightarrow \pi^{-1}(\mathcal{J}') \subseteq \pi^{-1}(\mathcal{J})$, de même que, si $\mathcal{I}' \subseteq \mathcal{I}''$ et $\mathcal{I}' \supseteq \mathcal{I}$, alors $\pi(\mathcal{I}') \subseteq \pi(\mathcal{I}'')$.

Corollaire 2.4.1 *Il y a bijection entre l'ensemble des idéaux premiers de $A/\mathcal{I}$ et l'ensemble des idéaux premiers de A contenant $\mathcal{I}$.*

Preuve : Il suffit de montrer que la bijection précédente envoie idéal premier sur idéal premier. Or, $\mathfrak{p} \in \mathrm{Spec}(A/\mathcal{I}) \Leftrightarrow \pi^{-1}(\mathfrak{p})$ premier, car π est un homomorphisme d'anneaux.

Inversement, si $\mathcal{Q}$ est un idéal premier de A contenant $\mathcal{I}$, alors $\pi(xy) = \pi(x)\pi(y) \in \pi(\mathcal{Q}) \Rightarrow xy \in \pi^{-1}(\pi(\mathcal{Q})) = \mathcal{Q} \Rightarrow x \in \mathcal{Q}$ ou $y \in \mathcal{Q}$, d'où $\pi(x) \in \pi(\mathcal{Q}) ou \pi(y) \in \pi(\mathcal{Q})$.

Lemme 2.4.1 *$\mathfrak{p}$ est premier ssi $A/\mathfrak{p}$ est intègre.*

Preuve : C.N. : $(x + \mathfrak{p}) \cdot (y + \mathfrak{p}) = 0 + \mathfrak{p}$ dans $A/\mathfrak{p}$ signifie que $xy \in \mathfrak{p}$, d'où $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$; c'est-à-dire $x + \mathfrak{p} = 0 + \mathfrak{p}$ ou $y + \mathfrak{p} = 0 + \mathfrak{p}$.

Supposons $A/\mathfrak{p}$ est intègre. Alors, $xy \in \mathfrak{p} \Leftrightarrow xy + \mathfrak{p} = 0$ dans $A/\mathfrak{p}$. Mais, $xy + \mathfrak{p} = (x + \mathfrak{p}) \cdot (y + \mathfrak{p})$, d'où, $A/\mathfrak{p}$ étant intègre, $x + \mathfrak{p} = 0 + \mathfrak{p}$ ou $y + \mathfrak{p} = 0 + \mathfrak{p}$.

Lemme 2.4.2 *(i) $\mathfrak{m}$ maximal ssi $A/\mathfrak{m}$ est un corps.*
(ii) si $\mathfrak{m}$ est maximal, alors $\mathfrak{m}$ est premier.

Preuve : (ii) est une conséquence immédiate de (i).

(i) CN : Soit $x \in A$ tel que $x + \mathfrak{m} \neq 0 + \mathfrak{m}$ dans $A/\mathfrak{m}$. Alors $x \notin \mathfrak{m}$, d'où $Ax + \mathfrak{m} = A$, autrement dit, $\exists b \in A$, $\exists m \in \mathfrak{m}$ tels que $ab + m = 1$. Donc, $(a + \mathfrak{m}) \cdot (b + \mathfrak{m}) = 1 + \mathfrak{m}$.
CS : Il faut montrer que si $\mathcal{I} \subseteq A$ est un idéal tel que $\mathfrak{m} \subseteq \mathcal{I}$, alors $\mathcal{I} = \mathfrak{m}$. Or dans un corps K seul 0 est un idéal propre. Par conséquent, $\mathcal{I}/\mathfrak{m}$, qui est un idéal propre de $A/\mathfrak{m}$, est 0, autrement dit $\mathcal{I} \subseteq \mathfrak{m}$, donc $\mathcal{I} = \mathfrak{m}$.

Exercices :

• Les idéaux de $\mathbb{Z}$ sont soit $\mathbb{Z}$, soit de la forme $n\mathbb{Z}, n \in \mathbb{Z}$. Quels sont les idéaux premiers, maximaux ?

• De même, les idéaux de $K[X]$ sont soit $K[X]$, soit de la forme $PK[X]$ où $P \in K[X]$. Quels sont les idéaux premiers, maximaux ?

• Quels sont les idéaux de $K[X_1, \ldots, X_n]$? Donner des exemples d'idéaux premiers, maximaux.

Remarque : $\mathfrak{p}$ premier n'implique pas $\mathfrak{p}$ maximal (cf. exercices ci-dessus).

Proposition 2.4.3 *i) Soit A un anneau et $\mathfrak{m}$ un idéal propre de A tel que, tout x de A n'appartenant pas à $\mathfrak{m}$ est inversible, alors A est local d'idéal maximal $\mathfrak{m}$.*

ii) Soit $\mathfrak{m}$ un idéal maximal d'un anneau A et supposons que tout élément x de $1 + \mathfrak{m}$ est inversible, alors $(A, \mathfrak{m})$ est local.

Preuve : i) Il est bien clair que $\mathfrak{m}$ est maximal, puisque tout élément non nul de $A/\mathfrak{m}$ est inversible, donc $A/\mathfrak{m}$ est un corps. De plus, si $\mathcal{I}$ est un idéal de A contenant strictement $\mathcal{M}$, alors, il existe $x \in \mathcal{I},\ x \notin \mathfrak{m}$, donc x est inversible, par hypothèse, donc $1 = x^{-1}x \in \mathcal{I}$, d'où $\mathcal{I} = A$.

Supposons qu'il existe un idéal $\mathcal{I}$ de A qui ne soit pas contenu dans $\mathfrak{m}$. Alors, par maximalité de $\mathfrak{m}$, $\mathcal{I} + \mathfrak{m} = A$. Par conséquent, il existe $x \in \mathcal{I},\ m \in \mathfrak{m}$ tels que $x + m = 1$. Ou encore, $x = 1 - m$, donc $x \in 1 + \mathfrak{m}$, i.e. x est inversible. Or, $x \in \mathcal{I}$, donc $\mathcal{I} = A$.

2.5 Localisation et anneaux de fractions

2.5.1 Définition

Définition 2.5.1 *On dit qu'un sous-ensemble S d'un anneau commutatif A est une partie multiplicative de A si $1 \in S$ et si, pour tous $x, y \in S$, $xy \in S$ (ie. S est un monoïde unitaire).*

Considérons alors l'ensemble des couples $\{(a, s) \mid a \in A,\ s \in S\} = A \times S \subset A \times A$ sur lequel on met la relation $(a, s)R(a', s') \Leftrightarrow \exists t \in S$ tq. $t(as' - a's) = 0$.

On vérifie facilement qu'il s'agit d'une relation d'équivalence, car elle est :

réflexive : $1(as - as) = 0$,

symétrique : $(a, s)R(a', s') \Leftrightarrow t(as' - a's) = 0 \Rightarrow t(a's - as') = 0 \Rightarrow (a', s')R(a, s)$.

transitive : $(a, s)R(a', s')$ et $(a', s')R(a", s") \Rightarrow \exists t, t' \in S$ tq. $t(as' - a's) = 0,\ t'(a's" - a"s') = 0$. D'où, multipliant la première égalité par $t's"$, la deuxième par ts et, faisant la différence, on obtient $tt's'(as" - a"s) = 0$, donc $(a, s)R(a", s")$.

L'ensemble quotient $(A \times S)/R$ est noté $S^{-1}A$ et la classe d'équivalence d'un couple (a, s) est notée $\dfrac{a}{s}$.

2.5.2 Structure d'anneau sur $S^{-1}A$

On va définir deux opérations sur $S^{-1}A$. On a naturellement *envie* de définir les deux opérations de la manière suivante :

$$\begin{array}{rccc} + : & S^{-1}A \times S^{-1}A & \to & S^{-1}A \\ & (\frac{a}{s}, \frac{a'}{s'}) & \mapsto & \frac{as'+a's}{ss'} \end{array}$$

et

$$\begin{array}{rccc} \times : & S^{-1}A \times S^{-1}A & \to & S^{-1}A \\ & (\frac{a}{s}, \frac{a'}{s'}) & \mapsto & \frac{aa'}{ss'} \end{array} .$$

Le problème est que, a priori, il n'y a guère de raison pour que de telles *applications* existent. En fait, il faut vérifier qu'à un couple $(\dfrac{a}{s}, \dfrac{a'}{s'})$, on associe **une seule image** par $+$ (et de même par $\times$). Autrement dit, si on prend d'autres représentants (b, t), (b', t') des classes de (a, s) et (a', s'), obtient-on par $+$ (respect. $\times$) la même image ? Il faut donc vérifier que

$$\frac{as' + a's}{ss'} = \frac{bt' + b't}{tt'}$$

(et de même pour $\times$) ou, de manière équivalente, a-t-on $(as' + a's, ss')R(bt' + b't, tt')$?

Or, $(a, s)R(b, t) \Rightarrow \exists \sigma \in S,\ \sigma(at - bs) = 0$ et $(a', s')R(b', t') \Rightarrow \exists \rho \in S,\ \rho(a't' - b's') = 0$. D'où, en multipliant la première égalité par $\rho s't'$ et la deuxième par σst et en faisant la différence,

on obtient $\rho\sigma\left((as'+a's)tt'-(bt'-b't)ss'\right)=0$. Ce qui prouve que $(as'+a's,ss')R(bt'+b't,tt')$.

On procède de la même façon pour la multiplication. On multiplie la première relation par $\sigma a't'$, la deuxième par ρbs et on fait la somme. On trouve alors

$$\sigma\rho a't'(at-bs)+\rho\sigma bs(a't'-b's')=\sigma\rho(aa'tt'-bb'ss').$$

Les deux opérations sont donc bien définies. Leurs propriétés (associativité, existence de neutre et, pour +, existence de symétriques, ainsi aussi que commutativité) se déduisent aisément des propriétés correspondantes dans A. Ainsi, $S^{-1}A$ est muni, naturellement d'une structure d'anneau (commutatif).

Définition 2.5.2 *L'anneau $S^{-1}A$ est appelé localisé de A en S ou anneau des fractions de A relativement à S.*

On a une application naturelle $\phi : A \to S^{-1}A$ définie par $a \mapsto \frac{a}{1}$ et on vérifie immédiatement que c'est un homomorphisme d'anneaux tel que $\forall s \in S$, $\phi(s)$ est inversible dans $S^{-1}A$.

Reamarques : 1) Si $0 \in S$, alors $S^{-1}A = \{0\}$;

2) Si A est intègre, ϕ est injective et on identifie A au sous-anneau $\phi(A)$ de $S^{-1}A$. En d'autres termes, cela revient à étendre A en rendant plus d'éléments inversibles.

Exemples : a) $A = \mathbb{Z}$, $S = A \setminus \{0\}$ est une partie multiplicative et $S^{-1}A = \mathbb{Q}$. De manière analogue, si $A = k[X]$, anneau de polynômes sur le corps k, $S = A \setminus \{0\}$, alors $S^{-1}A$ est le corps des fractions rationnelles, à une indéterminée, sur k. Plus généralement encore, si A est *intègre* et $S = A \setminus \{0\}$, l'anneau des fractions de A, $S^{-1}A$ est, en fait, un corps, qu'on appelle précisément, le corps des fractions de A.

b) On peut, de manière encore plus générale, prendre pour S, l'ensemble $S = A \setminus \{\text{diviseurs de zéro de A}\}$. C'est une partie multiplicative et l'anneau de fractions correspondant est l'*anneau total des fractions* de A, notion qui généralise celle de corps des fractions.

c) Soit $f \in A$ un élément non diviseur de zéro dans un anneau et $S = \{1, f, f^2, \ldots, f^k, \ldots\}$. Alors $S^{-1}A = \{a/f^k;\ k \in \mathbb{Z}\}$. On notera A_f si possible.

d) Soit $\mathfrak{p}$ un idéal *premier* d'un anneau A, alors $S = A \setminus \mathfrak{p}$ est une partie multiplicative. L'anneau $S^{-1}A$ possède alors un unique idéal maximal $\phi(\mathfrak{p})$, c'est donc un anneau local. C'est de là que vient l'expression de *localisation* (la notion de "local" a d'ailleurs une signification géométrique qu'on ne peut développer ici). Dans ce cas, on notera $S^{-1}A$ par $A_{\mathfrak{p}}$.

2.5.3 Propriétés

Proposition 2.5.1 *Soit $f : A \to B$ un homomorphisme d'anneaux et $S \subset A$ une partie multiplicative tels que, pour tout $s \in S$, $f(s)$ est un élément inversible de B. Alors f se factorise à travers $S^{-1}A$, autrement dit, il existe un unique $h : S^{-1}A \to B$ telle que $f = h \circ \phi$ où $\phi : A \to S^{-1}A$ est l'application naturelle.*

Preuve : A cause de la factorisation, on a envie de définir $h(\frac{a}{s}) = f(a)f(s)^{-1}$ (déjà parce que l'on doit avoir $1 = h(1) = h(s\frac{1}{s}) = h(s)h(\frac{1}{s})$). Le problème est que, défini ainsi, h dépend de la représentation de la classe de (a, s) par le représentant (a, s). Qu'en est-il si on choisit un autre représentant : (b, t), c'est-à-dire, un couple de $a \times S$ tel que $(a, s)R(b, t) \Rightarrow \exists\sigma \in S,\ \sigma(at-bs) = 0$? Mais alors $f(a)f(t) = f(b)f(s)$, et, par conséquent : $f(a)f(s)^{-1} = f(b)f(t)^{-1}$. On peut donc définir ainsi l'*application h*. L'unicité provient de la construction même.

Proposition 2.5.2 *Soit A un anneau et S une partie multiplicative de A. Alors*

(i) Pour tout idéal $\mathcal{I}$ de A, $S^{-1}\mathcal{I} = \{\frac{a}{s} |\ a \in I, s \in S\}$ est l'idéal de $S^{-1}A$ engendré par $\phi(I)$. De plus, tout idéal de $S^{-1}A$ est du type $S^{-1}\mathcal{I}$ pour un idéal $\mathcal{I}$ de A.

(ii) S^{-1} respecte l'inclusion et l'on a $S^{-1}(\mathcal{I}+\mathcal{J}) = S^{-1}\mathcal{I}+S^{-1}\mathcal{J}$, $S^{-1}(\mathcal{I}\mathcal{J}) = S^{-1}\mathcal{I}S^{-1}\mathcal{J}$ et $S^{-1}(\mathcal{I}\cap\mathcal{J}) = S^{-1}\mathcal{I}\cap S^{-1}\mathcal{J}$.

(iii) Les idéaux premiers de $S^{-1}A$ sont en bijection avec les idéaux premiers de A qui ne rencontrent pas S.

Preuves : (i) On vérifie immédiatement que $S^{-1}\mathcal{I}$ est un idéal de $S^{-1}A$. De plus, $S^{-1}(\mathcal{I}) \supset \phi(\mathcal{I})$, d'où $\phi(\mathcal{I})S^{-1}A$, qui est l'idéal engendré par $\phi(\mathcal{I})$, est inclus dans $S^{-1}(\mathcal{I})$.

Mais, comme $\forall a \in \mathcal{I}$, $\frac{a}{s} = \frac{a}{1}\frac{1}{s} \in \phi(\mathcal{I})S^{-1}A$, on en déduit que $S^{-1}(\mathcal{I}) \subseteq \phi(\mathcal{I})S^{-1}A$.

Soit alors $\mathcal{J}$ un idéal propre de $S^{-1}A$. Alors $\phi^{-1}(\mathcal{J})$ est un idéal de A et $\phi^{-1}(\mathcal{J})\cap S = \emptyset$ (sinon $\exists s \in S,\ s \in \phi^{-1}(\mathcal{J})$, d'où $\phi(s) = s/1 \in \mathcal{J}$, et, par conséquent, $1 = (1/s)(s/1) \in \mathcal{J}$, donc $\mathcal{J} = S^{-1}A$).

De plus, $S^{-1}(\phi^{-1}(\mathcal{J})) = \mathcal{J}$ car, d'une part,

$$S^{-1}(\phi^{-1}(\mathcal{J})) = \{\frac{x}{s};\ x \in \phi^{-1}(\mathcal{J})\} = \{\frac{x}{1}\frac{1}{s};\ \frac{x}{1} \in \mathcal{J}\} \subseteq \mathcal{J},$$

d'autre part, $\frac{y}{t} \in \mathcal{J} \Rightarrow \frac{y}{1} = \frac{t}{1}\frac{y}{t} \in \mathcal{J}$, d'où $y \in \phi^{-1}(\mathcal{J})$ et donc $\frac{y}{t} \in S^{-1}(\phi^{-1}(\mathcal{J}))$, c'est-à-dire $\mathcal{J} \subseteq S^{-1}(\phi^{-1}(\mathcal{J}))$.

(ii) se vérifie immédiatement.

(iii) Si $\mathfrak{q}$ est un idéal premier de $S^{-1}A$, alors $\phi^{-1}(\mathfrak{q})$ est un idéal premier de A ne rencontrant pas S et, de plus, par (i), $S^{-1}(\phi^{-1}(\mathfrak{q})) = \mathfrak{q}$. Il reste donc à montrer que si $\mathfrak{p}$ est un idéal premier de A ne rencontrant pas S, alors $S^{-1}\mathfrak{p}$ est un idéal premier de $S^{-1}A$ (ce qui est clair par définition de $S^{-1}\mathfrak{p}$) et qu'on a : $\phi^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$. Or, l'inclusion $\supseteq$ est toujours vérifiée (raison ensembliste). Par ailleurs, si $x \in \phi^{-1}(S^{-1}\mathfrak{p})$, alors $\phi(x) \in S^{-1}\mathfrak{p}$, c'est-à-dire $\exists y \in \mathfrak{p}$ tel que $\frac{x}{1} = \phi(x) = \frac{y}{t}$, ce qui signifie : $\exists s \in S$ tel que $s(tx - y) = 0$, ie. $stx \in \mathfrak{p}$. Or, $st \notin \mathfrak{p}$, d'où $x \in \mathfrak{p}$.

Exemple : Soit A un anneau et $\mathfrak{p}_1,\ \mathfrak{p}_2$ deux idéaux premiers de A. Soit $S = A\setminus\mathfrak{p}_1$ et $\mathcal{I} = \mathfrak{p}_1\cap\mathfrak{p}_2$. Soient encore, $t \in \mathfrak{p}_2$, $t\notin\mathfrak{p}_1$ et $x \in \mathfrak{p}_1$, $x\notin\mathfrak{p}_2$, alors $y = tx \in \mathcal{I} = \mathfrak{p}_1 \cap \mathfrak{p}_2$, d'où $x = \frac{y}{t} \in S^{-1}\mathcal{I}$ et donc $x \in \phi^{-1}(S^{-1}\mathcal{I})$, mais $x\notin\mathcal{I}$. Conclusion : $\phi^{-1}(S^{-1}\mathcal{I}) \neq \mathcal{I}$. Donc, en général, S^{-1} ne réalise pas de bijection entre les idéaux de A ne rencontrant pas S et ceux de $S^{-1}A$.

2.6 Quelques résultats remarquables

Définition 2.6.1 *On dit que deux idéaux $\mathcal{I},\ \mathcal{J}$ d'un anneau commutatif A sont étrangers si $\mathcal{I} + \mathcal{J} = A$.*

Théorème 2.6.1 (dit théorème Chinois) Etant donnés deux idéaux étrangers $\mathcal{I},\ \mathcal{J}$, l'homomorphisme naturel

$$\phi : A \to A/\mathcal{I} \times A/\mathcal{J}$$

défini par $x \mapsto (x + \mathcal{I}, x + \mathcal{J})$ est surjectif, de noyau le produit $\mathcal{I}\mathcal{J}$.

Preuve : Comme $\mathcal{I}$ et $\mathcal{J}$ sont étrangers, il existe $a \in \mathcal{I},\ b \in \mathcal{J}$ tels que $1 = a + b$. Pour montrer la surjectivité de ϕ, qui est un homomorphisme d'anneaux, il suffit de montrer que les éléments $(\overline{1}, \tilde{0})$ et $(\overline{0}, \tilde{1})$ du produit sont dans l'image de ϕ. Or $a = 1 - b \mapsto (\overline{0}, \tilde{1})$ et $b \mapsto (\overline{1}, \tilde{0})$.
D'où, pour tout couple $(\overline{\alpha}, \tilde{\beta}) \in A/\mathcal{I} \times A/\mathcal{J}$ et remarquant que α, β sont des représentants de $\overline{\alpha},\ \tilde{\beta}$,

$$(\overline{\alpha},\tilde{\beta}) = \phi(\beta a + \alpha b) = \phi(\beta)\phi(a) + \phi(\alpha)\phi(b) = (\overline{\beta},\tilde{\beta})(0,1) + (\overline{\alpha},\tilde{\alpha})(1,0).$$

Le noyau de ϕ est l'idéal $\{a \in A;\ a \in \mathcal{I} \text{ et } a \in \mathcal{J}\}$, ie. $\ker(\phi) = \mathcal{I} \cap \mathcal{J}$. Mais, si x est dans cette intersection, comme $x = xa + xb$ et que $xa,\ xb \in \mathcal{I}\mathcal{J}$, x aussi, d'où, $\mathcal{I} \cap \mathcal{J} = \mathcal{I}\mathcal{J}$.

Remarque-exercices : Ce résultat se généralise à un nombre fini quelconque d'idéaux 2 à 2 étrangers. Déduire de ce résultat général, le polynôme d'interpolation de Lagrange, à savoir : il existe un unique polynôme de $K[X]$, de degré $d-1$ prenant en d points distincts $a_1, \ldots, a_d$ les valeurs $b_1, \ldots, b_d$ qui s'écrit

$$f(X) = \sum_{i=1}^{d} b_i \frac{(X-a_1)\cdots(X\ \hat{-}\ a_i)\cdots(X-a_d)}{(a_-a_1)\cdots(a_i\ \hat{-}\ a_i)\cdots(a_i-a_d)}$$

où on écrit $X\ \hat{-}\ a$ pour dire qu'on omet l'élément $X - A$.

Proposition 2.6.1 *(i) Soit A un anneau commutatif et $\mathcal{I} \subseteq \mathcal{J}$ deux idéaux de A. Alors l'application $\phi : A/\mathcal{I} \to A/\mathcal{J}$, définie par $\phi(x+\mathcal{I}) \mapsto x + \mathcal{J}$, est un épimorphisme d'anneaux dont le noyau est l'idéal $\mathcal{J}/\mathcal{I}$ de $A/\mathcal{I}$. De plus, ϕ définit un isomorphisme*

$$\bar{\phi} : \frac{A/\mathcal{I}}{\mathcal{I}/\mathcal{J}} \cong \frac{A}{\mathcal{J}}.$$

(ii) Si $\mathcal{I},\ \mathcal{J}$ sont deux idéaux de A, alors l'application composée

$$\psi : \mathcal{I} \to \mathcal{I} + \mathcal{J} \to \frac{\mathcal{I}+\mathcal{J}}{\mathcal{J}}$$

telle que $\psi(x) = x + \mathcal{J}$ est un homomorphisme de groupes dont le noyau est $\mathcal{I} \cap \mathcal{J}$. L'application

$$\bar{\psi} : \frac{I}{I \cap J} \to \frac{I+J}{J}$$

est un isomorphisme de groupes.

Preuve : (i) L'application ϕ est bien définie, car si x' est un autre représentant de $x + \mathcal{I}$, on a $x' - x \in \mathcal{I} \subseteq \mathcal{J}$, donc $x' + \mathcal{J} = x + \mathcal{J}$. La surjection est immédiate et le fait qu'il s'agisse d'un homomorphisme d'anneaux provient des définitions des opérations dans les deux quotients.

Le noyau $\ker\phi = \{x + \mathcal{I} \mid x \in \mathcal{J}\}$, c'est donc l'image de $\mathcal{J}$ par la surjection naturelle $A \to A/\mathcal{I}$, càd. $\mathcal{J}/\mathcal{I}$. Dès lors, ϕ se factorise à travers le quotient $\frac{A/\mathcal{I}}{\mathcal{I}/\mathcal{J}}$ définissant l'isomorphisme $\bar{\phi}$.

(ii) Que ψ soit un homomorphisme de groupes dont le noyau est $\mathcal{I} \cap \mathcal{J}$ est bien clair, d'où $\bar{\psi}$, obtenu par passage au quotient, qui est injective. Il reste donc à montrer la surjectivité de $\bar{\psi}$. Or on peut définir une application inverse par $x + \mathcal{J} \mapsto x + \mathcal{I} \cap \mathcal{J}$. Celle-ci est bien définie car, si $x, y \in \mathcal{I}$ tels que $x - y \in \mathcal{J}$, alors $x - y \in \mathcal{I} \cap \mathcal{J}$. On vérifie alors que cette application est bien la réciproque de $\bar{\psi}$.

Définition 2.6.2 *Le radical de Jacobson d'un anneau A est l'intersection de tous les idéaux maximaux de A. On le notera $R(A)$ ou aussi $\sqrt{A}$.*

Proposition 2.6.2 *Un élément x de A appartient à $R(A)$ ssi $1 - xy$ est inversible dans A, pour tout y dans A.*

Preuve : $\Rightarrow$: Soit $x \in R(A)$. Si $1-xy$ n'est pas inversible pour un $y \in A$, alors $1-xy \in \mathfrak{m}$, pour un idéal maximal $\mathfrak{m}$. Mais $x \in R(A) \subseteq \mathfrak{m}$, d'où $xy \in \mathfrak{m}$, donc $1 \in \mathfrak{m}$, ce qui est absurde.
$\Leftarrow$: Soit à présent $1-xy$ inversible pour tout $y \in A$ et supposons que $\exists \mathfrak{m}$ tel que $x \notin \mathfrak{m}$. Alors, $(x)+\mathfrak{m} = A$, d'où, $\exists m \in \mathfrak{m},\ \exists y \in A$ tels que $xy + m = 1$.
Autrement dit : $m = 1 - xy \in \mathfrak{m}$, ce qui est absurde puisque $1-xy$ est inversible.

Proposition 2.6.3 *Le nilradical $\mathcal{N}(A)$ est l'intersection de tous les idéaux premiers de A.*

Preuve : Soit $\mathcal{N}'$ l'intersection de tous les idéaux premiers de A. Il nous faut montrer $\mathcal{N}' = \mathcal{N}$.

Montrons d'abord $\mathcal{N} \subseteq \mathcal{N}'$. Pour cela, soit $x \in A$ nilpotent, i.e. $\exists n > 0$ tel que $x^n = 0$. Mais alors, $x^n \in \mathfrak{p}$, d'où $x \in \mathfrak{p},\ \forall \mathfrak{p}$ idéal premier de A.

Inversement : Soit $x \in A$ non nilpotent. On va montrer que $\exists \mathfrak{p}$ idéal premier tel que $x \notin \mathfrak{p}$.

Soit $\Sigma = \{\mathcal{I} \text{ idéal } \mid\ \forall n > 0, x^n \notin \mathcal{I}\}$. Clairement, $0 \in \Sigma$, donc $\Sigma \neq \emptyset$ et Σ est inductivement ordonné, par conséquent, d'après le lemme de Zorn, Σ admet un élément maximal, soit $\mathfrak{p}$. On va montrer que $\mathfrak{p}$ est premier.

Soient $u, v \notin \mathfrak{p}$. Alors, $\mathfrak{p} \subset \mathfrak{p} + (u)$ et $\mathfrak{p} \subset \mathfrak{p} + (v)$, strictement, d'où, par la maximalité de $\mathfrak{p}$, ni l'un, ni l'autre de ces idéaux n'appartient à Σ. Donc, $\exists m > 0,\ \exists n > 0$ tels que $x^m \in \mathfrak{p} + (u)$ et $x^n \in \mathfrak{p} + (v)$, c'est-à-dire, $x^{m+n} \in (\mathfrak{p} + (u))(\mathfrak{p} + (v)) = \mathfrak{p} + (uv)$. Donc, $\mathfrak{p} + (uv)$ n'appartient pas à Σ, autrement dit, $uv \notin \mathfrak{p}$. Donc $\mathfrak{p}$ est un idéal premier qui, par construction ne contient pas x.

Chapitre 3

Anneaux euclidiens, principaux, factoriels

Tous les anneaux considérés seront commutatifs.

3.1 Anneaux euclidiens et principaux

3.1.1 Division euclidienne

Définition 3.1.1 *Dans un anneau A, on dit qu'un élément a divise un élément b, et on note $a|b$, s'il existe $c \in A$ tel que $b = ac$, autrement dit aussi pour les idéaux principaux $bA \subseteq aA$.*

Si, à la fois, $a|b$ et $b|a$, alors on dit que a et b sont associés. La relation d'association est une relation d'équivalence. Si A est **intègre**, deux élements a, b sont associés ssi ils diffèrent d'un inversible ie. $\exists u \in A$, u inversible, tq. $a = bu$ (en effet : $a = bc$ et $b = ad$ implique que $a = acd \Rightarrow a(1 - cd) = 0$ et, par l'intégrité, $cd = 1$, donc c, d sont inversibles). Les élément associés à a et les éléments inversibles sont des *diviseurs impropres* de a. Si un élément, non nul, n'a pas de diviseurs autres qu'impropres, alors on dit qu'il est *irréductible* dans A (on en donnera une version équivalente plus loin).

Définition 3.1.2 *Soit A un anneau commutatif intègre et $\nu : A \setminus \{0\} \to \mathbb{N}$ une application telle que*

1) pour tous $a, b \in A - \{0\}$, $\nu(a) \leq \nu(ab)$,

2) pour tous $a, b \in A$, $b \neq 0$, il existe $q, r \in A$ tels que $a = bq + r$ avec $\nu(r) < \nu(b)$ ou $r = 0$.

On dit alors que ν est une valuation euclidienne.

Exemples : Nous verrons plus loin que la valeur absolue sur $\mathbb{Z}$ ou le degré sur $K[X]$ sont des valuations euclidiennes.

Définition 3.1.3 *Un anneau A est euclidien si A est intègre et si A est muni d'une valuation euclidienne.*

Un anneau A est principal s'il est intègre et si tout idéal de A est principal *ie. peut-être engendré par un seul élément.*

Remarque : Dans un anneau euclidien A, muni de la valuation euclidienne ν, on peut définir une *division euclidienne* : par définition de ν, étant donnés deux éléments quelconques $a, b \in A$,

$$\exists q, r \in A, \text{ tq. } a = bq + r \text{ où } r = 0 \text{ ou } \nu(r) < \nu(b).$$

Exemples : 1. Prenons $A = \mathbb{Z}$. Alors, l'application $\mathbb{Z}^* \to \mathbb{N}$ qui à un entier k associe sa valeur absolue $|k|$ est une valuation euclidienne. En effet, d'une part, si $b \neq 0$, $|b| > 1$ et donc $|a| \leq |a||b| \leq |ab|$. D'autre part, si $b > 0$, comme $\mathbb{Z}$ est archimédien, il existe $q \in \mathbb{Z}$ tel que $bq \leq a < b(q+1)$, d'où $0 \leq r = a - bq < b$; d'où le résultat lorsque $b > 0$ et si $b \leq 0$, par ce qui précède, il existe q', r tels que $a = |b|q' + r$, prenant alors $q = -q'$, on obtient $a = qb + r$

2. Considérons à présent $A = k[X]$, l'anneau de polynômes à une variable sur le corps k. L'application $d : k[X]^* \to \mathbb{N}$ définie par $d(P) = \deg(P)$, degré du polynôme P est aussi une valuation euclidienne. En effet, si $P = QR$, alors $\deg(P) = \deg(Q) + \deg(R) \geq \deg(R)$. D'autre part, si S, T sont deux polynômes de $k[X]$, alors il existe $Q, R \in k[X]$ tels que $S = TQ + R$ où $R = 0$ ou $\deg(R) < \deg(T)$. On procède par récurrence sur le degré de S. Si $\deg(S) < \deg(T)$, on prend $Q = 0, R = S$.

Si $\deg(S) = \deg(T) = n$, alors $S(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$ et $T(X) = b_n X^n + b_{n-1}X^{n-1} + \cdots + b_0$, d'où faisant $R = S - \frac{a_n}{b_n}T$, on obtient $\deg(R) < n$ et on pose $Q = \frac{a_n}{b_n}$.

On suppose donc que, pour tout S, $\deg(S) \leq k$ et tout T, il existe un couple Q, R tel que $S = QT + R$ avec $R = 0$ ou $\deg(R) < \deg(T)$. Soit maintenant S un polynôme de degré $k+1$ et soit a_{k+1} son coefficient dominant. Notant b_ℓ le coefficient dominant de T, écrivons $S' = S - \frac{a_{k+1}}{b_\ell}X^{k+1-\ell}T$. Il n'y a donc plus de terme de degré $k+1$ dans S' qui est donc un polynôme de degré $\leq k$. On en déduit, par l'hypothèse de récurrence, qu'il existe un couple (Q', R') tel que $S' = Q'T + R'$ où $R' = 0$ ou $\deg(R') < \deg(T)$.

Comme $S = S' + \frac{a_{k+1}}{b_\ell}X^{k+1-\ell}T = Q'T + R' + \frac{a_{k+1}}{b_\ell}X^{k+1-\ell}T = (Q' + \frac{a_{k+1}}{b_\ell}X^{k+1-\ell})T + R'$, le couple $Q = Q' + \frac{a_{k+1}}{b_\ell}X^{k+1-\ell}$, $R = R'$ satisfait aux conditions.

Remarque : on notera que, dans ces deux cas, le couple (quotient, reste) est *unique*. En effet, dans le cas de $\mathbb{Z}$, $a = bq_1 + r_1 = bq_2 + r_2 \Rightarrow b(q_1 - q_2) = r_2 - r_1$, d'où, puisque $r_i < b \Rightarrow |r_2 - r_1| \leq max r_i < b$, $q_1 - q_2 = 0$, et donc aussi $r_1 = r_2$. On le montrera aussi dans le cas $k[X]$ plus loin.

Théorème 3.1.1 *Soit A un anneau euclidien. Alors, pour tout idéal $\mathcal{I}$ de A, il existe $c \in A$ tel que $\mathcal{I} = Ac$.*

Preuve : Soit $\nu : A - \{0\} \to \mathbb{N}$ la valuation euclidienne sur A. Soit alors $c \neq 0$ tel que $\nu(c) = \min\{\nu(d);\ d \in \mathcal{I}\}$.

Soit $d \in \mathcal{I}$ quelconque. Il existe donc q, r tels que $d = cq + r$ où $\nu(r) < \nu(c)$ ou $r = 0$. Si $r \neq 0$, on a $r = d - cq \in \mathcal{I}$ puisque $d, c \in \mathcal{I}$. Or $\nu(r) < \nu(c)$ contredit la minimalité de c, donc $r = 0$ et $d = cq$. Par conséquent, $d \in Ac$, pour tout $d \in \mathcal{I}$, d'où $\mathcal{I} \subset cA$; mais, comme $c \in \mathcal{I}$, on a aussi l'inclusion inverse, d'où $\mathcal{I} = Ac$.

Corollaire 3.1.1 *Tout anneau euclidien est principal.*

Exemples : 1) Nous avons déjà vu que $\mathbb{Z}$ et $k[X]$ étaient principaux, mais on peut aussi obtenir le résultat comme conséquence du corollaire et des exemples ci-dessus.

2) Tous les anneaux principaux ne sont pas euclidiens. En ce qui concerne les sous-anneaux de la forme $\mathbb{Z}[\alpha] = \{m + n\alpha;\ m, n \in \mathbb{Z}\}$, α racine d'un polynôme de degré 2, seuls ceux contenus dans $\mathbb{Q}(\sqrt{d})$ avec $d = -11, -7, -3, -2, -1, 2, 3, 5, 6,\ 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$ sont euclidiens, du moins pour la valeur absolue. Notons ainsi qu'en 2004, un Canadien, Malcolm

Harper, a montré que $\mathbb{Z}[\sqrt{14}]$ était en fait euclidien pour une valuation euclidienne bizarre, autre que la norme. Les autres ne sont pas euclidiens, certains ne sont même pas factoriels (notion que nous verrons un peu plus loin). Par exemple : $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal, mais non euclidien, $\mathbb{Z}[\sqrt{10}]$ n'est pas principal, $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel.

Proposition 3.1.1 *Etant donnés $a, b \in A$, anneau principal, il existe un élement $d \in A$ tel que*
1) d divise a et d divise b,
2) $\forall e \in A$ tel que $e|a$ et $e|b \Rightarrow e|d$. On dira que d est "le" plus grand commun diviseur de a et b.

Preuve : Il suffit de considérer l'idéal (a, b) engendré par a et b. Comme l'anneau A est principal, il existe $d \in A$ tel que $(a, b) = dA$. Clairement donc d divise a et b et si e divise à la fois a et b, alors $a = ea',\ b = eb'$, mais $d \in (a, b) \Rightarrow d = ak + b\ell = a'ke + b'\ell e = (a'k + b'\ell)e$, donc $e|d$.

Remarque : il faut noter que 1) et 2) ne caractérisent pas nécessairement un seul élément $d \in A$. Mais si d et d' vérifient tous deux 1) et 2), alors on a : $d|d'$, donc $d' = \lambda d$, et $d'|d$, d'où $d = \mu d'$, $\lambda, \mu \in A$. Par conséquent, $d = \mu\lambda d \Rightarrow (1 - \mu\lambda)d = 0$, d'où, puisque A est intègre, $\mu\lambda = 1$, autrement dit λ et μ sont inversibles. Donc deux pgcd sont égaux *à multiplication par un élément inversible près*, autrement dit les deux sont *associés*. Le pgcd est donc défini uniquement si on le considère comme une classe modulo association.

Corollaire 3.1.2 Identité de Bezout Etant donnés $a, b \in A$, anneau principal, si le $\text{pgcd}(a, b) = d$, alors il existe $u, v \in A$ tels que $au + bv = d$.

Inversement, s'il existe $u, v \in A$ tels que $au + bv = e$ alors le pgcd de a et b divise e. En particulier, si $e = 1$, alors a et b sont premiers entre eux.

Preuve : Comme $(a, b) = dA$, on a $d \in (a, b)$, donc, comme ci-dessus, il existe donc $u, v \in A$ tels que $d = au + bv$.

Inversement, supposons que $e \in A$ tel qu'il existe u, v avec $au + bv = e$; on en déduit que $e \in (a, b) = dA$ si on note d le pgcd de a et b. Donc $d|e$ et si $e = 1$, nécessairement $d = 1$.

Calcul pratique du pgcd dans le cas d'un anneau euclidien : l'algorithme d'Euclide Etant donnés $a, b \in A$, anneau euclidien, on sait qu'il existe $q, r \in A$ tels que $a = bq_0 + r_0$ où $r_0 = 0$ ou $\nu(r_0) < \nu(b)$, ν désignant une valuation euclidienne sur A.

Ecrivons alors $a = bq_0 + r_0$ et si $r_0 \neq 0$, $b = r_0q_1 + r_1$, ainsi de suite $r_{i-1} = r_iq_{i+1} + r_{i+1}$ tant que $r_i \neq 0$. Cette succession de "divisions" s'arrête nécessairement puisque ν prend toutes ses valeurs dans $\mathbb{N}$ et que $\nu(r_{k+1} < \nu(r_k)$ pour tout k tel que $r_{k+1} \neq 0$, autrement dit, on a :

$$\nu(b) > \nu(r_0) > \nu(r_1) > \cdots > \nu(r_{i-1}) > \nu(r_i) > \cdots$$

Comme il n'y a qu'un nombre fini d'entiers plus petits que $\nu(b)$, la suite décroissante ci-dessus s'arrête au bout d'un nombre fini de pas. Donc, nécessairement, il existe i tel que $r_{i+1} = 0$. Je prétends qu'alors r_i est le pgcd de a et b.

En effet, la dernière ligne s'écrit alors $r_{i-1} = r_iq_{i+1}$, d'où $r_{i-2} = r_{i-1}q_i + r_i = r_iq_{i+1}q_i + r_i = r_i(q_{i+1}q_i + 1)$, donc r_i divise r_{i-2}.

Supposons alors que r_i divise tous les restes $r_{i-1}, r_{i-2}, \ldots, r_{i-k}$ et montrons que cela implique que r_i divise r_{i-k-1}. Or $r_{i-k-1} = r_{i-k}q_{i-k+1} + r_{i-k+1}$ et, par notre hypothèse, r_i divise r_{i-k} et r_{i-k+1}, donc $r_i|r_{i-k-1}$. Cela jusqu'à $k = i$, càd. $i - k = 0$, d'où $b = r_0q_1 + r_1$, et donc r_i divisant r_0 et r_1 divise b, mais aussi, $a = bq_0 + r_0$. Donc r_i divise à la fois a et b.

Mais, inversement, le pgcd d de a, b divise r_0 et par suite, divise tous les restes successifs, donc aussi r_i. D'où $r_i|d$, d étant le pgcd, et $d|r_i$. Autrement dit, $r_i = ud$ où u est un élément inversible de A.

Remarque : l'algorithme ci-dessus fournit une façon de calculer un couple u, v tel que $d = au+bv$. On part de la dernière ligne et on remonte les calculs.

Lemme de Gauss *Dans un anneau principal, si $a|bc$ et $(a, b) = 1$, alors $a|c$.*

Preuve : Si $(a, b) = 1$, alors il existe $u, v \in A$ tels que $au + bv = 1$. Mais $a|bc \Rightarrow \exists\alpha$ tq. $bc = \alpha a \Rightarrow c = (au + bv)c = auc + vbc = auc + v\alpha a = a(uc + v\alpha)$, donc $a|c$.

Définition 3.1.4 *$m \in A$ est un plus petit commun multiple (ppcm) de a et b ssi $a|m$ et $b|m$ et, pour tout m' tel que $m'|a$ et $m'|b$, alors $m|m'$. Il est uniquement déterminé en tant que classe modulo association.*

Lemme 3.1.1 *Dans un anneau principal A, deux éléments a, b quelconques admettent un ppcm m et on a $ab = umd$ où d est le pgcd de a et b et u un inversible de A.*

Preuve : Il suffit de remarquer que le ppcm est un générateur de $aA \cap bA$. En effet, m est un multiple de a, donc appartient à l'iidéal aA et de b, donc appartient à bA, donc à l'intersection. Comme A est principal, l'idéal intersection peut être engendré par un seul élément, notons celui-ci m. Alors m est un multiple commun à a et b. De plus, si m' est un autre multiple commun à a et b, alors lui aussi est dans l'intersection qui s'écrit mA, donc est un multiple de m.

La relation avec le pgcd vient de ce qu'on peut écrire $a = a'd$, $b = b'd$ avec $(a', b') = 1$; alors $a'b'd = ab' = a'b$, donc $a'b'd$ est un diviseur commun à a et b.

Si maintenantt $m = ka,\ m = \ell b$, d'où $m = ka'd = \ell b'd$. Comme $(a', b') = 1,\ ka' = \ell b' \Rightarrow a'|\ell$ (et $b'|k$), càd. $\ell = \ell' a'$ d'où $m = \ell' a'b'd$, donc $a'b'd|m$, d'où $a'b'd$ est le ppcm de $a,\ b$.

3.1.2 Eléments irréductibles

Définition 3.1.5 *Un élément $a \neq 0$ d'un anneau A est dit irréductible si a n'est pas inversible et si : $a = bc$ implique b inversible ou c inversible.*

On vérifie que cette définition est équivalent à celle donnée précédemment, elle est simplement mieux formalisée.

Proposition 3.1.2 *Si A est un anneau intègre, alors, si l'idéal aA est premier, a est irréductible.*

Preuve : Si $a = bc$, alors $bc \in aA$, donc, puisque aA est premier, $b \in aA$ ou $c \in aA$. D'où,

soit $b = ab'$ et, par conséquent, $a = ab'c \Rightarrow a(1 - b'c) = 0 \Rightarrow b'c = 1$ car $b \neq 0$ et A intègre, donc c est inversible,

soit $c = ac'$ et on conclut d'une manière identique.

Remarque : la réciproque à cette proposition est **fausse** en général. Contre-exemple : prenons $A = \mathbb{Z}[i\sqrt{5}]$. L'élément $1 + i\sqrt{5}$ est irréductible (ce qu'il convient de vérifier), alors que $(1 + i\sqrt{5})(1 - i\sqrt{5}) = 6 = 2 \times 3$. Donc $2 \times 3 \in (1 + i\sqrt{5})\mathbb{Z}$, mais ni 2, ni 3 n'appartiennent à cet idéal. On a cependant le résultat suivant :

Proposition 3.1.3 *Si l'anneau A est principal, alors $a \in A$ irréductible implique que l'idéal aA est premier.*

Preuve : Soit $a \in A$ irréductible et $b, c \in A$ tels que $bc \in aA$, càd. $\exists \lambda \in A$ tq. $bc = \lambda a$. Soit $d = (a, b)$ le pgcd de a, b et écrivons $a = da',\ b = db'$ avec $(a', b') = 1$. Comme a est irréductible, cela implique que d est inversible ou a' l'est.

Si d est inversible, $bc = db'c = \lambda da' \Rightarrow b'c = \lambda a'$ (car A est intègre), donc $a'|b'c$ et que a' et b' sont premiers entre eux, par Gauss, $a'|c$, donc $c \in aA = a'A$.

Si, au contraire, a' est inversible, alors $aA = dA$ et comme $b \in dA$, $b \in aA$.

Remarque : certains disent qu'un élément $a \in A$ est premier lorsque l'idéal aA est premier, autrement dit a est premier si $a|bc$ et a ne divise pas b, alors $a|c$. On traduit alors la remarque ci-dessus par : lorsque A est commutatif intègre, un élément premier est irréductible, mais la réciproque n'est pas vraie. Exemple : dans $\mathbb{Z}[i\sqrt{5}]$, l'élément $1 + i\sqrt{5}$ est irréductible, mais n'est pas premier.

Notons encore que cela montre que $\mathbb{Z}[i\sqrt{5}]$ n'est pas principal.

3.2 Anneaux factoriels

Définition 3.2.1 *Un anneau A est factoriel si A est intègre et si tout élément a de A admet une **unique** décomposition de la forme $a = up_1 \cdots p_r$ où u est inversible et les p_i des élements irréductibles de A (pas nécéssairement distincts).*

Remarques : L'unicité signifie ici que si $a = vq_1 \cdots q_s$ avec v inversible et q_j irréductibles, alors $r = s$ et il existe une permutation $\sigma \in \mathfrak{S}_r$ telle que $\forall i \in \{1, \ldots, r\},\ p_i = \lambda_i q_{\sigma(i)}$, les λ_i étant des éléments inversibles de A. Il y a donc unicité des éléments irréductibles et de leur nombre, mais pas de l'élément inversible.

Exemple : dans l'anneau $\mathbb{Z}$, tout entier n admet une décomposition en facteurs premiers ; $28 = 2 \times 2 \times 7$ par exemple.

Proposition 3.2.1 *Dans un anneau principal A, toute chaîne croissante $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ d'idéaux de A est stationnaire ; autrement dit, il existe i tel que $I_i = I_{i+k}$ pour tout $k > 0$.*

Preuve : Tous les idéaux I_s sont principaux : $\forall s,\ \exists a_s$ tel que $I_s = Aa_s$. Soit $I = \cup_s I_s$. C'est un idéal de A puisque les idéaux I_s sont emboîtés, donc il existe $a \in A$ tel que $I = Aa$. Mais $a \in I = \cup_s I_s$, donc il existe j tel que $a \in I_j$. Mais alors, $a_j \in I = Aa$, donc $a_j = \lambda a$ et d'autre part, $a \in Aa_j$, donc $a = \mu a_j$. D'où : $a = \mu a_j = \mu\lambda a \Rightarrow a(1 - \mu\lambda) = 0 \Rightarrow \mu\lambda = 1$, autrement dit $Aa_j = Aa$ et, par conséquent, pour tout $k \geq j$, $I_k = Aa$.

Théorème 3.2.1 *Tout anneau principal est factoriel.*

Pour la démonstration, nous allons utiliser le lemme suivant, utile à se rappeler par ailleurs :

Lemme 3.2.1 *Soit $p, q \in A$, irréductibles, non associés, alors $pgcd(p, q) = 1$.*

Preuve : Soit d le pgcd de p et q et supposons-le non inversible. Alors $p = dp'$ et $q = dq'$, d'où, par les irréductibilités, p' et q' sont inversibles. Par conséquent, les idéaux principaux $(p) = (d) = (q)$ coïncident, d'où $p_u q$ pour un inversible u, autrement dit p et q sont associés.

Preuve du théorème : Montrons d'abord l'unicité d'une telle décomposition. Supposons donc $\alpha p_1 \cdots p_r = \beta q_1 \cdots q_s$ avec α, β inversibles et p_i, q_j des éléments irréductibles, pour tous i, j. De cette égalité, on déduit que p_1 divise le produit $\beta q_1 \cdots q_s$. Par le lemme précédent, si p_1 ne

divisait aucun des q_j, p_1 serait premier avec tous les q_j, ce qui contredirait le lemme de Gauss. Donc, p_1 divise l'un des q_j, et, posant $\sigma(1) = j$, $q_j = q_{\sigma(1)}$ où $\sigma : \{1, \ldots, r\} \to \{1, \ldots, s\}$, ie. $p_1 = u_1 q_{\sigma(1)}$ avec u_1 inversible. Quitte à réindicer les q_j, on peut supposer $\sigma(1) = 1$. L'égalité se ramène alors, après simplification possible parce que A est intègre, à $\alpha p_2 \cdots p_r = \beta q_2 \cdots q_s$. On conclut donc par récurrence descendante sur le nombre d'irréductibles.

Supposons qu'un élément $a \neq 0$ de A ne soit pas inversible et n'admette pas de décomposition en facteurs irréductibles. Alors a lui-même n'est pas un élément irréductible, on peut donc le décomposer en un produit $a = a_1 b_1$ et, si a_1, b_1 étaient tous deux décomposables en produits d'irréductibles, cela fournirait une telle décomposition de a ; donc l'un des a_1, b_1 n'admet pas non plus de décomposition, supposons qu'il s'agisse de a_1. Mais, $a = a_1 b_1 \Rightarrow Aa \subseteq Aa_1$. Et, on peut recommencer le même raisonnement avec $a_1 = a_2 b_2$ et déduire que a_2 n'admet pas dé décomposition. Ainsi de suite, on peut fabriquer une chaîne d'idéaux $Aa \subseteq Aa_1 \subseteq Aa_2 \subseteq \cdots$. Mais, une telle chaîne d'idéaux est stationnaire, donc il existe i tel que $Aa_i = Aa_{i+1}$. Donc $a_i = a_{i+1} b_{i+1} \Rightarrow b_{i+1}$ inversible, donc a_i est irréductible, ce qui est contradictoire.

Remarque : Nous verrons qu'il existe des anneaux non factoriels et qu'il existe des anneaux factoriels qui ne sont pas principaux (par exemple : $\mathbb{R}[X, Y]$ est factoriel, mais, comme on l'a déjà mentionné, pas principal).

Chapitre 4

Anneaux de polynômes

Les premiers exemples d'anneau en dehors des anneaux de nombres sont les anneaux de polynômes à une ou plusieurs indéterminées sur un anneau commutatif.

4.1 Anneau de polynômes à une indéterminée

4.1.1 Définition

Soit A un anneau commutatif et considérons E le sous-ensemble du produit

$$\Pi = \prod_{n\in\mathbb{N}} A = \{(a_i),\ i \in \mathbb{N},\ a_i \in A\}$$

constitué des $(a_i)_i$ tels que tous les $a_i = 0$ sauf pour un nombre fini d'indices i (c'est évidemment un sous-ensemble de l'ensemble de toutes les suites à valeurs dans A, càd. l'ensemble des applications $u : \mathbb{N} \to A$).

Munissons E d'une structure d'anneau par les opérations d'addition

$$\begin{array}{rccc} + : & E \times E & \to & E \\ & ((a_i)_{i\in\mathbb{N}}, (b_i)_{i\in\mathbb{N}}) & \mapsto & (a_i + b_i)_{i\in\mathbb{N}} \end{array}$$

ce dernier est bien dans E puisque tous ses éléments sont nuls sauf le nombre fini de ceux tels que ou $a_i \neq 0$ ou $b_i \neq 0$, et de multiplication

$$\begin{array}{rccc} \times : & E \times E & \to & E \\ & ((a_i)_{i\in\mathbb{N}}, (b_i)_{i\in\mathbb{N}}) & \mapsto & (c_i)_{i\in\mathbb{N}} \end{array}$$

où, pour tout k, $c_k = a_0b_k + a_1b_{k-1} + \cdots + a_ib_{k-i} + \cdots + a_kb_0 = \sum_{i=0}^{k} a_ib_{k-i}$. Comme $c_k = 0$ dès que00 k est suffisamment grand, on obtient bien encore un élément de E.

Il s'agit bien entendu de vérifier que l'addition confère à E une structure de groupe abélien (on peut d'ailleurs, montrer que c'est un sous-groupe de l'espace des suites) et que la multiplication est associative (ce qui est plutôt fastidieux), commutative, qu'elle admet un élément neutre $(1, 0, \ldots, 0, \ldots)$. E muni de ces deux lois possède alors une structure d'anneau commutatif. On appelle E, muni de ces duex lois, *l'anneau de polynômes à une indéterminée sur l'anneau* A et on le note $A[X]$. Le cas le plus fréquent est lorsque A est un corps.

Notons qu'on peut encore définir une application $A \times E \to E$ par $\alpha(a_i)_{i\in\mathbb{N}} = (\alpha a_i)_{i\in N}$ qui possède des propriétés analogues à celles d'une multiplication externe pour un espace vectoriel

(dans le cas où A est un corps, on sait que l'ensemble des suites à valeurs dans ce corps est muni de cette manière d'une structure d'espace vectoriel sur le corps). Parmi ces propriétés figure la distributivité par rapport l'addition.

Remarquons aussi que E est un sous-anneau de l'espace des suites $u : \mathbb{N} \to A$ à valeurs dans A (et aussi, voir TD, un sous-A-module).

4.1.2 Premières propriétés

Ecrivons X la suite $(0, 1, 0, \ldots)$ dont tous les termes sont nuls, excepté le deuxième qui vaut 1. Utilisons la règle de calcul de la multiplication, on trouve $X^2 = X \times X = (0, 0, 1, 0, \ldots)$, puis $X^3 = (0, 0, 0, 1, 0, \ldots)$, et ainsi de suite, X^k est la suite dont tous les termes sont nuls sauf le terme d'indice $k + 1$ qui vaut 1.

Considérons alors le polynôme $P = (a_0, a_1, \ldots, a_d, 0, \ldots)$ dont tous les termes d'indice $> d$ sont nuls. Alors

$$P = (a_0, a_1, \ldots, a_d, 0, \ldots) = a_0(1, 0, \ldots) + a_1(0, 1, 0, \ldots) + a_2(0, 0, 1, 0, \ldots) + \cdots a_d(0, 0, \ldots, 0, 1, 0, \ldots)$$

$$= a_0 1 + a_1 X + a_2 X^2 + \cdots a_d X^d$$

où $1 = (1, 0, \ldots)$ désigne l'élément neutre de $A[X]$. On retrouve ainsi la notation habituelle d'un polynôme.

Remarquons encore que l'application $a \mapsto a1$ est un homomorphisme injectif d'anneaux et permet donc d'identifier A avec le sous-anneau de $A[X]$ image de A par ce morphisme.

Définition 4.1.1 *Les termes non nuls de $P = (a_i)$ sont appelés les coefficients de P. Si $a_d \neq 0$ et $a_k = 0, \forall k > d$, d s'appelle le degré de P, on écrira* $\deg(P)$*, et a_d s'appelle coefficient dominant de P, a_0 est le terme constant de P.*

En particulier, par définition du produit, pour deux polynômes P, Q, si l'un des coefficients dominants au moins n'est pas un diviseur de zéro de A (pourquoi cette condition ?), on a :

$$\deg(P + Q) \leq \max\{\deg(P), \deg(Q)\} \text{ et } \deg(PQ) = \deg(P) + \deg(Q).$$

Rappelons (voir chap. précédent) que, lorsque k est un corps, $k[X]$ est un anneau euclidien, donc principal et factoriel. Plus généralement, sur un anneau A, on a le résultat suivant :

Théorème 4.1.1 *Soit A un anneau commutatif, $S, T \in A[X]$ deux polynômes de degré ≥ 0, et supposons que le coefficient dominant de T est inversible dans A. Alors, il existe un unique couple $Q, R \in A[X]$ tels que $S = QT + R$ avec $R = 0$ ou* $\deg(R) < \deg(T)$.

Preuve : Cette démonstration est tout-à-fait identique au cas où A est un corps faite dans le chapitre précédent, tenant simplement compte de l'hypothèse supplémentaire sur le coefficient dominant de T.

Ecrivons $S = a_0 + a_1 X + \cdots + a_n X^n$ et $T = b_0 + b_1 X + \cdots + b_d X^d$ où b_d est inversible dans A. Si $\deg(S) < \deg(T)$, il suffit de prendre $Q = 0$ et $R = T$ pour répondre à la question. Si $\deg(S) = \deg(T) = 0$, on peut prendre $R = 0$ et $Q = a_n b_d^{-1}$.

Faisons alors une récurrence sur $\deg(S) = n$, càd. supposons que pour tout polynôme de degré $m < n$, il existe un quotient et un reste dans la division par T. Soit alors S de degré n et, d'après ce qui précède, on peut supposer $\deg(T) < \deg(S)$. Alors $S(X) - a_n b_d^{-1} X^{n-d} T(X) = a_n X^n + \cdots + a_0 - a_n b_d^{-1} X^{n-d}(b_d X^d + \cdots + b_0) = S_1(X)$ est un polynôme de degré $< n$ (puisqu'on

s'est arrangé pour éliminer les termes de degré n !). Par l'hypothèse de récurrence, il existe donc Q_1, R, $R = 0$ ou $\deg(R) < \deg(T)$, tels que $S_1 = Q_1T + R$. Par conséquent,

$$S(X) = a_n b_d^{-1} X^{n-d} T(X) + Q_1(X)T(X) + R(X) = (a_n b_d^{-1} X^{n-d} + Q_1(X))T(X) + R(X).$$

On pose donc $Q(X) = a_n b_d^{-1} X^{n-d} + Q_1(X)$.

En ce qui concerne l'unicité, supposons que $S = TQ_1 + R_1 = TQ_2 + R_2$, alors $T(Q_1 - Q_2) = R_2 - R_1$. Mais, comme le coefficient dominant de T est inversible, on a $\deg(T(Q_1 - Q_2)) = \deg(T) + \deg(Q_1 - Q_2) > \deg(R_2 - R_1)$, ce qui n'est possible que si $Q_1 - Q_2 = 0$ et donc aussi $R_1 = R_2$.

A tout polynôme $P(X) = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ est associé une fonction, notée en général de la même façon, $P : A \to A$ définie par $x \in A \mapsto a_0 + a_1x + \cdots + a_nx^n \in A$. Ceci définit donc une application $k[X] \to k^k$, ensemble des fonctions de k dans k. Vue la définition d'un polynôme comme l'ensemble fini $(a_0, \ldots, a_n)$, on peut remarquer que $P(x)$ est le produit de la matrice ligne $(a_0, \ldots, a_n)$ par la matrice colonne $(1, x, \ldots, x^n)$ d'éléments de A.

Remarque : si $P \in A[X]$ où A est un anneau et si A est un sous-anneau de B, alors P définit aussi une fonction de B dans B. Ce qui motive la définition "générale" suivante :

Définition 4.1.2 *Soit $P \in A[X]$ un polynôme sur un sous-anneau A d'un anneau B. Alors un élément $b \in B$ est appelé racine ou zéro de P si $P(b) = 0$.*

Théorème 4.1.2 *Si k est un corps et P un polynôme de $k[X]$, de degré $n \geq 0$, alors P admet au plus n racines dans k et $a \in k$ est une racine de P ssi $X - a$ divise P.*

Preuve : Si $P(a) = 0$, alors faisons le division euclidienne de P par $X - a$: $P(X) = (X - a)Q(X) + R(X)$ où $R = 0$ ou $\deg(R) < \deg(X - A) = 1$, donc R est une constante et, comme $R(a) = P(a) = 0$, $(X - a)$ divise P. Donc a est racine ssi $X - a | P$.

Alors, si $a_1, \ldots, a_k$ sont n racines distinctes, le produit $(X - a_1) \cdots (X - a_k)$ divise P (en effet, si $a \neq b$ et a, b sont racines, alors $(X - a)Q_1(X) = (X - b)Q_2(X) \Rightarrow (a - b)Q_2(a) = 0 \Rightarrow Q_2(a) = 0 \Rightarrow X - a \mid Q_2$). Or, le degré de ce produit est k, donc $k \leq n$.

Corollaire 4.1.1 *Si k est un corps et $P(X) \in k[X]$ un polynôme admettant une infinité de racines **distinctes**, alors $P = 0$.*

Remarque : cela suppose que k contient une telle infinité d'élément distincts, ce n'est pas le cas des corps finis bien sûr.

Corollaire 4.1.2 *Soit k un corps fini à q éléments et $P \in k[X]$ un polynôme de degré $< q$. Si $P : k \to k$ est la fonction nulle, alors le polynôme P est le polynôme nul.*

Exemple : soit $A = \mathbb{Z}/p\mathbb{Z}$, p un nombre premier. Pour tout $a \in A$, on a $a^p = a$, d'où au polynôme $X^p - X$, non nul, est associée la fonction polynôme nulle. Par contre, le théorème précédent permet d'identifier, *pour un corps infini*, l'anneau de polynômes avec l'anneau des fonctions polynômes correspondant.

Théorème 4.1.3 *Soit k un corps et G un sous-groupe fini du groupe multiplicatif k^*. Alors G est cyclique. En particulier, si k est un corps fini, alors k^* est cyclique.*

Preuve : k étant commutatif, G est un groupe commutatif, donc G admet une décomposition primaire

$$G \cong \frac{\mathbb{Z}}{p_1^{\alpha_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p_k^{\alpha_k}\mathbb{Z}},$$

les p_i étant des nombres premiers distincts ou non. Il suffit alors de montrer que, si G_i est le sous-groupe de G correspondant à la partie p_i-primaire, G_i est cyclique.

Soit $a \in G_i$ un élément d'ordre maximal : $a^{p_i{}^r} = 1$ et, $\forall x \in G_i$, $x^{p_i{}^r} = 1$. Donc tous les éléments de G_i sont racines du polynôme $X^{p_i{}^r} - 1$. Le groupe cyclique engendré par a possède p_i^r éléments, qui sont tous racines de ce polynôme de degré p_i^r. Si donc G_i était plus grand, cela voudrait dire que $X^{p_i{}^r} - 1$ a plus de p_i^r racines, ce qui est impossible.

4.1.3 Anneaux de polynômes à plusieurs indéterminées

On peut de même que dans le paragraphe précédent définir les polynômes à m variables sur un anneau A comme une application $\phi : \mathbb{N}^m \to A$ nulle en dehors d'un nombre fini d'éléments (ce qui peut être vu comme un sous-ensemble de $\prod_{\mu \in \mathbb{N}^m} A^m$) et munir cet ensemble d'une addition et d'une multiplication convenables (ainsi un élément de $A[X, Y]$ peut se voir comme une matrice "infinie" où tout est nul en-dehors d'un rectangle fini). Mais, il est plus facile d'utiliser une construction par récurrence : $A[X_1, \ldots, X_m] = (A[X_1, \ldots, X_{m-1}])[X_m]$.

Quel que soit le point de départ, un monôme de $A[X_1, \ldots, X_m]$ s'écrira comme $aX_1^{s_1} \cdots X_m^{s_m}$ et un polynôme sera une somme finie de tels monômes.

On a alors différentes notions de degré : le *degré (total)* du monôme $aX_1^{s_1} \cdots X_m^{s_m}$ par rapport à l'ensemble des indéterminées est $\sum_{i=1}^m s_i \in \mathbb{N}$. Le *degré (total)* d'un polynôme $P(X_1, \ldots, X_m)$ est alors le maximum de tous les degrés totaux de tous les monômes de P. On peut aussi parler du degré en X_i du monôme $aX_1^{s_1} \cdots X_m^{s_m}$ comme s_i. Ces notions de degré se comporte de la même façon que dans le cas d'une seule indéterminée par rapport à la somme et au produit. Conséquence : *si A est intègre, alors $A[X_1, \ldots, X_n]$ l'est.*

Définition 4.1.3 *Un polynôme $P \in A[X_1, \ldots, X_n]$ est homogène de degré d si tous ses monômes sont de degré (total) d.*

Exemple : un polynôme homogène de degré 0 est une constante non nulle, un polynôme homogène de degré 1 sur k en les indéterminées X, Y est de la forme $aX + bY$, de degré 2 sur k en X, Y, de la forme $aX^2 + bXY + cY^2$. Sa fonction polynôme associée définit une forme quadratique.

Exercice : montrer qu'un polynôme P est homogène de degré d ssi $P(UX_1, \ldots, UX_n) = U^d P(X_1, \ldots, X_n)$ dans $A[X_1, \ldots, X_n, U]$.

Un homomorphisme d'anneaux $f : A \to B$ alors l'application $\tilde{f} : A[X_1, \ldots, X_m] \to B[X_1, \ldots, X_m]$ telle que $\tilde{f}(a) = f(a), \forall a \in A$ et, pour tout $i = 1, \ldots, m$, $\tilde{f}(X_i) = X_i$, commutant aux opérations d'addition et multiplication, est un homomorphisme d'anneaux.

Exemple : on rencontre souvent la situation précédente dans le cas de passage au quotient $A \to A/I$ ou d'extension de corps $k \subset K$.

De même que dans le cas d'une indéterminée, on peut associer au polynôme

$$P(X_1, \ldots, X_m) = \sum_{\alpha=(\alpha_1,\ldots,\alpha_m)} a_\alpha X_1^{\alpha_1} \cdots X_m^{\alpha_m} \in A[X_1, \ldots, X_m]$$

une application $A^m \to A$ définie par $\forall b = (b_1, \ldots, b_m) \in A^m$,

$$P(b_1, \ldots, b_m) = \sum_{\alpha} a_\alpha b_1^{\alpha_1} \cdots b_m^{\alpha_m} \in A.$$

On dira qu'on a *substitué* le m-uplet $(b_1, \ldots, b_m)$ dans P.

Un certain nombre des résultats précédents se transpose au cas de plusieurs indéterminées. Ainsi :

Théorème 4.1.4 *Soit k un corps et $T_1, \ldots, T_n$ des sous-ensembles infinis de k et $P \in k[X_1, \ldots, X_n]$ un polynôme. Si $P(a_1, \ldots, a_n) = 0$, pour tout $(a_1, \ldots, a_n) \in T_1 \times \cdots \times T_n$, alors $P = 0$.*

Preuve : il suffit de faire une récurrence sur le nombre de variables. Supposons $n \geq 2$ et écrivons P comme un polynôme en X_n à coefficients dans $k[X_1, \ldots, X_{n-1}]$:

$$P(X) = P_0(X_1, \ldots, X_{n-1}) + P_1(X_1, \ldots, X_{n-1})X_n + \cdots + P_d(X_1, \ldots, X_{n-1})X_n^d.$$

S'il existe $(b_1, \ldots, b_{n-1}) \in T_1 \times \cdots \times T_{n-1}$ tel que $P_j(b_1, \ldots, b_{n-1}) \neq 0$ pour un j, alors $P(b_1, \ldots, b_{n-1}, X_n)$ est un polynôme non nul de $k[X_n]$ qui s'annule pour toutes les valeurs de T_n, ce qui est impossible, donc le fonction $P_j \equiv O$ sur $T_1 \times \cdots \times T_{n-1}$, pour tout j. D'où, par l'hypothèse de récurrence, $P = 0$.

4.2 Factorialité

Comme tout anneau principal est factoriel, l'anneau de polynôme sur un corps $k[X]$ est factoriel. Mais, on a des résultats plus généraux.

SUITE A COMPLETER