Université de Nantes - X1MF040 - Algèbre

Erwan Brugallé, Vincent Franjou, Christoph Sorger

25 novembre 2020

Table des matières

Introduction

La notion centrale du cours est celle d'anneau commutatif (unitaire) qui formalise le calcul habituel sur les entiers. Elle nous permettra de revoir et préciser les structures vues précédemment en licence, même si nous demandons quasiment pas de pré-requis : toutes les définitions importantes seront rappelés.

La première partie traite d'aspects arithmétiques, et spécifiquement de la divisibilité dans les anneaux commutatifs. L'accent est mis sur la factorisation, et sera appliqué surtout aux anneaux de polynômes. Le seul théorème subtil du cours est d'ailleurs un théorème de Gauss sur la factorisation des polynômes.

Une seconde partie du cours aborde d'autres aspects des polynômes : l'élimination pour aborder le théorème de Bézout sur l'intersection des courbes, les polynômes symétriques qui apparaissent dans la théorie des équations. On complètera par la théorie des groupes utile à la théorie de Galois des équations : c'est en effet ce thème qui clôture le module d'algèbre du second semestre.

Le cours contient quelques exercices dans le texte principal, dans le but d'illustrer tel ou tel énoncé. Les exercices du cours proprement dit sont séparés, et comportent indications et solutions.

1 Anneaux

1.1 Introduction

Dans ce cours d'algèbre commutative la notion centrale est celle d'anneau commutatif. Cette notion prend ses origines en géométrie algébrique et en théorie de nombres algébrique. Dans le premier domaine, on étudie essentiellement les anneaux des polynômes à plusieurs variables $k[X_1, \ldots, X_n]$ sur un corps k ; dans le second on étudie essentiellement l'anneau des entiers relatifs $\mathbb{Z}$.

1.2 Définitions, premières propriétés

DÉFINITION 1.2.1. — On appelle *anneau* un ensemble non vide A, muni de deux lois internes : une loi d'addition $(a, b) \mapsto a + b$ et une loi de multiplication $(a, b) \mapsto a \cdot b$ vérifiant les propriétés suivantes :

- A muni de l'addition est un groupe abélien, noté $(A, +)$;
- pour tous $a, b, c \in A$, on a $a(bc) = (ab)c$ (associativité de $\cdot$) ;
- pour tous $a, b \in A$, on a $ab = ba$ (commutativité de $\cdot$) ;
- il existe un élément $1 \in A$ tel que pour tout $a \in A$, $1 \cdot a = a$;
- pour tous $a, b, c \in A$, on a $a \cdot (b + c) = a \cdot b + a \cdot c$ (distributivité).

Les anneaux ainsi définis sont *commutatifs* et *unitaires*. Il existe des notions plus générales d'anneaux, notamment des anneaux non commutatifs, mais où l'on doit du coup imposer que 1 est aussi neutre à droite et la distributivité à droite : $(a + b)c = ac + bc$. Un exemple d'usage courant d'anneau non commutatif est donné par l'ensemble des matrices carrées $n \times n$, avec l'addition et la multiplication des matrices. Pour ce cours d'algèbre commutative cependant, *nos anneaux seront toujours supposés commutatifs.*

Observons que $A \setminus \{0\}$ muni de la multiplication n'est pas un groupe en général, puisque nous n'imposons pas l'existence d'inverses pour la multiplication. Par exemple, dans notre premier d'exemple d'anneau, les entiers relatifs $\mathbb{Z}$, l'entier 2 n'est pas inversible.

Les axiomes ci-dessus nous permettent de calculer comme on a l'habitude pour $\mathbb{Z}$. Les notations sont utilisées librement. Par exemple, si $a \in A$ et si n est un entier positif ou nul, on définit par récurrence a^n, en posant $a^0 = 1$ et $a^n = a(a^{n-1})$.

EXERCICE 1.2.2. — Comme exercice, on pourra démontrer que

a) pour $a \in A$, on a $0a = 0$ ou autrement dit 0 est absorbant pour la multiplication ;

b) si $e \in A$ est tel que $ea = a$ pour tout $a \in A$, alors $e = 1$ ou autrement dit l'élément neutre pour la la multiplication est unique ;

c) pour tout $a \in A$, on a (-1)a = -a ;

d) pour tout $a \in A$ et pour tous entiers $m, n \geq 0$, on a $a^{m+n} = a^m a^n$;

e) pour tout $a, b \in A$ et tout entier $n \geq 0$ on a (formule du binôme)

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

Si jamais $1 = 0$ dans un anneau A, alors A est nécessairement réduit à $\{0\}$. On dit alors que A est *l'anneau nul*.

Définition 1.2.3. — Un élément $a \in A$ est dit *inversible* s'il existe $b \in A$ tel que $ab = 1$.

L'élément b dans la définition ci-dessus est unique et appelé *l'inverse* de a. Il est noté a^{-1}.

Proposition 1.2.4. — Soit A un anneau. Les éléments inversibles de A forment un groupe pour la multiplication, noté $A^\times$.

Démonstration. Observons d'abord que la multiplication définit une loi interne sur $A^\times$: Si a, b sont inversibles alors ab est encore inversible. En effet ab est d'inverse $b^{-1}a^{-1}$. Enfin, l'ensemble des éléments inversibles contient 1, et est stable par passage à l'inverse. □

Définition 1.2.5. — On dira que l'anneau non nul A est un *corps* si tout élément non nul de A est inversible.

Définition 1.2.6. — Soit A un anneau et soit a un élément de A. On dit que a est un *diviseur de zéro* s'il existe un élément $b \in A$, $b \neq 0$, tel que $ab = 0$. Un anneau non nul A est appelé *intègre* s'il n'a pas de diviseur de zéro autre que l'élément 0.

Par définition, l'anneau nul n'est donc ni intègre ni un corps.

Exemples 1.2.7. — L'anneau $\mathbb{Z}$ est intègre ; ses inversibles sont exactement $\{\pm 1\}$. Dans $\mathbb{Q}$ tout élément non nul est inversible : c'est donc un corps.

1.3 Morphismes entre anneaux

Comme dans le cas des groupes, une fois que nous avons défini nos objets, les anneaux, nous définissons les morphismes entre ces objets :

Définition 1.3.1. — Soient A et B deux anneaux. Un *morphisme d'anneaux* $f : A \to B$ est un morphisme de groupes abéliens qui respecte la multiplication et envoi 1 sur 1. Autrement dit, pour un morphisme d'anneaux, on a

- pour tous $a, b \in A$, $f(a + b) = f(a) + f(b)$ et $f(ab) = f(a)f(b)$;
- $f(1) = 1$;

La composition de deux morphismes d'anneaux est encore un morphisme. Un morphisme d'un anneau dans lui-même est appelé un *endomorphisme*.

On dira qu'un morphisme d'anneaux $f : A \to B$ est un *isomorphisme*, s'il existe un morphisme d'anneaux $g : B \to A$ tel que $f \circ g = \mathrm{Id}_B$ et $g \circ f = \mathrm{Id}_A$. Comme dans le cas des groupes, le lecteur vérifiera l'énoncé suivant :

Proposition 1.3.2. — Un morphisme d'anneaux $f : A \to B$ est un isomorphisme si, et seulement si, il est bijectif.

Soit $f : A \to B$ un morphisme d'anneaux. Si $a \in A$ est un élément inversible dans A alors $f(a)$ est encore inversible dans B, d'inverse $f(a^{-1})$. En effet,

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(1) = 1.$$

Ainsi le morphisme d'anneaux f induit un morphisme de groupes noté $f^\times : A^\times \to B^\times$.

Définition 1.3.3. — Soit A un anneau. Une partie $B \subseteq A$ est un *sous-anneau*, si B contient les éléments 0 et 1 et si B est stable par addition, multiplication et prise d'opposé.

Notez que l'anneau nul n'est sous-anneau que de lui-même, et qu'un noyau de morphisme d'anneaux n'est un sous-anneau que pour le morphisme vers l 'anneau nul.

Si $f : A \to B$ est un morphisme d'anneaux, l'image $f(A)$ est un sous-anneau de B. L'image réciproque d'un sous-anneau C de B est un sous-anneau de A.

Exercice 1.3.4. — (Anneau produit)

a) Soient A et B deux anneaux. On munit l'ensemble $A \times B$ d'une addition et d'une multiplication composante par composante, c'est-à-dire par : $(a, b)+(a', b') := (a+a', b+b')$ et $(a, b)(a', b') := (aa', bb')$.

i) Montrer que cela définit une structure d'anneaux sur $A \times B$.

ii) Sous quelles conditions est-ce que $A \times B$ est intègre ?

iii) Montrer que les éléments $e = (1, 0)$ et $f = (0, 1)$ sont des *idempotents*, c'est-à-dire satisfont à $e^2 = e$ et $f^2 = f$.

b) Soit maintenant A un anneau et e un idempotent.

i) Montrer que $1 - e$ est encore idempotent.

ii) Montrer que $eA = \{ea\,;\, a \in A\}$ est un anneau pour les lois de A. Quel est l'élément neutre pour la multiplication ?

iii) Montrer que l'anneau A est isomorphe à l'anneau produit $eA \times (1 - e)A$.

1.4 Anneaux de polynômes, séries formelles

Soit A un anneau. L'anneau des polynômes $A[X]$ est défini comme suit. Un *monôme* est une expression de la forme aX^n où $a \in A$ et $n \in \mathbb{N}$. Un *polynôme* est une somme fine de monômes. Puis, l'addition et la multiplication s'effectuent "comme on a l'habitude".

Afin de gérer efficacement l'écriture des formules pour un nombre quelconques de monômes, il est commode de considérer des monômes à coefficients nuls pour tous les degrés qui n'apparaissent pas. Autrement dit, on considère l'ensemble $A^{(\mathbb{N})}$ des familles presque nulles de coefficients dans A, c'est-à-dire les suites d'éléments de A dont tous les termes, sauf un nombre fini, sont nuls. Un polynôme est donc vu comme une suite presque nulle de coefficients. Si $P = (a_n)_{n\in\mathbb{N}}$ est un élément de $A^{(\mathbb{N})}$, on le note

$$P =: \sum_{n\in\mathbb{N}} a_n X^n$$

ce qui permet de calculer sans y penser. En effet, l'addition de P et Q est donnée par :

$$(\sum_{n\in\mathbb{N}} a_n X^n) + (\sum_{n\in\mathbb{N}} b_n X^n) = \sum_{n\in\mathbb{N}} (a_n + b_n) X^n;$$

et la multiplication PQ par

$$(\sum_{n\in\mathbb{N}} a_n X^n)(\sum_{n\in\mathbb{N}} b_n X^n) = \sum_{n\in\mathbb{N}} (\sum_{i+j=n} a_i b_j) X^n$$

où l'expression $\sum_{i+j=n} a_i b_j$ est bien, cette fois, une somme effectuée dans l'anneau A. Pour chacune de ces opérations, le résultat est bien une suite presque nulle, c'est-à-dire un polynôme.

L'élément 0 est la famille identiquement nul et 1 la famille donnée par $1_0 = 1$ et $1_n = 0$ si $n \neq 0$; avec nos notations : $1 = X^0$. On obtient ainsi une structure d'anneau, l'anneau des polynômes à coefficients dans A, noté $A[X]$. Cette construction vient avec un morphisme d'anneau injectif canonique $i : A \to A[X], a \mapsto aX^0$ permettant d'identifier A au sous-anneau de $A[X]$ des polynômes constants.

1.4.1 Anneau des séries formelles

Si l'on regarde la construction précédente, on observe qu'on peut aussi bien la faire pour l'ensemble $A^{\mathbb{N}}$ des suites d'éléments de A. On notera toujours $P = (a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$ par $P := \sum_{n\in\mathbb{N}} a_n X^n$. La formules d'addition et de multiplication des polynômes gardent le même sens (c'est même plus facile puisque il ne faut plus vérifier que la "somme" obtenue est finie). On appellera P une *série formelle* et l'anneau ainsi obtenu *l'anneau des séries formelles*. On le notera $A[[X]]$.

Par construction, l'anneau des polynômes $A[X]$ est un sous-anneau de l'anneau des séries formelles $A[[X]]$. L'impression de similarité dans la construction ne doit cependant pas cacher le fait que ces anneaux ont des propriétés très différentes, comme on le verra plus tard. Pour l'instant, on pourra déterminer ses inversibles :

EXERCICE 1.4.2. — Soit A un anneau. Déterminer $(A[X])^\times$. Quid de $(A[[X]])^\times$?

1.4.3 Propriété universelle des anneaux de polynômes

Le couple $(A, i : A \to A[X])$ est solution du problème universel suivant :

PROPOSITION 1.4.4. — Soit $f : A \to B$ un morphisme d'anneaux (commutatifs) et soit b un élément de B. Il existe un unique morphisme d'anneaux $g : A[X] \to B$ rendant commutatif le diagramme

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle i}\downarrow & \nearrow_{g} & \\ A[X] & & \end{array}$$

et tel que $g(X) = b$.

Démonstration. S'il existe un tel morphisme, il est obligatoirement donné par la formule

$$g(\sum_n a_n X^n) = \sum_n f(a_n) b^n$$

ce qui montre l'unicité. On définit donc l'application g par cette formule, puis on vérifie soigneusement qu'elle définit un morphisme d'anneau (la commutativité joue ici un rôle). □

EXEMPLE 1.4.5. — Soit A un anneau et $a \in A$. Appliqué à $id : A \to A$ on obtient le morphisme d'évaluation : le morphisme

$$\begin{aligned} ev_a : A[X] &\to A \\ P &\mapsto P(a) \ , \end{aligned}$$

est le seul morphisme d'anneaux qui vaut l'identité sur A et qui envoie X sur a.

1.4.6 Degré et conséquences

Sur l'anneau $A[X]$ on dispose d'une fonction *degré* : un polynôme non nul $P \in A[X]$ peut s'écrire $\sum_{n=0}^{d} a_n X^n$ avec $a_d \neq 0$ pour un unique entier $d \geq 0$. On définit le *degré* de P, et on note $\deg P$, par ce nombre d. L'élément a_d est appelé le *coefficient dominant* de P.

Dans ces notes écrites, par convention, $\deg 0 := -\infty$. Si $P, Q \in A[X]$; on a

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

Avec nos conventions et celles, habituelles, que $\max(-\infty, x) = -\infty$ et $-\infty + x = -\infty$ pour tout $x \in \mathbb{N} \cup \{-\infty\}$, ces inégalités sont vraies même si P, Q, $P+Q$ ou PQ est nul.

PROPOSITION 1.4.7. — Si A est intègre, $A[X]$ est encore intègre.

La propriété d'être intègre d'un anneau se transfère donc à l'anneau de polynômes à coefficients dans cet anneau.

Démonstration. Il s'agit de montrer que si P et Q sont des polynômes non nuls, alors leur produit PQ est encore non nul. On peut écrire

$$P = \sum_{n=0}^{\deg P} a_n X^n \text{ et } Q = \sum_{n=0}^{\deg Q} b_n X^n$$

avec $a_{\deg P} \neq 0$ et $b_{\deg Q} \neq 0$. Le terme de PQ de degré $\deg P + \deg Q$ a pour coefficient $a_{\deg P} a_{\deg Q}$. Comme A est intègre, ce coefficient est non nul. Ainsi PQ est non nul. □

En particulier, on voit dans l'argument ci-dessus que pour les anneaux intègres, on a

$$\deg(PQ) = \deg P + \deg Q.$$

La division euclidienne des entiers naturels se généralise aux polynômes, et c'est bien sûr un outil puissant.

THÉORÈME 1.4.8. — Soit A un anneau et P et D deux polynômes de $A[X]$. On suppose que D est non nul de coefficient dominant inversible. Alors il existe un unique couple (Q, R) de polynômes dans $A[X]$ tel que

- $P = QD + R$;
- $\deg R < \deg D$.

Attention à l'hypothèse sur D : l'inversibilité du coefficient dominant est essentielle.

Démonstration. Montrons d'abord l'unicité. Soit (Q', R') un autre couple tel que

$$P = Q'D + R' \text{ et } \deg R' < \deg D$$

Par hypothèse, $QD + R = Q'D + R'$ d'où $(Q - Q')D = R' - R$. Supposons $Q \neq Q'$ et raisonnons sur le degré de $(Q - Q')D$. D'un côté nous savons que

$$\deg((Q - Q')D) = \deg(R' - R) \leq \max(\deg(R'), \deg(R)) < \deg(D)$$

De l'autre côté, nous savons que le coefficient u de D est inversible. Si a est le coefficient dominant de $(Q - Q')$, nous avons $au \neq 0$ puisqu'un élément inversible ne peut être diviseur de zéro. Mais alors

$$\deg((Q - Q')D) = \deg(Q - Q') + \deg D \geq \deg D$$

Contradiction. Ainsi $Q = Q'$. Mais alors $R = R'$.
Pour l'existence, on raisonne par récurrence sur le degré de P, le cas de degré 0 étant évident. Si $\deg P < \deg D$ il suffit de prendre $Q = 0$ et $R = P$. Sinon, soit a le coefficient dominant de P et u celui de D. Le polynôme

$$P' := P - au^{-1}X^{\deg P - \deg D}D$$

est de degré au plus $\deg P$, avec coefficient en degré $\deg P$ égal à $a - au^{-1}u = 0$. Ainsi, $\deg P' < \deg P$. Par récurrence, il existe alors $Q', R' \in A[X]$, tels que $P' = Q'D + R'$ et $\deg R' < \deg D$. Il suit que

$$P = P' + au^{-1}X^{\deg P - \deg D}D = (Q' + au^{-1}X^{\deg P - \deg D})D + R'$$

et il suffit donc de prendre $Q = Q' + au^{-1}X^{\deg P - \deg D}$ et $R = R'$. □

1.4.9 Polynômes à plusieurs variables

Pour finir cette section notons qu'on peut considérer des anneaux de polynômes à plusieurs variables. Il suffit d'itérer la construction en considérant les polynômes à coefficients dans $A[X]$. Il nous faut aménager la notation $A[X]$, et l'on note $A[X, Y]$ l'anneau des polynômes à coefficients dans $A[X]$ ou autrement dit $A[X, Y] = (A[X])[Y]$.
Commencer d'abord avec X ou avec Y ne change rien : on peut considérer un polynôme de deux variables X et Y comme un polynôme en Y à coefficients dans $A[X]$, ou comme un (autre) polynôme en X à coefficients dans $A[Y]$, l'emploi de X et Y permettant d'éviter toute confusion.
La propriété universelle montre d'ailleurs qu'il existe un unique endomorphisme d'anneaux de $A[X, Y]$ qui conserve les polynômes constants et échange les polynômes X et Y. C'est un isomorphisme involutif.

2 Idéaux

Nous allons étudier dans ce paragraphe la question du passage d'un anneau au quotient. Considérons à titre de rappel le groupe additif $(\mathbb{Z}, +)$ de l'anneau $\mathbb{Z}$, *i.e.* le groupe abélien $\mathbb{Z}$ muni de l'addition. Pour tout entier $n \geq 0$, nous disposons du sous-groupe $n\mathbb{Z} \subseteq \mathbb{Z}$ des entiers relatifs multiples de n. Si $n = 0$, ce sous-groupe est le sous-groupe trivial ; si $n = 1$, c'est le groupe $\mathbb{Z}$ entier ; et si $n \geq 2$, c'est une sous-groupe propre et non trivial de $(\mathbb{Z}, +)$. Comme appris en licence, on peut former le quotient $\mathbb{Z}/n\mathbb{Z}$. Ensemblistement, il s'agit des classes classes d'équivalence sous la relation d'équivalence

$$a \sim b \Leftrightarrow a - b \in n\mathbb{Z}$$

On notera parfois une classe $a + n\mathbb{Z}$ par $[a]_{n\mathbb{Z}}$ ou simplement par $[a]$ quand il n'y a pas de risque de confusion par rapport au sous-groupe par lequel on prend le quotient. Il est important de comprendre que $\mathbb{Z}/n\mathbb{Z}$ vient avec une application canonique

$$\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

qui associe à $a \in \mathbb{Z}$ la classe $a + n\mathbb{Z}$. On cherche alors à munir le quotient $\mathbb{Z}/n\mathbb{Z}$ d'une structure de groupe de manière à ce que l'application π soit un morphisme de groupes. Pour cela, nous n'avons pas le choix et nous devons poser dans le quotient :

$$[a] + [b] := [a + b]$$

La seule difficulté que l'on peut avoir avec cette définition est qu'elle dépend, a priori, du choix des représentant a et b des classes $[a]$ et $[b]$. Nous devons donc vérifier que si $a \sim a'$ et $b \sim b'$ alors $a + b \sim a' + b'$. Mais ceci vient du fait que

$$(a + b) - (a' + b') = (a - a') + (b - b') \in n\mathbb{Z}$$

puisque si $(a - a') \in n\mathbb{Z}$ et $(b - b') \in n\mathbb{Z}$, la somme $(a - a') + (b - b')$ est encore dans $n\mathbb{Z}$, par définition d'un sous-groupe.

On souhaite faire de même pour $\mathbb{Z}$ considéré cette fois-ci en tant qu'anneau, *i.e.* munir le quotient $\mathbb{Z}/n\mathbb{Z}$ d'une multiplication de sorte que la projection canonique π soit un morphisme d'anneau. Quand on regarde $n\mathbb{Z} \subseteq \mathbb{Z}$, on observe cependant que $n\mathbb{Z} \subseteq \mathbb{Z}$ n'est pas un sous-anneau si $n \geq 2$, puisque $1 \notin n\mathbb{Z}$ dans ce cas. La notion de sous-anneau n'est donc visiblement pas la bonne notion pour le passage au quotient. Pour cela, on introduit la notion de *idéal*, qui sera bien un sous-groupe additif de $\mathbb{Z}$, avec la bonne propriété de compatibilité avec la multiplication :

2.1 Définitions, premières propriétés

Définition 2.1.1. — Soit A un anneau. Un sous-groupe additif I de A est un *idéal* si pour tout a dans A et tout x dans I, $ax \in I$.

Pour montrer qu'une partie $I \subseteq A$ est un idéal il suffit donc de vérifier que
- $0 \in I$;

- si $x, y \in I$ alors $x - y \in I$;
- si $a \in A$ et $x \in I$ alors $ax \in I$.

Exemples 2.1.2. —
a) Le noyau d'un morphisme d'anneaux $f : A \to B$ est un idéal de A ;
b) Soit $x \in A$. Alors $(x) = \{ax \ ; a \in A\}$ est un idéal de l'anneau A. Un tel idéal est dit principal.

Remarque 2.1.3. — Un idéal est l'anneau entier si, et seulement si, il contient 1.

Exemple 2.1.4. — Tout anneau a deux idéaux extrêmes : l'idéal nul (0) et l'anneau lui même. Si l'anneau est un corps K alors ce sont ses seuls idéaux. En effet, soit I un idéal non nul d'un corps K. Il a donc un élément non nul $x \in I$, qui est inversible puisque K est un corps. Soit $a \in K$ quelconque. Par définition d'un idéal, $(ax^{-1})x$ est dans I. On a donc $a \in I$; et cela pour tout a. Ainsi $I = K$. Réciproquement, soit x non nul dans K. Comme x est non nul, l'idéal (x) est non nul aussi. Si K n'a que deux idéaux, l'idéal (x) est égal à K et en particulier il contient l'élément 1. Il existe donc un élément $a \in K$ tel que $ax = 1$. Par conséquent x est inversible. Ainsi, tout élément non nul de K est inversible, c'est donc un corps.

Exemple 2.1.5. — Si I est un idéal de $\mathbb{Z}$, il existe un unique entier $n \geq 0$ tel que $I = (n)$. L'argument qui suit, bien que élémentaire, doit être parfaitement compris et maitrisé.

Soit I un idéal de $\mathbb{Z}$. Si $I = (0)$ alors $n = 0$ convient. Si $I \neq (0)$, considérons le plus petit n de $I \cap \mathbb{N}^*$. Par définition $(n) \subseteq I$. Montrons l'inclusion inverse. Prenons $x \in I$; la division euclidienne de x par n s'écrit : $x = qn + r$, avec $0 \leq r \leq n - 1$ et $q \in \mathbb{Z}$. Comme x et qn sont dans I, l'élément $r = x - qn$ est aussi dans l'idéal I. Comme $r < n$, on doit avoir $r = 0$ par minimalité de n. Ainsi $x = qn$. On conclut : $I \subseteq (n)$, d'où $I = (n)$.

2.2 Opérations sur les idéaux

On peut effectuer plusieurs opérations sur les idéaux comme par exemple prendre leur intersection, somme ou produit.

2.2.1 (Intersection d'idéaux). — Si I et J sont deux idéaux de A, l'intersection $I \cap J$ est encore un idéal de A. Plus généralement, l'intersection d'une famille non vide d'idéaux est encore un idéal.

Démonstration. Considérons une famille $(I_t)_t$ d'idéaux de A et posons $I = \bigcap_t I_t$. On sait que c'est un sous-groupe de A. Soit $a \in A$ et $x \in I$. Pour tout t, $x \in I_t$ et comme I_t est un idéal, $ax \in I_t$. Ainsi $ax \in I$. □

Étant donné un sous-ensemble E de A, on pose

$$(E) = \bigcap_{E \subseteq I \subseteq A} I$$

où I parcourt l'ensemble des idéaux de A contenant E. Cet ensemble est non-vide puisque A est un idéal de A. D'après ce que nous venons de voir, $\langle E \rangle$ est un idéal. C'est est le plus petit idéal contentant E et on dit que c'est l'*idéal engendré* par la partie E.

PROPOSITION 2.2.2. — Soit E une partie de A. Alors l'idéal (E) est l'ensemble des combinaisons linéaires presque nulle $\sum_{e\in E} a_e e$.

Démonstration. Soit S_E l'ensemble des combinaisons linéaires presque nulle $\sum_{e\in E} a_e e$. Comme $\sum a_e e$ est un élément de tout idéal qui contient E, c'est un élément de (E). Ainsi $S_E \subseteq (E)$. Réciproquement, montrons que S_E est un idéal de A. Il contient $0 = \sum_{e\in E} 0e$. Si $\sum a_e e$ et $\sum b_e e$ sont des éléments de S_E, la combinaison linéaire $\sum (a_e + b_e)e \in S_E$. Enfin, on note que si $a \in A$ et si $x = \sum a_e e$, alors $ax = a(\sum a_e e) = \sum (aa_e)e \in S_E$. Par conséquent, S_E est un idéal est ainsi $(E) \subseteq S_E$. □

EXEMPLE 2.2.3. — Soit A un anneau et $x \in A$. Alors $(x) = (\{x\})$. Plus généralement, on note $(x_1, \dots x_n) = (\{x_1, \dots, x_n\})$. D'après ce que nous venons de voir,

$$(x_1, \dots x_n) = \{a_1x_1 + \cdots + a_nx_n \,;\, a_1, \dots, a_n \in A\}.$$

2.2.4. — (Somme d'idéaux) Si I et J sont deux idéaux d'un anneau A, l'ensemble des sommes $x + y$ avec $x \in I$ et $y \in J$ est un idéal de A que l'on note $I + J$. On vérifie (exercice) que c'est aussi l'idéal engendré par la réunion $I \cup J$. Plus généralement, pour une famille $(I_t)_t$ d'idéaux de A, l'ensemble des sommes presque nulles $\sum_t a_t$ où pour tout t, $a_t \in I_t$ est un idéal de A, noté $\sum_t I_t$. C'est aussi l'idéal engendré par la partie $\cup_t I_t$.

2.2.5. — (Produits d'idéaux) Si I et J sont deux idéaux d'un anneau A, l'ensemble des produis xy avec $x \in I$ et $y \in J$ n'est pas forcément un idéal de A. Par définition l'idéal IJ est l'idéal engendré par ces produits. C'est donc l'ensemble des combinaisons linéaire finies $\sum x_t y_t$ avec $x_t \in I$ et $y_t \in J$.

PROPOSITION 2.2.6. — Soit A un anneau. Soient I et J deux idéaux de A. Alors $IJ \subseteq I \cap J$. De plus, si $I + J = A$, alors on a égalité $IJ = I \cap J$.

Dans le cas où $I + J = A$, les idéaux I et J sont dits *étrangers* ou *comaximaux*. Dans la littérature, on dit parfois *premiers entre eux*, en s'inspirant du cas de l'anneau des entiers relatifs pour lequel $I = (a)$ et $J = (b)$ sont étrangers si et seulement si les éléments a et b sont premiers entre eux. Nous préférons cependant de dire *comaximaux* puisque dans certains anneaux, comme par exemple les anneaux de polynômes à plusieurs variables, dire *premiers entre eux* peut prêter à confusion : dans $\mathbb{Q}[X, Y]$, on a $(X)+(Y) \neq \mathbb{Q}[X, Y]$, alors que X est Y n'ont pas de diviseur en commun autre que les inversibles. On y reviendra en détail plus tard dans le cours quand on étudiera les notions de pgcd dans les anneaux factoriels.

Démonstration. Montrons la première assertion. Si $x \in I$ et $y \in J$, le produit xy appartient à la fois à I et à J. Par conséquent, $xy \in I \cap J$. Ainsi l'idéal IJ, qui est engendré par ces produits, est contenu dans $I \cap J$.

Pour la seconde assertion, on observe que si $I + J = A$, alors il existe x et y tels que $x + y = 1$. Soit $z \in I \cap J$ et écrivons

$$z = z1 = z(x + y) = zx + zy$$

Comme $z \in J$ et $x \in I$, $zx = xz \in IJ$. De même, $zy \in IJ$. Par conséquent, $zx + zy \in IJ$ et donc $z \in IJ$, d'où $I \cap J \subseteq IJ$. □

Exercice 2.2.7. — Donner un exemple où l'inclusion de IJ dans $I \cap J$ est stricte.

2.2.8. — (Nilradical) Soit I un idéal d'un anneau A. On définit le *radical* de I comme suit

$$\sqrt{I} = \{a \in A\,;\ \text{il existe } n \geq 1, a^n \in I\}$$

C'est un idéal de A qui contient I. On définit le *nilradical* d'un anneau A comme le radical de l'idéal nul. Par définition, il est formé des éléments $a \in A$ tels qu'il existe un entier $n \geq 1$ avec $a^n = 0$. De tels éléments sont appelés *nilpotent*.

Exercice 2.2.9. — Soit A un anneau et $x \in A$ un élément nilpotent. Si $n \geq 0$ est tel que $x^{n+1} = 0$ calculer

$$(1+x)(1-x+x^2-\cdots+(-1)^n x^n).$$

En déduire que $1+x$ est inversible dans A.

2.3 Idéaux et morphismes d'anneaux

Soit $f : A \to B$ un morphisme d'anneaux. On appelle noyau de f et l'on note $\operatorname{Ker} f$ l'ensemble des $a \in A$ tels que $f(a) = 0$.

Proposition 2.3.1. — Soit $f : A \to B$ un morphisme d'anneaux. Alors $\ker f$ est un idéal.

Démonstration. Un morphisme d'anneaux est en particulier un morphisme de groupes abéliens. On sait donc que $\operatorname{Ker} f$ est un sous-groupe additif de A. De plus, si $x \in \operatorname{Ker} f$ et si $a \in A$, alors on a $f(ax) = f(a)f(x) = f(a)0 = 0$. Ainsi $ax \in \operatorname{Ker} f$ et $\operatorname{Ker} f$ est donc bien un idéal. □

Proposition 2.3.2 (Image réciproque d'un idéal). — Soient $f : A \to B$ un morphisme d'anneaux et $J \subseteq B$ un idéal de B. Alors l'image réciproque

$$I = f^{-1}(J) = \{a \in A\,;\ f(a) \in J\}$$

est encore un idéal de A.

On retrouve bien entendu la proposition précédente pour $J = (0)$.

Démonstration. On sait déjà, f étant un morphisme de groupe abéliens, que l'image réciproque I est un sous-groupe de A. De plus, si $a \in A$ et $x \in I$, alors $f(ax) = f(a)f(x) \in J$, puisque $f(x)$ l'est et J est un idéal. Ainsi, $ax \in f^{-1}(J)$ et I est donc bien un idéal. □

Remarque 2.3.3 (Image d'un idéal). — Par contre, l'image d'un idéal par un morphisme d'anneaux $f : A \to B$ n'est pas forcément un idéal dans B. Par exemple, pour le morphisme d'anneaux $f : \mathbb{Z} \to \mathbb{Q}$ défini par l'injection, les images de $(n) \subseteq \mathbb{Z}$ ne sont un idéal uniquement quand $n = 0$. En effet, $\mathbb{Q}$ est un corps et a donc exactement deux idéaux : l'idéal nul et $\mathbb{Q}$ lui même.

On retiendra donc que *les idéaux se comportent bien sous prise d'image réciproque mais pas sous prise d'image.*

L'image d'un idéal est cependant un idéal dans l'image $f(A)$.

PROPOSITION 2.3.4. — Soient $f : A \to B$ un morphisme d'anneaux et $I \subseteq A$ un idéal de A. Alors $J = f(I) \subseteq f(A)$ est un idéal de l'anneau $f(A)$. En particulier, si f est *surjectif*, l'image d'un idéal de A est bien un idéal de B.

Démonstration. On sait déjà, f étant en particulier un morphisme de groupes abéliens, que J est un sous-groupe additif de $f(A)$. Soit $z \in f(A)$ et $x \in J$. On choisit $c \in A$ tel que $f(c) = z$ et $a \in A$ tel que $f(a) = x$. Alors $zx = f(c)f(a) = f(ca)$ et comme I est un idéal, $ca \in I$, d'où $zx \in J$. L'image $J = f(I)$ est donc bien un idéal de l'anneau $f(A)$. □

Question : à quel moment est-ce que l'on a utilisé dans l'argument précédent que J est vu dans l'anneau image $f(A)$ et non dans B plus généralement ?

3 Anneaux quotient

Maintenant que nous avons introduit la notion d'idéal et que nous en avons étudié les premières propriétés, nous allons montrer comment passer au quotient d'un anneau A par un idéal $I \subseteq A$.

3.1 Définitions, premières propriétés

Soit A un anneau et I un sous-groupe additif de A. Comme $(A,+)$ est abélien, le quotient A/I est un groupe abélien. La projection canonique

$$\pi : A \to A/I$$

qui associé à $a \in A$ sa classe modulo I est un morphisme de groupe dont le noyau est le sous-groupe additif $I \subseteq A$.
On cherche à munir le quotient A/I d'une structure d'anneau de sorte que la projection canonique soit un morphisme d'anneau. Pour la partie additive nous savons déjà qu'il faut poser

$$[a] + [b] := [a+b]$$

pour s'assurer que $\pi : (A,+) \to (A/I,+)$ soit une morphisme de groupes abéliens. Pour la partie multiplicative, nous avons à nouveau pas le choix et nous devons poser

$$[a] \cdot [b] := [a \cdot b]$$

À nouveau, nous devons vérifier que cette définition ne dépend pas des représentants choisis. Pour cela, soient a' et b' deux éléments de A tels que $a \sim a'$ et $b \sim b'$. Nous devons nous assurer que $ab \sim a'b'$. Pour cela, remarquons que

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b-b') + (a-a')b'$$

Nous savons que $a-a' \in I$ et $b-b' \in I$. Si l'on fait l'hypothèse supplémentaire que I n'est pas seulement un sous-groupe additif, mais satisfait en plus à la condition d'idéal, alors $a(b-b') \in I$ et $(a-a')b' \in I$. Ainsi la somme $a(b-b')+(a-a')b' \in I$ et la multiplication définie ci-dessus ne dépend pas des représentants des classe modulo I.

En conclusion, si A est un anneau et $I \subseteq A$ est un idéal, nous pouvons munir le quotient A/I d'une structure d'anneau de sorte à ce que la projection canonique

$$\pi : A \to A/I$$

soit un morphisme d'anneau.

Une dernière remarque sur les notations des éléments du quotient A/I. Il s'agit des classes $a+I$ que nous notons parfois par $[a]_I$ ou plus simplement, quand il n'y a pas de risque de confusion, par $[a]$. Mais le plus souvent, on se dispensera des crochets qui alourdissent l'écriture sans donner plus de renseignement, et, voyant l'anneau quotient A/I comme un anneau ordinaire, on notera ses éléments donc par $x, y, z, \ldots$

Exemples 3.1.1. — Les exemples les plus courants sont l'anneau $\mathbb{Z}/n\mathbb{Z}$ des classes d'entiers modulo un entier n, $\mathbb{Z}/n\mathbb{Z}$ ou encore $k[X]/(P)$ ou k est un corps et P est un polynôme.

Par exemple, l'anneau $\mathbb{R}[X]/(X^2+1)$ est le corps des nombres complexes $\mathbb{C}$. La classe du monôme X est le nombre complexe noté i ; son carré vaut bien (-1) dans le quotient.

3.2 Propriété universelle

Les anneaux quotients vérifient la propriété universelle des quotients :

Proposition 3.2.1. — Soit A un anneau et I un idéal de A. Pour tout morphisme d'anneaux $f : A \to B$ s'annulant sur l'idéal I, *i.e.* tel que $I \subset \mathrm{Ker}(f)$, il existe un unique morphisme d'anneaux $g : A/I \to B$ rendant commutatif le diagramme

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle p}\downarrow & \nearrow_{g} & \\ A/I & & \end{array}$$

Démonstration. Le seul morphisme d'anneau g pouvant faire commuter le diagramme est obligatoirement défini par :

$$g([a]) = f(a).$$

Ici, à nouveau, la seule difficulté est de vérifier que la définition de g ne dépend pas du choix du représentant a de la classe $[a]$. Pour cela, soit $a' \in A$ tel que $a \sim a'$ et montrons que $f(a) = f(a')$. Nous avons, par définition d'un morphisme d'anneau, que

$$f(a) - f(a') = f(a - a').$$

Comme $a - a' \in I$ et comme par hypothèse $I \subseteq \mathrm{Ker}(f)$, nous avons $f(a - a') = 0$ et donc bien $f(a) = f(a')$, d'où la proposition. □

Corollaire 3.2.2. — Tout morphisme d'anneaux $f : A \to B$ se factorise par un isomorphisme d'anneaux $A/\mathrm{Ker}\, f \to f(A)$.

3.3 Les idéaux d'un anneau quotient

Soit A un anneau, $I \subseteq A$ un idéal, A/I l'anneau quotient et $\pi : A \to A/I$ la projection canonique.

On s'intéresse aux idéaux de l'anneau A/I. Soit $K \subseteq A/I$ un idéal de A/I. Comme π est un morphisme d'anneaux,

$$J = \pi^{-1}(K) \subseteq A$$

est un idéal. Cet idéal contient obligatoirement l'idéal $I = \pi^{-1}(0)$.

Proposition 3.3.1. — Soit A un anneau et I un idéal de A. L'application :

$$\begin{aligned} \text{idéaux de } A/I &\to \text{idéaux de } A \\ K &\mapsto \pi^{-1}(K) \end{aligned}$$

induite par la projection canonique $\pi : A \to A/I$ est une injection dont l'image est l'ensemble des idéaux de A contenant I.

Autrement dit, les idéaux du quotient A/I sont les idéaux de A contenant I. Pour tout idéal J de A qui contient I, il existe ainsi un unique idéal K de A/I tel que $J = \pi^{-1}(K)$. De plus on a $K = \pi(J)$ puisque l'image d'un idéal est un idéal dans ce cas en raison de la surjectivité de π (proposition 2.3.4). En raison de la proposition, les idéaux du quotient sont souvent notés J/I où J est un idéal de A contenant I.

Démonstration. Si $J \subseteq A$ est un idéal on sait, d'après la proposition 2.3.4, que $\pi(J) \subseteq A/I$ est un idéal de A/I, puisque π est surjectif. On dispose donc de deux applications :

$$\begin{aligned} \text{idéaux de } A/I &\leftrightarrows \text{idéaux de } A \text{ contenant } I \\ K &\mapsto \pi^{-1}(K) \\ \pi(J) &\hookleftarrow J \end{aligned}$$

Pour montrer la proposition, il suffit de vérifier que ces applications sont des bijections réciproques l'une de l'autre, ou encore que :

a) $\pi(\pi^{-1}(K)) = K$, et que
b) $\pi^{-1}(\pi(J)) = J$ si J contient I.

Pour la première assertion, l'inclusion $\pi(\pi^{-1}(K)) \subseteq K$ est valable pour toute application π, l'égalité résulte de la surjectivité de π : un élément x de $\pi(\pi^{-1}(K))$ est de la forme $x = \pi(a)$ pour $a \in \pi^{-1}(K)$. Ainsi, $x \in K$. Réciproquement, si $x \in K$, on choisit $a \in A$ tel que $x = \pi(a)$. Ainsi, $\pi(a) = x \in K$, d'où $a \in \pi^{-1}(K)$ et x est donc bien dans $\pi(\pi^{-1}(K))$.

Pour la seconde assertion, l'inclusion $\pi^{-1}(\pi(J)) \supset J$ est valable pour toute application π. En fait, pour tout idéal J de A, on a :

$$\pi^{-1}(\pi(J)) = J + I.$$

En effet, si $x \in J + I$, alors x est de la forme $a + b$ avec $a \in J$ et $b \in I$. On voit donc que $\pi(x) = \pi(a) + \pi(b) = \pi(a) \in \pi(J)$, d'où $\pi(x) \in \pi(J)$. Inversement, si $x \in \pi^{-1}(\pi(J))$, alors $\pi(x) = \pi(a)$ pour un a dans J. On a alors $\pi(x - a) = 0$, autrement dit $x - a \in I$. Ainsi $x = a + (x - a)$ appartient bien à $J + I$. En particulier, si J contient I, alors $J + I = J$, ce qui démontre la seconde assertion. □

Proposition 3.3.2. — Soit A un anneau, I un idéal de A et J un idéal de A contenant I. Alors la composition des surjections canoniques

$$A \to A/I \to (A/I)/(J/I)$$

a pour noyau J. En particulier, on a un isomorphisme canonique

$$A/J \simeq (A/I)/(J/I).$$

Démonstration. Si $a \in J$, alors son image sous

$$A \to A/I \to (A/I)/(J/I)$$

est nul. Si $a \in A$ appartient au noyau de ce morphisme, $\pi(a) \in J/I$. Comme $J/I = \pi(J)$, on voit que $a \in \pi^{-1}(\pi(J)) = J$. Son noyau est donc bien J. Comme ce morphisme est surjectif, le corollaire 3.2.2 nous donne l'isomorphisme recherché. □

Le quotient d'un anneau quotient est donc encore un quotient du même anneau.

3.4 Le théorème chinois sous sa forme générale

THÉORÈME 3.4.1. — Soit A un anneau. Soient I et J deux idéaux comaximaux de A. L'application diagonale induit un isomorphisme d'anneaux

$$A/IJ \simeq A/I \times A/J.$$

Démonstration. On considère le morphisme d'anneaux

$$\varphi : A \to A/I \times A/J$$

qui associe à l'élément $a \in A$, l'élément $(\pi_I(a), \pi_J(a))$. Ce morphisme est surjectif. En effet, comme $I + J = A$, il existe des éléments $x \in I$ et $y \in J$ tels que $x + y = 1$. Dans A/I, on a $1 = \pi_I(y)$ et dans A/J, on a $1 = \pi_J(x)$. Par conséquent, on a $\varphi(x) = (0, 1)$ et $\varphi(y) = (1, 0)$ dans $A/I \times A/J$. Si $a, b \in A$, on en déduit que

$$\varphi(bx + ay) = (0, \pi_J(b)) + (\pi_J(a), 0) = (\pi_I(a), \pi_J(b))$$

et φ est donc bien surjectif. Son noyau est $I \cap J$. À nouveau, comme $I + J = A$, on sait d'après la proposition 2.2.6, que $I \cap J = IJ$. Le corollaire 3.2.2 montre alors que l'on a l'isomorphisme recherché, d'où la proposition. □

4 Idéaux premiers

4.1 Définitions, premières propriétés

Soit I un idéal de A. On dit que I est un idéal propre de A si $I \neq A$.

Définition 4.1.1. — Soit A un anneau et soit I un idéal de A. On dit que I est un idéal *premier* s'il vérifie les deux conditions suivantes :
- l'idéal I est propre ;
- si $a, b \in A$ sont tels que $ab \in I$, alors $a \in I$ ou $b \in I$.

Cette notion généralise celle de nombre premier. En effet, si un produit d'entiers ab est multiple d'un nombre premier p, alors a ou b est multiple de p. La condition que I est propre, donc que $I \neq A$, est analogue à la convention qui dit que 1 n'est pas un nombre premier.
Parfois on utilise la seconde assertion sous sa forme contraposée : si a et b sont deux éléments de A n'appartenant pas à I, alors leur produit ab n'appartient pas à I.

Proposition 4.1.2. — Un idéal I d'un anneau A est premier si et seulement si l'anneau quotient A/I est intègre.

Démonstration. Dire que A/I est intègre signifie d'abord que A/I n'est pas l'anneau nul ou autrement dit que I est propre. Ensuite, si un produit xy d'éléments de A/I est nul, alors x ou y est nul. Maintenant on écrit $x = [a]$ et $y = [b]$ pour $a, b \in A$. Comme $xy = [a][b] = [ab]$, on voit que $xy = 0$ équivaut à $ab \in I$. □

Exemple 4.1.3. — L'idéal (0) d'un anneau est premier si et seulement si A est intègre.

Exemple 4.1.4. — Dans l'anneau $\mathbb{Z}$, un idéal (n) est premier si, et seulement si, n est premier.

Exemple 4.1.5. — Si k est un corps, les idéaux (X) et (X, Y) de $k[X, Y]$ sont premiers.

Proposition 4.1.6. — Soit $f : A \to B$ un morphisme d'anneaux. Alors l'image réciproque d'un idéal premier est encore premier.

Démonstration. Soit $Q \subseteq B$ un idéal premier et $P = f^{-1}(Q)$. Observons d'abord que P est propre. En effet, $f(1_A) = 1_B \notin Q$, puisque sinon, Q ne serait pas propre. Ainsi $1 \notin P$ et P n'est pas propre. Soient $a, b \in A$ avec $ab \in P$. Ainsi $f(ab) = f(a)f(b) \in Q$. Comme Q est premier, $f(a)$ ou $f(b)$ appartient à Q, ce qui signifie $a \in P$ ou $b \in P$. □

En utilisant la proposition 4.1.2, on peut raisonner sans manipuler d'éléments, comme suit. L'idéal P n'est autre que le noyau de $A \to B \to B/Q$. Par la propriété universelle des quotients, on obtient une injection $A/P \hookrightarrow B/Q$. L'anneau A/P est donc isomorphe à un sous-anneau de B/Q. Comme B/Q est intègre, et qu'un sous-anneau d'un anneau intègre est encore intègre, l'anneau A/P est intègre, et par conséquent l'idéal P premier.

Définition 4.1.7. — Soit A un anneau et soit I un idéal de A. On dit que I est un idéal *maximal* s'il est propre et si les seuls idéaux de A contenant I sont I et A.

Un idéal maximal est donc un élément maximal de l'ensemble des idéaux propres de A pour la relation d'ordre donné par l'inclusion.

PROPOSITION 4.1.8. — Un idéal I d'un anneau A est maximal si et seulement si l'anneau quotient A/I est un corps.

Démonstration. Remarquons d'abord que dire que A/I est nul équivaut à dire que I n'est pas propre : si I est maximal, A/I n'est pas nul ; si A/I est un corps, il est en particulier non nul puisque l'anneau nul n'est pas un corps. Ensuite, d'après l'exemple 2.1.4, A/I est un corps si et seulement s'il a deux idéaux, 0 et A/I. Par image réciproque, d'après la proposition 3.3.1, cela signifie que I et A sont les deux seuls idéaux de A contenant I. □

EXEMPLE 4.1.9. — L'idéal (0) d'un anneau est maximal si et seulement si A est un corps.

EXEMPLE 4.1.10. — Un idéal maximal est premier. En effet, si I est maximal, A/I est un corps et donc en particulier intègre. Cependant la réciproque n'est pas vraie en général. Dans l'anneau $\mathbb{Z}$, l'idéal (0) est premier puisque $\mathbb{Z}$ est intègre mais non maximal puisque $\mathbb{Z}$ n'est pas un corps.

Voici un exemple plus intéressant.

EXEMPLE 4.1.11. — Soit k un corps. Dans l'anneau des polynômes à deux variables $k[X,Y]$ l'idéal (X,Y) est maximal puisque le quotient $k[X,Y]/(X,Y)$ est isomorphe à k. Pour le démontrer, on considère le morphisme d'évaluation $k[X,Y] \to k$ qui associe au polynôme $P(X,Y)$ sa valeur $P(0,0)$ en $(0,0)$. C'est évidemment un morphisme surjectif. Soit P dans le noyau. Alors P n'a pas de terme constant. C'est donc un élément de (X,Y) d'après la proposition 2.2.2. Ainsi le quotient $k[X,Y]/(X,Y)$ est bien isomorphe à k.
L'idéal (X) n'est pas maximal puisque l'inclusion $(X) \subsetneq (X,Y)$ est stricte. C'est cependant un idéal premier : $k[X,Y]/(X) \simeq k[Y]$ est intègre. Pour voir le dernier isomorphisme on raisonne comme ci-dessus en considérant cette fois-ci l'application $P \mapsto P(0,Y)$.

EXEMPLE 4.1.12. — Soit $f : A \to B$ un morphisme d'anneaux. On a vu que l'image réciproque d'un idéal premier de B sous f est encore premier. Un énoncé analogue pour les idéaux maximaux n'est pas vrai en général. Par exemple, si l'on prend pour f le morphisme d'anneaux injectif $f : \mathbb{Z} \to \mathbb{Q}$, alors l'image réciproque de l'idéal (0) n'est pas maximal.

4.2 Existence d'un idéal maximal

Un anneau admet-t-il toujours un idéal maximal ? Un idéal propre est-il toujours contenu dans un idéal maximal ? Pour répondre en général à ces questions, il faut s'autoriser à utiliser l'axiome du choix ou, sous sa forme équivalente, le lemme de Zorn. Rappelons qu'un ensemble ordonné est totalement ordonné si tous les éléments de cet ensemble sont comparables. Le lemme de Zorn affirme alors que si E est un ensemble ordonné non vide satisfaisant à la propriété : *toute partie totalement ordonnée non vide a une borne supérieure dans* E, alors E a un élément maximal.

THÉORÈME 4.2.1. — Tout anneau non nul possède au moins un idéal maximal

Démonstration. On va appliquer le lemme de Zorn à l'ensemble E des idéaux propres de A ordonné par l'inclusion. Cet ensemble n'est pas vide puisqu'il contient l'idéal nul. Montrons que toute famille (I_t) totalement ordonnée d'idéaux propres a une borne supérieure dans E, à savoir l'idéal $I = \cup_t I_t$. Il s'agit de vérifier d'une part que I est bien un idéal et d'autre part que I est propre.
En général, la réunion d'une famille d'idéaux n'est pas un idéal. Ici, dans le cas de la réunion d'une famille totalement ordonné, c'est cependant le cas. Il est clair que $0 \in I$. Si $x, y \in I$, il existe s et t tels que $x \in I_s$ et $y \in I_t$. On a $I_t \subseteq I_s$ ou $I_s \subseteq I_t$ puisque la famille est totalement ordonné. Sans restriction, on peut supposer que $I_s \subseteq I_t$. Alors $x + y \in I_t$ et donc $x + y \in I$. Si $a \in A$ et $x \in I$, on sait qu'il existe t tel que $x \in I_t$. Comme I_t est un idéal $ax \in I_t$ et par conséquent $ax \in I$.
Pour montrer que l'idéal I est propre, il suffit de montrer qu'il ne contient pas 1. C'est bien le cas puisqu'aucun idéal I_t, lui-même propre, ne contient 1. □

Avec un peu d'attention, on voit qu'on montre ainsi un peu plus :

PROPOSITION 4.2.2. — Dans un anneau non nul, tout idéal propre est contenu dans un idéal maximal.

Le lecteur pourra aussi déduire cet énoncé de la proposition 4.2.4.

PROPOSITION 4.2.3. — Soit A un anneau. Un élément de A est inversible si et seulement si il n'appartient à aucun idéal maximal.

Démonstration. Si a est inversible, l'idéal (a) contient 1 et est donc égal à A. Ainsi, le seul idéal contenant a est égal à A et a ne peut appartenir à aucun idéal maximal. Réciproquement, si a n'est pas inversible, $(a) \neq A$. D'après le corollaire précédent, il existe un idéal maximal de A contenant (a) et donc en particulier a. □

On termine la section en précisant la relation entre idéaux d'un anneau et dans un quotient, donné dans la proposition 3.3.1.

PROPOSITION 4.2.4. — Soit A un anneau, I un idéal de A et $\pi : A \to A/I$ la surjection canonique. La bijection donnée par π^{-1} entre idéaux de A/I et idéaux de A contenant I induit des bijections entre
- idéaux premiers de A/I et idéaux premiers de A contenant I ;
- idéaux maximaux de A/I et idéaux maximaux de A contenant I.

Démonstration. Soit J un idéal de A contenant I. Il s'agit de montrer que J est premier (resp. maximal) si et seulement $J/I \subseteq A/I$ l'est. Or, sait déjà que A/J est isomorphe à $(A/I)/(J/I)$ d'après la proposition 3.3.2. En utilisant les critères sur l'anneaux quotient pour qu'un idéal soit premier ou maximal (propositions 4.1.2 et 4.1.8), on voit que J/I est premier (resp. maximal) dans A/I si et seulement si J est premier (resp. maximal) dans A. □

5 Localisation

5.1 Définitions, premières propriétés

Dans cette section nous allons généraliser le passage de l'anneau des entiers $\mathbb{Z}$ au corps des rationnels $\mathbb{Q}$ aux anneaux quelconques. Ce passage permet d'inverser les entiers non nuls et donc de résoudre les équations du premier degré. Pour un anneau A, il s'agit aussi d'inverser des éléments prescrits. On procédera en imitant le *calcul de fractions* que l'on apprend au collège. les éléments que l'on souhaite inverser apparaissent donc comme dénominateurs, et on commence donc par s'intéresser à ceux-ci.

Définition 5.1.1. — Soit A un anneau. Une partie S de A est dite *multiplicative* si elle vérifie les propriétés

a) $1 \in S$;

b) si $s, s' \in S$, alors $ss' \in S$.

Autrement dit, une partie S de A est multiplicative si tout produit (fini) d'éléments de S appartient à S.

Exemple 5.1.2. — On vérifie sans peine que les parties suivantes sont multiplicatives dans leurs anneaux respectifs.

a) $S = \{1\}$;

b) $S = \mathbb{Z} \setminus \{0\}$ dans $\mathbb{Z}$;

c) $S = k[X] \setminus \{0\}$ dans $k[X]$ pour un corps k ;

d) $S = A \setminus \{0\}$ est multiplicative si, et seulement si, l'anneau est intègre ;

e) pour un idéal P dans un anneau A, la partie $S = A \setminus P$ est multiplicative si, et seulement si, l'idéal P est premier ;

f) $S = \{1, 10, 100, \dots\ 10^k \dots\}$, l'ensemble des puissances de 10 dans $\mathbb{Z}$;

g) $S = \{a^k \mid k \in \mathbb{N}\}$ l'ensemble des puissances d'un élément a.

h) Soit $f : A \to B$ un morphisme d'anneaux. Si T est une partie multiplicative de B, alors $f^{-1}(T)$ est encore une partie multiplicative de A.
Inversement, si S est une partie multiplicative de A, alors $f(S)$ est encore une partie multiplicative de B. On bénéficie ici du fait que l'on n'a pas exclu que 0 soit dans S, mais cette largeur de vue initiale ne produit pas de nouvelle fraction au dénominateur nul (voir le paragraphe 5.1.7).

i) Si I est un idéal de A, alors l'ensemble $S = 1 + I$ des éléments de la forme $1 + x$ avec $x \in I$, est une partie multiplicative. En effet, c'est l'image réciproque de la partie multiplicative $\{1\}$ de A/I sous la surjection canonique $\pi : A \to A/I$.

Notre but est ici de construire, pour un anneau A et une partie multiplicative S de A, un anneau $S^{-1}A$, aussi petit que possible, et un morphisme d'anneaux $i : A \to S^{-1}A$ tel que $i(S)$ est formé d'éléments inversibles dans $S^{-1}A$.
On souhaite par exemple retrouver pour $A = \mathbb{Z}$ et $S = \mathbb{Z} \setminus \{0\}$ le corps des rationnels $\mathbb{Q}$ et pour $A = \mathbb{Z}$ et $S = \{1, 10, 100, \dots\}$, l'ensemble des nombre décimaux, c'est-à-dire l'ensemble des nombres rationnels qui peuvent s'écrire de la forme $a/10^n$ avec $a \in \mathbb{Z}$ et $n \in \mathbb{N}$.

REMARQUE 5.1.3. — Afin de ne pas répéter un cours élémentaire, nous donnons une définition qui traite le cas général où l'anneau A n'est pas supposé intègre. C'est cela qui introduit ci-dessous un élément supplémentaire (noté u ci-dessous) par rapport à la définition usuelle de l'égalité de deux fractions, que l'on commentera à la remarque 5.1.5. Cette complication, et les décorations qui en résultent, ne seront pas utiles ce semestre qui traite surtout de divisibilité dans les anneaux intègres, mais elle s'avère utile au semestre suivant pour localiser des modules sur un anneau.

5.1.4. — Soit A un anneau et S une partie multiplicative de A. On définit sur l'ensemble $A \times S$ la relation d'équivalence $\sim$ comme suit :

$$(a, s) \sim (b, t) \text{ si il existe } u \text{ dans } S \text{ tel que : } u(at - bs) = 0$$

C'est bien une relation d'équivalence. En effet,

a) (réflexivité) on a $(a, s) \sim (a, s)$ puisque $1 \in S$ et $1(as - as) = 0$;

b) (symétrie) si $(a, s) \sim (b, t)$, il existe $r \in S$ tel que $r(at-bs) = 0$ et donc $r(bs-at) = 0$ d'où $(b, t) \sim (a, s)$;

c) (transitivité) si $(a, s) \sim (b, t)$ et si $(b, t) \sim (c, u)$, on choisit $v, w \in S$ tels que $v(at - bs) = 0$ et $w(bu - ct) = 0$. Comme

$$t(au - cs) = u(at - bs) + s(bu - ct),$$

il suit que : $vwt(au - cs) = 0$, et puisque $r = vwt \in S$, on a : $(a, s) \sim (c, u)$.

La classe de (a, s) est notée comme fraction $\frac{a}{s}$. On désigne par $S^{-1}A$ l'ensemble des classes d'équivalence, et on note

$$i : A \to S^{-1}A$$

l'application qui associe à un élément a la classe $a/1$ dans $S^{-1}A$. Souvent, on appellera le morphisme $i : A \to S^{-1}A$ *morphisme canonique*.

On munit maintenant $S^{-1}A$ d'une structure d'anneau de sorte que i est un morphisme d'anneaux. On va imiter la définition habituelle pour la somme et le produit de fractions. En fait, ces formules sont nécessaires. Il faut que l'élément $0 \in S^{-1}A$ soit la classe $0/1$, l'élément $1 \in S^{-1}A$ la classe $1/1$. Si l'on définit le produit de fractions par : $\frac{a}{s}\frac{b}{t} := \frac{as}{st}$, alors l"inverse de $i(s) = \frac{s}{1}$, pour s dans S, doit alors être $\frac{1}{s}$. Pour une somme de fractions, on doit avoir :

$$i(st)(\frac{a}{s} + \frac{b}{t}) = i(at + bs) = \frac{at + bs}{1} = i(st)\frac{at + bs}{st}$$

et comme les éléments de $i(S)$ doivent être inversibles, ceci impose que :

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}.$$

On est donc amené à poser :

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st} \quad \frac{a}{s}\frac{b}{t} := \frac{as}{st} \ .$$

Il s'agit maintenant de vérifier d'abord que la définition a un sens, c'est-à-dire ne dépend pas du choix des représentants, puis que l'on a ainsi bien défini une structure d'anneau

sur $S^{-1}A$. Ces vérifications sont un peu longues mais sans surprise, familières pour les entiers, et sont laissés au lecteur.
Montrons, pour terminer la construction, que l'application $i : A \to S^{-1}A$ est bien un morphisme d'anneaux. On a bien : $i(0) = 0/1 = 0$ et $i(1) = 1/1 = 1$ et pour tous a, b de A, on a :

$$i(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = i(a) + i(b)$$

pour la somme et

$$i(ab) = \frac{ab}{1} = \frac{a}{1}\frac{b}{1} = i(a)i(b)$$

pour le produit.
Enfin, si $s \in S$, alors $i(s) = s/1$ et $i(s)1/s = s/s = 1$. Ainsi, $i(s)$ est inversible dans $S^{-1}A$ pour tout $s \in S$.

Remarque 5.1.5. — Dans la construction ci-dessus, la relation d'équivalence peut paraître surprenante puisque elle semble moins forte que la règle habituelle $at = bs$. Bien sûr, dans le cas où la partie multiplicative S ne contient ni 0, ni diviseur de zéro, il s'agit de la même relation d'équivalence. C'est le cas si l'anneau A est intègre et si S ne contient pas 0. Si S contient des diviseurs de zéro, la règle $at = bs$ ne définit pas une relation transitive, ce qui explique pourquoi l'on procède comme ci-dessus.
Le calcul de fractions dans un anneau non intègre, et donc l'utilisation d'un élément $r \in S$ tel que $r(at - bs) = 0$ dans la relation d'équivalence, demande un peu d'attention en général. Il vaut mieux, si l'anneau n'est pas intègre, écrire la relation explicitement pour ne pas se laisser induire en erreur par ses habitudes du calcul des fractions. Bien entendu, dès que A est intègre, on calcule comme on en a l'habitude. Ce sera toujours le cas dans les exemples de ce semestre.

L'anneau $S^{-1}A$ est en général appelé le *localisé* de l'anneau A par rapport à la partie multiplicative S. Cette appellation provient de l'exemple (e)) ci-dessous, pour des anneaux de polynômes, ainsi qu'ils apparaissent en géométrie algébrique.

Exemples 5.1.6. — a) Soit A un anneau et $S = \{1\}$. Alors $S^{-1}A = A$.
b) Soit $A = \mathbb{Z}$ est $S = \mathbb{Z} \setminus \{0\}$. Alors $S^{-1}A = \mathbb{Q}$.
c) Soit A un anneau intègre et $S = A \setminus \{0\}$. Alors $S^{-1}A$ est un corps. En effet, soit $a/s \in S^{-1}A$. Si cet élément est nul, il existe par définition $b \in A \setminus \{0\}$, tel que $ab = 0$. Comme A est intègre, $a = 0$. En particulier $1/1 \neq 0$ et l'anneau $S^{-1}A$ est non nul. Si a/s est non nul, on a $a \neq 0$ et s/a est donc un élément de $S^{-1}A$. Comme on a $(a/s)(s/a) = 1$, il suit que (a/s) est inversible. L'anneau $S^{-1}A$ est donc bien un corps. Ce corps est appelé *corps de fractions de l'anneau* A et noté $K(A)$. Dans le cas particulier où $A = k[X]$ pour un corps k, le corps $S^{-1}k[X]$ est noté $k(X)$ et est appelé le *corps des fractions rationnelles à coefficients dans* k.
d) Soit A un anneau et $S = \{1, a, a^2, a^3, \ldots\}$ pour un élément $a \in A$. L'anneau $S^{-1}A$ est parfois noté A_a ; il est appelé le *localisé de* A *par rapport à* a.
Dans le cas où $A = \mathbb{Z}$ et $f = 10$, l'anneau $\mathbb{Z}_{10}$ est l'anneau des nombres décimaux.
e) Soit A un anneau et P un idéal premier. L'anneau $S^{-1}A$ pour $S = A \setminus P$ sera noté A_P et appelé le *localisé de* A *en* P.

Attention aux notations : pour un nombre premier $p \in \mathbb{Z}$, il faut bien distinguer entre les localisations des deux derniers exemples :

$$\{\frac{a}{s} \in \mathbb{Q} \mid \text{le seul facteur premier de } s \text{ est } p\}$$

rarement noté $\mathbb{Z}_p$, qui cause trop de confusion, et

$$\mathbb{Z}_{(p)} = \{\frac{a}{s} \in \mathbb{Q} \mid \text{aucun facteur premier de } s \text{ est } p\}$$

En particulier, dans ces notations, on a : $\mathbb{Z}_p \cap \mathbb{Z}_{(p)} = \mathbb{Z}$ dans $\mathbb{Q}$. Dans la littérature (surtout celle en langue anglaise), on trouve plutôt $\mathbb{Z}_p$ comme notation pour le quotient $\mathbb{Z}/(p)$ ou pour l'anneau des entiers p-adiques.

5.1.7. — Soit A un anneau et S une partie multiplicative. Est-ce qu'il peut arriver que $S^{-1}A$ est l'anneau nul ? D'après la définition la fraction a/s est nulle dans $S^{-1}A$ si et seulement si il existe $r \in S$ tel que $r(a1 - s0) = ra = 0$. Dire que $S^{-1}A$ est nul signifie que $1/1 = 0$, c'est-à-dire qu'il existe $r \in S$ tel que $r1 = r = 0$, ou autrement dit que $0 \in S$. On voit donc que *l'anneau $S^{-1}A$ est nul si et seulement si* $0 \in S$. Cela explique l'interdiction de diviser par zéro dans le calcul des fractions du collège : sinon, toute fraction serait égale à 0.

5.1.8. — Soit A un anneau et S une partie multiplicative. Sous quelle condition est-ce que le morphisme canonique $i : A \to S^{-1}A$ est injectif ? Supposons que $a \in \mathrm{Ker}(i)$. Alors $a/1 = 0/1$ dans $S^{-1}A$ ou autrement dit il existe $r \in S$ tel que $ra = 0$. On voit donc que i est injectif si, et seulement si, S ne contient ni 0, ni diviseur de zéro de A. En particulier, *si A est intègre, le morphisme canonique est toujours injectif*, pourvu que S ne contienne pas 0.

Au début de la section, on avait dit qu'on cherchait un anneau "aussi petit que possible". Cela se traduit par la propriété universelle suivante.

Proposition 5.1.9. — Soit A un anneau,S une partie multiplicative de A et soit $i : A \to S^{-1}A$ le morphisme canonique. Alors, pour tout morphisme d'anneau $f : A \to B$ tel que $f(S) \subseteq B^\times$, il existe un unique morphisme d'anneaux $g : S^{-1}A \to B$ rendant commutatif le diagramme

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle i}\downarrow & \nearrow_{g} & \\ S^{-1}A & & \end{array}$$

Démonstration. Si l'application g existe, on doit avoir :

$$g(a/s)f(s) = g(a/s)g(s/1) = g(a/1) = f(a)$$

et, puisque $f(s)$ est inversible :

$$g(a/s) = f(a)f(s)^{-1}.$$

La relation ci-dessus nous dira que g est unique, dès que g existe. Pour l'existence, on définira g par cette formule, puis on montre d'abord que g est bien défini, c'est-à-dire ne dépend pas des représentants d'une classe, puis que g définit bien un morphisme d'anneaux. Ces vérifications sont immédiates et laissés au lecteur. □

L'anneau A_a obtenu par localisation d'un élément a de A est en fait un anneau quotient :

PROPOSITION 5.1.10. — Soient A un anneau et a un élément de A. Soit $S = \{1, a, a^2, \ldots\}$ la partie multiplicative des puissances de a. Le morphisme canonique

$$f : A[X] \to S^{-1}A, \quad P \mapsto P(1/a)$$

est surjectif avec pour noyau l'idéal $(1 - aX)$. En particulier, on a un isomorphisme

$$\overline{f} : A[X]/(1 - aX) \simeq S^{-1}A$$

Démonstration. Un élément de $S^{-1}A$ s'écrit sous la forme b/a^n pour un certain $b \in A$ et $n \in \mathbb{N}$. Il est image du monôme bX^n de $A[X]$ et f est donc bien surjectif. On a $f(1 - aX) = 1 - a/a = 0$ donc le noyau de f contient bien l'idéal $(1 - aX)$. Pour montrer que noyau est précisément $(1 - aX)$, on va montrer que le morphisme $\overline{f}$ est un isomorphisme, en construisant son inverse. Considérons le morphisme

$$A \to A[X]/(1 - aX), \quad b \mapsto [b]$$

ou autrement dit le morphisme qui associe à l'élément $b \in A$ la classe du polynôme constant b dans le quotient $A[X]/(1 - aX)$. Dans ce quotient $[aX] = 1$ et $[a]$ est donc inversible d'inverse $[X]$. Ainsi, par la propriété universelle du localisé (proposition 5.1.9), il existe un unique morphisme $g : S^{-1}A \to A[X]/(1-aX)$ tel que l'on ait $g(b) = g(b/1) = [b]$. Par construction, $g(b/a^n) = [bX^n]$. Montrons que g est bien l'inverse de $\overline{f}$. Si $P \in A[X]$, on a par définition $g(f(P)) = g(P(1/a)$. Si l'on écrit $P = \sum b_n X^n$, on voit que

$$g(P(1/a)) = g(\sum b_n/a^n) = \sum g(b_n/a^n) = \sum [b_n X^n] = [P],$$

d'où $g \circ \overline{f} = \mathrm{Id}$. Si on applique d'abord g et ensuite $\overline{f}$ on trouve

$$\overline{f}(g(b/a^n)) = \overline{f}[bX^n] = f(bX^n) = b/a^n.$$

Ainsi on a $\overline{f} \circ g = \mathrm{Id}$ et $\overline{f}$ est donc bien un isomorphisme. □

5.2 Idéaux d'un anneau localisé

Le localisé d'un anneau conserve bien des aspects de l'anneau d'origine et peut en être vu comme une simplification. C'est en particulier le cas en ce qui concerne les idéaux. Soit A un anneau et $S \subseteq A$ une partie multiplicative.
Si I est un idéal de A, l'ensemble $S^{-1}I$ formé des fractions x/s dont le numérateur x est dans I est un idéal de l'anneau $S^{-1}A$. C'est un idéal propre si et seulement si I ne rencontre pas S. Inversement, si J est un idéal de l'anneau $S^{-1}A$, son image réciproque $i^{-1}(J)$ dans A est un idéal de A.

PROPOSITION 5.2.1. — Soit A un anneau et soit $S \subseteq A$ une partie multiplicative de A.
a) Pour tout idéal J dans $S^{-1}A$, on a $S^{-1}(i^{-1}J) = J$;
b) pour tout idéal I dans A, on a : $(S^{-1}I) \cap A \supset I$;
c) si J est un idéal premier de $S^{-1}A$, l'idéal $I = i^{-1}(J)$ est l'unique idéal premier de A disjoint de S tel que $S^{-1}I = J$.

Démonstration. La démonstration est laissé en exercice. □

PROPOSITION 5.2.2. — Soit A un anneau et soit $S \subseteq A$ une partie multiplicative de A. Alors l'application $J \mapsto i^{-1}J$ induit une bijection entre les idéaux premiers de $S^{-1}A$ est les idéaux premiers de A ne rencontrant pas S.

COROLLAIRE 5.2.3. — Soit A un anneau et soit $S \subseteq A$ une partie multiplicative de A. Si S ne contient pas l'élément 0, alors il existe un idéal premier disjoint de S.

Démonstration. Comme S ne contient pas 0, l'anneau $S^{-1}A$ est non nul. Utilisons le théorème qui assure l'existence d'un idéal maximal (théorème 5.2.1). Soit $P = i^{-1}M$. Alors P est premier comme image réciproque d'un premier par un morphisme (proposition 5.1.6), et il est disjoint de S. □

Si A est intègre, le morphisme canonique $i : A \to S^{-1}A$ est injectif. En identifiant A avec son image dans $S^{-1}A$, l'idéal $i^{-1}J$ de A n'est autre que $J \cap A$ où l'intersection est prise dans $S^{-1}A$. Dans ce cas, la bijection ci-dessus est donnée par $J \mapsto J \cap A$.

5.2.4. — Soit A un anneau et $P \subseteq A$ un idéal premier de A. D'après ce que nous avons vu, les idéaux premiers de l'anneau A/P sont les idéaux premiers de A *contenant* P ; les idéaux premiers de l'anneau A_P sont les idéaux premiers *contenu dans* P. Selon les questions, si l'on est intéressé par les idéaux contenant P, il sera naturel de passer au quotient A/P ; si l'on s'intéresse aux idéaux premiers contenus dans P, on passera au localisé A_P.

EXEMPLE 5.2.5. — Soit P un idéal premier de A. Le localisé A_P n'a qu'un seul idéal maximal, le localisé $S^{-1}P \subseteq S^{-1}A$ de l'idéal P.

C'est cet exemple qui justifie le terme de localisation. En effet, si l'on cherche à n'étudier que les phénomènes qui font intervenir un premier p, ou un idéal premier P, on peut se placer dans l'anneau localisé en P. Cet anneau n'a alors plus qu'un seul premier, tous les autres étant devenus inversibles, faisant disparaître toute divisibilité les concernant.

6 Divisibilité dans les anneaux intègres

Tous les anneaux considérés dans cette section sont intègres.

6.1 Divisibilité et idéaux

Clarifions la relation entre divisibilité et inclusion des idéaux. Dans un anneau A, on dit que x divise y, et on note $x|y$, s'il existe d dans A tel que $y = dx$; ou, autrement dit, si y est dans l'idéal principal (x) ou encore si $(y) \subset (x)$. C'est à dire

$$x|y \Leftrightarrow y \in (x) \Leftrightarrow (y) \subset (x).$$

On peut paraphraser en considérant l'application de l'ensemble A vers l'ensemble des idéaux de A, qui associe à un élément x l'idéal principal (x) qu'il engendre :

$$A \to \{\text{idéaux de } A\}$$
$$x \mapsto (x) = xA$$

Cette application transforme donc divisibilité en inclusion. Plus précisément, si A est ordonné par divisibilité et l'ensemble de ses idéaux par inclusion, cette application est décroissante.
Quelle est l'ambiguïté du choix d'un générateur d'un idéal principal ? Autrement dit, quand deux éléments engendrent-ils le même idéal principal ? La proposition suivante donne la réponse pour les anneaux intègres.

Proposition 6.1.1. — Deux éléments x et y d'un anneau intègre A engendrent le même idéal principal si et seulement s'il existe un élément inversible u telle que : $y = ux$. Quand c'est le cas, on dit que x et y sont *associés*.

Démonstration. Par définition : $x|y$ et $y|x \Leftrightarrow (x) = (y)$. Si $y = ax$ et $x = by$, alors $xy = abxy$ et donc $(1 - ab)xy = 0$. Comme l'anneau est intègre, ceci entraine : $ab = 1$, si bien que a et b sont inversibles. La réciproque est claire. □

Remarque 6.1.2. — De manière pédante, on peut voir la multiplication par les unités comme une action du groupe multiplicatif $A^\times$ sur l'ensemble A. Deux éléments sont associés quand ils sont dans la même orbite sous cette action, et l'application $x \mapsto (x)$ passe au quotient pour définir une bijection de l'espace des orbites sur l'ensemble des idéaux principaux de A. Notez que cette bijection renverse l'ordre.

6.2 Plus grand diviseur commun

Définition 6.2.1. — Soit A un anneau intègre, et a et b deux éléments de A. On dit que $c \in A$ est un *plus grand diviseur commun* (pgcd) de a et b si c divise a et b, et si pour tout $d \in A$ on a

$$d|a \text{ et } d|b \Longleftrightarrow d|c.$$

On dit que $c \in A$ est un *plus petit commun multiple* (ppcm) de a et b si a et b divisent c, et si pour tout $d \in A$ on a

$$a|d \text{ et } b|d \Longleftrightarrow c|d.$$

REMARQUE 6.2.2. — Il n'y a en général pas unicité du pgcd ou du ppcm. Cependant, deux pgcds (ou ppcms) de a et b sont nécéssairement associés. Un pgcd (ou ppcm) est donc unique, lorsqu'il existe, à multiplication par une unité près.

DÉFINITION 6.2.3. — Deux éléments a et b sont dits *premiers* entre eux si leur pgcd existe et est associé à 1.

EXEMPLE 6.2.4. — Le nombre 6 est un pgcd de 12 et 18 dans $\mathbb{Z}$ (le deuxième pgcd est -6). Un ppcm est donné par 36.

EXEMPLE 6.2.5. — Dans l'anneau $\mathbb{Q}[X,Y]$, on voit facilement en considérant les degrés en X et en Y que les éléments X et Y ont 1 pour pgcd.

On a essentiellement unicité, si existence, des pgcd et ppcm. L'existence n'est cependant pas toujours assurée.

EXEMPLE 6.2.6. — Considérons le sous-anneau de $\mathbb{C}$ engendré par $\mathbb{Z}$ et $i\sqrt{5}$; autrement dit l'anneau $\mathbb{Z}[i\sqrt{5}]$ des nombres qui peuvent s'écrire $a+ib\sqrt{5}$ pour des entiers relatifs a et b. L'élément 6 admet les deux factorisations suivantes :

$$6 = 2 \times 3 \qquad \text{et} \qquad 6 = (1+i\sqrt{5})(1-i\sqrt{5}).$$

Donc 2 et $1+i\sqrt{5}$ sont deux diviseurs de 6 et $2+2i\sqrt{5}$. Supposons qu'il existe $a+ib\sqrt{5}$ divisant 6 et $2+2i\sqrt{5}$, et divisible par 2 et $1+i\sqrt{5}$. En prenant le carré du module de ces nombres complexes, on obtient que 4 et 6 divisent a^2+5b^2, tandis que ce dernier divise 36 et 24. On en déduit donc que $a^2+5b^2=12$, ce qui est impossible dans $\mathbb{Z}$.
Il n'existe donc pas de ppcm de 6 et $2+2i\sqrt{5}$ dans $\mathbb{Z}[i\sqrt{5}]$.

En traduisant les propriétés de divisibilité en termes d'idéaux, on obtient :

$$d|a \text{ et } d|b \iff (a,b) \subset (d) \qquad \text{et} \qquad a|d \text{ et } b|a \iff (d) \subset (a) \cap (b),$$

ce qui se reformule en la proposition suivante.

PROPOSITION 6.2.7. — Soit A un anneau intègre, et soit a et b deux éléments non nuls de A.

a) Si a et b admettent un pgcd, alors l'idéal engendré par $\text{pgcd}(a,b)$ est le plus petit idéal principal contenant l'idéal (a,b).

b) Si a et b admettent un ppcm, alors l'idéal engendré par $\text{ppcm}(a,b)$ est le plus grand idéal principal contenu dans l'idéal $(a) \cap (b)$.

COROLLAIRE 6.2.8 (identité de Bézout). — Soit A un anneau intègre, et a, b des éléments de A. Si l'idéal (a,b) est principal, alors tout générateur de cet idéal est pgcd de a et b. Si l'idéal $(a) \cap (b)$ est principal, alors tout générateur de cet idéal est ppcm de a et b.

On obtient ainsi l'existence de pgcd et de ppcm lorsque tous les idéaux de A sont principaux. On dit alors que A est un anneau principal. Comme toujours, le premier exemple d'anneau principal est celui des entiers $\mathbb{Z}$. Cette propriété n'est cependant pas nécessaire, comme le montre l'exemple suivant.

EXEMPLE 6.2.9. — Les polynômes X et Y ont 1 pour pgcd dans $\mathbb{Q}[X,Y]$, alors que l'idéal (X,Y) est l'idéal propre des polynômes nuls en $(0,0)$ qui n'est pas principal.

L'existence d'un pgcd et d'un ppcm est en fait assurée pour une large classe d'anneaux, les anneaux factoriels, qui font l'objet du chapitre suivant.

6.3 Éléments irréductibles et éléments premiers

Définition 6.3.1. — Soit A un anneau intègre. Un élément a de A est dit irréductible si
- a n'est pas inversible ;
- si $b, c \in A$ sont tels que $a = bc$, alors b ou c est inversible.

Autrement dit, un élément non nul a dans A est irréductible s'il n'est pas une unité, et s'il n'a que des factorisations $a = bc$ *banales*, avec b ou c une unité. En d'autres termes, un élément irréductible est un élément minimal pour la divisibilité parmi les éléments non inversibles. On observe que $0 = 0 \cdot 0$ n'est pas irréductible.

Définition 6.3.2. — Un élément d'un anneau intègre est *premier* si l'idéal qu'il engendre est premier.

En d'autres termes, un élément est premier si, quand il divise un produit, il divise l'un des facteurs.

Proposition 6.3.3. — Tout élément premier d'un anneau intègre est irréductible.

Démonstration. Soit a un élément premier, et $a = bc$ une factorisation. Par hypothèse, on peut supposer que a divise b. Les éléments a et b sont donc associés, et il existe $u \in A^\times$ tel que $b = ua$. On a alors $a = auc$, soit $a(1 - uc) = 0$. Par intégrité de A, on déduit $uc = 1$, et la factorisation $a = bc$ est banale. □

Exemple 6.3.4. — Il faut prêter attention cependant au fait que la réciproque n'est pas vraie en général. En voici un exemple.
Revenons au sous-anneau $\mathbb{Z}[i\sqrt{5}]$ des nombres qui peuvent s'écrire $a + ib\sqrt{5}$ pour des entiers relatifs a et b, vu à l'exemple 6.2.6. Notez qu'une telle écriture est unique car $\sqrt{5} \notin \mathbb{Q}$. En particulier les multiples de 2 dans $\mathbb{Z}[i\sqrt{5}]$ sont les nombres de la forme $a + ib\sqrt{5}$ avec a et b pairs. L'élément 6 est divisible par 2, en revanche, aucun des deux facteurs de la factorisation $6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ n'est divisible par 2. L'idéal (2) n'est donc pas premier, ou autrement dit l'élément 2 n'est pas premier dans cet anneau.
L'élément 2 est cependant irréductible dans cet anneau. En effet, supposons : $2 = xy$. Les éléments x et y s'écrivent $x = a + ib\sqrt{5}$ et $y = c + id\sqrt{5}$. En prenant le carré du module de ces nombres complexes, on voit que :

$$4 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Ceci force $b = d = 0$ d'où $2 = ac$. Mais alors $a = \pm 1$ ou $c = \pm 1$, et $2 = xy$ est donc banale.

On a donc montré le résultat suivant.

Proposition 6.3.5. — Dans un anneau intègre, chaque assertion ci-dessous entraîne la suivante :
a) l'idéal engendré par a est maximal ;
b) l'élément a est premier ;
c) l'élément a est irréductible.

Chaque implication n'est en général pas une équivalence.

Nous allons introduire dans la suite deux familles d'anneaux où les difficultés liées à la non existence de ppcm, ou à l'existence d'éléments irréductibles non maximaux, disparaissent : les anneaux principaux et les anneaux factoriels.

6.4 Anneaux principaux

Définition 6.4.1. — On dit qu'un anneau est *principal* s'il est intègre et si tous ses idéaux sont principaux.

Exemple 6.4.2. — L'anneau des entiers $\mathbb{Z}$ est principal : c'est l'exemple 3.1.4.

Exemple 6.4.3. — Si k est un corps, alors $k[X]$ est principal.

Exemple 6.4.4. — L'anneau $\mathbb{Q}[X,Y]$ n'est pas principal puisque l'idéal (X,Y) n'est pas principal.

La Proposition 6.2.8 se reformule ainsi dans un anneau principal.

Proposition 6.4.5 (identité de Bézout). — Soit A un anneau principal, et a, b des éléments de A. Alors un pgcd (resp. ppcm) de a et b existe toujours, et tout générateur de l'idéal (a,b) (resp. $(a)\cap(b)$) en est un.

En particulier, si A est un anneau principal, deux éléments a et b sont premiers entre eux si, et seulement si, les idéaux (a) et (b) sont comaximaux. Dans un anneau principal, tout élément irréductilbe est premier.

Proposition 6.4.6. — Soit A un anneau principal et $a \in A$. Alors les trois assertions ci-dessous sont équivalentes :

a) l'idéal engendré par a est maximal ;
b) l'élément a est premier ;
c) l'élément a est irréductible.

Démonstration. Il nous suffit de montrer que la troisième propriété implique la première dans un anneau principal. On montre la contraposée. Si (a) n'est pas maximal, il existe un idéal propre $I \neq A$ contenant strictement (a). Comme A est principal il existe x dans A tel que $(x) = I$. Ainsi, $a = dx$ pour d dans A. L'élément x n'est pas inversible, sinon I ne serait pas propre. L'élément d n'est pas inversible non plus, sinon on aurait $(a) = I$. On a donc trouvé une factorisation non banale de a, et a n'est pas irréductible. □

En particulier, dans un anneau principal un élément irréductible est premier. Cet énoncé est parfois appelé *lemme de Gauß*. Le lecteur est encouragé à en donner une démonstration directe. On retrouve aussi pour les anneaux principaux le résultat, bien connu pour les entiers, qu'un entier relatif est irréductible si, et seulement s'il est un nombre premier (ou l'opposé d'un nombre premier).

6.5 Anneaux euclidiens

L'argument utilisé dans les Exemples 6.4.2 et 6.4.3 repose sur la division euclidienne dans $\mathbb{Z}$ et $k[X]$. Ceci nous amène à la définition suivante :

Définition 6.5.1. — Un anneau *euclidien* est un anneau intègre muni d'une fonction $\delta : A \setminus \{0\} \to \mathbb{N}$, que nous appelons ici *degré*, telle que pour tous a, b dans A, avec $b \neq 0$, il existe q, r dans A tels que :
a) $a = bq + r$;
b) $r = 0$ ou $\delta(r) < \delta(b)$.

L'élément r est souvent appelé le *reste* de la division de a par b. Il faut cependant ne pas oublier que la paire (q, r) n'est en général pas définie de manière unique par les éléments a, b. Ce n'est déjà pas le cas pour le premier exemple suivant.

Exemple 6.5.2. — a) L'anneau $\mathbb{Z}$ muni de la fonction $\delta(a) = |a|$ est un anneau euclidien.
b) Si k est un corps, l'anneau $A = k[X]$ muni de la fonction $\delta(P) := \deg(P)$ est un anneau euclidien. En effet, si Q est non nul dans $k[X]$, le coefficient dominant de Q est automatiquement inversible, étant donné que k est un corps. On peut alors utiliser le théorème 2.3.9 pour conclure.

Proposition 6.5.3. — Un anneau euclidien est principal.

Démonstration. On reprend l'argument de l'exemple 3.1.4. Soit I un idéal d'un anneau euclidien A dont on veut montrer qu'il est principal. Comme l'idéal nul est principal, on suppose maintenant que : $I \neq 0$. Soit alors a un élément non nul dans I de degré $\delta(a)$ minimal. Bien entendu, $(a) \subset I$ et il s'agit de montrer que $I = (a)$. Soit x un élément quelconque de I et choisissons q et r tels que $x = aq + r$. Comme $r = x - aq$ appartient à I, son degré ne peut être strictement inférieur au degré minimal $\delta(a)$. C'est donc que $r = 0$ et $x = aq$ est dans l'idéal principal (a). Par suite, $I = (a)$ et tout idéal de A est principal. Comme A est aussi intègre, A est principal. □

Voici un exemple d'anneau euclidien où le degré n'est pas aussi évident que dans $\mathbb{Z}$ of $k[X]$.

Exemple 6.5.4 (entiers de Gauß). — Soit $Z[i]$ l'ensemble des nombres complexes de la forme $a + ib$ avec $a, b \in \mathbb{Z}$. C'est un sous-anneau du corps $\mathbb{C}$. En effet, il est stable par addition, soustraction et multiplication puisque $(a + ib)(c + id) = (ac - bd) + i(ad + bc)$. C'est donc l'anneau engendré par $\mathbb{Z}$ et $i = \sqrt{-1}$ dans $\mathbb{C}$. On l'appelle *l'anneau des entiers de Gauß*.
Montrons que $\mathbb{Z}[i]$ est euclidien (et donc principal). Pour cela on définit : $\delta(a + ib) = |a + ib|^2 = a^2 + b^2$. Reste à vérifier que δ vérifie la condition requise pour un anneau euclidien. Soient x, y deux éléments de $\mathbb{Z}[i]$ avec $y \neq 0$. Soit $z = x/y$ dans $\mathbb{C}$, et approchons-le au mieux par des entiers de Gauß. Ce nombre est de la forme $z = z' + iz''$. Observons qu'il existe $a, b \in \mathbb{Z}$ tels que $|z' - a| \leq 1/2$ et $|z'' - b| \leq 1/2$. Soit $q = a + ib$ et $r = x - yq$.

Ce sont des éléments de $\mathbb{Z}[i]$. Remarquons aussi que $|z-q|^2 \leq 1/4+1/4 = 1/2$ par construction de q. On obtient :

$$|r|^2 = |x-yq|^2 = |y|^2|(x/y)-q|^2 \leq |y|^2/2 < |y|^2.$$

Par suite, $\delta(r) < \delta(y)$.

Pour finir, mentionnons qu'un idéal principal n'est pas nécessairement euclidien. L'exemple suivant, que nous citons pour la culture générale sans le détailler, fait le délice des agrégatifs.

Exemple 6.5.5. — L'anneau $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal mais non euclidien.

7 Anneaux factoriels

7.1 Définition

On dit qu'un anneau A est *factoriel* si tout élément non inversible de A peut se factoriser en produit d'éléments irréductibles de A, et ce de manière essentiellement unique. On demande donc *l'existence* d'une décomposition en produit d'irréductibles, et son *unicité* dans un sens que l'on va préciser dans un instant. L'existence signifie que pour tout est un élément non nul a dans A, il existe un entier $n \geq 0$, des éléments $p_1, \ldots, p_n$ irréductibles dans A et un élément inversible $u \in A$ tels que : $a = up_1 \ldots p_n$. On permet expressément $n = 0$ dans la décomposition ci-dessus : dans ce cas $a = u$ est inversible. L'unicité s'entend à l'ordre des facteurs irréductibles près, et à des éléments inversibles près, puisque on peut toujours remplacer un facteur irréductible par un irréductible associé.

Définition 7.1.1. — On dit qu'un anneau intègre A est *factoriel* si tout élément non nul de A peut s'écrire comme produit

$$up_1 \ldots p_n$$

pour des éléments $p_1, \ldots, p_n$ irréductibles dans A et u inversible dans A, et ce de manière essentiellement unique, au sens suivant : si

$$up_1 \ldots p_n = u'p'_1 \ldots p'_m$$

sont deux factorisations d'un même élément en produit d'irréductibles, alors $m = n$ et il existe une permutation σ de $\{1, \ldots, n\}$ et des éléments inversibles u_i, pour $i = 1, \ldots, n$, tels que :

$$p'_{\sigma(i)} = u_i p_i.$$

L'anneau $\mathbb{Z}$ est un anneau factoriel : tout entier se décompose en facteurs premiers et cette décomposition est essentiellement unique. Elle est même unique à l'ordre des facteurs près si l'on choisit toujours les facteurs irréductibles positifs.
Il est souvent commode de *normaliser* la décomposition en facteurs irréductibles. Pour cela, on choisit une famille $(p_i)_{i \in I}$ d'éléments irréductibles de A telle que :

- tout élément irréductible de A est associé à l'un des p_i ;
- si $i \neq j$, p_i et p_j ne sont pas associés.

Ce choix étant effectué, tout élément non nul de A s'écrit, cette fois-ci de manière unique, sous la forme

$$a = u \prod_{i \in I} p_i^{r_i}$$

où u est un élément inversible de A et où les r_i sont des entiers positifs ou nuls, avec seul un nombre fini d'entre eux étant non nuls.

7.2 Divisibilité dans un anneau factoriel

Dans un anneau factoriel, la relation de divisibilité se lit sur les exposants qui apparaissent dans un décomposition normalisée. Un élément $a = u\prod p_i^{r_i}$ divise un élément $b = v\prod p_i^{s_i}$ si, et seulement si : pour tout i,$r_i \leq s_i$. En effet, si $c \in A$ est tel que $b = ac$, on écrit $c = w\prod p_i^{t_i}$, puis on observe que l'on a

$$b = v\prod_{i\in I} p_i^{s_i} = uw\prod_{i\in I} p_i^{r_i+t_i}$$

d'où, par unicité, que $s_i = r_i+t_i$ pour tout i. Pour la réciproque, on prend $c = uv\prod_i p_i^{s_i-r_i}$. Il est commode de nommer les exposants qui apparaissent dans une décomposition en facteurs irréductibles. Soit a est un élément d'un anneau factoriel, et $a = u\prod p_i^{r_i}$ sa décomposition normalisée. Pour un irréductible p, soit i l'indice tel que p_i est associé à p. L'entier r_i s'appelle la *valuation p-adique* de a ; c'est le plus grand entier n tel que p^n divise a. On le note parfois : $\nu_p(a)$.

Exemple 7.2.1. — $\nu_3(2016) = 2$.

Remarque 7.2.2. — Pour tout élément a d'un anneau factoriel, considérons la somme $\nu(a)$ de ses valuations p_i-adiques. On obtient un entier naturel, et cette correspondance respecte l'ordre de divisibilité : si x divise a, alors $\nu(x)$ est inférieur à $\nu(a)$. C'est une sorte de degré défini dans tout anneau factoriel. On en déduit que si A est un anneau factoriel, toute suite croissante d'idéaux principaux de A est stationnaire (c'est-à-dire constante à partir d'un certain rang).

Lemme 7.2.3 (Propriété d'Euclide). — Dans un anneau factoriel, tout élément irréductible est premier.

Démonstration. On montre que si a est irréductible et si $a|bc$, alors $a|b$ ou $a|c$. Pour simplifier, on suppose avoir normalisée la décomposition en facteurs irréductibles dans A par le choix d'une famille $(p_i)_{i\in I}$ d'éléments irréductibles. Si a est irréductible, on a donc : $a = up_j$ pour un $j \in I$. Soient $b = v\prod p_i^{s_i}$ et $c = w\prod p_i^{t_i}$ les décompositions en facteurs irréductibles de b et c. Si a divise bc, on sait que $s_j + t_j \geq 1$; c'est donc que : $s_j \geq 1$ ou $t_j \geq 1$. C'est donc que a divise b ou c. □

L'existence de pgcd et ppcm dans un anneau factoriel est assurée, pour exactement la même raison vue au collège en ce qui concerne les entiers. Pour simplifier, on suppose avoir normalisé la décomposition en facteurs irréductibles dans le lemme suivant.

Lemme 7.2.4. — Soit A un anneau factoriel, et a et b deux éléments de A. Si $a = u\prod p_i^{r_i}$ et $b = v\prod p_i^{s_i}$ sont les décompositions en facteurs irréductibles de$a$ et b, alors

$$\mathrm{pgcd}(a,b) = \prod_{i\in I} p_i^{\min(r_i,s_i)} \text{ et } \mathrm{ppcm}(a,b) = \prod_{i\in I} p_i^{\max(r_i,s_i)}.$$

Démonstration. Si a et b sont multiples de $x = w\prod p_i^{t_i}$, cela veut dire que pour tout i, on a $t_i \leq r_i$ et $t_i \leq s_i$, ou encore $t_i \leq \min(r_i, s_i)$. Ceci signifie que x divise $\prod_{i\in I} p_i^{\min(r_i,s_i)}$. La preuve pour le ppcm est analogue. □

7.3 Les anneaux principaux sont factoriels

Dans ce paragraphe nous démontrons le théorème suivant :

THÉORÈME 7.3.1. — Un anneau principal est factoriel.

En particulier, on retrouve que $\mathbb{Z}$ est factoriel. De même, l'anneau $k[X]$ des polynômes à coefficients dans un corps k est factoriel.
On procède en deux étapes. D'abord on montre l'existence d'une décomposition en éléments irréductibles, puis on montre qu'elle est essentiellement unique. Nous en profiterons pour caractériser chacune de ces deux propriétés.

7.3.2 Existence de la décomposition en produit d'irréductibles

L'existence d'une décomposition en produit d'irréductibles est souvent claire. En effet, si l'élément de départ a est réductible, on le décompose en un produit de diviseurs stricts, et s'ils sont réductibles, on les décompose à leur tour. Ce processus s'arrête dans $\mathbb{Z}$, ou dans un anneau de polynômes sur un corps, car le degré des diviseurs successifs décroît. C'est encore le cas dans tout anneau principal.

PROPOSITION 7.3.3. — Soit A un anneau principal et a non nul dans A. Alors il existe un entier positif ou nul n, des éléments irréductibles $p_1, \dots, p_n$ de A, et un inversible u de A tels que : $a = up_1 \dots p_n$.

Démonstration. Supposons qu'il existe un élément a non nul de A qui n'est pas produit d'éléments irréductibles, et montrons que l'anneau A ne peut être principal.
Nous allons construire une suite monotone d'éléments de A. On pose d'abord : $a_1 = a$. L'élément a n'est pas inversible (sinon $a = u$ est déjà une décomposition), ni irréductible (sinon $a = p$ est déjà une décomposition). Soit alors $a = bc$ une factorisation non banale. Comme a n'est pas produit d'éléments irréductibles, l'un des deux éléments b ou c au moins n'est pas produit d'éléments irréductibles. Soit a_2 cet élément. Ni b, ni c n'étant inversible, l'idéal (a_2) contient strictement l'idéal (a_1). On construit ainsi, par récurrence, une suite $a_1, a_2, \dots$ d'éléments de A tels que la suite d'idéaux

$$(a_1) \subset (a_2) \subset \dots$$

est strictement croissante. On conclut par le résultat suivant :

LEMME 7.3.4. — Dans un anneau principal, toute suite croissante d'idéaux stabilise (elle est constante à partir d'un certain rang).

Démonstration. Soit $((a_n))$ une suite d'idéaux principaux croissante (pour l'inclusion). Soit I la réunion de ces idéaux. Comme la suite est croissante, c'est un idéal de l'anneau. En effet, les stabilités à vérifier se produisent dans l'un des idéaux de la suite. Comme l'anneau est principal, il existe un élément x tel que : $I = (x)$. Comme I est la réunion des (a_n), il existe un entier n tel que $x \in (a_n)$, d'où $(x) \subset (a_n)$. Alors $a_n \subset I = (x) \subset (a_n)$, et la suite d'idéaux est constante à partir d'un tel rang n. □

Tout élément non nul d'un anneau principal admet donc une décomposition en éléments irréductibles □

7.3.5 Unicité de la décomposition en irréductibles

PROPOSITION 7.3.6. — Dans un anneau principal, toute décomposition en facteurs irréductibles d'un élément est essentiellement unique.

Démonstration. On procède par récurrence sur le nombre minimal de facteurs irréductibles intervenant dans une décomposition d'un élément $a \in A$. On commence quand ce nombre est 0, c'est-à-dire quand a est inversible. Dans ce cas, comme un irréductible n'est pas inversible, il n'y jamais de facteur irréductible. Pour montrer le pas de récurrence, donnons nous maintenant deux décompositions $a = up_1 \dots p_m = u'p'_1 \dots p'_n$ d'un même a tel que le nombre m de facteurs est minimal, non nul. Un élément irréductible étant premier dans un anneau principal d'après le lemme de Gauß (proposition 6.4.6), l'élément irréductible p_m divise l'un des p'_i. Quitte à les renuméroter (ce qui introduit une première permutation des indices), on peut supposer que c'est p'_n. Il existe ainsi u_m dans A tel que : $p_m = u_m p'_n$. Comme p_m est irréductible, u_m est inversible. On peut donc simplifier (l'anneau est intègre) pour obtenir la relation suivante :

$$up_1 \dots p_{m-1} = u'u_m p'_1 \dots p'_{n-1}$$

Si l'hypothèse de récurrence est satisfaite, on a $m - 1 = n - 1$, d'où $m = n$; de plus, il existe une permutation σ et des éléments inversibles u_i, pour $i = 1, \dots, m-1$ tels que $p'_{\sigma(i)} = u_i p_i$. Ceci achève de montrer l'unicité au cran n, et achève la récurrence. La décomposition d'un élément en facteurs irréductibles est donc essentiellement unique. □

REMARQUE 7.3.7. — Cette démonstration de l'unicité ne fait usage que de la propriété d'Euclide. En fait, le lecteur montrera à l'aide des arguments développés la caractérisation suivante.

PROPOSITION 7.3.8. — Dans un anneau intègre dont tout élément non inversible est produit d'irréductibles, les propriétés suivantes sont équivalentes :

a) *propriété de Gauß* : pour tous éléments a, x, y, si a divise xy et a est premier avec x, alors a divise y ;

b) *propriété d'Euclide* : tout irréductible est premier ;

c) l'anneau est factoriel.

Au vu des arguments de ce paragraphe, un anneau intègre A est factoriel si, et seulement si, il vérifie les deux propriétés suivantes :

- toute suite croissante d'idéaux principaux dans A est stationnaire ;
- tout élément irréductible de A est premier.

La première propriété assure l'existence et la seconde l'unicité de la décomposition.

7.4 Le théorème de Gauß

Dans ce paragraphe nous démontrerons le théorème suivant :

THÉORÈME 7.4.1 (Gauß). — Soit A un anneau factoriel. Alors l'anneau $A[X]$ est factoriel.

COROLLAIRE 7.4.2. — Soit n un entier positif non nul. Si A est un anneau factoriel, l'anneau $A[X_1, \dots, X_n]$ est aussi factoriel. En particulier, si k est un corps, l'anneau $k[X_1, \dots, X_n]$ est factoriel.

Démonstration du corollaire. Cela se voit par récurrence sur n, puisque $A[X_1, \ldots, X_n] = (A[X_1, \ldots, X_{n-1}])[X_n]$. □

Pour tout le paragraphe, on se donne un anneau factoriel A. Nous étudions la divisibilité dans l'anneau $A[X]$. Commençons par les éléments inversibles. Comme A est intègre, le degré d'un produit est la somme des degrés des facteurs. En particulier, si $PQ = 1$, alors P et Q sont de degré nul ; ce sont donc des éléments de A. On en déduit que les éléments inversibles de $A[X]$ sont les polynômes constants, inversibles dans A.
Poursuivons en cherchant les éléments irréductibles de $A[X]$. La première chose est de s'assurer qu'on ne peut peut factoriser une constante ; c'est le cas quand tous les coefficients ont un diviseur commun. On est donc amené à la définition suivante.

Définition 7.4.3. — Soit A un anneau factoriel et soit P dans $A[X]$. Le *contenu* de P, et on note $\mathrm{ct}(P)$ le pgcd des coefficients de P. On dira que P est *primitif* si $\mathrm{ct}(P) = 1$.

Un polynôme est donc primitif si ses coefficients sont premiers entre eux. Comme on l'a déjà expliqué, afin que le contenu soit un élément bien défini de A, on aura normalisée la décomposition en facteurs irréductibles. Sans cette hypothèse, le contenu n'est bien défini qu'à multiplication par un inversible près.
Tout polynôme P dans $A[X]$ est donc produit $\mathrm{ct}(P)P_1$, pour un polynôme primitif P_1.
La propriété fondamentale du contenu est qu'il est multiplicatif :

Proposition 7.4.4. — Soit A un anneau factoriel. Pour P, Q dans $A[X]$: $\mathrm{ct}(PQ) = \mathrm{ct}(P)\,\mathrm{ct}(Q)$.

Démonstration. Écrivons $P = \mathrm{ct}(P)P_1$ et $Q = \mathrm{ct}(Q)Q_1$ avec $P1$ et Q_1 primitifs. $PQ = \mathrm{ct}(P)\,\mathrm{ct}(Q)P_1Q_1$, d'où $\mathrm{ct}(PQ) = \mathrm{ct}(P)\,\mathrm{ct}(Q)\,\mathrm{ct}(P_1Q_1)$. Il suffit donc de montrer :

Lemme 7.4.5 (lemme de Gauß). — Le produit de deux polynômes primitifs est encore primitif.

Démonstration du lemme de Gauß. Supposons donc P et Q primitifs. Il nous suffit de montrer que si p est un élément irréductible de A, alors p ne divise pas tous les coefficients de PQ. Pour cela, effectuons une réduction modulo p. La réduction modulo p, morphisme d'anneaux $A \to A/(p)$, s'étend en une réduction modulo p, morphisme d'anneaux $\rho : A[X] \to A/(p)[X]$, simplement en réduisant modulo p chaque coefficient d'un polynôme. Considérons les réductions modulo p de P et Q dans l'anneau $A/(p)[X]$. Comme P et Q sont primitifs, p ne divise pas tous les coefficients, et ces réductions sont non nulles. Comme l'anneau A est factoriel, l'irréductible p est premier (lemme 7.2.3). L'anneau $A/(p)$ est donc intègre, et donc $A/(p)[X]$ aussi. Par conséquent le produit des réductions $\rho(P)\rho(Q) = \rho(PQ)$ est non nul dans $A/(p)[X]$. Ceci signifie que p ne divise pas tous les coefficients de PQ. □

Nous avons pris l'habitude de voir un élément a de A comme un élément de $A[X]$, en le voyant comme le polynôme constant a.
Soit A un anneau intègre et soit $P = a_0 + a_1X + \cdots + a_nX^n$ un polynôme dans $A[X]$. Si K est le corps de fractions de A, on peut voir P comme un polynôme de $K[X]$, simplement

en voyant les coefficients dans K (via l'injection canonique $A \to K$, $a \mapsto a/1$). Nous avons l'habitude de faire cela pour les polynômes à coefficients dans $\mathbb{Z}$, en les voyant comme des polynômes à coefficients dans $\mathbb{Q}$.
À l'aide du contenu, nous montrons qu'utiliser des polynômes dans $K[X]$, et pas juste dans $A[X]$, ne fournit pas davantage de factorisations.

PROPOSITION 7.4.6. — Soit A un anneau factoriel de corps des fractions K, P un polynôme de $A[X]$ et $P = QR$ une factorisation de P dans $K[X]$. Alors : $P = \mathrm{ct}(P)Q_1R_1$ pour des polynômes primitifs Q_1 et R_1 dans $A[X]$, proportionnels à Q et R.

Démonstration. En chassant un dénominateur commun, on obtient : $Q = \frac{1}{d}Q_0$ pour un polynôme Q_0 dans $A[X]$ et d dans A. Après mise en facteur du contenu de Q_0, on obtient : $Q = qQ_1$ pour un élément q de K et Q_1 un polynôme primitif de $A[X]$. On fait de même pour R, ce qui donne : $P = \frac{a}{b}Q_1R_1$ pour a, b dans A, et Q_1, R_1 primitifs. On obtient alors : $bP = aQ_1R_1$ dans $A[X]$. En prenant les contenus, on obtient : $b\,\mathrm{ct}(P) = a$, d'où le résultat. □

Nous décrivons maintenant les éléments irréductibles de $A[X]$.

PROPOSITION 7.4.7. — Soit A un anneau factoriel et K son corps de fractions. Alors les éléments irréductibles de $A[X]$ sont exactement
a) les éléments irréductibles de A ;
b) les polynômes primitifs de $A[X]$, irréductibles en tant que polynômes de $K[X]$.

Démonstration. Montrons d'abord que les éléments en question sont bien irréductibles.
a) Soit donc a irréductible de A et $a = PQ$ une factorisation dans $A[X]$. Comme A est intègre, on a $\deg(P) + \deg(Q) = \deg(PQ) = 0$, donc P et Q sont nécessairement de degré 0, ou autrement dit des éléments de A. L'élément a étant irréductible dans A, la relation est banale dans A et donc aussi dans $A[X]$ (on a vu que ces deux anneaux ont les mêmes inversibles). L'élément a est donc bien irréductible dans l'anneau $A[X]$.

REMARQUE 7.4.8. — On peut aussi montrer que le quotient est intègre, en utilisant l'isomorphisme $A[X]/(p) \simeq A/(p)[X]$.

b) Soit maintenant $P \in A[X]$ primitif, irréductible dans $K[X]$ et $P = QR$ une factorisation dans $A[X]$. Vue dans $K[X]$, cette relation doit être banale ; autrement dit, Q ou R est inversible dans $K[X]$, c'est-à-dire constant. Quitte à changer la notation, on peut supposer que cela soit Q. Nous avons : $\mathrm{ct}(P) = \mathrm{ct}(Q)\,\mathrm{ct}(R)$, et, puisque P est primitif, $\mathrm{ct}(P) = 1$; l'élément $\mathrm{ct}(Q)$ est donc inversible dans A. Comme Q est constant, il est lui aussi inversible dans A, et donc dans $A[X]$. Ainsi, la décomposition est banale, ce qui montre que P est irréductible dans $A[X]$.
Montrons maintenant que les éléments en question sont les seuls éléments irréductibles. Pour cela, soit P un élément irréductible de $A[X]$ et écrivons $P = \mathrm{ct}(P)P_1$ avec P_1 primitif. Cette relation doit être banale, donc P_1 est inversible dans $A[X]$ ou $\mathrm{ct}(P) = 1$.
a) Dans le premier cas, P_1 est constant, inversible dans A. On observe alors qu'une relation non banale $\mathrm{ct}(P) = ab$ dans A nous donnerait une relation non banale $P = a(bP_1)$ dans $A[X]$, contredisant l'hypothèse que P est irréductible. Le contenu $\mathrm{ct}(P)$ est donc irréductible dans A.

b) Dans le second cas, P est primitif. Soit $P = QR$ une factorisation avec $Q, R \in K[X]$. La proposition 7.4.6 donne une relation $P = Q_1 R_1$ dans $A[X]$, avec Q_1 et R_1 associés à Q et R dans $K[X]$. Comme P est irréductible dans $A[X]$, cette décomposition doit être banale dans $A[X]$: l'un des facteurs est constant, la décomposition est donc banale aussi dans $K[X]$. La relation $P = QR$ l'est tout autant. Le polynôme P est donc irréductible dans $K[X]$.

□

Comme on voit dans la proposition ci-dessus, le corps des fractions K de l'anneau factoriel A joue un rôle important dans la description des éléments irréductibles de $A[X]$. Comme K est un corps, l'anneau $K[X]$ est principal, et donc *factoriel* d'après le théorème 7.3.1. On va utiliser cette observation pour démontrer le théorème de Gauß.

Démonstration du théorème de Gauß 7.4.1. Montrons d'abord l'existence de la décomposition en facteurs irréductibles. Soit K le corps des fractions de A. Soit P un élément de $A[X]$. Il admet une décomposition en facteurs irréductibles dans $K[X]$:

$$P = c \prod_{i=1}^{r} P_i$$

et la proposition 7.4.6 montre que l'on peut choisir $c = \mathrm{ct}(P)$ avec des polynômes P_i dans $A[X]$ qui sont primitifs et irréductibles dans $K[X]$. L'élément c admet dans A une décomposition en facteurs irréductibles $c = u \prod_{j=1}^{s} p_j$, avec u inversible et les p_j irréductibles dans A. On obtient donc l'égalité

$$P = u \prod_{j=1}^{s} p_j \prod_{i=1}^{r} P_i$$

D'après la proposition 7.4.7, les p_j et les P_i sont irréductibles dans $A[X]$. Par conséquent l'élément $P \in A[X]$ admet une décomposition en facteurs irréductibles dans $A[X]$.
On montre l'unicité en vérifiant la propriété d'Euclide.

a) Si p est un élément irréductible de A qui divise un produit QR de deux polynômes de $A[X]$, il divise aussi $\mathrm{ct}(QR) = \mathrm{ct}(Q)\,\mathrm{ct}(R)$. Il divise donc $\mathrm{ct}(Q)$ ou $\mathrm{ct}(R)$ et par la suite aussi Q ou R.

b) Si $P \in A[X]$ est un polynôme primitif, irréductible dans $K[X]$, qui divise un produit QR de deux polynômes de $A[X]$, alors il divise l'un des facteurs dans $K[X]$, disons Q. Nous avons donc $Q = SP$ avec $S \in K[X]$. D'après la proposition 7.4.6, cette relation impose que S est aussi dans $A[X]$. Ainsi P divise Q dans $A[X]$.
Nous avons donc montré l'existence et l'unicité de la décomposition en facteurs irréductibles dans l'anneau $A[X]$, d'où le théorème. □

7.5 Critères d'irréductibilité

Cette section met en place des critères pour décider si un polynôme P dans $A[X]$ est irréductible. Au vu de la proposition 7.4.7, il est déjà important de comprendre cette question quand A est un corps k. En fait, quand on parle de polynôme irréductible sans référence à l'anneau de coefficients, on entend toujours qu'il s'agit d'irréductibilité dans

un anneau de polynômes à coefficients dans un corps. On n'hésitera donc pas à préciser systématiquement dans quel anneau a lieu l'irréductibilité.
Par définition, dans l'anneau $k[X]$, un polynôme est irréductible s'il est de degré ≥ 1 et s'il ne s'écrit pas comme produit de deux polynômes de degrés ≥ 1.

PROPOSITION 7.5.1. — Soit k un corps.
a) Un polynôme $P \in k[X]$ qui a une racine dans k est irréductible dans $k[X]$ si, et seulement si, il est de degré 1.
b) Un polynôme $P \in k[X]$ de degré 2 ou 3 est irréductible dans $k[X]$ si, et seulement si, il n'a pas de racine dans k.

Démonstration. Commençons par noter que pour un polynôme de degré 1, $P = aX + b$, l'élément $-b/a \in k$ est bien entendu une racine de P.

Montrons la première assertion. Supposons que P est de degré 1. Si $P = QR$ alors $\deg Q + \deg R = 1$ et l'un des deux degrés est donc nul. Autrement dit, Q ou R sont constants non nuls, donc inversibles dans $k[X]$, et la décomposition est nécessairement banale. Le polynôme P est donc irréductible.
Pour la réciproque, on rappelle que si un polynôme admet x pour racine, alors il est divisible par $X - x$. Cet énoncé est valable pour des coefficients dans un anneau intègre quelconque. Montrons-le. Pour un élément x, effectuons la division euclidienne d'un polynôme P par le polynôme unitaire $X - x$: $P = (X - x)Q + R$ avec $\deg R < 1$. Le polynôme R est donc constant. On calcule sa valeur en évaluant en x : $P(x) = R$. On a donc, pour tout P :

$$P = (X - x)Q + P(x).$$

Si $P(x) = 0$, on a donc $P = (X - x)Q$ et la divisibilité annoncé. (Comme une constante non nulle n'est pas divisible par un polynôme de degré 1, on a même l'équivalence.)
Comme enfin $\deg Q = \deg P - 1$, on voit que P n'est pas irréductible dès que $\deg P \geq 2$.
a) b) Montrons la dernière assertion. Soit P un polynôme de degré 2 ou 3. Soit $P = QR$ une décomposition non banale. Par hypothèse, on a $\deg Q + \deg R = \deg P \leq 3$ et aussi $\deg(Q), \deg(R) \geq 1$ puisque la décomposition n'est pas banale. Cela implique que $\deg(Q) = 1$ ou $\deg(R) = 1$ et un des deux polynômes a donc a une racine dans k. Par suite, P a une racine dans k.

□

EXEMPLE 7.5.2. — Montrons que le polynôme $P(X, Y) = Y^2 + X^2 + 1$ est irréductible dans $\mathbb{C}[X, Y]$. Tout d'abord, les anneaux $\mathbb{C}[X]$ et $\mathbb{C}[X, Y] = (\mathbb{C}[X])[Y]$ sont factoriels, et $P(X, Y)$ est primitif vu comme polynômes en Y à coefficients dans $\mathbb{C}[X]$ puisque

$$pgcd(1, X^2 + 1) = 1 \qquad \text{dans } \mathbb{C}[X].$$

Donc $P(X, Y)$ est irréductible dans $\mathbb{C}[X, Y]$ si et seulement si il est irréductible dans $\mathbb{C}[X, Y] = (\mathbb{C}(X))[Y]$, l'anneau des polynômes en Y dont les coefficients sont des fractions rationnelles en X. Puisque $P(X, Y)$ est de degré 2 en Y, il est réductible dans $(\mathbb{C}(X))[Y]$ si et seulement si il existe deux fractions rationnelles $Q_1(X)$ et $Q_2(X)$ tels que

$$P(X, Y) = (Y - Q_1(X))(Y - Q_2(X)) = Y^2 - (Q_1(X) + Q_2(X))Y + Q_1(X)Q_2(X).$$

On voit donc que $Q_2(X) = -Q_1(X)$ et $X^2+1 = -Q_1(X)^2$. En particulier $Q_1(X)$ est un polynôme et X^2+1 a une racine double. Cela constitue une contradiction.

Il est souvent utile de tester l'irréductibilité à l'aide d'une réduction modulo un premier p, ou, mieux, modulo un idéal maximal. En effet, la réduction préserve les produits, si bien qu'une irréductibilité après réduction entraine souvent l'irréductibilité.
Le critère suivant est un peu plus subtil, et souvent utile.

PROPOSITION 7.5.3 (critère d'Eisenstein). — Soit A un anneau factoriel et K son corps des fractions. Soit

$$P(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

un polynôme de degré $n \geq 1$ à coefficients dans A. Supposons qu'il existe un élément irréductible $p \in A$ tel que
- p ne divise pas a_n ;
- p divise les a_k sauf pour $k = n$;
- p^2 ne divise pas a_0.

Alors P est irréductible dans $K[X]$.

Attention à la portée de l'énoncé : on suppose que les coefficients sont dans A mais la conclusion porte sur l'irréductibilité dans $K[X]$.

EXEMPLE 7.5.4. — Soit $P(X) = 2X^3 + 12X^2 + 6 \in \mathbb{Z}[X]$. Seuls $p = 2$ ou $p = 3$ peuvent convenir pour appliquer le critère, puisque p doit diviser a_0. Comme 2 divise a_3, uniquement 3 peut convenir et effectivement, 3 ne divise pas a_3, divise a_2, $a_1 = 0$ et a_0, mais 9 ne divise pas a_0. Ainsi P est irréductible dans $\mathbb{Q}[X]$.
Ici P n'est pas irréductible dans $\mathbb{Z}[X]$ puisque $P = 2(X^3+6X^2+3)$ est une décomposition non banale dans $\mathbb{Z}[X]$.

EXEMPLE 7.5.5. — Revenons au polynôme $P(X,Y) = Y^2 + X^2 + 1$ de l'Exemple 7.5.2. Vu comme polynôme en Y à coefficients dans $\mathbb{C}[X]$, on a dans ce cas

$$a_2 = 1, \qquad a_1 = 0, \qquad \text{et} \qquad a_0 = X^2 + 1.$$

On peut alors appliquer le théorème d'Eisenstein avec $p = X - i$.

EXEMPLE 7.5.6. — Quand aucun p ne convient pour appliquer le critère, il se peut qu'un changement de variables affine $Y = aX + b$ permet quand même de conclure. Par exemple si $P(X) = X^2 + X + 2$, on voit de suite que le coefficient 1 devant X interdit toute utilisation du critère. Cependant, par le changement de variables affine $Y = X - 3$, on obtient $(Y+3)^2 + (Y+3) + 2 = Y^2 + 7Y + 14$ pour lequel $p = 7$ convient. Ainsi P est irréductible (que l'irréductibilité d'un polynôme est invariant sous changement de variables affine sera démontré en T.D.).

On verra d'autres exemples d'application du critère d'Eisenstein en T.D. dont celui, célèbre, aux polynômes cyclotomiques pour un nombre premier p :

$$\frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + 1$$

où l'on montrera, grâce au changement de variables $Y = X - 1$, que $P(X)$ est irréductible.

Démonstration du critère d'Eisenstein. Supposons que $P = QR$ soit une décomposition de P dans $K[X]$. D'après la proposition 7.4.6, on peut supposer que les facteurs Q et R sont dans $A[X]$.
On va maintenant réduire cette équation modulo p. Rappelons, avant de continuer, que $A[X]/pA[X] \simeq (A/pA)[X]$, mais que cet anneau n'est pas forcément factoriel. En revanche, il est intègre parce que p, irréductible dans l'anneau factoriel A, y est aussi premier. Si on note L le corps des fractions de A/pA, l'anneau $L[X]$ est bien sûr factoriel.
Comme p divise tous les coefficients de P hormis a_n, modulo p, on trouve : $[a_n]X^n = [Q][R]$. Par unicité de la décomposition dans l'anneau factoriel $L[X]$, on a : $[Q] = [\alpha]X^k$ et $[R] = [\beta]X^{n-k}$ avec $\alpha, \beta \in A$. On a donc :

$$Q = \alpha X^k + pQ_1 \text{ et } R = \beta X^{n-k} + pR_1$$

D'où :

$$P = QR = \alpha\beta X^n + p(\beta X^{n-k}Q_1 + \alpha X^k R_1) + p^2 Q_1 R_1.$$

L'hypothèse que le terme constant de P n'est pas multiple de p^2 nous dit que $k = 0$ ou $k = n$. Si $k = n$, on a $Q = \alpha X^n + pQ_1$, avec $\deg Q_1 < n$. Ainsi $\deg Q = n$ d'où $\deg R = 0$. De même si $k = 0$ on a $\deg Q = 0$. La relation $P = QR$ est donc banale dans $K[X]$. Par conséquent P est bien irréductible dans $K[X]$. □

8 Polynômes symétriques

8.1 Polynômes symétriques élémentaires

Soit A un anneau. Pour un entier n, on note S_n le groupe symétrique, c'est-à-dire le groupe des bijections de l'ensemble $\{1, \ldots, n\}$. On dit qu'un polynôme $P \in A[X_1, \ldots, X_n]$ est *symétrique* si pour toute permutation $\pi \in S_n$ on a :

$$P(X_1, \ldots, X_n) = P(X_{\pi(1)}, \ldots, X_{\pi(n)}) \tag{8.1}$$

Un polynôme constant est symétrique ; si P et Q sont symétriques, alors la somme $P+Q$ et le produit PQ sont encore symétriques. L'ensemble des polynômes symétriques est donc un sous-anneau de l'anneau des polynômes, noté

$$A[X_1, \ldots, X_n]^{S_n} \subseteq A[X_1, \ldots, X_n].$$

Les *polynômes symétriques élémentaires* $s_{n,k} := \sum_{i_1<\ldots<i_k} X_{i_1} \cdots X_{i_k}$ sont symétriques pour $0 < k \leq n$. Explicitement, pour $n = 4$, il sont donnés par :

$$\begin{aligned}
s_{4,1} &= X_1 + X_2 + X_3 + X_4 \\
s_{4,2} &= X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 \\
s_{4,3} &= X_1X_2X_3 + X_1X_2X_4 + X_1X_3X_4 + X_2X_3X_4 \\
s_{4,4} &= X_1X_2X_3X_4
\end{aligned}$$

En général, le polynôme symétrique $s_{n,k}$ est est la somme des $\binom{n}{k}$ monômes de degré k sans facteur carré.

Remarque 8.1.1. — Souvent, on notera $s_{n,k}$ simplement par s_k. Ce n'est pas satisfaisante,puisque le nombre de variables en jeux dépend du contexte et n'apparaît pas dans cette notation, mais c'est la notation habituelle dans la littérature.

Un autre exemple de polynômes symétriques est donné par les sommes de puissances

$$t_k := X_1^k + \ldots + X_n^k$$

pour $k > 0$. Plus généralement, si l'on part d'un monôme $X^d := X_1^{d_1} \ldots X_n^{d_n}$, on construit un polynôme symétrique $\sum X^d$ en faisant la somme de tous les monômes dans la même orbite que X^d sous l'action de S_n, c'est-à-dire ceux obtenus de X^d en lui appliquant une permutation des variables (on reviendra sur cette propriété au chapitre suivant pour illustrer la notion d'orbite sous l'action d'un groupe).

Exercice 8.1.2. — Les polynômes $\sum X^d$ pour $d_1 \geq \cdots \geq d_n$ forment une A-base de $A[X_1, \ldots, X_n]^{S_n}$. Ceci signifie que tout polynôme symétrique s'écrit d'une manière unique comme combinaison linéaire à coefficients dans A des polynômes symétriques

$$\sum X^d, \ d_1 \geq \cdots \geq d_n$$

8.1.3 Formules de Girard-Viète

Les polynômes symétriques élémentaires sont souvent définis par l'égalité suivante entre deux polynômes à coefficients dans l'anneau $A[X_1, \dots X_n]$:

$$(X - X_1) \cdots (X - X_n) = X^n - s_1(X_1, \dots, X_n)X^{n-1} + \cdots (-1)^n s_n(X_1, \dots, X_n). \quad (8.2)$$

Il s'agit de la formule de Girard et Viète sur la relation entre coefficients et racines d'un polynôme. On utilise cette formule pour factoriser le polynôme général de degré n. Plus précisément, et afin d'éviter une division par le coefficient dominant, on considère le polynôme général unitaire sur l'anneau A :

$$X^n + a_1 X^{n-1} + \cdots + a_i X^{n-i} + \cdots + a_n.$$

C'est un polynôme à coefficients dans l'anneau $A[a_1, \dots, a_i, \dots, a_n]$ des polynômes en n variables. La formule (8.2) explique la factorisation de ce polynôme obtenue en spécialisant les variables par :

$$a_i \mapsto (-1)^i s_i(X_1, \dots X_n),\ 1 \leq i \leq n.$$

On note f_n le morphisme d'anneaux

$$f_n \ : \ A[a_1, \dots a_n] \to A[X_1, \dots X_n]$$

induit. Le terme de spécialisation est un peu inadapté ici, car le morphisme f_n n'est pas une surjection, mais, comme on va le voir ci-dessous, une injection.

8.2 Théorème fondamental sur les polynômes symétriques

On remarque d'abord que le morphisme f_n prend ses valeurs dans l'anneau des polynômes symétriques. En fait :

THÉORÈME 8.2.1. — Pour tout anneau A, et tout $n \geq 1$, le morphisme f_n défini par

$$a_i \mapsto (-1)^i s_i(X_1, \dots X_n),\ 1 \leq i \leq n,$$

induit un isomorphisme d'anneaux

$$A[a_1, \dots, a_n] \to A[X_1, \dots, X_n]^{S_n}.$$

Autrement dit, tout polynôme symétrique est un polynôme en les polynômes symétriques s_i, et ceci de manière unique. L'unicité dans cet énoncé, qui traduit l'injectivité de f_n, est souvent exprimé de la manière suivante : *les polynômes symétriques élémentaires sont algébriquement indépendants*. En effet, on dit généralement que des éléments sont algébriquement indépendants quand la seule relation polynomiale entre eux est triviale.

Démonstration. Nous allons donner deux algorithmes indépendants qui, pour tout polynôme symétrique, fournissent la représentation de ce polynôme en un polynôme en les polynômes symétriques élémentaires.

Algorithme 1 : La première démonstration procède par récurrence sur le nombre n de variables. On commence par remarquer que l'énoncé est banal pour $n = 1$.

Soit maintenant $n > 0$, et $q : A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_{n-1}]$ le morphisme d'anneaux défini par : $q(X_n) = 0$ et $q(X_i) = X_i$ pour $i < n$. On remarque que q envoie un polynôme symétrique sur un polynôme symétrique. De plus : $q(s_n) = 0$ et, pour $i < n$, $q(s_i)$ est le $i^{\text{ème}}$ polynôme symétrique élémentaire en les variables $X_1, \ldots, X_{n-1}$.

Soit $f_{n-1} : A[a_1, \ldots, a_{n-1}] \to A[X_1, \ldots, X_{n-1}]$. Par récurrence, on suppose que f_{n-1} est un isomorphisme sur le sous-anneau des polynômes symétriques. Nous avons un diagramme de suites exactes courtes (cela signifie simplement ici que q est surjectif et de noyau (a_n) et (X_n) respectivement)

$$\begin{array}{ccccc} (a_n) & \to & A[a_1, \ldots, a_n] & \xrightarrow{q} & A[a_1, \ldots, a_{n-1}] \\ & & \downarrow f_n & & \downarrow f_{n-1} \\ (X_n) & \to & A[X_1, \ldots, X_n] & \xrightarrow{q} & A[X_1, \ldots, X_{n-1}] \end{array}$$

et il découle du calcul des $q(s_i)$ que ce diagramme est commutatif (cela signifie simplement que les différentes composées possibles sont égales, ici : $q \circ f_n = f_{n-1} \circ q$).

Montrons d'abord que f_n est surjective sur $A[X_1, \ldots, X_n]^{S_n}$. Soit $P \in A[X_1, \ldots, X_n]$ un polynôme symétrique. Le polynôme $q(P)$ est encore symétrique (cette fois en les variables $X_1, \ldots X_{n-1}$). Par hypothèse de récurrence, il existe un polynôme Q dans $A[a_1, \ldots, a_{n-1}]$ tel que $f_{n-1}(Q) = q(P)$. Puisque q est surjectif, il existe un polynôme de $A[X_1, \ldots X_n]$ tel que $q(Q_1) = Q$. Afin de ne pas augmenter le degré, le plus simple est de choisir le polynôme Q lui-même. La différence $R := P - f_n(Q)$ est alors un polynôme vérifiant : $q(R) = 0$; on peut préférer écrire directement : $R(X_1, \ldots, X_n) = P(X_1, \ldots X_{n-1}, X_n) - P(X_1, \ldots, X_{n-1}, 0)$. Ainsi R est dans le noyau de q : d'où $X_n | R$. Ceci signifie que R est combinaison linéaire (à coefficients dans l'anneau A) de monômes $X^d = X_1^{d_1} \cdots X_n^{d_n}$ avec $d_n \geq 1$. Grâce à la symétrie de R, on a également $X_i | R$ pour $i = 1, \ldots, n-1$ et par suite R est combinaison linéaire de monômes $X^d = X_1^{d_1} \cdots X_n^{d_n}$ où tous les exposants sont non nuls. Il en résulte que : $s_n | R$. Soit $\tilde{P} := R/s_n$ le quotient ; le degré de $\tilde{P}$ est strictement plus petit que celui de P. On peut donc supposer, par récurrence sur le degré de P, que $\tilde{P}$ est dans l'image de f_n. Il existe alors un polynôme $\tilde{Q} \in A[a_1, \ldots, a_n]$ avec $f_n(\tilde{Q}) = \tilde{P}$, et on a : $P = s_n f_n(\tilde{Q}) + f_n(Q) = f_n((-1)^n a_n \tilde{Q} + Q)$. Ceci conclut les récurrences et montre la surjectivité de f_n.

L'injectivité de f_n se montre de manière analogue. Supposons Q dans le noyau de f_n. Alors $q(Q)$ est dans le noyau de f_{n-1}. Par hypothèse de récurrence, $q(Q)$ est nul. Par conséquent, $Q = a_n \tilde{Q}$ avec $\tilde{Q}$ un polynôme de degré strictement plus petit. Puisque $0 = f_n(Q) = s_n \cdot f_n(\tilde{Q})$, le polynôme $\tilde{Q}$ est dans $\mathrm{Ker}(f_n)$. Par récurrence sur le degré de Q, on obtient que $\tilde{Q} = 0$ et donc que $Q = a_n \tilde{Q} = 0$. Ceci achève la première démonstration.

Algorithme 2 : Cet algorithme remonte à Waring, l'unicité a été formulée et démontrée par Gauß.

On se concentre sur l'ordre de divisibilité sur les monômes. Cet ordre n'est que partiel. L'idée est de mettre un ordre total sur les monômes unitaires $X^d = X_1^{d_1} \cdots X_n^{d_n}$ qui reste compatible avec la divisibilité. L'ordre lexicographique convient : on pose $X^d > X^{d'}$ s'il existe i avec la propriété $d_j = d'_j$ pour tout $j < i$ et $d_i > d'_i$.

Comme on dispose maintenant d'un ordre total sur les monômes, on peut considérer le monôme principal d'un polynôme ; un polynôme est une combinaison linéaire des monômes unitaires, et le monôme principal est le monôme le plus haut parmi ceux qui ont un coefficient non nul.

Commençons par la surjectivité de f_n. Soit $P = \sum P_t X^t$ un polynôme symétrique. Grâce à la symétrie de P, son monôme principal X^d, $d = (d_1, \dots d_n)$, vérifie : $d_1 \geq d_2 \geq \dots \geq d_n$. Il n'est pas difficile d'écrire un polynôme symétrique qui a même monôme principal : le polynôme

$$Q := P_d s_1^{d_1 - d_2} s_2^{d_2 - d_3} \cdots s_{n-1}^{d_{n-1} - d_n} s_n^{d_n}$$

convient, et celui-ci est évidemment dans l'image de f_n. La différence $P - Q$ a donc un monôme principal strictement plus petit que celui de P. On répète le processus en travaillant avec $Q - P$ au leu de P. Son itération produit un algorithme qui se termine par le polynôme nul puisque les monômes principaux décroissent strictement. On obtient le polynôme antécédent de P en ajoutant les antécédents de Q trouvés à chaque étape.

De même, on démontre l'injectivité de f_n : le polynôme $s_1^{\nu_1} \cdots s_n^{\nu_n}$ a comme monôme principal $X_1^{\nu_1 + \dots + \nu_n} X_2^{\nu_2 + \dots + \nu_n} \dots X_n^{\nu_n}$. Maintenant, la famille $(\nu_1 + \dots + \nu_n, \nu_2 + \dots + \nu_n, \dots, \nu_n)$ détermine la famille $(\nu_1, \nu_2, \dots, \nu_n)$ par un système triangulaire. Il en résulte que les images de monômes différents $a_1^{\nu_1} \cdots a_n^{\nu_n}$ sous f_n ont des monômes principaux différents. L'injectivité de f_n en résulte. □

La mise en œuvre pratique du deuxième algorithme est aisée.

8.3 Applications

Une conséquence importante du théorème est le principe suivant

Corollaire 8.3.1. — Soient A et B deux anneaux tels que $A \subseteq B$ et

$$P = X^n + a_1 X^{n-1} + \dots + a_n \in A[X]$$

un polynôme qui se décompose sur B en facteurs du premier degré :

$$(X - \lambda_1) \cdot \dots \cdot (X - \lambda_n).$$

Alors tout élément de B, qui s'exprime de manière symétrique et polynômiale en les racines $\lambda_1, \dots, \lambda_n$, est déjà dans A.

Démonstration. Soit $f : A[X_1, \dots, X_n] \to B$ le morphisme d'anneau tel que $f : X_i \mapsto \lambda_i$. Supposons qu'il existe un polynôme symétrique P avec $f(P) = b$. D'après les formules de Girard et Viète, on a $f(s_i) = (-1)^i a_i \in A$. D'après le théorème ci-dessus, il existe donc un polynôme Q dans $A[a_1, \dots, a_n]$ avec $P = Q(s_1, \dots, s_n)$. Mais alors, $b = f(P) = Q(f(s_1), \dots, f(s_n))$ est dans A. □

Que se passe-t-il pour les sommes des puissance $t_k := X_1^k + \dots + X_n^k$? D'après le théorème, ils doivent s'exprimer en fonction des s_i. On voit facilement

$$\begin{aligned} t_1 &= s_1 \\ t_2 &= s_1^2 - 2s_2 \\ t_3 &= s_1^3 - 3s_1 s_2 + 3s_3 \end{aligned}$$

Ici, et dans la suite, on pose $s_k = 0$, si k est strictement plus grand que le nombre de variables en jeu. Pour les t_k avec $k \geq 4$, l'écriture des t_k en tant que polynômes en les s_k est moins évident :

PROPOSITION 8.3.2. — (Newton) Nous avons

$$s_0 t_n - s_1 t_{n-1} + s_2 t_{n-2} - \ldots + (-1)^n t_0 s_n = 0. \tag{8.3}$$

Démonstration. On remarque que par définition $s_0 = 1$ et que $t_0 = n$. Si l'on évalue l'équation (8.2) en les X_i on obtient

$$0 = X_i^n - s_1 X_i^{n-1} + \ldots + (-1)^n s_n.$$

On obtient la proposition en sommant sur $i = 1, \ldots, n$. □

Ainsi, on peut exprimer les t_n de manière récursive en les s_k, $k \leq n$, sans que l'on soit obligé de faire appel aux algorithmes du théorème 8.2.1 Remarquons que le facteur devant s_n est égal à $n = t_0$ dans l'identité (8.3). Ainsi, si l'on résout dans le sens inverse, on doit prendre des dénominateurs : les formules

$$\begin{aligned} s_1 &= t_1 \\ s_2 &= \frac{1}{2}(t_1^2 - t_2) \\ s_3 &= \frac{1}{6}t_1^3 - \frac{1}{2}t_1 t_2 + \frac{1}{3}t_3 \end{aligned}$$

sont valables uniquement dans les $\mathbb{Q}$-algèbres.

9 Résultant

Nous allons définir le *résultant* de deux polynômes. Ce résultant permettra de dire quand deux polynômes P et Q sont premiers entre eux, juste par inspection de leurs coefficients.

9.1 Introduction

Soit k un corps. Nous avons vu que $k[X]$ est un anneau factoriel. On se pose maintenant la question de caractériser quand deux éléments P, Q de $k[X]$ sont premiers entre eux, c'est-à-dire quand $\text{pgcd}(P, Q) = 1$. Une première méthode consiste à appliquer l'algorithme d'Euclide, puisque celui-ci fournit le pgcd. Cependant, il n'est pas facile d'écrire le résultat de l'algorithme en fonction des coefficients des polynômes.

On se propose d'exprimer une condition à l'aide d'un déterminant ne dépendant que des coefficients des deux polynômes. Commençons d'abord avec $k = \mathbb{C}$. D'après le théorème de Gauss-d'Alembert, tout polynôme de $\mathbb{C}[X]$ est produit de polynômes de degré 1. La question revient donc à se demander quand deux polynômes P, Q de $\mathbb{C}[X]$ ont une racine en commun. En fait, même si l'on commence avec des polynômes à coefficients rationnels, l'algorithme d'Euclide montre que deux polynômes sont premiers entre eux dans $\mathbb{Q}[X]$ si, et seulement si, ils le sont comme polynômes de $\mathbb{C}[X]$. On voit que travailler dans $\mathbb{C}$, où l'on dispose de racines, ne change rien au problème.

9.2 Première approche : une condition nécessaire

Supposons d'abord que P et Q sont de degré 1 :

$$P = a_0 + a_1 X \text{ et } Q = b_0 + b_1 X.$$

Les polynômes P et Q ont une racine en commun si la racine $-a_0/a_1$ de P et celle $-b_0/b_1$ de Q coïncident. Ceci est bien sûr le cas quand $-a_0/a_1 = -b_0/b_1$, autrement dit quand : $a_0 b_1 - b_0 a_1 = 0$ ou encore quand

$$\det \begin{pmatrix} a_0 & a_1 \\ b_0 & b_1 \end{pmatrix} = 0$$

Le lien avec le déterminant provient de l'observation suivante. On cherche à résoudre le système de deux équations linéaires en les variables x_0 et x_1 :

$$\begin{pmatrix} a_0 & a_1 \\ b_0 & b_1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Si z est une racine commune, $(1, z)$ est une solution non triviale du système, puisque

$$\begin{pmatrix} a_0 & a_1 \\ b_0 & b_1 \end{pmatrix} \begin{pmatrix} 1 \\ z \end{pmatrix} = \begin{pmatrix} a_0 + a_1 z \\ b_0 + b_1 z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Réciproquement, si (z_0, z_1) est une solution non triviale, alors $z = z_1/z_0$ est la racine commune. En effet, si P et Q sont de degré 1, une solution non triviale (z_0, z_1) a automatiquement $z_0 \neq 0$. Alors $\frac{1}{z_0}(z_0, z_1) = (1, z)$ est encore une solution puisque l'espace des

solutions est, en tant que noyau de l'application linéaire $\mathbb{C}^2 \to \mathbb{C}^2$ définie par la matrice

$$\begin{pmatrix} a_0 & a_1 \\ b_0 & b_1 \end{pmatrix}$$

un sous-espace vectoriel de $\mathbb{C}^2$. On voit donc que P et Q ont une racine en commun si, et seulement si, cette application linéaire a un noyau non trivial. Ceci est le cas exactement quand le déterminant de M est trivial, ou autrement dit quand $a_0b_1 - b_0a_1 = 0$.

Si P et Q sont de degré 2, on peut bien entendu déterminer les racines de P et Q puis comparer le résultat pour vérifier si P et Q ont une racine en commun. Cette méthode demande de résoudre deux équations de degré deux. C'est faisable, mais calculer toutes les racines peut sembler beaucoup si c'est juste pour vérifier que P et Q ont une racine en commun. Par ailleurs, cette méthode ne se généralise pas forcément très bien en degré supérieur : d'après Abel-Ruffini et Galois, il n'existe pas de formule universelle pour résoudre les équations de degré supérieur ou égal à cinq. Enfin, elle ne semble pas fournir de condition explicite facilement exprimable.

Il est plus judicieux de résoudre à nouveau un système linéaire, mais cette fois-ci en les indéterminées x_0, x_1, x_2. Pour que

$$P = a_0 + a_1X + a_2X^2 \text{ et } Q = b_0 + b_1X + b_2X^2$$

aient une racine commune,il est nécessaire au moins que le système homogène

$$\begin{cases} a_0x_0 + a_1x_1 + a_2x_2 = 0 \\ b_0x_0 + b_1x_1 + b_2x_2 = 0 \end{cases}$$

ait une solution non nulle, à savoir $(1, z, z^2)$ si z est une racine commune. Le problème est que nous avons deux équations à partir de P et Q, alors que nous avons trois indéterminées, et la condition est donc toujours vérifiée. L'idée est alors d'ajouter des équations, au plus simple. Multiplier P par X ajoutera sans doute une équation correcte, mais aussi une indéterminée : x_3. Si on multiplie aussi Q par X, on tombe alors sur le bon nombre d'équations et indéterminées :

$$\begin{pmatrix} a_0 & a_1 & a_2 & 0 \\ 0 & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & 0 \\ 0 & b_0 & b_1 & b_2 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Si z est une racine commune à P et Q, le vecteur $(1, z, z^2, z^3)$ est une solution non triviale de ce système. Une condition nécessaire pour que P et Q aient une racine commune est donc l'annulation du déterminant de la matrice du système, ce qui s'exprime par l'identité :

$$(a_0b_2 - b_0a_2)^2 = (a_0b_1 - b_0a_1)(a_1b_2 - b_1a_2)$$

Il n'est pas clair à ce stade que la condition soit suffisante. Même montrer que, si ce déterminant est nul, il y a une solution de première coordonnée $x_0 = 1$, demande une justification.

En général, soient

$$P = a_0 + a_1X + \cdots + a_mX^m \text{ et } Q = b_0 + b_1X + \cdots + b_nX^n$$

deux polynômes de degré inférieur ou égal à m et n respectivement. On peut supposer $m \geq n$, quitte à échanger les rôles de P et Q. On cherche un système analogue à ceux pour $m = n = 1$ et $m = n = 2$. D'abord, si $m > n$, on ajoute $m - n$ équations, en multipliant Q par $X, X^2, \ldots, X^{m-n}$. Cela n'ajoute pas d'indéterminée. Ensuite, on multiplie par des puissance de X pour arriver à autant d'équations que d'indéterminées. Si on multiplie avec k puissances de X on arrive à $2 + m - n + 2k$ équations et $n + 1 + k$ indéterminées. L'égalité est atteinte pour $k = n - 1$, ce qui donne un système à $m + n$ équations avec $m + n$ indéterminées. Par exemple, pour $m = 3$ et $n = 2$, on arrive au système

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

De nouveau, une condition nécessaire pour l'existence d'une racine commune, est l'annulation du déterminant de la matrice du système.

9.3 Coefficients de Bézout

Revenons à notre question initiale : quand est-ce P et Q sont-ils premiers entre eux dans $k[X]$? Comme $k[X]$ est principal, cela revient à dire qu'il existe U, V dans $k[X]$ tels que :

$$UP + VQ = 1.$$

L'idée est, comme ci-dessus, de traduire en un problème linéaire. Il suffit pour cela de considérer l'application k-linéaire

$$k[X] \times k[X] \to k[X]\,;\, (U, V) \mapsto UP + VQ.$$

L'image est l'idéal engendré par P et Q, c'est-à-dire l'idéal engendré par le pgcd de P et Q, que l'on notera D. En particulier, P et Q sont premiers entre eux si, et seulement si, cette application linéaire est surjective.

Il est alors classique de calculer l'indétermination des coefficients de Bézout, ou, autrement dit, de déterminer le noyau de notre application linéaire. Nous laissons cet exercice au lecteur, et donnons simplement la réponse. Notons P_1 et Q_1 les polynômes tels que : $P = DP_1$ et $Q = DQ_1$. Un couple (U, V) est dans le noyau si, et seulement si, il est de la forme $(TQ_1, -TP_1)$ pour un polynôme T de $k[X]$. On a ainsi paramétré le noyau par les polynômes de $k[X]$.

Nous aimerions faire le lien entre cette application linéaire et le déterminant considéré plus haut. Pour cela, nous allons nous ramener à des espaces de dimension finie.

9.4 Matrice de Sylvester

Rappelons que, pour tout entier naturel r, on désigne par $k[X]_{r-1}$ le k-espace vectoriel des polynômes de degré $< r$, (qui par convention contient 0). Il est de dimension r avec une base $(1, X, \ldots, X^{r-1})$.

Pour P et Q des polynômes de degrés respectivement inférieur ou égal à m et n, considérons l'application linéaire

$$\rho : k[X]_{n-1} \times k[X]_{m-1} \to k[X]_{m+n-1} \,;\, (U, V) \mapsto UP + VQ.$$

On observe que ρ est bien définie, c'est-à-dire on a bien, au niveau des degrés, que $\deg(UP + VQ) \leq m + n - 1$ pour tout (U, V) de $k[X]_{n-1} \times k[X]_{m-1}$. Lue dans la base

$$\big((1,0), (X,0), \ldots, (X^{n-1},0); (0,1), (0,X), \ldots, (0,X^{m-1})\big)$$

de l'espace vectoriel $k[X]_{n-1} \times k[X]_{m-1}$ et la base de $\{1, X, \ldots, X^{m+n-1}\}$ de $k[X]_{m+n-1}$, et en supposant que $m \geq n$ pour la mise en page, la matrice de ρ est la suivante :

$$R = \begin{pmatrix}
a_0 & 0 & \ldots & 0 & b_0 & 0 & \ldots & & 0 \\
a_1 & a_0 & & \vdots & b_1 & b_0 & & & \\
\vdots & \vdots & \ddots & & \vdots & \vdots & & & \vdots \\
a_{n-1} & a_n & \ldots & a_0 & b_{n-1} & b_{n-2} & \ddots & & \\
a_n & a_{n+1} & \ldots & a_1 & b_n & b_{n-1} & \ldots & & \\
a_{n+1} & a_{n+2} & \ldots & a_2 & 0 & b_n & \ldots & b_0 & 0 \\
\vdots & \vdots & & \vdots & \vdots & & & & b_0 \\
a_m & & & & & & \ddots & & \vdots \\
0 & a_m & & & & & & & \\
\vdots & & \ddots & & & & & & \\
0 & & \ldots & a_m & 0 & 0 & \ldots & 0 & b_n
\end{pmatrix}$$

où le vecteur colonne $(a_0, \ldots, a_m)$ est recopié n fois en décalant vers le bas, puis le vecteur colonne $(b_0, \ldots, b_n)$ est recopié m fois en décalant vers le bas. Cette matrice est souvent appelée la *matrice de Sylvester*.

9.5 Résultant

Définition 9.5.1. — On appelle *résultant* de P et de Q est on note $\mathrm{Res}_{m,n}(P, Q)$ le déterminant de la matrice de Sylvester R.

On voit que si a_m et b_n sont tous deux nuls, autrement dit si les deux polynômes sont de degré strictement plus petits que m et n respectivement, alors la dernière ligne est nulle, et donc le déterminant est nul. Il se trouve qu'à part ce cas banal, la nullité du déterminant n'a lieu que quand P et Q ne sont pas premiers entre eux.

Proposition 9.5.2. — Soient m et n deux entiers naturels. Soit k un corps et soient P, Q deux polynômes dans $k[X]$ de degrés inférieurs ou égaux à m et n respectivement. Alors, $\mathrm{Res}_{m,n}(P, Q)$ est non nul si, et seulement si,

- les polynômes P et Q sont premiers entre eux, et
- le degré de P égale m ou le degré de Q égale n.

En particulier, si P est de degré m ou si Q de degré n, alors leur résultant $\mathrm{Res}_{m,n}(P,Q)$ est nul si, et seulement si, les polynômes P et Q ne sont pas premiers entre eux.

Démonstration. Si $P = Q = 0$, alors $\mathrm{Res}_{m,n}(P,Q) = 0$. Supposons qu'ils ne sont pas tous deux nuls. L'algèbre linéaire nous enseigne que le déterminant est non nul exactement quand le noyau de ρ est nul.Nous allons déterminer la dimension du noyau de ρ en fonction des degrés des polynômes. Reprenons les notations du paragraphe 9.3. Le noyau de ρ est l'intersection de son espace de définition $k[X]_{n-1} \times k[X]_{m-1}$avec le noyau trouvé dans ce paragraphe là, noyau que l'on a paramétré comme étant l'ensemble des $(TQ_1, -TP_1)$. Un tel couple appartient à $k[X]_{n-1} \times k[X]_{m-1}$ si, et seulement si, :

$$\deg T + \deg Q_1 < n \quad \text{et} \quad \deg T + \deg P_1 < m.$$

Comme $\deg D = \deg P - \deg P_1 = \deg Q - \deg Q_1$, cette condition s'écrit :

$$\deg T < \deg D + n - \deg Q \quad \text{et} \quad \deg T < \deg D + m - \deg P.$$

On obtient que la dimension du noyau de ρ est égale à :

$$\dim(\mathrm{Ker}\,\rho) = \deg D + \inf(m - \deg P, n - \deg Q).$$

Cet entier est nul si, et seulement si, $\deg D = 0$ et $\inf(m - \deg P, n - \deg Q) = 0$, ce qui termine la preuve. □

Remarque 9.5.3 (détermination de l'image de ρ). — Quand P et Q sont premiers entre eux, on savait le polynôme constant 1 dans l'image de ρ, par la relation de Bézout. L'argument donné ne se contente pas de redémontrer ce résultat, il donne la surjectivité de ρ. Il donne aussi dans tous les cas la dimension de l'image de ρ. En particulier, si P est de degré m et Q de degré n, l'image de ρ est exactement l'ensemble des polynômes multiple de D et de degré strictement inférieur à $m + n$.

Remarque 9.5.4. — On a remarqué que la matrice R est transposée de la matrice du système considérée au paragraphe 9.2. Bien sûr, cela ne change pas le déterminant. Mieux, les solutions $(x_0, \ldots, x_{m+n-1})$ du système homogène forment le noyau de la transposée R^t. Mais celui-ci, par un résultat classique de dualité linéaire, n'est autre que *l'orthogonal* de l'image de R. Ainsi, les solutions du système homogène vérifient les équations linéaires définies par les polynômes qui se trouvent dans l'image de ρ. On peut donc exploiter la détermination de l'image faite dans la remarque précédente pour faire le lien entre les deux approches.

Par exemple, P et Q ne sont pas premiers entre eux, si, et seulement si, le polynôme 1 n'est pas dans l'image de ρ,

$$1 \notin \mathrm{Im}\rho = (\mathrm{Ker}\, R^t)^\perp$$

c'est-à-dire que la relation d'orthogonalité correspondante, $x_0 = 0$, n'est pas vérifiée par toute solution du système $(x_0, \ldots, x_{m+n-1}) \in \mathrm{Ker}\, R^t$; il y a donc une solution avec

première coordonnée non nulle, que l'on peut choisir égale à 1. On voit aussi que si $(1, z, \ldots, z^i, \ldots, z^{m+n-1})$ est solution, alors, par orthogonalité avec D, z est racine de D. Réciproquement, si z est racine de D, $(1, z, \ldots, z^i, \ldots, z^{m+n-1})$ est orthogonal aux polynômes multiples de D qui forment l'image de ρ, et est donc solution du système homogène.

On obtient comme conséquence directe de la proposition l'énoncé suivant :

COROLLAIRE 9.5.5. — Soient A un anneau intègre et K son corps des fractions. Soient m et n deux entiers naturels et soient P, Q deux polynômes dans $A[X]$ de degrés inférieurs ou égaux à m et n respectivement. Alors, $\mathrm{Res}_{m,n}(P, Q)$ est non nul si, et seulement si,
- les polynômes P et Q sont premiers entre eux dans $K[X]$, et
- le degré de P égale m ou le degré de Q égale n.

C'est d'ailleurs quand l'anneau A est lui-même un anneau de polynômes que le résultant s'avère le plus utile. Comme exemple, nous donnons l'énoncé suivant, qui est la clef de la démonstration du théorème de Bézout qui sera démontré à la fin du cours.

COROLLAIRE 9.5.6. — Soit $A = \mathbb{C}[Y]$ et soient P, Q dans $A[X] = \mathbb{C}[X, Y]$. Dans $\mathbb{C}[X, Y]$, on écrit

$$P = P_m(Y)X^m + \cdots + P_0(Y) \text{ et } Q = Q_n(Y)X^n + \cdots + Q_0(Y),$$

où les P_i et les Q_j sont des éléments de $\mathbb{C}[Y]$. Soit $R = \mathrm{Res}_{m,n}(P, Q)$ dans $\mathbb{C}[Y]$. Un élément y de $\mathbb{C}$ est racine de R si, et seulement si,
- les polynômes $P(X, y)$ et $Q(X, y)$ ont une racine commune dans $\mathbb{C}$, ou
- $P_m(y) = Q_n(y) = 0$.

Démonstration. D'après la formule qui définit le résultant on a

$$R(y) = \mathrm{Res}_{m,n}(P, Q)(y) = \mathrm{Res}_{m,n}(P(X, y), Q(X, y))$$

Il suffit d'appliquer le théorème précédent aux polynômes $P(X, y)$ et $Q(X, y)$ de $\mathbb{C}[X]$. □

EXEMPLE 9.5.7. — Prenons $P(X, Y) = X^2Y^2 + X - 2$ et $Q(X, Y) = XY - 2$. On calcule : $\mathrm{Res}^X_{2,1}(P, Q)(Y) = 2Y(Y + 1)$. Pour $Y = -1$, les coefficients dominants sont non nuls, et l'annulation du résultant signifie que les polynômes $P(X, -1) = X^2 + X - 2$ et $Q(X, -1) = -X - 2$ ont une racine commune (ici, c'est -2). Pour $Y = 0$ en revanche, le théorème ne permet pas de conclure quant à une racine commune ; et en effet les polynômes $P(X, 0) = X - 2$ et $Q(X, 0) = -2$ n'ont pas de racine commune.

10 Théorie des groupes - rappels

10.1 Groupes et morphismes

Définition 10.1.1. — Un *groupe* est un ensemble non vide G muni d'une loi interne $G \times G \to G$, $(x, y) \mapsto x \cdot y$ telle que :
- pour tous $x, y, z \in G$, on a $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (associativité)
- il existe un élément $e \in G$ tel que pour tout $x \in G$ on ait $e \cdot x = x \cdot e = x$ (existence d'un élément neutre) ;
- pour tout $x \in G$ il existe $y \in G$ tel que l'on ait $x \cdot y = y \cdot x = e$ (existence d'un inverse) ;

On dit qu'un groupe G est *commutatif*, ou encore *abélien*, si $x \cdot y = y \cdot x$ pour tous $x, y \in G$.

Remarques 10.1.2. —

a) Observons d'abord qu'un élément neutre dans un groupe est nécessairement unique. En effet, si e, e' sont neutres, alors en appliquant deux fois G_2),

$$e' = e' \cdot e = e.$$

b) De même, un élément inverse dans un groupe est obligatoirement unique. En effet, si y et y' sont des inverses pour x, alors

$$y' = y' \cdot e = y' \cdot (x \cdot y) = (y' \cdot x) \cdot y = e \cdot y = y.$$

c) La loi interne $\cdot$ a de multiples notations. Le plus souvent nous la notons *multiplicativement*, c'est-à-dire on écrira simplement xy. Dans ce cas, on note l'inverse d'un élément x par x^{-1} et l'élément neutre par 1.

d) Si G est abélien, on note la loi interne souvent *additivement*, c'est-à-dire on écrira $x + y$. Dans ce cas, l'inverse d'un élément x est noté par $-x$, l'élément neutre par 0 puis on pose $x - y := x + (-y)$.

La notion de groupe a été dégagée par Évariste Galois vers 1830 dans son étude des équations polynomiales et l'impossibilité de résoudre celles-ci en degré supérieur ou égale à 5. Le premier groupe ainsi étudié est le groupe symétrique $\mathfrak{S}_n$, c'est-à-dire les permutations de l'ensemble $\{1, 2, \ldots, n\}$ avec pour loi interne la composition.
D'autres exemples sont le groupe $\mathbb{Z}$ des entiers relatifs (pour l'addition), l'ensemble des rationnels $\mathbb{Q}$ non nuls (pour la multiplication) ou encore l'ensemble des matrices $n \times n$ inversibles (pour la multiplication des matrices).
Une fois définie la notion de groupe, on s'intéresse à des applications entre ceux-ci qui respectent la loi interne :

Définition 10.1.3. — Si G et H sont deux groupes, un *homomorphisme de groupes* $f : G \to H$ est une application f telle que $f(xx') = f(x)f(x')$ pour tous x, x' de G.

Si $f : G \to H$ est un homomorphisme, on vérifie que $f(e_G) = e_H$ et $f(x^{-1}) = f(x)^{-1}$ dans H pour tout $x \in G$. On dit aussi simplement *morphisme* au lieu de homomorphisme. On dit qu'un morphisme de groupes $f : G \to H$ est un *isomorphisme* s'il existe un morphisme

de groupes $g : H \to G$ tel que $f \circ g = \mathrm{Id}_H$ et $g \circ f = \mathrm{Id}_G$. Le morphisme g est alors appelé morphisme réciproque de f. On note $f : G \xrightarrow{\sim} H$ pour signifier que le morphisme f est un isomorphisme.

PROPOSITION 10.1.4. — Un morphisme de groupes est un isomorphisme si et seulement si il est bijectif.

Démonstration. Si $f : G \to H$ est un isomorphisme, son morphisme réciproque est en particulier une bijection réciproque, donc f est bien bijectif. Réciproquement, si f est bijectif, notons $g : H \to G$ sa bijection réciproque. Il faut montrer que g est un morphisme de groupes. Soient $x, y \in H$. On a

$$f(g(xy)) = xy = f(g(x))f(g(y)) = f(g(x)g(y)).$$

Comme f est bijectif, on a donc $g(xy) = g(x)g(y)$. □

DÉFINITION 10.1.5. — Un sous-ensemble H d'un groupe G en est un *sous-groupe* si :
- $e \in H$;
- si $x, y \in H$, alors $xy \in H$;
- si $x \in H$, alors $x^{-1} \in H$.

On utilisera la notation $H < G$ pour H sous-groupe de G.

Autrement dit un sous-groupe de G est un sous-ensemble de G que la loi de G munit d'une structure de groupe. Tout groupe G a toujours deux sous-groupes naturels : le groupe G lui-même et $\{e\}$.

EXEMPLE 10.1.6. — L'image ou l'image réciproque d'un sous-groupe par un morphisme de groupes $f : G \to G'$ est encore un sous-groupe. En particulier, l'image réciproque de l'élément neutre de G' est un sous-groupe de G, appelé le *noyau* de f et noté $\mathrm{Ker}\, f$. On rappelle qu'un morphisme de groupes est injectif si et seulement si $\mathrm{Ker}\, f = \{e\}$.

Le fait que $H < G$ est équivalent au fait que la relation

$$x \sim_H y \iff xy^{-1} \in H$$

soit une relation d'équivalence sur G. Dans ce cas, on note G/H l'ensemble des classes d'équivalence, et $[x]_H$ la classe d'équivalence de $x \in G$, appelée *classe à gauche de x par H*. On a bien évidemment

$$[x]_H = xH.$$

Comme pour toute relation d'équivalence, nous avons une application naturelle

$$\begin{array}{ccc} \pi : G & \longrightarrow & G/H \\ x & \longmapsto & [x]_H \end{array}$$

Pour $x \in G$, l'application

$$\begin{array}{ccc} G & \longrightarrow & G \\ y & \longmapsto & xy \end{array}$$

est une bijection. En particulier, les cardinaux de H et xH sont égaux. Dans le cas où G est fini, on en déduit alors le résultat suivant. On rappelle que l'ordre d'un groupe désigne son cardinal lorsque celui-ci est fini.

THÉORÈME 10.1.7 (Lagrange). — Soit G un groupe fini et $H \subseteq G$ un sous-groupe de H. Soit r le nombre des classes à gauches par H. Alors nous avons

$$\mathrm{ord}(G) = r\,\mathrm{ord}(H)$$

En particulier, l'ordre de H divise l'ordre de G.

DÉFINITION 10.1.8. — Soit G un groupe fini et $H \subseteq G$ un sous-groupe de G. Le nombre r des classes à gauches sous H de G est appelé *l'indice* de H dans G. Il sera noté $|G : H|$.

Étant donné un groupe G et $H < G$, on peut se demander si il existe une loi de groupe sur l'ensemble G/H faisant de l'application $\pi : G \to G/H$ un morphisme de groupes, c'est à dire

$$\forall x, y \in G,\ [xy]_H = [x]_H[y]_H.$$

Remarquons que cette relation nous dit exactement quelle doit être la loi de groupe sur G/H. Il reste donc à vérifier que cette relation est bien définie, et qu'elle induit bien une structure de groupe sur G/H. Cherchons tout d'abord à quelle condition la relation $[xy]_H = [x]_H[y]_H$ est bien définie, c'est à dire ne dépend pas des représentants choisis des classes $[xy]_H, [x]_H$, et $[y]_H$. En d'autres termes, à quelle condition a-t-on

$$\forall x, x', y, y' \in G, x \sim_H x' \text{ et } y \sim_H y' \Longrightarrow xy \sim_H x'y'?$$

Si $xx'^{-1} = h \in H$ et $yy'^{-1} = \widetilde{h} \in H$, alors $xyy'^{-1}x'^{-1} = x\widetilde{h}x'^{-1} = x\widetilde{h}x^{-1}h$. On déduit alors la relation $[xy]_H = [x]_H[y]_H$ est bien définie si et seulement si

$$\forall x \in G,\ xHx^{-1} \subset H.$$

On vérifie alors sans difficulté qu'on obtient une loi de groupe sur G/H faisant de $\pi : G \to G/H$ un morphisme de groupes.

DÉFINITION 10.1.9. — Soit G un groupe et $x, g \in G$. Nous appelons $xgx^{-1} \in G$ *le conjugué de g par x*. Un sous-groupe $H \subseteq G$ est dit distingué (ou normal) si

$$\forall x \in G, xHx^{-1} \subset H.$$

On utilisera dans ce cas la notation $H \lhd G$.

EXEMPLE 10.1.10. — Un groupe G quelconque contient toujours au moins deux sous-groupes distingués :

$$G \lhd G \qquad \text{et} \qquad \{e\} \lhd G.$$

EXEMPLE 10.1.11. — Si $f : G \to G'$ est un morphisme de groupes, alors $\mathrm{Ker}\, f \lhd G$.

EXEMPLE 10.1.12. — Si G est abélien, alors tout sous-groupe de G est distingué.

Les groupes quotients permettent de factoriser les morphismes de groupes.

THÉORÈME 10.1.13. — Soit $f : G \to G'$ un morphisme de groupes, et $H < \operatorname{Ker} f$ tel que $H \lhd G$. Alors il existe un unique morphisme de groupes $\overline{f} : G/H \to G'$ tel que $f = \overline{f} \circ \pi$, i.e. rendant commutatif le diagramme

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{f}} & \\ G/H & & \end{array}$$

De plus $\overline{f}$ est injectif si et seulement si $H = \ker f$.

Ainsi, les sous-groupes distingués de G correspondent exactement aux noyaux de morphismes surjectifs $f : G \to G'$. En particulier, on peut chercher à étudier un groupe G en étudiant le groupe "plus petit" G/H avec $H \lhd G$. De ce point de vue, les groupes ne possédant pas de tels sous-groupe distingués non-triviaux constituent des groupes "irréductibles".

DÉFINITION 10.1.14. — Un groupe G est dit simple si

$$H \lhd G \iff H = G \text{ ou } H = \{e\}.$$

Les groupes finis simples sont complètement classifiés. Il s'agit d'une œuvre titanesque dont la réalisation s'étend sur plus d'un siècle ! Il y a, comme nous le verrons,

- les groupes cycliques $\mathbb{Z}/p$, avec p premier ;
- les groupes alternés $\mathfrak{A}_n$, avec $n \geq 5$.

Il y a de plus 16 séries de groupes dits de type de Lie puis 26 autres qui n'apparaissent pas dans une série. Ces derniers groupes simples finis sont appelés *sporadiques* pour cette raison. Le plus grand groupe sporadique s'appelle le *monstre*. L'existence de ce groupe avait été conjecturée par Fischer et Griess en 1973 puis construit par Griess en 1982. Il a

$$\begin{aligned} &2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \\ &= 808017424794512875886459904961710757005754368000000000 \end{aligned}$$

éléments. Il y a des relations intéressantes et a priori non suspectées entre le monstre et certaines fonctions qui apparaissent dans la théorie des fonctions modulaires. Ces relations ont semblé tellement bizarres au début qu'elles sont connues sous le nom de *moonshine* (clair de lune). Pour avoir expliqué beaucoup des questions liées au moonshine, Richard Borcherds a reçu la médaille Fields en 1998.

10.2 Groupes cycliques

Soit G un groupe. Si $H_i \subseteq G,\ i \in I$ est une famille de sous-groupes de G, alors on vérifie aisément que

$$H = \bigcap_{i \in I} H_i \subseteq G$$

est encore un sous-groupe de G. Par conséquent pour $U \subset G$, on peut définir le le sous-groupe de G *engendré* par U par

$$\langle U \rangle = \bigcap_{\substack{H \text{ sous-groupe de } G \\ U \subset H}} H$$

C'est aussi le plus petit sous-groupe de G contenant U.

LEMME 10.2.1. — On a

$$\langle U\rangle = \{x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_k^{\varepsilon_k} \mid k\geq 0,\ x_1,\cdots,x_k\in U,\ \varepsilon_1,\cdots,\varepsilon_k=\pm 1\}.$$

Dans le cas particulier où $U=\{x\}$, on note $\langle x\rangle = \langle\{x\}$ le sous-groupe engendré par l'élément x. On a alors

$$\langle x\rangle = \{x^k; k\in\mathbb{Z}\}\subseteq G.$$

DÉFINITION 10.2.2. — Un groupe G est dit *cyclique* s'il existe $x\in G$ tel que $G=\langle x\rangle$. De même, un sous-groupe $H\subseteq G$ est dit cyclique s'il existe $x\in H$ tel que $H=\langle x\rangle$.

LEMME 10.2.3. — Soit $(G,\times)$ un groupe cyclique. Alors

$$\begin{array}{lll} |G|=+\infty & \Longrightarrow & (G,\times)\simeq(\mathbb{Z},+)\\ |G|=n<+\infty & \Longrightarrow & (G,\times)\simeq(\mathbb{Z}/n\mathbb{Z},+).\end{array}$$

En particulier, G est abélien.

Démonstration. Si $G=\langle x\rangle$, on a un morphisme de groupes surjectif

$$\begin{array}{rccc} f: & (\mathbb{Z},+) & \longrightarrow & (G,\times)\\ & k & \longmapsto & x^k\end{array},$$

induisant un isomorphisme $(\mathbb{Z}/\operatorname{Ker} f,+)\simeq(G,\times)$. □

On en déduit immédiatement la classification des groupes d'ordre premier.

COROLLAIRE 10.2.4. — Un groupe G est d'ordre p premier si et seulement si G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Démonstration. Soit $x\in G\setminus\{e\}$, et soit $H=\langle x\rangle < H$. Comme $x\neq e$, on a $H\neq\{e\}$. Mais comme l'ordre de H divise l'ordre de G qui est premier, on a $|H|=p$, c'est à dire $H=G$. Donc G est cyclique d'ordre p, isomorphe à $\mathbb{Z}/p\mathbb{Z}$ par le Lemme 10.2.3. □

REMARQUE 10.2.5. — Le Corollaire 10.2.4 est faux sans l'hypothèse $|G|$ premier. Par exemple, le groupe à 4 éléments $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ n'est pas isomorphe à $\mathbb{Z}/4\mathbb{Z}$. En effet, tous les éléments du premier groupe sont d'ordre au plus 2, alors que 1 est d'ordre 4 dans le second. On remarque donc au passage que

$$H\lhd G \not\Longrightarrow G\simeq H\times G/H.$$

En théorie des groupes, on prendra donc bien garde à ne pas faire de "simplifications" hâtives inspirées de l'arithmétique des entiers (où par exemple $6=3\times 6/3$).

On comprend parfaitement les sous-groupes d'un groupe cyclique.

PROPOSITION 10.2.6. — Tout sous-groupe H d'un groupe cyclique G est cyclique. De plus si $|G|=n<+\infty$, alors G contient un unique sous-groupe d'ordre d pour tout diviseur d de n.

Démonstration. La proposition est connue si $G \simeq \mathbb{Z}$. On suppose donc maintenant $G = \mathbb{Z}/n\mathbb{Z}$ avec $n \neq 0$, et on note $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ l'application quotient. Si $H < G$, alors $\pi^{-1}(H) = m\mathbb{Z}$ avec $m|n$ (puisque $n\mathbb{Z} \subset m\mathbb{Z}$). Donc $H = m\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\frac{n}{m}\mathbb{Z}$ est bien cyclique. On a montré que $|H| = d$ si et seulement si $\pi^{-1}(H) = \frac{n}{d}\mathbb{Z}$, ce qui assure bien l'unicité de $H < G$ de cardinal d. □

Corollaire 10.2.7. — Soit G un groupe abélien. Alors G est simple si et seulement si G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

Démonstration. Le groupe $\mathbb{Z}/p\mathbb{Z}$ avec p premier est simple par le théorème de Lagrange. Réciproquement, supposons G simple, et soit $x \in G \setminus \{e\}$. Comme G est abélien, on a $\langle x \rangle \lhd G$, et donc $\langle x \rangle = G$ par simplicité de G. Donc G est cyclique, et même fini puisque $\mathbb{Z}$ n'est pas simple (par exemple il contient $2\mathbb{Z}$ comme sous-groupe non trivial). D'après la Proposition 10.2.6, le groupe $\mathbb{Z}/n\mathbb{Z}$ contient un sous-groupe non trivial si n n'est pas premier, et n'est donc pas simple. Le groupe G est donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$ avec p premier. □

10.3 Groupes symétriques

Le calcul dans le groupe symétrique a été pratiqué en licence. Nous en rappelons cependant les règles les plus importantes pour fixer les notations. Étant donné $n \in \mathbb{N}$, le groupe symétrique $\mathfrak{S}_n$ est l'ensemble des bijections de l'ensemble $X_n = \{1, \ldots, n\}$ avec pour structure de groupe la composition des bijections. Ses éléments sont appelés des *permutations*. Le groupe $\mathfrak{S}_n$ est clairement fini de cardinal $n!$.

Pour toute suite $(n_1, \ldots, n_k)$ d'éléments deux à deux différents de X_n on note $\sigma = (n_1 \ldots n_k)$ la permutation définie dans $\mathfrak{S}_n$ par :

$$\sigma(i) = \begin{cases} n_{j+1}, \text{ si } i = n_j, j < k, \\ n_1, \text{ si } i = n_k, \\ i \text{ sinon.} \end{cases}$$

Si $k = 1$, *i.e.* pour $(1) = (2) = \ldots$ on trouve par convention l'identité. Les permutations de cette forme s'appellent des *k-cycles* ; les 2-cycles s'appellent des transpositions. Il est clair par définition que $(n_1 \ldots n_k) = (n_k\, n_1 \ldots n_{k-1})$ (d'où le nom de cycle). Deux cycles $(n_1 \ldots n_k)$ et $(m_1 \ldots m_\ell)$ sont *disjoints*, si les ensembles $\{n_1, \ldots, n_k\}$ et $\{m_1, \ldots, m_\ell\}$ sont disjoints (dans X_n). Dans ce cas, ces deux cycles commutent :

$$(n_1 \ldots n_k)(m_1 \ldots m_\ell) = (m_1 \ldots m_\ell)(n_1 \ldots n_k)$$

puisqu'ils opère sur des sous-ensemble différents de X_n. Finalement, si l'inverse du cycle $(n_1 \ldots n_k)$ est donné par le cycle $(n_k \ldots n_1)$.

Proposition 10.3.1. — Toute permutation $\sigma \in \mathfrak{S}_n$ s'écrit de manière unique (à ordre des facteurs près) comme produit de cycles disjoints.

Démonstration. Les ensembles $U_i = \{\sigma^k(i) \mid k \in \mathbb{Z}\}$ avec $i \in \{1, \cdots, n\}$ fournissent une partition $B_1, \ldots, B_s$ de $i \in \{1, \cdots, n\}$. En d'autres termes, U_i et U_j sont soit confondus,

soit disjoints. On pose $\lambda_i = |B_i|$, et on peut supposer sans perte de généralité que $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_s$. Les B_i formant une partition de $i \in \{1, \cdots, n\}$, on a $\sum \lambda_i = n$.
Tout ensemble B_i définit de un λ_i-cycle ζ_i comme suit : pour $x \in B_i$ quelconque on pose $\zeta_i = (x\, \sigma(x)\, \sigma^2(x) \ldots \sigma^{\lambda_i - 1}(x))$. Les cycles $\zeta_1, \zeta_2, \ldots, \zeta_s$ sont deux à deux disjoints et nous avons $\sigma = \zeta_1 \zeta_2 \ldots \zeta_s$. □

On appelle une suite de nombre naturels $n_1 \geq n_2 \geq \cdots \geq n_s \geq 1$ une *partition* de l'entier $n = \sum_{i=1}^{s} n_i$, notée $[n_1, \cdots, n_s]$. Nous associons ainsi une partition $\lambda(\sigma) = [\lambda_1, \cdots, \lambda_s]$ de n à toute permutation $\sigma \in \mathfrak{S}_n$, qu'on appellera le *type de cycle* de σ.
L'écriture en cycle disjoints est extrêmement efficace et permet entre autres de lire le type de cycle directement en regardant les longueurs de cycles. Par exemple, le type de cycle de $(145)(27) \in \mathfrak{S}_8$ est la partition $[3, 2, 1, 1, 1]$. Réciproquement, on voit bien que toute partition de n apparaît comme type de cycles d'une permutation.
Le lemme suivant se démontre par un calcul direct.

Lemme 10.3.2. — Soit σ une permutation et $(n_1 \ \ldots \ n_k)$ un k-cycle de $\mathfrak{S}_n$. Alors on a

$$\sigma \cdot (n_1 \ \ldots \ n_k) \cdot \sigma^{-1} = (\sigma(n_1) \ \ldots \ \sigma(n_k)).$$

Corollaire 10.3.3. — Deux permutations $\sigma, \sigma' \in \mathfrak{S}_n$ sont conjuguées si, et seulement si, ils ont le même type de cycle. En particulier, l'application

$$\begin{array}{rcl} \{\text{classes de conjugaisons de } \mathfrak{S}_n\} & \to & \{\text{partitions de } n\} \\ \sigma & \mapsto & \lambda(\sigma), \end{array}$$

est une bijection.

On définit la *signature* d'une permutation σ de partition associée $[\lambda_1, \cdots, \lambda_s]$ par

$$\varepsilon(\sigma) = (-1)^{\sum_{i=1}^{s} (\lambda_i - 1)}.$$

Le théorème suivant est fondamental en mathématiques.

Théorème 10.3.4. — L'application $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ est un morphisme de groupes.

On définit le groupe alterné $\mathfrak{A}_n \lhd \mathfrak{S}_n$ comme le noyau de ε, et ses éléments sont appelés *permutations paires*. Il est facile de voir que la signature est surjective sur $\{\pm 1\}$ pour $n \geq 2$. En particulier, le groupe $\mathfrak{A}_n$ a $\frac{1}{2}n!$ éléments pour $n \geq 2$, et $\mathfrak{S}_n$ n'est pas simple pour $n \geq 3$.

Exemple 10.3.5. — On a

$$\begin{array}{lll} n = 1 : & \mathfrak{S}_1 = \{Id\} & \mathfrak{A}_1 = \{Id\} \\ n = 2 : & \mathfrak{S}_2 = \{Id, (12)\} \simeq \mathbb{Z}/2\mathbb{Z} & \mathfrak{A}_2 = \{Id\} \\ n = 3 : & \mathfrak{S}_3 = \{Id, (12), (13), (23), (123), (132)\} & \mathfrak{A}_3 = \{Id, (123), (132)\} \simeq \mathbb{Z}/3\mathbb{Z} \end{array}$$

On voit facilement que $\mathfrak{S}_n$ est commutatif si et seulement si $n \leq 2$ (si $n \geq 3$, nous avons par exemple $(13) \cdot (12) \cdot (13)^{-1} = (23)$), et que $\mathfrak{A}_n$ est commutatif si et seulement si $n \leq 3$

(si $n \geq 4$, nous avons par exemple $(124) \cdot (123) \cdot (124)^{-1} = (243)$). De plus $\mathfrak{A}_n$ est simple si $n \leq 3$. Le groupe $\mathfrak{A}_4$ admet un sous-groupe distingué propre non trivial :

$$V_4 = \{Id, (12)(34), (13)(24), (14)(23)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Que V_4 est effectivement un sous-groupe se voit par calcul direct. Comme V_4 est constitué exactement des éléments de $\mathfrak{S}_4$ de type de cycle $[1,1,1,1]$ et $[2,2]$, il est distingué dans $\mathfrak{S}_4$ par la proposition 10.3.3. Le groupe V_4 est donc aussi distingué dans $\mathfrak{A}_4$, et $\mathfrak{A}_4$ n'est donc pas simple.

PROPOSITION 10.3.6. — a) Le groupe $\mathfrak{S}_n$ est engendré par les transpositions pour $n \geq 2$.

b) Le groupe alterné $\mathfrak{A}_n$ est engendré par les 3-cycles pour $n \geq 3$.

Démonstration. a) Il suffit de le montrer pour les k-cycles pour lesquels c'est conséquence de la relation $(n_1 \ \ldots \ n_k) = (n_1 n_2)(n_2 \ \ldots \ n_k)$.

b) Nous savons déjà que tout élément de $\mathfrak{A}_n$ s'écrit comme produit d'un nombre pair de transpositions. Il suffit donc de montrer la proposition pour les produits de deux transpositions. Plusieurs cas se présentent. Le cas $(ab)(ab) = 1$ est clair puisque $1 = (123)^3$. Dans le cas $(ab)(bc)$ avec $a \neq c$, on observe $(ab)(bc) = (abc)$. Finalement, il reste le cas $(ab)(cd)$ avec a, b, c, d distincts. Mais alors on a $(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)$. □

THÉORÈME 10.3.7. — Le groupe $\mathfrak{A}_n$ est simple pour $n \geq 5$.

Démonstration. Observons d'abord que tous les 3-cycles sont conjugués dans $\mathfrak{A}_n$ pour $n \geq 5$. Soit $\zeta_1 = (abc)$ et $\zeta_2 = (def)$ deux 3-cycles. Comme ils ont le même type de cycle, ils sont conjugués dans $\mathfrak{S}_n$, il existe donc une permutation $\sigma \in \mathfrak{S}_n$ telle que $\zeta_2 = \sigma\zeta_1\sigma^{-1}$. Puisque $n \geq 5$, il existe une transposition (xy) qui commute avec ζ_1. Pour $\mu = \sigma(xy)$, on a aussi $\zeta_2 = \sigma\mu\zeta_1\mu^{-1}\sigma^{-1}$. Une des deux permutations σ ou $\sigma(xy)$ étant dans $\mathfrak{A}_n$, ζ_1 et ζ_2 sont bien conjugués dans $\mathfrak{A}_n$.

Soit maintenant $\{Id\} \neq H \lhd \mathfrak{A}_5$. Si H contient un 3-cycle, alors H contient tous les 3-cycles par la remarque précédente. Mais nous avons vu dans la proposition 10.3.6 que $\mathfrak{A}_n$ est engendré par les 3-cycles, et donc $H = \mathfrak{A}_n$. Pour démontrer la proposition, il reste donc de montrer que H contient nécessairement un 3-cycle. Soit $\sigma \in H \setminus \{Id\}$.

Si σ contient un cycle z de longueur $m \geq 4$ dans sa décomposition en cycles disjoints, on peut, pour simplifier, supposer que $z = (12\cdots m)$. Alors H contient aussi l'élément $(123)\sigma(123)^{-1}\sigma^{-1} = (124)$, et donc $H = \mathfrak{A}_n$.

Supposons maintenant que σ contient un 3-cycle ainsi qu'un cycle disjoint de longueur 2 ou 3, par exemple $\sigma = (123)(45\cdots)\cdots$. Alors H contient aussi $(124)\sigma(124)^{-1}\sigma^{-1} = (12534)$, et donc $H = \mathfrak{A}_n$ par le cas précédent.

Supposons σ contient deux transposition disjointes, par exemple $\sigma = (12)(34)$. Alors H contient aussi $(125)\sigma(125)^{-1}\sigma^{-1} = (152)$, et encore une fois $H = \mathfrak{A}_n$. □

11 Théorèmes de Sylow

Les Théorèmes de Sylow donnent beaucoup d'informations sur la structure des groupes finis. Dans un premier temps, nous énoncerons ces théorèmes et en donnerons des applications. Nous démontrerons les Théorèmes de Sylow ensuite, après avoir fait quelques rappels sur les actions de groupes.

11.1 Théorèmes de Sylow - énoncé

Définition 11.1.1. — Un groupe de cardinal p^k, avec p un nombre premier, est appelé un *p-groupe*.
Soit G un groupe d'ordre $p^m u$, où p est un nombre premier ne divisant pas u. Un sous-groupe $H < G$ d'ordre p^m est appelé *p-sous-groupe de Sylow*, ou encore p-Sylow, de G.

On note N_p le nombre de p-Sylow de G. Le théorème suivant, contenant les 3 théorèmes de Sylow, montre que les nombres N_p possibles sont étroitement liés aux propriétés arithmétiques de $|G|$, et donnent beaucoup d'informations sur la structure du groupe G.

Théorème 11.1.2 (Sylow). — Soit G un groupe d'ordre $p^m u$, où p est un nombre premier ne divisant pas u. Alors

a) Il existe un p-Sylow de G ; plus précisément $N_p = 1 \bmod p$ et $N_p | \, u$;
b) Tout p-sous-groupe de G est contenu dans un p-Sylow ;
c) Tous les p-Sylow de G sont conjugués.

Une conséquence très importante de ce théorème est qu'un p-Sylow d'un groupe fini G est distingué dans G si et seulement si $N_p = 1$. Avant de prouver le Théorème 11.1.2, nous illustrons son utilisation par deux exemples.

Proposition 11.1.3. — Un groupe d'ordre pq avec p et q deux nombres premiers distincts n'est pas simple.

Démonstration. On peut supposer $p < q$. Par le Théorème 11.1.2, nous avons $N_q = 1 \bmod q$ et $N_q | p$. On a donc nécessairement $N_q = 1$, et le groupe admet un sous-groupe distingué non-trivial. □

Proposition 11.1.4. — Tout groupe d'ordre 6 est isomorphe soit à $\mathbb{Z}/6\mathbb{Z}$, soit à $\mathfrak{S}_3$.

Démonstration. On remarque que $\mathbb{Z}/6\mathbb{Z}$ et $\mathfrak{S}_3$ sont bien deux groupes d'ordre 6, non isomorphes puisque le premier est abélien et pas le deuxième. Soit G un groupe d'ordre 6. Comme $6 = 2 \times 3$, le Théorème 11.1.2 nous donne en particulier que

$$N_2 = 1 \bmod 2 \text{ et } N_2 | 3, \qquad N_3 = 1 \bmod 3 \text{ et } N_3 | 2.$$

On déduit que $N_3 = 1$, et on note H_3 le 3-Sylow de G. On a donc $H_3 \lhd G$, et $H \simeq \mathbb{Z}/3\mathbb{Z}$ d'après le Corollaire 10.2.4. On a aussi $N_2 = 1$ ou $N_2 = 3$, nous traitons ces deux cas l'un après l'autre.

a) Supposons $N_2 = 1$, et notons $H_2 \lhd G$ le 2-Sylow de G. On a $H_2 \simeq \mathbb{Z}/2\mathbb{Z}$ et $H_2 \cap H_3 = \{e\}$, tout élément de $H_2 \cap H_3$ devant être d'ordre 1 car divisant 2 et 3. Notons de plus que les éléments de H_2 et H_3 commutent dans G : si $x \in H_2$ et $y \in H_3$, alors $xyx^{-1}y^{-1}$ est à la fois dans H_2 puisque $xyx^{-1}x^{-1} = x(yx^{-1}y^{-1})$, et dans H_3 puisque $xyx^{-1}x^{-1} = (xyx^{-1})y^{-1}$; on en déduit donc que $xyx^{-1}y^{-1} = e$, c'est à dire $xy = yx$. L'application

$$\begin{array}{rccc} \phi : & H_2 \times H_3 & \longrightarrow & G \\ & (x, y) & \longmapsto & xy \end{array}$$

vérifie alors $\phi((x, y)(x', y')) = \phi((x, y))\phi((x', y'))$, c'est à dire est un morphisme de groupes. Elle est de plus injective car $H_2 \cap H_3 = \{e\}$. Les deux groupes $H_2 \times H_3$ et G étant de cardinal 6, elle est donc aussi surjective. Nous avons ainsi montré

$$G \simeq H_2 \times H_3 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}.$$

b) Supposons $N_2 = 1$, et notons K_1, K_2 et K_3 les 2-Sylow de G. La conjugaison induit un morphisme de groupe

$$\begin{array}{rccc} \phi : & G & \longrightarrow & Bij(\{K_1, K_2, K_3\}) \simeq \mathfrak{S}_3 \\ & x & \longmapsto & (K_i \mapsto xK_ix^{-1}) \end{array}.$$

D'après le Théorème 11.1.2, l'image de ϕ doit être au moins de cardinal 3, et donc $|\operatorname{Ker}\phi| \leq 2$. Aucun des 2-Sylow K_i n'étant distingué dans G, on a nécessairement $|\operatorname{Ker}\phi| = 1$, i.e. ϕ est injective. Les deux groupes G et $\mathfrak{S}_3$ étant de cardinal 6, nous avons cette fois ci montré

$$G \simeq \mathfrak{S}_3.$$

□

11.2 Actions de groupe sur un ensemble - rappels

Une *action (à gauche)* du groupe G sur l'ensemble X est une application

$$\varphi : G \times X \to X$$

telle que $\varphi(e, x) = x$ et $\varphi(g, \varphi(h, x)) = \varphi(gh, x)$ pour tout $g, h \in G$, $x \in X$. Souvent on note φ par un point, *i.e.* $g.x$ au lieu de $\varphi(g, x)$, pour exprimer de manière plus suggestive que G *opère* sur X. Avec cette notation, les conditions ci-dessus s'expriment par $e.x = x$ et $g.(h.x) = (gh).x$ pour tout $g, h \in G$, $x \in X$.

Si X est un ensemble, on note $\mathfrak{S}_X$ l'ensemble des bijections de X. Si G opère sur X, on peut définir une application

$$\begin{array}{rccc} \rho : & G & \longrightarrow & \mathfrak{S}_X \\ & g & \longmapsto & (x \mapsto g.x) \end{array}.$$

On remarque d'abord que cette application est bien définie : en effet, $x \mapsto g.x$ est bien une bijection de X (de bijection inverse $x \mapsto g^{-1}.x$). La condition $e.x = x$ pour tout x signifie que $\rho(e) = \mathrm{Id}_X$; la condition $g.(h.x) = (gh).x$ pour tout $g, h \in G$, $x \in X$ dit

$\rho(gh) = \rho(g)\rho(h)$. Ainsi ρ est un morphisme de groupes. Réciproquement, si l'on se donne un morphisme de groupes $\rho : G \to \mathfrak{S}_X$, alors $g.x := \rho(g)(x)$ définit une action de groupes de G sur X.
Soit G un groupe agissant sur un ensemble X. *L'orbite* de $x \in X$ est le sous-ensemble

$$Gx := Orb^G(x) := \{gx \,|g \in G\} \subseteq X;$$

Le *stabilisateur* de $x \in X$ est le sous-groupe

$$G_x := Stab^G(x) := \{g \in G \mid gx = x\} \subseteq G$$

L'espace des orbites est l'ensemble des orbites et sera noté par X/G. La projection canonique $\pi : X \to X/G$ envoie tout élément x sur son orbite. On dira qu'une action est *transitive* si tout les éléments de X sont dans une même orbite. On dira qu'elle elle est *libre*, si tous les stabilisateurs sont triviaux. Finalement, $x \in X$ est un *point fixe* si $Gx = \{x\}$, ou autrement dit si $G_x = \{e\}$. L'ensemble des tous les points fixes est noté X^G.

Entre les cardinaux de X et de ses orbites et les ordres de G et des stabilisateurs, il y a des relations qui sont précisées par *l'équation des orbites :*

Proposition 11.2.1. — Soit G un groupe fini agissant sur X. Alors
a) $|X| = \sum_{B \in X/G} |B|$ si X est aussi fini ;
b) $|G| = |G_x| \cdot |Gx|$ pour tout $x \in X$.

Démonstration. Tout élément de X est exactement dans une orbite. L'ensemble X est donc la réunion disjointe de tous les orbites, d'où la première relation en passant aux cardinaux. Soit maintenant $x \in X$ quelconque et regardons l'application $p : G \to Gx$, $g \mapsto gx$. Par construction, p est surjective. Soit $y \in Gx$ quelconque et $g_0 \in p^{-1}(y)$. Alors $g \in p^{-1}(y)$ si, et seulement si, $gx = g_0x$, *i.e.* $(g_0)^{-1}gx = x$, d'où $(g_0)^{-1}g \in G_x$ ou autrement dit $g \in g_0G_x$. En particulier, on a $|p^{-1}(y)| = |G_x|$ pour tout $y \in Gx$. Ainsi

$$|G| = \sum_{y \in Gx} |p^{-1}(y)| = |Gx| \cdot |G_x|,$$

d'où la seconde relation. □

Exemple 11.2.2. — Le groupe symétrique $\mathfrak{S}_n$ des bijections de $X_n = \{1, \ldots, n\}$ opère sur l'ensemble $\{1, \cdots, n\}$ par $(\sigma, k) \mapsto \sigma(k)$. L'opération est transitive : si $x, y \in X_n$ sont distincts, la transposition $\tau = (x\, y)$ envoie l'élément x sur y. Ainsi tous les éléments sont dans la même orbite. Le stabilisateur de tout élément x est isomorphe au groupe symétrique $\mathfrak{S}_{n-1}$.

On déduit de la proposition 11.2.1 le lemme suivant, qui sera un point clef dans la démonstration des Theorèmes de Sylow, ou plus généralement dans l'étude des p-groupes.

Lemme 11.2.3. — Soit p un nombre premier et G un p-groupe opérant sur un ensemble fini X. Alors on a

$$|X| \equiv |X^G| \bmod p,$$

où X^G désigne l'ensemble des points fixes de X sous l'action de G.

Démonstration. Soient $B_i \subseteq X$, $i = 1, \dots, n$, les orbites sous l'action de G. On choisit pour tout i un élément $b_i \in B_i$ et on désigne par G_i le stabilisateur G_{b_i}. D'après l'équation des orbites, nous avons

$$|X| = \sum_i |B_i| \text{ et } |B_i| = |G|/|G_i|.$$

Les points fixes sous l'action correspondent aux orbites de longueur 1. Pour tous les autres orbites, $|B_i|$ est un diviseur non trivial de $|G|$ et donc divisible par p aussi, d'où la proposition. □

11.3 Théorèmes de Sylow - preuve

La preuve du Théorème 11.1.2 est extrêmement astucieuse, et repose sur le choix d'actions de groupes bien choisies.

Étape 1. Considérons l'ensemble X des sous-ensembles de G ayant p^m éléments. Le groupe G opère sur X par translation à gauche : pour $Y = \{y_1, \dots, y_{p^m}\} \in X$ et $g \in G$ on a $g.Y = \{gy_1, \dots, gy_{p^m}\}$.
Soit $H = G_Y$ le stabilisateur de Y. Comme dans la preuve du Théorème de Lagrange, les ensembles Hy pour $y \in Y$ ont tous le même cardinal et forment une partitions de Y. Ainsi $|H|$ divise $|Y| = p^m$, et le groupe H est un p-groupe.
On a de plus $|G| = |G_Y| \cdot |GY|$, d'où l'on déduit que G_Y est un p-Sylow de G si et seulement si $|GY| = u$, ou encore si et seulement si p ne divise pas $|GY|$.
Soit $X_0 \subseteq X$ l'ensemble des éléments de X dont l'orbite est de cardinal u. De même que dans la preuve du Lemme 11.2.3, l'équation des orbites nous donne l'égalité

$$|X| = |X_0| \bmod p.$$

LEMME 11.3.1. — Soit p un nombre premier, $u \in \mathbb{N}$ et $0 \leq k \leq m$. Alors

$$\binom{u}{k} \equiv \binom{up^m}{kp^m} \bmod p$$

Démonstration. Pour $k \in \{1, \cdots, p-1\}$, le nombre premier p ne divise ni $k!$ ni $(p-k)!$. Comme p divise $p!$, on déduit du Lemme de Gauss que p divise $\binom{p}{k}$. On a ainsi

$$(x+y)^p = x^p + y^p \bmod p.$$

Par récurrence, nous avons donc $(x+y)^{p^m} = x^{p^m} + y^{p^m} \bmod p$ et finalement

$$(x+y)^{up^m} = (x^{p^m} + y^{p^m})^u \bmod p.$$

En faisant l'expansion à gauche et à droite par la formule du binôme, le lemme suit en comparant les coefficients de chaque coté. □

Puisque $|X| = \binom{p^m u}{p^m} = u \bmod p \neq 0 \bmod p$, on conclu que $|X_0| \neq 0$. En d'autres termes il existe un p-Sylow de G.

Étape 2. Soit $S < G$ un p-Sylow et $H < G$ un p-sous-groupe quelconque. Nous allons appliquer le Lemme 11.2.3 directement sur l'action de H sur l'ensemble G/S par multiplication à gauche. Comme

$$|G/S| = |G|/|S| = u \not\equiv 0 \bmod p,$$

il existe un point fixe $yS \in G/S$, *i.e.* une classe à droite yS avec $HyS = yS$. Mais ceci signifie que $y^{-1}Hy \subseteq S$ ou autrement dit $H \subseteq ySy^{-1}$. Ainsi H est contenu dans le p-Sylow ySy^{-1}.
Dans le cas où H est lui même un p-Sylow, on obtient une inclusion $H \subseteq ySy^{-1}$ entre groupes de même cardinal. Cette inclusion est donc une égalité, et H et S sont conjugués dans G.

Étape 3. On considère maintenant l'action de G par conjugaison sur l'ensemble $\mathcal{S}_p$ des p-Sylow de G : $(g, S) \mapsto gSg^{-1}$ pour $g \in G$ et $S \in \mathcal{S}_p$. Nous venons de voir que tous les p-Sylow sont conjugués, c'est à dire qu'il n'existe qu'une seule orbite pour cette action. Ainsi $N_p = |\mathcal{S}_p|$ divise $|G|$.

Étape 4. Étant donné un p-Sylow S_0 de G, on considère la restriction de l'action précédente à S_0 : $(g, S) \mapsto gSg^{-1}$ pour $g \in S_0$ et $S \in \mathcal{S}_p$. Nous allons montrer que S_0 est le seul point point fixe de $\mathcal{S}_p$ pour l'action de S_0. Le Lemme 11.2.3 impliquera alors

$$N_p = 1 \bmod p.$$

En particulier p ne divise pas N_p. Puisque N_p divise $p^m u$ par l'étape 3, on en déduit alors que

$$N_p | u.$$

Soit donc S un point fixe pour l'action de S_0 sur $\mathcal{S}_p$, c'est à dire

$$\forall g \in S_0, \quad gSg^{-1} = S.$$

Les groupes S et S_0 sont encore des p-Sylow du groupe $\langle S \cup S_0 \rangle < G$. Donc par ce qui précède, ils sont conjugués dans $\langle S \cup S_0 \rangle$. Par hypothèse, on a $gSg^{-1} = S$ pour tout $g \in S_0$. Comme on a aussi $gSg^{-1} = S$ pour tout $g \in S$, on en déduit que S est distingué dans $\langle S \cup S_0 \rangle$. Les groupes S et S_0 étant conjugués dans $\langle S \cup S_0 \rangle$, on obtient alors $S = S_0$.

12 Produit semi-direct de groupes

12.1 Produit semi-direct - version plongée

Étant donné un espace vectoriel E et deux sous-espaces vectoriels F et G, on sait que l'on a $E = F \oplus G$ si et seulement si $F \cap G = \{0\}$ et $E = F + G$. Les choses ne sont malheureusement pas aussi simples en théorie des groupes. Nous avons néanmoins le résultat suivant, dont la preuve est identique à une partie de la preuve de la Proposition 11.1.4.

PROPOSITION 12.1.1. — Soit G un groupe, et $H, K \lhd G$ deux sous-groupes distingués vérifiant $H \cap K = \{e\}$ et $G = HK$. Alors l'application

$$\begin{array}{rccc} \phi : & H \times K & \longrightarrow & G \\ & (h,k) & \longmapsto & hk \end{array}$$

est un isomorphisme de groupe.

Démonstration. De même que pour les groupes H_2 et H_3 dans la preuve de la Proposition 11.1.4, on montre que les éléments de H et K commutent. L'application ϕ est donc un morphisme de groupe, qui est bijectif par hypothèse. □

Si un seul des deux groupes H ou K est distingué dans G, alors G est toujours isomorphe au produit $H \times K$, mais maintenant muni d'une *autre* structure de groupe que la structure produit.

THÉORÈME 12.1.2. — Soit G un groupe, et $H \lhd G$ et $K < G$ deux sous-groupes vérifiant $H \cap K = \{e\}$ et $G = HK$. Alors $H \times K$ muni de la loi

$$(h,k)(h',k') = (hkh'k^{-1}, kk')$$

est un groupe, et l'application

$$\begin{array}{rccc} \phi : & H \times K & \longrightarrow & G \\ & (h,k) & \longmapsto & hk \end{array}$$

est un isomorphisme de groupe.
On dit alors que G est le produit semi-direct de H par K, noté $G = H \rtimes K$.

Si les éléments de K et G commutent, alors la loi de groupe de $H \rtimes K$ est simplement la loi produit, c'est à dire $H \rtimes K = H \times K$ comme groupes.

Démonstration. Vérifions que $H \rtimes K$ est bien un groupe.
a) Associativité :

$$\begin{aligned} (h,k)\Big((h',k')(\widetilde{h},\widetilde{k})\Big) &= (h,k)(h'k'\widetilde{h}k'^{-1}, k'\widetilde{k}) \\ &= (hkh'k'\widetilde{h}k'^{-1}k^{-1}, kk'\widetilde{k}) \\ &= (hkh'k^{-1}kk'\widetilde{h}k'^{-1}k^{-1}, kk'\widetilde{k}) \\ &= (hkh'k^{-1}, kk')(\widetilde{h},\widetilde{k}) \\ &= \Big((h,k)(h',k')\Big)(\widetilde{h},\widetilde{k}) \end{aligned}$$

b) L'élément (e, e) est clairement neutre.
c) On vérifie aisément que l'inverse est (h, k) est $(k^{-1}h^{-1}k, k^{-1})$.

Vérifions ensuite que ϕ est bien un morphisme de groupes :

$$\phi\Big((h,k)(h',k')\Big) = \phi(hkh'k^{-1}, kk') = hkh'k' = \phi((h,k))\phi((h',k')).$$

De plus ϕ est bijectif par hypothèse, c'est donc bien un isomorphisme de groupe. □

De nombreux groupes, quand ils ne sont pas des produits directs de groupes sympathiques, en sont souvent un produit semi-direct.

EXEMPLE 12.1.3. — On a $\mathfrak{A}_n \lhd \mathfrak{S}_n$ et $\mathfrak{S}_n/\mathfrak{A}_n = \mathbb{Z}/2\mathbb{Z}$. Pour $K = \{Id, (12)\}$, on a bien $\mathfrak{A}_n \cap K = \{Id\}$ et $\mathfrak{A}_n K = \mathfrak{S}_n$, et donc $\mathfrak{S}_n = \mathfrak{A}_n \rtimes K$.

EXEMPLE 12.1.4. — Soit $G = Aff(\mathbb{R}^n)$ le groupe des transformations affines bijectives de $\mathbb{R}^n$. On a un morphisme de groupe

$$\begin{array}{ccc} Aff(\mathbb{R}^n) & \longrightarrow & GL_n(\mathbb{R}) \\ f & \longmapsto & \vec{f} \end{array}$$

dont le noyau est précisément le sous-groupe $\mathcal{T}$ des translations. On a ainsi $Aff(\mathbb{R}^n) = \mathcal{T} \rtimes GL_n(\mathbb{R})$.

REMARQUE 12.1.5. — Étant donné $H \lhd G$, on peut se demander si il existe $K < G$ tel que $G = H \rtimes K$. Il est facile de voir que c'est le cas si et seulement si la projection canonique $\pi : G \to G/H$ admet une section, c'est à dire si il existe un morphisme de groupes $s : G/H \to G$ tel que $\pi \circ s = Id_{G/H}$. Dans ce cas, il suffit de prendre $K = \text{Im } s$. L'existence d'une telle section n'est jamais garantie, comme le montre l'exemple $G = \mathbb{Z}/4\mathbb{Z}$, le sous-groupe $H =< 2 >$ et $G/H \simeq \mathbb{Z}/2\mathbb{Z}$.

12.2 Produit semi-direct - version abstraite

La définition précédent du produit semi-direct $H \rtimes K$ nécessite d'avoir au départ un groupe G ambiant. Un autre point de vue est de partir de deux groupes abstraits H et K, et de construire le groupe G comme l'ensemble $H \times K$ d'une structure de groupe potentiellement différente de la structure produit.
Pour cela, on remarque que dans le cas où G est donné et $H \lhd G$ et $K < G$, on peut réécrire le produit sur $H \rtimes K$ comme

$$(h,k)(h',k') = (h\rho_k(h'), kk'),$$

où

$$\rho_k(h') = kh'k^{-1}.$$

On a alors $\rho_k \in Aut(H)$, et l'application

$$\begin{array}{rccc} \rho : & K & \longrightarrow & Aut(H) \\ & k & \longmapsto & \rho_k \end{array}$$

est un morphisme de groupes. Cette observation se généralise dans le théorème suivant.

THÉORÈME 12.2.1. — Soit H et K deux groupes et

$$\begin{array}{rccc} \rho: & K & \longrightarrow & Aut(H) \\ & k & \longmapsto & \rho_k \end{array}$$

un morphisme de groupes. Alors l'ensemble $H \times K$ muni de la loi

$$(h,k)(h',k') = (h\rho_k(h'), kk')$$

est un groupe, appelé produit semi-direct de H par K et noté $H \rtimes_\rho K$.

On note souvent $H \rtimes K$ au lieu de $H \rtimes_\rho K$ si le morphisme ρ est clair.

Démonstration. Il s'agit encore une fois de vérifications formelles sans difficultés.
a) Associativité :

$$\begin{aligned} (h,k)\Big((h',k')(\widetilde{h},\widetilde{k})\Big) &= (h,k)(h'\rho_{k'}(\widetilde{h}), k'\widetilde{k}) \\ &= (h\rho_k(h'\rho_{k'}(\widetilde{h})), kk'\widetilde{k}) \\ &= (h\rho_k(h')\rho_k \circ \rho_{k'}(\widetilde{h})), kk'\widetilde{k}) \\ &= (h\rho_k(h')\rho_{kk'}(\widetilde{h})), kk'\widetilde{k}) \\ &= (h\rho_k(h'), kk')(\widetilde{h},\widetilde{k}) \\ &= \Big((h,k)(h',k')\Big)(\widetilde{h},\widetilde{k}) \end{aligned}$$

b) L'élément (e_H, e_K) est clairement neutre.
c) On vérifie aisément que l'inverse est (h,k) est $(\rho_{k^{-1}}(h^{-1}), k^{-1})$.
Vérifions ensuite que ϕ est bien un morphisme de groupes :

$$\phi\Big((h,k)(h',k')\Big) = \phi(hkh'k^{-1}, kk') = hkh'k' = \phi((h,k))\phi((h',k')).$$

De plus ϕ est bijectif par hypothèse, c'est donc bien un isomorphisme de groupe. □

EXEMPLE 12.2.2. — Si $\rho_k = Id_H$ pour tout $k \in K$, alors $H \rtimes_\rho K = H \times K$.

On pourrait penser que cette nouvelle version du produit semi-direct abstraite est plus générale que la version plongée de la section précédente. Le résultat suivant montre qu'il n'en est rien, il s'agit simplement d'une autre interprétation. Soit H et K deux groupes et

$$\begin{array}{rccc} \rho: & K & \longrightarrow & Aut(H) \\ & k & \longmapsto & \rho_k \end{array}$$

un morphisme de groupes, et $G = H \rtimes_\rho K$. Il est clair que H est isomorphe au sous-groupe $H_0 = H \times \{e_k\}$ de G, et que K est isomorphe au sous-groupe $K_0 = \{e_H\} \times K$ de G.

PROPOSITION 12.2.3. — On a $H_0 \lhd G$ et $H_0K_0 = G$. En particulier, G est isomorphe au produit semi-direct $H_0 \rtimes K_0$ défini au Théorème 12.1.2.

Démonstration. La projection $(h,k) \mapsto k$ est un morphisme de groupes de G sur K de noyau H_0, et donc $H_0 \lhd G$. On a de plus clairement $G = H_0K_0$, le résultat découle maintenant du Théorème 12.1.2. □

Revenons, pour terminer, sur les deux exemples de la section précédente.

EXEMPLE 12.2.4. — On a $\mathfrak{S}_n = \mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$, en particulier $\mathfrak{S}_3 = \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

EXEMPLE 12.2.5. — Puisque le groupe $\mathcal{T}$ des translations de $\mathbb{R}^n$ est naturellement isomoprhe à $\mathbb{R}^n$, on a $Aff(\mathbb{R}^n) = \mathbb{R}^n \rtimes GL_n(\mathbb{R})$.

13 Le théorème de Bézout

THÉORÈME 13.0.1. — Soit P et Q deux polynômes premiers entre eux de $\mathbb{C}[X,Y]$ de degré p et q respectivement. Alors, on a

$$\#\{(x,y)\in\mathbb{C}^2\ ;\ P(x,y)=Q(x,y)=0\}\leq pq$$

En particulier, cet ensemble est fini.

Par degré d'un polynôme à deux variable on entend le degré maximal des monômes qui le composent : si $P=\sum a_{r,s}X^rY^s$, alors $\deg P=\max_{a_{r,s}\neq 0}\{r+s\}$. L'inégalité peut être stricte : si $P=X+1$ et $Q=X+2$ alors l'ensemble des (x,y) tels que $P(x,y)=Q(x,y)=0$ est vide alors que $pq=1$.

13.0.2 Ensembles algébriques affines

Avant de démontrer ce théorème, nous allons le placer dans son contexte naturel, qui est celui des *s*ous-ensembles algébriques d'un espace affine. Soit k un corps et considérons *l'espace affine de dimension n sur k.*

$$\mathbb{A}^n_k:=\{(x_1,\dots,x_n)\,|\,x_i\in k\ \forall i=1,\dots,n\},$$

Soient $P_1,\dots,P_\ell$ dans $k[X_1,\dots,X_n]$ des polynômes en n indéterminées. On note :

$$V(P_1,\dots,P_\ell)=\{(x_1,\dots,x_n)\in\mathbb{A}^n_k\mid P_i(x_1,\dots,x_n)=0\ \forall i=1,\dots,\ell\}.$$

REMARQUE 13.0.3. — La notation V est un anglicisme (V pour *vanishing*). En français, elle rappelle le terme *variété*. La notation Z (pour zéro de polynômes) est peut-être encore plus courante, et fonctionne dans de nombreuses langues.

EXEMPLE 13.0.4. — Sur $\mathbb{A}^2_\mathbb{R}$ on a, si $P=X^2+Y^2-1$,

$$V(P)=\{(x,y)\in\mathbb{A}^2_\mathbb{R}\,|\,x^2+y^2=1\}$$

qui n'est autre que le cercle. Si on ajoute $Q=X$, alors on a un ensemble à deux éléments

$$V(P,Q)=\{(x,y)\in\mathbb{A}^2_\mathbb{R}\,|\,x^2+y^2=1,\ x=0\}=\{(0,1),\ (0,-1)\}.$$

Si cependant on ajoutait $Q=X+1$ on trouverait un singleton

$$V(P,Q)=\{(x,y)\in\mathbb{A}^2_\mathbb{R}\,|\,x^2+y^2=1,\ x=1\}=\{(-1,0)\}.$$

Finalement, si on ajoutait $Q=X+2$, on trouverait l'ensemble vide.

$$V(P,Q)=\{(x,y)\in\mathbb{A}^2_\mathbb{R}\,|\,x^2+y^2=1,\ x=2\}=\emptyset.$$

Si on c'était placé sur les complexes, on aurait trouvé toutes les racines : Sur $\mathbb{A}^2_\mathbb{C}$ on a, si $P=X^2+Y^2-1$ et $Q=X+2$, alors :

$$V(P,Q)=\{(x,y)\in\mathbb{A}^2_\mathbb{C}\,|\,x^2+y^2=1,x=-2\}=\left\{(-2,i\sqrt{3}),(-2,-i\sqrt{3})\right\}.$$

Soit $J = \langle P_1, \dots, P_\ell \rangle$ l'idéal de $k[X_1, \dots, X_n]$ engendré par les polynômes $P_1, \dots, P_\ell$. Alors pour tout P dans J, on a :

$$P(x_1, \dots, x_n) = 0 \text{ pour } (x_1, \dots, x_n) \in V(P_1, \dots, P_\ell).$$

En effet, on peut écrire $P = \sum_{i=1}^{\ell} Q_i P_i$ pour certains Q_i dans $k[X_1, \dots, X_n]$.
Généralement, nous définissons pour un idéal $J \subseteq k[X_1, \dots, X_n]$ *le sous-ensemble algébrique déterminé par l'idéal* J par :

$$V(J) := \{(x_1, \dots, x_n) \in \mathbb{A}_k^n \mid P(x_1, \dots, x_n) = 0 \quad \forall P \in J\}.$$

Exercice 13.0.5. — a) Si $J = \langle P_1, \dots, P_\ell \rangle$, alors $V(J) = V(P_1, \dots, P_\ell)$.
b) $V(\langle 0 \rangle) = \mathbb{A}_k^n$;
c) $V(k[X_1, \dots, X_n]) = \emptyset$;
d) $\bigcup_{j=1}^{\ell} V(I_j) = V(\bigcap_{j=1}^{\ell} I_j)$;
e) $\bigcap_{\lambda \in \Lambda} V(I_\lambda) = V\left(\sum_{\lambda \in \Lambda} I_\lambda\right)$.
On en déduit que les sous-ensembles algébriques de $\mathbb{A}_k^n$ sont les fermés d'une topologie sur $\mathbb{A}_k^n$. Cette topologie est appelée la *topologie de Zariski* de $\mathbb{A}_k^n$. On dira donc parfois *fermé de Zariski* au lieu de *sous-ensemble algébrique*.

Exemple 13.0.6. — On considère l'espace vectoriel $\mathrm{M}_n(k)$ des matrices carrée $n \times n$, que l'on voit comme l'espace affine de dimension n^2. Le déterminant définit un polynôme non nul det en les n^2 variables que sont les coefficients d'une matrice $n \times n$. Les matrices inversibles forment alors l'ouvert de Zariski complémentaire de $V(\det)$ dans $\mathrm{M}_n(k)$.

Exercice 13.0.7. — Montrer que les matrices carrées $n \times n$ à coefficients complexes admettant n valeurs propres distinctes forment un ouvert de Zariski dans $\mathrm{M}_n(\mathbb{C})$.

13.0.8 Démonstration du théorème de Bézout

Il s'agit de montrer que si P et Q sont sont premiers entre eux dans $\mathbb{C}[X, Y]$, alors l'ensemble $V(P, Q)$ dans $\mathbb{A}_{\mathbb{C}}^2$ est fini, de cardinal au plus pq.
Commençons par montrer que ce nombre est fini. Comme P et Q sont premiers entre eux dans $\mathbb{C}[X, Y]$, ils le sont aussi dans $\mathbb{C}(Y)[X]$ et leur résultant est un polynôme non nul $R(Y)$ dans $\mathbb{C}[Y]$. Ainsi, les racines communes à P et Q n'ont qu'un nombre fini d'ordonnées y possibles, les racines de R. De même il n'y a qu'un nombre fini d'abscisses possibles. Ainsi $V(P, Q)$ est fini.
Montrons maintenant l'estimée : $\#V(P, Q) \leq pq$. Quitte à faire un changement de variables linéaire, on peut supposer qu'une droite horizontale ne contienne au plus qu'un point de $V(P, Q)$: en effet, il n'y a qu'un nombre fini de directions à éviter, donc c'est possible. Cela change les polynômes P et Q mais non leurs degrés, ni bien sûr le fait qu'ils sont premiers entre eux. Il nous suffit donc de montrer que l'ensemble des *ordonnées* des points de $V(P, Q)$ est de cardinal au plus pq.
Écrivons : $P = P_m(Y)X^m + \cdots + P_0(Y)$ et $Q = Q_n(Y)X^n + \cdots + Q_0(Y)$, où P_m et Q_n sont non nuls. Soit $R(Y) = Res_{m,n}(P, Q)$ le résultant par rapport à X. Si y est l'ordonnée

d'un point de $V(P,Q)$, les polynômes $P(X;y)$ et $Q(X;y)$ ont une racine commune et par suite, $R(y)=0$. Il suffit donc de montrer : $\deg R \leq pq$.
Observons que les P_i sont de degrés $\leq p-i$ et que les Q_j sont de degrés $\leq q-j$. Le coefficient de la matrice qui définit le résultant R_{ij} à la ligne i et à la colonne j satisfait à :

- pour $1 \leq j \leq n$, on a $R_{ij} = P_{i-j}$ si $0 \leq i-j \leq m$, et $R_{ij}=0$ sinon ;
- pour $n+1 \leq j \leq m+n$, on a $R_{ij} = Q_{i-j+n}$ si $0 \leq i-j+n \leq n$, et $R_{ij}=0$ sinon.

Le degré de R_{ij} est donc majoré par $p-i+j$ si $1 \leq j \leq n$, et par $q-n-i+j$ si $n+1 \leq j \leq m+n$.

Rappelons enfin que le déterminant de R est une somme de produits $\prod_{j=1}^{m+n} \pm R_{\sigma(j)j}$, où σ est une permutation de $\{1,\dots,j,\dots,m+n\}$. Au niveau des degrés :

$$\begin{aligned}\deg \prod_{j=1}^{m+n} R_{\sigma(j)j} = \sum_{j=1}^{m+n} \deg R_{\sigma(j)j} &\leq \sum_{j=1}^{n}(p-\sigma(j)+j) + \sum_{j=n+1}^{m+n}(q-n-\sigma(j)+j) \\ &\leq pn+(q-n)m - \sum_{j=1}^{n+m}\sigma(j) + \sum_{j=1}^{n+m} j = pn+(q-n)m \\ &= pq-(p-m)(q-n) \leq pq.\end{aligned}$$

Ceci achève la démonstration du théorème 13.0.1.

13.1 Calcul du résultant

Le résultant se comporte bien par division euclidienne et par échange des deux polynômes : on renvoie le lecteur à l'exercice 4.6. On obtient ainsi une méthode de calcul du résultant par algorithme d'Euclide.

13.2 Le principe de prolongement des identités algébriques

Ce titre pompeux désigne un résultat puissant, dont la démonstration est élémentaire.

THÉORÈME 13.2.1. — Soient k un corps infini, n un entier positif, et P un polynôme non nul dans $k[X_1,\dots,X_n]$. Si un polynôme Q de $k[X_1,\dots,X_n]$ s'annule hors de $V(P)$:

$$\forall x \in \mathbb{A}^n \setminus P^{-1}(0),\ Q(x)=0,$$

alors il est nul.

La conclusion dit qu'on peut prolonger l'identité algébrique (polynomiale) : $Q(x)=0$ à tous les points.

Démonstration. On va montrer que le polynôme Q est nul. Comme P est non nul et que l'anneau $k[X_1,\dots,X_n]$ est intègre, il suffit de montrer que le polynôme PQ est nul. Le polynôme PQ s'annule sur $V(P)$ où P est nul, et sur son complémentaire car Q y est nul par hypothèse. Il s'annule donc en tout point de $\mathbb{A}^n$; le résultat découle donc de la proposition qui suit. □

PROPOSITION 13.2.2. — Soit k un anneau intègre infini. Pour un entier positif n, on se donne n ensembles infinis d'éléments de k notés I_1, ..., I_n. Un polynôme P dans $k[X_1, \ldots, X_n]$ qui s'annule en tout n-uplet $(x_1, \ldots, x_n)$ de $I_1 \times \cdots \times I_n$ est nul.

Démonstration. Quand n vaut 1, l'énoncé dit qu'un polynôme avec une infinité de racines est nul. Ceci se montre en utilisant qu'un polynôme admet a comme racine si, et seulement si, il est divisible par $X - a$; le nombre de ses racines ne peut donc excéder son degré.
Le résultat général se montre alors par récurrence sur l'entier n, récurrence dont la rédaction est laissée au lecteur. □

COROLLAIRE 13.2.3. — Soient k un corps infini, n un entier positif, et P un polynôme non nul dans $k[X_1, \ldots, X_n]$. Si deux polynôme Q_1 et Q_2 de $k[X_1, \ldots, X_n]$ coïncident hors de $V(P)$:

$$\forall x \in \mathbb{A}^n \setminus P^{-1}(0),\ Q_1(x) = Q_2(x),$$

alors il sont égaux.

Cette propriété mérite qu'on l'entoure d'un peu de vocabulaire.

DÉFINITION 13.2.4. — Une partie D de $\mathbb{A}^n$ est *Zariski-dense* si on peut prolonger les identités algébriques valides sur D : si un polynôme de $k[X_1, \ldots, X_n]$ est nul sur D, alors il est nul.

On laisse au lecteur le soin de vérifier, ce qui ne saute pas aux yeux, que la terminologie est compatible avec la topologie de Zariski.

EXEMPLES 13.2.5. — a) La proposition 13.2.2 dit qu'un produit cartésien $I_1 \times \cdots \times I_n$ d'ensembles infinis est Zariski-dense.

b) Le théorème 13.2.1 dit que le complémentaire de $V(P)$, pour P non nul, est Zariski-dense.

c) L'exemple 13.0.6 montre donc que $\mathrm{GL}_n(k)$ est Zariski-dense dans $\mathrm{M}_n(k)$ si k est infini.

d) Plus généralement, tout ouvert de Zariski non vide est Zariski-dense.

e) Si k est $\mathbb{R}$ ou $\mathbb{C}$, toute partie dense est Zariski-dense. En effet, un polynôme définit une fonction polynomiale continue, et la nullité d'une fonction continue se teste sur une partie dense.
Notons que dans ce cas, on peut aussi déduire le théorème 13.2.1 de la proposition 13.2.2 en remarquant que l'ouvert non vide $\mathbb{A}^n \setminus P^{-1}(0)$ contient un pavé, et qu'une boule non vide (de $\mathbb{R}$ ou $\mathbb{C}$) est infinie.

Ces exemples montrent l'intérêt de la notion : si l'on veut raisonner par un argument de densité des matrices inversibles, et que l'on manipule des polynômes, on peut utiliser la densité de Zariski de $\mathrm{GL}_n(k)$, qui ne nécessite aucune topologie sur le corps k.
Illustrons cela en montrant que si A et B sont deux matrices carrées $n \times n$ à coefficients dans un corps infini k, alors AB et BA ont mêmes polynômes caractéristiques. Pour cela, fixons B et remarquons que chaque coefficient du polynôme caractéristique de AB, comme de BA, est un polynôme en les n^2 coefficients de A. Quand A est une matrice inversible, AB et BA sont semblables et ont même polynôme caractéristique. Comme les matrices inversibles sont Zariski-denses dans $\mathrm{M}_n(k)$, les coefficients sont les mêmes pour toute matrice A.

Remarque 13.2.6. — Cet exemple ne se veut qu'une illustration de la méthode. En fait, le résultat se généralise au cas où A est de taille $n \times p$ et B de taille $p \times n$: on trouve alors que les polynômes caractéristiques de AB et BA ne diffèrent que d'une puissance de X. Pour le montrer, on utilise le produit par blocs :

$$\begin{pmatrix} I_n & 0 \\ B & I_p \end{pmatrix} \begin{pmatrix} XI_n - AB & -A \\ 0 & XI_p \end{pmatrix} \begin{pmatrix} I_n & 0 \\ -B & I_p \end{pmatrix} = \begin{pmatrix} XI_n & -A \\ 0 & XI_p - BA \end{pmatrix}.$$

Il suffit d'en prendre le déterminant pour arriver au résultat. On pourra par exemple voir `https://en.wikipedia.org/wiki/Characteristic_polynomial`.
Vous pourrez voir au second semestre que l'équation ci-dessus montre en fait davantage.

Exercice 13.2.7. — Montrer le théorème de Cayley-Hamilton à partir du résultat de l'exercice 13.0.7.