Plan du cours :

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.

Le cours contient quelque exercices dans le texte principal. Ce sont des exercices, en général directs, dans le but d'illustrer tel ou tel définition ou énoncé. Les exercices du cours proprement dit sont séparés, avec indications et solutions.

Définitions, énoncés et leurs démonstrations doivent être compris. Les exercices sont très important pour ce cours qui peut paraître abstrait sinon : ils permettront de bien comprendre les notions abordés et doivent être assimilés.

1. Rappels sur les groupes

1.1. Définitions, premières propriétés

Définition 1.1.1. — Un *groupe* est un ensemble G muni d'une loi de composition interne $(x, y) \mapsto x \cdot y$ telle que :

- il existe un élément $e \in G$ tel que pour tout $x \in G$ on ait $e \cdot x = x \cdot e = g$ (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) ;
- pour tous $x, y, z \in G$, on a $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (associativité)

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

La loi interne $\cdot$ a de multiples notations : en général, on écrira simplement xy (multiplicativement) ou $x + y$ (additivement).

L'usage veut que si la loi interne est noté multiplicativement, on note l'inverse par x^{-1} et l'élément neutre par 1. Si G est abélien, on note la loi interne souvent additivement, l'inverse par $-x$ et l'élément neutre par 0.

La notion de groupe a été dégagé 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 d'intéresse à des applications entre ceux-ci qui respectent la loi interne :

Définition 1.1.2. — 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 $x, x' \in G$.

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 $x \in G$. Parfois on dira 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 1.1.3. — Un homomorphisme 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 1.1.4. — Un sous-ensemble F d'un groupe G en est un *sous-groupe* si :

- on a $e \in F$;
- si $x, y \in F$, alors $xy \in F$;
- si $x \in F$, alors $x^{-1} \in F$.

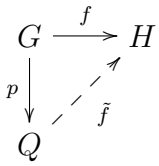
Autrement dit un *sous-groupe de* G est un sous-ensemble de G que la loi de G munit d'une structure de groupe. Tout groupe a toujours deux sous-groupes naturels : le groupe lui-même et le sous-ensemble réduit à l'élément neutre.

On observe que l'image ou l'image réciproque d'un sous-groupe par un morphisme de groupes $f : G \to H$ est encore un sous-groupe (exercice : le vérifier). En particulier, l'image réciproque de l'élément neutre est un sous-groupe de G, appelé le *noyau* de f et noté $\mathrm{Ker}\, f$.

On pourra vérifier qu'un morphisme de groupes est injectif, si et seulement si $\operatorname{Ker} f = \{e\}$.

1.2. **Propriété universelle**

Soient $f : G \to H$ un morphisme de groupes et $p : G \to Q$ un morphisme de groupes surjectif. On cherche un morphisme de groupes $\tilde{f} : Q \to H$ tel que l'on ait : $f = \tilde{f} \circ p$ ou, comme on dit, tel que le diagramme suivant soit commutatif.



Proposition 1.2.1. — Avec les notations qui précèdent :

a) Un morphisme de factorisation $\tilde{f}$ existe si et seulement si $\operatorname{Ker}(f)$ contient $\operatorname{Ker}(p)$.

b) Quand $\tilde{f}$ existe, il est unique. Il est surjectif si, et seulement si, f est surjectif, et il est injectif si, et seulement si, $\operatorname{Ker}(f) = \operatorname{Ker}(p)$.

Démonstration. a) Il est clair que si $\tilde{f}$ existe, alors $\operatorname{Ker}(p)$ est inclus dans $\operatorname{Ker}(\tilde{f} \circ p) = \operatorname{Ker}(f)$. Réciproquement, supposons que $\operatorname{Ker}(p)$ est inclus dans $\operatorname{Ker}(f)$. Pour tout x dans Q, choisissons g dans G tel que $p(g) = x$. Posons $\tilde{f}(x) = f(g)$. Cette définition ne dépend pas du choix de g dans $p^{-1}(x)$, car deux éléments de même image ne diffèrent que par un élément du noyau : si $p(g') = x$, alors $p(gg'^{-1}) = p(g)p(g')^{-1} = xx^{-1} = 1$, d'où $gg'^{-1} \in \operatorname{Ker}(p)$. Comme $Ker(p) \subset \operatorname{Ker}(f)$, $f(g') = f(g)$. Une fois que $\tilde{f}$ est bien définie, il est facile de vérifier qu'elle respecte les produits : si $p(g) = x$ et $p(g') = x'$, alors $p(gg') = xx'$ et donc $\tilde{f}(xx') = f(gg') = f(g)f(g') = \tilde{f}(x)\tilde{f}(x')$.

b) L'unicité résulte de la surjectivité de p. Il en résulte aussi que f et $\tilde{f}$ ont même image. Enfin, on observe que $\operatorname{Ker}(\tilde{f}) = p(\operatorname{Ker}(f))$, de sorte que $\tilde{f}$ est injectif si et seulement si $\operatorname{Ker}(f) = \operatorname{Ker}(p)$.

□

2. Anneaux

2.1. Définitions, premières propriétés

Définition 2.1.1. — On appelle *anneau* un groupe abélien A, noté additivement, muni d'une opération de multiplication $(a, b) \mapsto ab$ vérifiant les propriétés suivantes :

- il existe un élément $1 \in A$ tel que pour tout $a \in A$, $1a = a$ (élément neutre pour la multiplication) ;
- pour tous $a, b, c \in A$, on a $a(bc) = (ab)c$ (associativité) ;
- pour tous $a, b, c \in A$, on a $a(b + c) = ab + ac$ (distributivité)
- pour tous $a, b \in A$, on a $ab = ba$ (commutativité) ;

Les anneaux ainsi définis sont *commutatifs* et *unitaires*. Il existe de notions plus générales d'anneaux, notamment des anneaux non commutatifs où l'on relâche l'hypothèse sur la commutativité (mais où l'on doit du coup imposer que 1 est aussi neutre à droite et la distributivité à droite : $(a+b)c = ac+bc$). Ces anneaux interviennent notamment quand on considère l'ensemble des matrice $n \times n$ avec l'addition et la multiplication des matrices. Pour ce cours cependant, nos anneaux seront toujours supposés commutatifs, sauf mention du contraire.

Les axiomes ci-dessus nous permettent de calculer comme on a l'habitude pour les entiers relatifs, qui sont notre premier example d'anneau.

Si $a \in A$ et si n est un entier positif ou nul, on définit an par récurrence a^n, en posant $a^0 = 1$ et $a^n = a(a^{n-1})$.

Exercice 2.1.2. — Comme exercice pour s'habituer aux axiomes, 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 2.1.3. — Un élément $a \in A$ est dit *inversible* ou une *unité* s'il existe $b \in A$ tel que $ab = 1$. Cet élément est unique et appelé *l'inverse de* a. Il est généralement noté a^{-1}.

Proposition 2.1.4. — L'ensemble des éléments inversible d'un anneau, noté $A^\times$, est un groupe pour la multiplication.

Démonstration. Observons d'abord que la multiplication définit une loi interne : Si $a, b \in A^\times$ alors $(ab)(a^{-1}b^{-1}) = (aa^{-1})(bb^{-1})$. Ainsi ab est aussi inversible (est d'inverse $a^{-1}b^{-1}$). Maintenant il est clair que 1 est l'élément neutre pour cette loi et pour $a \in A^\times$ l'élément a^{-1} est son inverse. □

Définition 2.1.5. — 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.

Définition 2.1.6. — On dira que l'anneau non nul A est un *corps* si tout élément non nul de A est inversible.

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

Exemple 2.1.7. — 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.

2.2. Morphismes entre anneaux

Comme dans le cas des groupes, une fois que nous avons défini nos objets, les anneaux, nous définissions les homomorphismes entre objets :

Définition 2.2.1. — Soient A et B deux anneaux. Un *homomorphisme d'anneaux* $f : A \to B$ est un morphisme de groupes abéliens qui respecte la multiplication et envoi 1 sur 1.

Autrement dit, un homomorphisme d'anneaux est une application telle que

– on a $f(0) = 0$ et $f(1) = 1$;

– pour tous $a, b \in A$, $f(a + b) = f(a) + f(b)$ et $f(ab) = f(a)f(b)$.

Comme dans le cas des groupes, on dira simplement morphisme entre anneaux au lieu de homomorphisme. 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 $f \circ g = \mathrm{Id}_H$ et $g \circ f = \mathrm{Id}_G$. Comme dans le cas des groupes, le lecteur vérifiera l'énoncé suivant :

Proposition 2.2.2. — Un morphisme d'anneaux $f : A \to B$ est un isomorphisme si et seulement si il est bijectif.

Soit $f : A \to B$ est 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 2.2.3. — Soit A un anneau. On dira qu'une partie $B \subset A$ est un sous-anneau si B contient les éléments 0 et 1 et si B est stable par addition, multiplication et stable par opposé.

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 2.2.4. — (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 sous-anneau de A.

iii) Montrer que $A \simeq eA \times (1 - e)A$.

2.3. **Anneaux de polynômes, séries formelles**

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

Autrement dit, on considère l'ensemble $A^{(\mathbb{N})}$ des familles presque nulles, c'est-à-dire les suites dont tous les termes, sauf un nombre fini, sont nuls, d'éléments de A indexés par l'ensemble $\mathbb{N}$, puis si $P = (a_n)_{n\in\mathbb{N}}$ est un élément de $A^{(\mathbb{N})}$, on le note

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

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, cette fois, une somme effectuée dans l'anneau A.

On observe que ces formules ont bien un sens, c'est-à-dire que toutes les sommes sont finies. L'élément 0 est la famille identiquement nul et 1 la famille donnée par $1_0 = 1$ et $1_n = 0$ si $n \neq 0$ ou, avec nos notations, par X^0. On obtient ainsi une structure d'anneau, l'anneau des polynômes $A[X]$. L'anneau A s'identifie au sous-anneau des polynômes constants de $A[X]$ par le morphisme injectif $a \mapsto aX^0$.

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

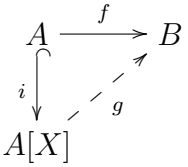
Par construction l'anneau des polynômes $A[X]$ est un sous-anneau de l'anneau des séries formelles $A[[X]]$. L'impression de similarité dans la construction ne doit cependant pas cacher le fait que ces anneaux ont des propriétés très différentes, comme on le verra plus tard. Pour l'instant, on pourra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

Exercice 2.3.1. — Soit A un anneau. Déterminer $(A[X])^\times$. Quid de $(A[[X]])^\times$?

L'anneau des polynômes jouit de la propriété universelle suivante :

Proposition 2.3.2. — Soit $f : A \to B$ un morphisme d'anneaux et soit b un élément de B. Il existe un unique morphisme d'anneaux

$g : A[X] \to B$ rendant commutatif le diagramme



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

Démonstration. S'il existe un tel morphisme, il est nécessairement 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 respecte la multiplication etc. □

Exemple 2.3.3. — Soit A un anneau, et a dans A. Le morphisme d'évaluation

$$ev_a : A[X] \to A$$
$$P \mapsto P(a) \ ,$$

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

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 note $\deg P$ par ce nombre d. L'élément a_d est appelé le *coefficient dominant* de P.

Par convention, $\deg 0 := -\infty$. Si P et Q sont deux polynômes de $A[X]$, 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 2.3.4. — Si A est intègre, $A[X]$ est encore intègre.

La propriété d'être intègre d'un anneau se transfert donc à l'anneau de polynômes à coefficients dans cet anneau. On verra d'autres tels propriétés de transfert plus tard dans le cours.

Démonstration. Il s'agit de montrer que si P et Q sont des polynômes non nuls, alors 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 $a_{\deg Q} \neq 0$. Le terme 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, $\deg(PQ) = \deg P + \deg Q$.

On a la division euclidienne, analogue à celle, connue, des entiers relatifs, aussi dans les anneaux de polynômes

Théorème 2.3.5. — Soit A un anneau et P et Q deux polynômes de $A[X]$. On suppose que Q est non nul de coefficient dominant inversible. Alors il existe un unique couple (R, S) de polynômes dans $A[X]$ tel que

- $P = RQ + S$;
- $\deg S < \deg Q$.

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

Démonstration. Montrons d'abord l'unicité. Supposons que l'on ait $P = RQ + S = R'Q + S'$. Alors $Q(R - R') = S' - S$ est de degré au plus $\max(\deg S', \deg S) < \deg Q$. Supposons $R \neq R'$. Soient u et a les coefficients dominants de Q et $R - R'$. Comme u est inversible et $a \neq 0$, on a $ua \neq 0$. Ainsi $Q(R-R')$ est de degré $\deg Q + \deg(R-R')$

est donc en particulier $\geq \deg Q$. Contradiction. Ainsi $R = R'$, puis $S = P - RQ = R - R'Q = S'$.

Pour l'existence on raisonne par récurrence sur le degré de P. Si $\deg P < \deg Q$ il suffit de prendre $R = 0$ et $S = P$. Sinon, soit a le coefficient dominant de P et u celui de Q. Alors le polynôme $P' = P - au^{-1}X^{\deg P - \deg Q}Q$ 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 $R', S' \in A[X]$, tels que $P' = R'Q + S'$ et $\deg S' < \deg Q$. Il suit que

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

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

Pour finir cette section notons qu'on peut considérer des anneaux de polynômes à plusieurs variables. 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 : il existe un unique endomorphisme d'anneaux de $A[X, Y]$ qui conserve les polynômes constants et échange les variables X et Y. C'est un isomorphisme involutif.

3. Idéaux d'un anneau

3.1. Définitions, premières propriétés

Nous allons étudier dans ce paragraphe la question du passage d'un anneau au quotient. Pour les groupes, cette question mène à la notion de sous-groupe distingué : si H est un sous-groupe d'un groupe G, le passage au quotient $G \to G/H$ est un morphisme de groupes si, et seulement si, le sous-groupe H est distingué. Pour les anneaux, la question amène la notion d'idéal.

Définition 3.1.1. — 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 $I \subset A$ 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 $ax \in I$.

Exemple 3.1.2. — Si A est un anneau et $x \in A$, l'ensemble $(x) = \{ax\,;\, a \in A\}$ est un idéal de A. Un tel idéal est dit *principal*.

Exemple 3.1.3. — Tout anneau a deux idéaux naturels : 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 est un idéal non nul de K. Il a donc un élément non nul $x \in I$, nécessairement inversible puisque K est un corps. Soit $a \in K$ quelconque. Par définition d'un idéal $(ax^{-1})x \in I$. On a donc $a \in I$ et par conséquent $I = K$. Réciproquement, soit $x \in K$ non nul et considérons l'idéal (x) de K. Comme x est non nul, l'idéal (x) est non nul aussi. Par conséquent, il est égal à K et en particulier 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 3.1.4. — Si I est un idéal de $\mathbb{Z}$, il existe un unique entier $n \geq 0$ tel que $I = (n)$. En effet, si $I = (0)$ alors $n = 0$ convient. Si

$I \neq (0)$, considérons le plus petit n de $I \cap \mathbb{N}^*$. Par définition $(n) \subset I$. Réciproquement, soit $x \in I$. 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 $x \in I$ et comme $qn \in I$, l'élément $r = x - qn \in I$. Comme $r < n$, on doit avoir $r = 0$ par le choix de n. Ainsi $x = qn$ et on a donc bien $I \subset (n)$, d'où $I = (n)$.

3.2. **Opérations sur les idéaux**

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

3.2.1 (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

$$\langle E \rangle = \bigcap_{E \subset I \subset A} I$$

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 3.2.2. — Soit E une partie de A. Alors l'idéal $\langle E \rangle$ est l'ensemble des combinaisons linéaires presque nulle $\sum_{e \in E} a_e e$.

Démonstration. Notons par 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 $\langle E \rangle$. Ainsi $S_E \subset \langle E \rangle$. 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 $\langle E \rangle \subset S_E$. □

Exemple 3.2.3. — Si A est un anneau et $x \in A$, alors $(x) = \langle \{x\} \rangle$. Plus généralement, on note $(x_1, \dots x_n) = \langle \{x_1, \dots, x_n\} \rangle$. D'après ce que nous venons de voir,

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

3.2.4. — (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 $\cup_t I_t$.

3.2.5. — (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 3.2.6. — Soit A un anneau. Soient I et J deux idéaux de A. Alors $IJ \subset I \cap J$. 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 *étrangers* 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 $z \in I$ et $x \in I$, $zx \in IJ$. De même, $zy \in IJ$. Par conséquent, $zx + zy \in IJ$ et donc $z \in IJ$, d'où $I \cap J \subset IJ$. □

Exercice 3.2.7. — Donner un exemple où l'inclusion de IJ dans $I \cap J$ est stricte.

3.2.8. — (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 3.2.9. — 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.

3.3. 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 3.3.1. — 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. □

3.3.2 (Image réciproque d'un idéal)**.** — Soient $f : A \to B$ un morphisme d'idéaux et $J \subset B$ 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 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.

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

3.3.3 (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 $(n) \subset \mathbb{Z}$ 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 $f(A)$. En effet, soient $I \subset A$ un idéal et $J = f(I)$. 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 que J est vu dans l'anneau image $f(A)$ et non dans B plus généralement ?

4. Anneaux quotient

4.1. 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. Le morphisme de groupes $\pi : A \to A/I$, qu'on appellera souvent la *surjection canonique*, a I pour noyau.

Supposons A/I muni d'une structure d'anneau de manière à ce que π soit un morphisme d'anneaux. Alors le produit dans A/I est donné par :

$$(a+I).(b+I) = \pi(a).\pi(b) = \pi(ab) = ab+I,$$

et le sous-groupe I, en tant que noyau du morphisme d'anneaux π, est nécessairement un idéal.

On va donc *définir* une multiplication sur A/I par la formule ci-dessus et montrer que si réciproquement I est un idéal, elle est bien définie, c'est-à-dire ne dépend pas des représentants choisis. Elle définira donc une structure d'anneaux sur A/I.

Vérifions que, pour tous a, b de A, la classe du produit $ab+I$ ne dépend que des classes $a+I$ et $b+I$. Or, si le sous-groupe additif I est un idéal :

$$(a+I)(b+I) = \{a'b' | a'-a \in I, b'-b \in I\} \subset ab+aI+Ib+II \subset ab+I.$$

Ainsi, si $a'+I = a+I$ et $b'+I = b+I$, alors $a'b' \in ab+I$ et $a'b'+I = ab+I$. L'élément 0 de A/I est défini par $0+I = I$ et l'élément 1 par $1+I$. Que A/I est ainsi muni d'une structure d'anneau découle ensuite directement du fait que A est un anneau. On a donc montré :

Proposition 4.1.1. — Soit A un anneau et I un sous-groupe additif de A. Les lois de A munissent le quotient A/I d'une structure d'anneau si, et seulement si, le sous-groupe I est un idéal de A.

Si $I \subset A$ est un idéal, A/I est en tant qu'ensemble le quotient de A par la relation d'équivalence $a \sim b \Leftrightarrow a - b \in I$. Si l'on note une classe d'équivalence de A/I par $[a]$, la structure d'anneau est donné par $[a]+[b] := [a+b]$ et $[a][b] = [ab]$. Cette notation a l'avantage d'être plus courte que $a + I$, mais est moins précise dans le sens qu'elle ne mentionne pas l'idéal I. Quand il n'y a pas de risque de confusion, on utilisera souvent la notation $[a]$ pour désigner une classe. Mais le plus souvent, on voit l'anneau A/I comme un anneau tout court, et on notera ses éléments donc par $x, y, z, \ldots$

4.2. **Propriété universelle**

Les anneaux quotients vérifient également la propriété universelle des quotients :

Proposition 4.2.1. — 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, il existe un unique morphisme d'anneaux $\tilde{f} : A/I \to B$ rendant commutatif le diagramme

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

Démonstration. D'après la proposition 1.2.1) il existe un unique morphisme de groupes $\tilde{f}$ faisant commuter le diagramme ; il est défini par :

$$\tilde{f}([a]) = f(a).$$

Il est immédiat que $\tilde{f}$ est un morphisme d'anneaux. □

Corollaire 4.2.2. — Tout homomorphisme d'anneaux $f : A \to B$ se factorise par un isomorphisme d'anneaux $A/\operatorname{Ker} f \to f(A)$.

4.3. **Les idéaux d'un anneau quotient**

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

On s'intéresse aux idéaux de l'anneau A/I. Soit $\mathcal{J} \subset A/I$ un idéal de A/I. Comme π est un morphisme d'anneaux, $J = \pi^{-1}(\mathcal{J}) \subset A$ est un idéal. Cet idéal contient obligatoirement l'idéal $I = \pi^{-1}(0)$.

Proposition 4.3.1. — Soit A un anneau et I un idéal de A. Alors la surjection canonique $\pi : A \to A/I$ induit une bijection

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

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

Démonstration. Construisons la bijection réciproque. Si $J \subset A$ est un idéal on sait déjà, d'après 3.3.3, que $\pi(J) \subset A/I$ est un idéal de A/I, puisque π est surjectif. Pour montrer la proposition, il suffit donc de vérifier que

- $\pi(\pi^{-1}(\mathcal{J})) = \mathcal{J}$ et que
- $\pi^{-1}(\pi(J)) = J$ si J contient I.

Pour la première assertion, on observe qu'un élément x de $\pi(\pi^{-1}(\mathcal{J}))$ est de la forme $x = \pi(a)$ pour $a \in \pi^{-1}(\mathcal{J})$. Ainsi, $x \in \mathcal{J}$. Réciproquement, si $x \in \mathcal{J}$, on choisit $a \in A$ tel que $x = \pi(A)$. Ainsi, $\pi(a) = x \in (J)$, d'où $a \in \pi^{-1}(\mathcal{J})$ et x est donc bien dans $\pi(\pi^{-1}(\mathcal{J}))$. Pour la seconde assertion, on observe d'abord que pour tout idéal J de A on a $\pi^{-1}(\pi(J)) = I + J$. En effet, si $x \in I + J$, alors x est de la forme $a + b$ avec $a \in I$ et $b \in J$. On voit donc que $\pi(x) = \pi(a) + \pi(b) = \pi(b) \in \pi(J)$, 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 $x = (x-a)+a$ appartient bien à $I + J$. En particulier, si J contient I, alors $I + J = J$ ce qui démontre la seconde assertion. □

Proposition 4.3.2. — 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 4.2.2 nous donne l'isomorphisme recherché. □

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

4.4. Le théorème chinois sous sa forme générale

Théorème 4.4.1. — Soit A un anneau. Soient I et J deux idéaux étrangers de A. Alors il existe un unique 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 3.2.6, que $I \cap J = IJ$. Le corollaire 4.2.2 montre alors que l'on a l'isomorphisme recherché, d'où la proposition. □

5. Idéaux premiers, maximaux

5.1. Définitions, premières propriétés

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

Définition 5.1.1. — Soit A un anneau et soit I un idéal de A. On dit que I est un idéal *premier* si

– 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 5.1.2. — 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 5.1.3. — L'idéal (0) d'un anneau est premier si et seulement si A est intègre.

Exemple 5.1.4. — Dans l'anneau $\mathbb{Z}$, un idéal (n) est premier si, et seulement si, n est premier.

Exemple 5.1.5. — Si k est un corps, les idéaux (X) et (X, Y) de $k[X, Y]$ sont premiers.

Proposition 5.1.6. — Soit $f : A \to B$ un morphisme d'anneaux. Alors l'image réciproque d'un idéal premier est encore premier.

Démonstration. Soit $Q \subset A$ 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 5.1.2 on peut raisonner mieux ainsi : 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 tout sous-anneau d'un anneau intègre est encore intègre, l'anneau A/P est intègre et par conséquent P premier.

Définition 5.1.7. — Soit A un anneau. Un idéal I est dit 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 5.1.8. — Un idéal I d'un anneau A est maximal si et seulement si l'anneau 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 3.1.3, A/I est un corps si et seulement s'il a deux idéaux, 0 et A/I. Par image réciproque, d'après la proposition 4.3.1, cela signifie que I et A sont les deux seuls idéaux de A contenant I. □

Exemple 5.1.9. — L'idéal (0) d'un anneau est maximal si et seulement si A est un corps.

Exemple 5.1.10. — 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.

Exemple 5.1.11. — 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.

Exemple 5.1.12. — 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. En effet, observons d'abord que (X, Y) est un idéal propre. Sinon, il existerait alors A et B dans $k[X, Y]$ tels que $1 = A(X, Y)X + B(X, Y)Y$. Or, le terme constant du membre de droite est nul, tandis que celui du membre de gauche est égal à 1. Contradiction. Ensuite, 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 3.2.2. Ainsi le quotient $k[X, Y]/(X, Y)$ s'identifie bien à k et (X, Y) est maximal.

L'idéal (X) n'est pas maximal puisque l'inclusion $(X) \subset (X, Y)$ 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 $P \mapsto P(0, Y)$.

5.2. **Existence d'un idéal maximal**

Est-ce qu'un anneau admet-t-il toujours un idéal maximal ? Est-ce que tout idéal propre est 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 5.2.1. — 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 $I_t \subset I_s$ ou $I_s \subset I_t$ puisque la famille est totalement ordonné. Sans restriction, on peut supposer que $I_s \subset I_t$. 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 la seconde assertion supposons le contraire, c'est-à-dire que $I = A$. Dans ce cas, $1 \in I$. Il existe donc t tel que $1 \in I_t$. Mais alors $I_t = A$ et I_t ne serait pas propre. Contradiction. □

Corollaire 5.2.2. — Dans un anneau non nul, tout idéal propre est contenu dans un idéal maximal.

Proposition 5.2.3. — 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 4.3.1.

Proposition 5.2.4. — 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 $J/I \subset A/I$ l'est. Or, sait déjà que A/J est isomorphe à $(A/I)/(J/I)$ d'après la proposition 4.3.2. En utilisant les critères sur l'anneaux quotient pour qu'un idéal soit premier ou maximal (propositions 5.1.2 et 5.1.8), on voit que J/I est premier (resp. maximal) dans A/I si et seulement si J est premier (resp. maximal) dans A. □

6. Localisation

6.1. 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. On procédera en imitant le *calcul de fractions* que l'on apprend au collège.

Définition 6.1.1. — Soit A un anneau. Une partie S de A est dite multiplicative si elle vérifie les propriétés
- $1 \in S$;
- 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 6.1.2. — On vérifie sans peine que les parties suivantes sont multiplicatives dans leurs anneaux respectivement.

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) $S = A \setminus \{0\}$ dans un anneau *intègre* A ;
e) $S = A \setminus P$ dans un anneau A si $P \subset A$ est un idéal *premier* ;
f) $S = \{1, 10, 100, \ldots\}$, l'ensemble des puissances de 10 dans $\mathbb{Z}$;
g) $S = \{a^n \ ; \ n \in \mathbb{N}\} = \{1, a, a^2, a^3, \ldots\}$ pour $a \in A$.
h) Soit $f : A \to B$ un morphisme d'anneau. Si S est une partie multiplicative de A, alors $f(S)$ est encore une partie multiplicative de B. Inversement, si T est une partie multiplicative de B, alors $f^{-1}(T)$ est encore une partie multiplicative de A.
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 sera 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 $S = \{1, 10, 100, \ldots\}$, 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 $n \in \mathbb{N}$.

6.1.3. — 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

$$(a, s) \sim (b, t) :\Leftrightarrow \text{un } u \in S \text{ tel que } r(at - bs) = 0$$

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

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

b) 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 $(b, t) \sim (a, s)$ (symétrie) ;

c) 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 $w(bu - ct) = 0$. Il suit, comme

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

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

On désigne par $S^{-1}A$ l'ensemble des classes d'équivalence. La classe de (a, s) est notée a/s. On note $i : A \to S^{-1}A$ l'application qui associe à $a \in A$ la classe $a/1$ dans $S^{-1}A$. On va maintenant munir $S^{-1}A$ d'une structure d'anneau de manière à ce que i est un morphisme d'anneaux. On va imiter la définition habituelle pour la somme et le produit de fractions. Par définition, l'élément $0 \in S^{-1}A$ est la classe $0/1$, l'élément $1 \in S^{-1}A$ est la classe $1/1$. Ensuite, on pose

$$(a/s) + (b/t) := (at + bs)/st, \quad (a/s)(b/t) := (ab/st).$$

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 seront laissés au lecteur. Montrons, pour terminer la construction, que l'application $i : A \to S^{-1}A$ est bien un morphisme d'anneaux avec ces définitions. On a bien $i(0) = 0/1 = 0$ et $i(1) = 1/1 = 1$ et pour tous $a, b \in A$, on a

$$i(a+b) = (a+b)/1 = a/1 + b/1 = i(a) + i(b)$$

pour la somme et

$$i(ab) = (ab)/1 = (a/1)(b/1) = i(a)i(b)$$

pour le produit. 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 $s \in S$. Souvent, on appellera le morphisme $i : A \to S^{-1}A$ *morphisme canonique*.

6.1.4. — Dans la construction ci-dessus, la relation d'équivalence peut paraître surprenante puisque elle semble moins forte que la règle habituelle $at = bs$. Dans le cas où A est intègre et $0 \notin S$, c'est bien sûr équivalent. En général cependant, la règle $at = bs$ ne nous donne pas une relation d'équivalence, ce qui explique pourquoi nous sommes obligé de procéder 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. Le plus simple dans un premier temps sera de toujours écrire la relation explicitement dans ce cas pour ne pas se laisser induire en erreur par ses habitudes du calcul de fraction. Bien entendu, dès que A est intègre, on calculera comme on a l'habitude.

Exemple 6.1.5. — Voilà quelques exemples d'anneaux $S^{-1}A$.

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 $S^{-1}A$ sera noté A_a et 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.

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 la géométrie algébrique.

Attention aux notations : Soit $p \in \mathbb{Z}$ un nombre premier et $(p) \subset \mathbb{Z}$ l'idéal premier associé. Il faut bien distinguer entre les localisations des deux derniers exemples :

$$\mathbb{Z}_p = \{\frac{a}{s} \in \mathbb{Q} \ ; \text{ le seul facteur premier de } s \text{ est } p\} \text{ et}$$

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

En particulier, on a $\mathbb{Z}_p \cap \mathbb{Z}_{(p)} = \mathbb{Z}$ dans $\mathbb{Q}$. Ces notations ne sont pas facilitées par le fait que dans la littérature on trouve parfois $\mathbb{Z}_p$ comme notation pour le quotient $\mathbb{Z}/(p)$ ou pour l'anneau des entiers p-adiques.

6.1.6. — 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 nous explique l'interdiction de diviser par zéro dans le calcul des fractions du collège. Sinon, toute fraction serait égale à 0.

6.1.7. — 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 aucun élément de S n'est un diviseur de zéro de A. En particulier, si A est intègre, le morphisme canonique est toujours injectif.

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 6.1.8. — Soit A un anneau, S une partie multiplicative de A et $i : A \to S^{-1}A$ le morphisme canonique. Alors, pour tout morphisme d'anneau $f : A \to B$ tel que $f(S) \subset B^\times$, 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 par la suite, puisque $f(s)$ est inversible, que

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

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 6.1.9. — 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 6.1.8) 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. □

6.2. **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 $S \subset A$ 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 6.2.1. — Soit A un anneau et soit $S \subset A$ 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 6.2.2. — Soit A un anneau et soit $S \subset A$ 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 6.2.3. — Soit A un anneau et soit $S \subset A$ une partie multiplicative de A. Alors si S ne contient pas l'élément 0, il existe un idéal premier disjoint de S.

Démonstration. Comme S ne contient pas 0, l'anneau $S^{-1}A$ est non nul. Il contient donc un idéal maximal M, d'après le théorème 5.2.1. Soit $P = i^{-1}M$. Alors P est premier d'après la proposition 5.1.6, 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 $J \mapsto J \cap A$.

6.2.4. — Soit A un anneau et $P \subset A$ 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 6.2.5. — Soit P un idéal premier de A. Le localisé A_P n'a qu'un seul idéal maximal, le localisé $S^{-1}P \subset S^{-1}A$ de l'idéal P.

7. Anneaux principaux

7.1. Définitions, premières propriétés

Définition 7.1.1. — On dit qu'un anneau est *principal* s'il est intègre et si tous ses idéaux sont principaux.

Exemple 7.1.2. — L'anneau des entiers $\mathbb{Z}$ est principal comme le montre l'exemple 3.1.4.

Quand on regarde l'argument utilisé dans l'exemple 3.1.4 on observe que nous avons essentiellement utilisé la division euclidienne dans $\mathbb{Z}$. Ceci nous amène à la définition suivante :

Définition 7.1.3. — Un anneau *euclidien* est un anneau intègre muni d'une fonction dite *degré* $\delta : A \setminus \{0\} \to \mathbb{N}$ telle que pour tous a et b dans A, avec $b \neq 0$, il existe $q, r \in A$ tels que

- $a = bq + r$;
- $r = 0$ 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 pas définie de manière unique par les éléments a, b en général. Ce n'est déjà même pas le cas pour $A = \mathbb{Z}$ muni de $\delta(a) = |a|$.

Exemple 7.1.4. — 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 $Q \in k[X]$ est non nul, le coefficient dominant de Q est automatiquement inversible, étant donné que k est un corps. On pourra alors utiliser le théorème 2.3.5 pour conclure.

Proposition 7.1.5. — Un anneau euclidien est principal.

Démonstration. On va reprendre l'argument de l'exemple 3.1.4. Soit I un idéal de A dont on veut montrer qu'il est principal. Comme l'idéal nul est principal, on peut supposer que $I \neq 0$. Soit alors $a \in I$

un élément non nul tel que $\delta(a)$ soit 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 $x = aq + r$. Si $r \neq 0$, on a $\delta(r) < \delta(a)$, ce qui est absurde puisque $r = x - aq$ appartient à I. Donc $r = 0$ et $x = aq \in (a)$. Par suite, $I = (a)$ et tout idéal de A est principal. Comme A est intègre, A est principal. □

Exemple 7.1.6. — Soit k un corps. L'anneau $k[X]$ est euclidien donc principal d'après la proposition précédente. Cependant, ceci ne reste pas vrai pour des anneaux de polynômes à plusieurs variables. Déjà, l'anneau $k[X, Y]$ n'est plus principal. Pour le voir, on va montrer que l'idéal (X, Y) n'est pas principal. On va raisonner par l'absurde. Supposons donc qu'il existe $P \in k[X, Y]$ tel que $(X, Y) = (P)$. Il existe alors Q et R dans $k[X, Y]$ tels que $X = QP$ et $Y = RP$. Si l'on écrit $P = a_0(X) + a_1(X)Y + \ldots$ comme un polynôme en Y à coefficients dans $k[X]$, la relation $X = QP$ nous dit alors que $deg_Y P + deg_Y Q = 0$, donc P ne fait pas intervenir Y. Par le même argument, la relation $Y = PR$ nous dit que P ne fait pas intervenir X. Le polynôme P est donc constant et non nul. Il suit que $(P) = (1)$, ce qui est impossible puisque (X, Y) est un idéal propre d'après l'exemple 5.1.12 .

Exemple 7.1.7. — 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*. On va montrer que $\mathbb{Z}[i]$ est euclidien et donc en particulier principal. Pour cela on définit $\delta(a + ib) = |a + ib|^2 = a^2 + b^2$. Reste à vérifier que δ vérifie les condition d'un anneau euclidien. Soient x, y deux éléments de $\mathbb{Z}[i]$ avec $y \neq 0$. Soit $z = x/y$ dans $\mathbb{C}$. 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. Alors on a

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

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

7.2. **Divisibilité et idéaux**

Clarifions la relation entre divisibilité et inclusion des idéaux. Dans un anneau intègre A, on dira que a divise b et on note $a|b$ s'il existe $c \in A$ tel que $b = ca$ ou autrement dit si $b \in (a)$ ou encore si $(b) \subset (a)$. L'application de l'ensemble A vers l'ensemble de ses idéaux, qui associe à un élément l'idéal principal qu'il engendre transforme donc divisibilité en inclusion. Quand est-ce que deux éléments engendrent le même idéal principal ?

Proposition 7.2.1. — 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 on doit avoir $ab = 1$, si bien que a et b sont inversibles. La réciproque est claire. □

Dans un anneau principal A, si a et b sont des éléments de A, l'idéal (a, b) est de la forme (c). Alors c divise a et b et c'est le plus grand des diviseurs au sens de l'inclusion des idéaux. D'après la proposition précédente, l'élément c est bien défini à un inversible près. On pourra donc *définir* le pgcd de a et b par un générateur de (a, b), sachant qu'il est bien défini à inversible près. Cette notion fait en fait sens dans des anneaux plus généraux, les anneaux factoriels, que l'on va étudier au chapitre suivant.

7.3. Éléments irréductibles ; éléments premiers

Définition 7.3.1. — 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. On observe que $0 = 0 \cdot 0$ n'est pas irréductible.

Définition 7.3.2. — 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 7.3.3. — Tout élément premier d'un anneau intègre est irréductible.

Démonstration. Montrons la contraposée. Soit a un élément réductible, et $a = bc$ une factorisation non banale : ni b, ni c ne sont associés à a, si bien que a divise bc, mais ne divise ni b, ni c. Ceci montre que a n'est pas premier. □

Exemple 7.3.4. — Il faut faire très attention cependant au fait que la réciproque n'est pas vraie en général. Considérons le sous-anneau de $\mathbb{C}$ engendré par $\mathbb{Z}$ et $i\sqrt{5}$ ou 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. Notez qu'une telle écriture est unique et qu'en particulier les multiples de 2 sont les nombres de la forme $a + ib\sqrt{5}$ avec a et b pairs. L'élément $(1 + i\sqrt{5})(1 - i\sqrt{5}) = 6$ est divisible par 2, mais aucun des facteurs 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 $y = c + id\sqrt{5}$. On 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.

Proposition 7.3.5. — 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.

Si l'anneau est principal, ces trois propriétés sont équivalentes.

Démonstration. Il suffit de montrer que la troisième propriété implique la première dans un anneau principal. Soit donc a irréductible et considérons l'idéal $(a) \subset A$. Si (a) n'est pas maximal, il existe un idéal maximal M tel que $(a) \subset M$ soit strictement contenu dans M. Comme A est principal il existe $m \in A$ tel que $(m) = M$. Mais alors $a = mn$ pour un $n \in A$. L'élément m n'est pas inversible, sinon M ne serait pas propre. L'élément n n'est pas inversible non plus, sinon on aurait $(a) = (m)$. On a donc trouvé une factorisation non banale de a, contraire à l'hypothèse que a est irréductible. □

En particulier, dans un anneau principal un élément irréductible est premier. Cet énoncé est parfois appelé *lemme de Gauß*.

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).

8. Anneaux factoriels

8.1. Définitions, premières propriétés

Définition 8.1.1. — On dit qu'un anneau A est *factoriel* si tout élément non nul de A peut s'écrire, de manière essentiellement unique, comme produit d'éléments irréductibles de A.

Dans la définition ci-dessus, on demande donc *l'existence* d'une décomposition en éléments irréductibles et son *unicité* dans un sens que l'on va préciser dans un instant. L'existence signifie que si a est un élément non nul de A, il existe $n \geq 0$, des éléments irréductibles $p_1, \ldots, p_n$ de 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 est à l'ordre et à des éléments inversibles près : si $a = up_1 \ldots p_n = u'p'_1 \ldots p'_m$, on demande que l'on a $m = n$ et qu'il existe une permutation $\sigma \in \Sigma_n$ 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.

Il est souvent utile 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. Un élément $a = u \prod p_i^{r_i}$ divise donc un élément $b = v \prod p_i^{s_i}$ si et seulement si pour tout i on a $r_i \leq s_i$. 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. Inversement, on il suffit de prendre $c = uv\prod_i p_i^{s_i-r_i}$.

Lemme 8.1.2. — Dans un anneau factoriel, tout élément irréductible est premier.

Démonstration. On va montrer que si a est irréductible et si $a|bc$ alors $a|b$ ou $a|c$. Pour simplifier on va supposer avoir normalisé la décomposition en facteurs irréductibles dans A. Comme a est irréductible, on a $a = up_j$ 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. Comme a divise bc, on sait que $s_j + t_j \geq 1$. Mais alors $s_j \geq 1$ ou $t_j \geq 1$. En particulier, a divise b ou c. □

La propriété ci-dessus dans un anneau factoriel que si un élément irréductible p divise ab alors p divise a ou b est appelé *propriété de Gauß*.

8.2. pgcd, ppcm

Soit A un anneau factoriel. Si a et b sont deux éléments (non nuls) de A, on peut définir leur ppcm et leur pgcd comme suit. Pour simplifier, on va supposer avoir normalisé la décomposition en facteurs irréductibles. Soient $a = u\prod p_i^{r_i}$ et $b = v\prod p_i^{s_i}$ les décompositions en facteurs irréductibles de a et b. On pose

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

Tout élément non nul de A qui divise a et b divise leur pgcd ; tout élément de A multiple de a et de b est multiple de leur ppcm.

Définition 8.2.1. — Deux éléments a et b sont dits *premiers* entre eux si leur pgcd est égal à 1.

Proposition 8.2.2. — Soit A un anneau factoriel et soient a et b deux éléments non nuls de A. L'idéal engendré par $\mathrm{pgcd}(a,b)$ est le plus petit idéal principal contenant l'idéal (a,b). L'idéal engendré par $\mathrm{ppcm}(a,b)$ est le plus grand idéal principal contenu dans l'idéal $(a)\cap(b)$. 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.

Démonstration. Soient $a = u\prod p_i^{r_i}$ et $b = v\prod p_i^{s_i}$ les décompositions en facteurs irréductibles de a et b. Un idéal principal (x) contient l'idéal (a,b) si et seulement si a et b sont multiples de x. Si $x = w\prod p_i^{t_i}$ est la décomposition en facteurs irréductibles de x, cela veut dire que pour tout i, on a $t_i \leq r_i$ et $t_i \leq s_i$ et donc $t_i \leq \min(r_i, s_i)$ ce qui signifie que x divise le pgcd de a et b. Pour l'énoncé sur le ppcm, on observe qu'un idéal principal (x) est contenu dans $(a)\cap(b)$ si et seulement si x est multiple de a et de b. Cela signifie que pour tout i, que $t_i \geq r_i$ et $t_i \geq s_i$, soit encore que $t_i \geq \max(r_i, s_i)$, soit encore que x est multiple du ppcm de a et b. □

Remarque 8.2.3. — Si l'on ne normalise pas la décomposition en facteurs irréductibles, le *ppcm* et le *pgcd* de deux éléments sera bien défini à multiplication par un élément inversible près, ou autrement dit un élément du monoïde quotient (pour la multiplication) $A/A^\times$.

8.3. Les anneaux principaux sont factoriels

Dans ce paragraphe nous démontrerons le théorème suivant :

Théorème 8.3.1. — 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 procédera en deux étapes. D'abord on montrera qu'il existe une décomposition en éléments irréductibles puis on montrera qu'elle est essentiellement unique.

Lemme 8.3.2. — Soit A un anneau principal et $a \in A$. Alors il existe $n \geq 0$, des éléments irréductibles $p_1, \ldots, p_n$ de A et un inversible u de A tels que $a = up_1 \ldots p_n$.

Démonstration. Supposons par l'absurde qu'il existe un élément a non nul de A dont qui n'est pas produit d'éléments irréductibles. Soit $a_1 = a$. L'élément a n'est pas inversible (sinon $a = u$ avec u inversible serait une décomposition), ni irréductible (sinon $a = p$ avec p irréductible serait une décomposition). Soit $a = bc$ une factorisation non banale. Comme a n'est pas produit d'éléments irréductibles, b ou c n'est pas produit d'éléments irréductibles. Soit a_2 cet élément. Ni b, ni c ne sont inversibles, l'idéal (a_2) contient donc strictement l'idéal (a_1). On construit ainsi, par récurrence, une suite $a_1, a_2, \ldots$ d'éléments de A tels que la suite d'idéaux

$$(a_1) \subset (a_2) \subset \ldots$$

soit strictement croissante. Soit I la réunion de ces idéaux. Comme la suite est croissante, c'est un idéal de A. Comme A est principal, il existe $x \in I$ 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 $(x) \subset (a_n)$. Comme $a_n \in I = (x)$, on a aussi $(a_n) \subset (x)$, d'où $(a_n) = (x)$. Mais (a_n) est strictement inclus dans (a_{n+1}) et $(a_{n+1}) \subset (x)$. Contradiction. Tout élément non nul d'un anneau principal admet donc une décomposition en éléments irréductibles. □

Lemme 8.3.3. — 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 $a \in A$. Si a est inversible, c'est-dire qu'il n'y pas de facteur irréductible, soit $a = u'p'_1 \ldots p'_m$ une autre décomposition. Si $m \neq 0$, les p_i sont inversibles, ce qui est absurde. Donnons nous maintenant deux décompositions $a = up_1 \ldots p_n = u'p'_1 \ldots p'_m$ de a et n minimal. Un élément irréductible étant premier dans un anneau principal

d'après le lemme de Gauß (proposition 7.3.5), l'élément irréductible p_n divise obligatoirement l'un des $p'_1, \ldots, p'_m$. Supposer que cela soit p_m, quitte à renuméroter. Il existe ainsi $u_n \in A$ tel que $p_n = u_n p' m$. Comme p_n est irréductible, u_n est inversible. On peut donc simplifier pour obtenir la relation suivante

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

D'après l'hypothèse de récurrence, on a $m-1 = n-1$, d'où $m = n$. De plus, il existe une permutation $\sigma \in \Sigma_{n-1}$ et des éléments inversibles u_i, pour $i = 1, \ldots, n-1$ tels que $p'_{\sigma(i)} = u_i p_i$. La décomposition d'un élément en facteurs irréductibles est donc essentiellement unique. □

Si l'on regarde la démonstration, on voit qu'un anneau A est en fait factoriel si et seulement si il vérifie les deux propriétés suivantes :

– toute suite d'idéaux principaux dans A est stationnaire ;

– tout élément irréductible de A est premier (propriété de Gauß).

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

8.4. **Le théorème de Gauß**

Dans ce paragraphe nous démontrerons le théorème suivant :

Théorème 8.4.1 (Gauß)**.** — Soit A un anneau factoriel. Alors l'anneau $A[X]$ est factoriel.

Corollaire 8.4.2. — Si A est un anneau factoriel, $A[X_1, \ldots, X_n]$ est un anneau factoriel. En particulier, si k est un corps, l'anneau $k[X_1, \ldots, X_n]$ est factoriel.

Démonstration. Cela se voit par récurrence sur n en utilisant l'isomorphisme $A[X_1, \ldots, X_n] \simeq (A[X_1, \ldots, X_{n-1}])[X_n]$. □

Dans tout le paragraphe A sera un anneau factoriel. Avant de démontrer le théorème on va commencer avec quelques préparations. Tout d'abord, on rappelle que les éléments inversibles de $A[X]$ sont exactement les polynômes constants égaux à un élément inversible de

A. En effet, comme A est intègre, nous avons $\deg PQ = \deg P + \deg Q$ pour deux polynômes $P, Q \in A[X]$. Si $PQ = 1$, on doit donc avoir $\deg P = \deg Q = 0$. Les polynômes P et Q sont donc constants ou autrement dit des éléments de A, inverses l'un de l'autre, c'est-à-dire inversibles.

Définition 8.4.3. — Soit A un anneau factoriel et soit $P \in A[X]$. On définit le *contenu* 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 déjà expliqué dans la section 8.2, on supposera implicitement avoir normalisé la décomposition en facteurs irréductibles. Sans cette hypothèse, le contenu serait bien définie à multiplication par un inversible près.

La propriété fondamentale du contenu est qu'il est multiplicatif :

Proposition 8.4.4. — Soit A un anneau factoriel et soient $P, Q \in A[X]$. Alors, $\mathrm{ct}(PQ) = \mathrm{ct}(P)\,\mathrm{ct}(Q)$.

Démonstration. Il suffit de montrer que si P et Q sont primitifs, alors leur produit PQ est encore primitif. En effet, si on écrit $P = \mathrm{ct}(P)P'$ et $Q = \mathrm{ct}(Q)Q'$ avec P' et Q' primitifs, on a $PQ = \mathrm{ct}(P)\,\mathrm{ct}(Q)P'Q'$, d'où $\mathrm{ct}(PQ) = \mathrm{ct}(P)\,\mathrm{ct}(Q)\,\mathrm{ct}(P'Q')$.

Supposons donc P et Q primitifs. Soit p un élément irréductible de A et montrer que p ne divise pas tous les coefficients de PQ. Pour cela, on considère des réductions modulo p de P et Q, c'est-à-dire les classes de $[P]$ et $[Q]$ dans l'anneau $A/(p)[X]$. Comme P et Q sont primitifs ces classes sons non nuls (sinon p diviserait les coefficients). Mais p est premier puisque A est factoriel d'après 8.1.2. L'anneau $A/(p)$ est donc intègre et donc $A/(p)[X]$ aussi. Par conséquent $[PQ] = [P][Q]$ est non nul dans $A/(p)[X]$ ce qui signifie que p ne divise pas tous les coefficients de PQ. Comme p était quelconque, on voit que PQ est primitif. □

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 $\mathbb{Q}$.

Nous avons déjà déterminé les éléments inversibles de l'anneau $A[X]$. Déterminons maintenant les éléments irréductibles de $A[X]$ pour un anneau factoriel A.

Proposition 8.4.5. — Soit A un anneau factoriel et K son corps de fractions. Alors les éléments irréductibles de $A[X]$ sont exactement
- les éléments irréductibles de A ;
- 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. Soit donc $a \in A$ irréductible et supposons que $P, Q \in A[X]$ sont tels que $a = PQ$. 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 $A[X]$. L'élément a est donc bien irréductible dans l'anneau $A[X]$.

Soit maintenant $P \in A[X]$ primitif, irréductible dans $K[X]$ et supposons $P = QR$ avec Q et R dans $A[X]$. Vu dans $K[X]$ cette relation doit être banale ou autrement dit, Q ou R est inversible dans $K[X]$, c'est-à-dire constant. Supposons que cela soit Q. Nous avons $\mathrm{ct}(P) = \mathrm{ct}(Q)\,\mathrm{ct}(R) = Q\,\mathrm{ct}(R)$, puisque Q est constant. Comme P est primitif, $\mathrm{ct}(P) = 1$ et l'élément Q est nécessairement inversible dans A donc dans $A[X]$. Ainsi, 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 primitif. Cette relation doit être banale, donc $\mathrm{ct}(P) = 1$ ou P_1 est inversible dans $A[X]$. On va montrer que dans le premier cas, P est irréductible dans $K[X]$ et que dans le second cas $\mathrm{ct}(P)$ est irréductible.

Dans le premier cas, P est primitif. Soit $P = QR$ une factorisation avec $Q, R \in K[X]$. On peut écrire $Q = qQ_1$ et $R = rR_1$, où q et r sont dans K et où Q_1 et R_1 sont deux polynômes primitifs de $A[X]$. En effet, on sort d'abord le dénominateur commun des coefficients, puis on sort le contenu. On a ainsi $P = (qr)Q_1R_1$. La fraction qr s'écrit a/b où $a, b \in A$. On obtient $bP = aQ_1R_1$ dans $A[X]$. Ces deux polynômes ont donc le même contenu, a et b respectivement. Par conséquent, $a = b$, d'où $qr = 1$, ce qui donne la relation $P = Q_1R_1$ dans $A[X]$. Comme P est irréductible dans $A[X]$, cette relation doit être banale dans $A[X]$, la relation $P = QR$ l'est donc aussi dans $K[X]$.

Dans le second 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 $A[X]$, ce qui contredit l'hypothèse que P est irréductible. □

Comme on voit dans la proposition ci-dessus, le corps de fraction 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 en particulier *factoriel* d'après le théorème 8.3.1. On va utiliser cette observation pour démontrer le théorème de Gauß.

Démonstration du théorème de Gauß 8.4.1. On va montrer 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 $K[X]$ d'où

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

où $c \in K$ et où les P_i sont des polynômes de $A[X]$ qui sont primitifs et irréductibles dans $K[X]$. On écrit maintenant $c = a/b$ avec a et b premiers entre eux. Alors, $bP = a\prod_{i=1}^{r} P_i$. En prenant le contenu de chaque côté on voit que $b\,\mathrm{ct}(P) = a$. Il suit que $c = a/b \in A$. L'élément c admet donc 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 8.4.5, 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 de Gauß. 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. Si $P \in A[X]$ est un polynôme primitif, irréductible dans K[X], qui divise un tel produit QR, il divise l'un des facteurs dans $K[X]$, disons Q. Nous avons donc $Q = SP$ avec $S \in K[X]$. Écrivons $S = (a/b)S_1$ avec S_1 dans $A[X]$ primitif et $a, b \in A$ premiers entre eux. On a alors $bQ = bSP = aS_1P$. En prenant le contenu de chaque côté, on voit $b\,\mathrm{ct}(Q) = a$ d'où $a/b = \mathrm{ct}(Q) \in A$. On a donc $S \in A[X]$, ce qui montre que 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. □

8.5. **Critères d'irréductibilité**

Dans cette section nous nous intéressons à comment décider si un polynôme $P \in A[X]$ est irréductible. En vu de la proposition 8.4.5, il est déjà important de comprendre cette question quand A est un corps k. 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 8.5.1. — 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. 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 nul, donc inversibles et la décomposition est nécessairement banale. Si $P = aX + b$, l'élément $-b/a \in k$ est bien entendu une racine de P.

Inversement, on observe que si $x \in k$ est une racine de P, on peut factoriser $P = (X - x)Q + R$ avec $\deg R < 1$. Le polynôme R est donc constant. Cette constante doit être nul puisque on a $P(x) = R(x) = 0$, d'où la factorisation $P = (X - x)Q$. Comme $\deg Q = \deg P - 1$, on voit que P n'est pas irréductible dès que $\deg P \geq 2$.

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.

□

Le critère suivant est souvent très utile.

Proposition 8.5.2 (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 8.5.3. — 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 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 8.5.4. — 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, si l'on fait le changement de variables affine $Y = X - 3$, on a $P(Y) = (Y+3)^2+(Y+3)+2 = Y^2+7Y+14$ 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 $K[X]$. Quitte à sortir le dénominateur commun, on peut écrire $R = (1/a)R'$ et $Q = (1/b)Q'$ avec $a, b \in A$ et aucun facteur irréductible de a ou b ne divise respectivement R' ou Q'. On a ainsi $abP = Q'R'$ dans $A[X]$. Supposons qu'un élément irréductible t divise ab. Il divise donc $Q'R'$ et donc, puisque t reste irréductible dans $A[X]$ d'après la proposition 8.4.5, Q' ou R' d'après la propriété de Gauß, valable dans $A[X]$ qui est factoriel d'après le théorème de Gauß 8.4.1. On peut donc diviser la relation par t. Quitte à continuer ainsi, on peut supposer que ab est inversible puis, en divisant encore, que $a = b = 1$. On a ainsi une relation $P = QR$ avec $Q, R \in A[X]$.

Réduisons maintenant cette équation modulo p. Rappelons, avant de continuer, que $A[X]/pA[X] \simeq (A/pA)[X]$. 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 $K(A/p)[X]$, on voit que l'on a $[Q] = [\alpha]X^k$ et $[R] = [\beta]X^{n-k}$ avec $\alpha, \beta \in A$. Dans $A[X]$ on a donc

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

Cela implique que l'on a

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

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 de départ est donc banale. Par conséquent P est bien irréductible dans $K[X]$. □

9. Résultant, Théorème de Bézout

9.1. Le résultant

Soit k un corps. Nous avons vu que $k[X]$ est un anneau factoriel. On se pose maintenant la question quand deux éléments $P, Q \in k[X]$ sont premiers entre eux, c'est-à-dire quand $\text{pgcd}(P, Q) = 1$. 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 $P, Q \in \mathbb{C}[X]$ ont une racine en commun.

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 auront 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 $-a_0/a_1 = -b_0/b_1$ ou autrement dit quand $a_0 b_1 - b_0 a_1 = 0$. On peut aussi chercher 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. Réciproquement, si (z_0, z_1) est une solution non triviale, alors $z = z_1/z_0$ est la racine commune. En effet, une solution non triviale (z_0, z_1) a automatiquement $z_0 \neq 0$, sinon P et Q ne seraient pas de degré 1. Alors $1/z_0(z_0, z_1) = (1, z)$ 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 $M = \left(\begin{smallmatrix} a_0 & a_1 \\ b_0 & b_1 \end{smallmatrix}\right)$, 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 $a_0 b_1 - b_0 a_1 = 0$.

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 généralisera pas forcément très bien en degré supérieur : on verra au second semestre qu'il n'existe pas de formule universelle pour résoudre les équations de degré supérieur ou égal à cinq. On peut donc se demander s'il n'est pas plus judicieux de résoudre à nouveau un système linéaire, cette fois ci en les indéterminées x^0, x^1, x^2. Le problème est que nous avons deux équations à partir de P et Q :

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

alors que nous avons trois indéterminées. 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 cependant sur les 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. Réciproquement, si on a une solution non trivial du système (z_0, z_1, z_2, z_3), on peut toujours supposer, comme ci-dessus, que $z_0 = 1$. Cependant, a priori, il n'est pas clair que $z_2 = z_1^2$. Toujours est-il qu'une condition nécessaire pour que P et Q aient une racine commune est donc l'annulation du déterminant de la matrice du système, c'est-à-dire que

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

En général, soient

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

deux polynômes de degré n et m respectivement. On peut supposer $n \geq m$, quitte à échanger les rôles de P et Q. On va chercher un système analogue à ceux pour $n = m = 1$ et $n = m = 2$. D'abord, si $n > m$, on va ajouter $n - m$ équations, on multipliant Q par $X, X^2, \ldots, X^{n-m}$. Cela n'ajoutera pas d'indéterminée. Ensuite, il faut multiplier avec des puissance de X pour arriver à autant d'équations que d'indéterminées. Si on multiplie avec k puissances de X on arrive à $2 + n - m + 2k$ équations avec $m + 1 + k$ indéterminées. Si on veut égalité, il faut poser $k = m - 1$, ce qui donne un système à $n + m$ équations avec $n + m$ indéterminées. Par exemple pour $n = 3$ et $m = 2$ on arrive à

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 \end{pmatrix} \begin{pmatrix} x^0 \\ x^1 \\ x^2 \\ x^3 \\ x^4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Encore, une condition nécessaire pour l'existence d'une racine en commun, est l'annulation du déterminant de la matrice du système.

Revenons à notre question initiale : quand est-ce que $P, Q \in k[X]$ sont premiers entre eux ? Comme $k[X]$ est principal, cela revient à dire qu'il existe $U, V \in k[X]$ tels que $UP + VQ = 1$. L'idée est de traduire en un problème linéaire, en s'inspirant du calcul ci-dessus. Pour cela, soit $k[X]_r$ le k-espace vectoriel des polynômes de degré $\leq r$. Il est de dimension $r+1$ avec une base naturelle $\{1, X, \ldots, X^r\}$. Considérons application linéaire

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

On observe qu'elle est bien définie, c'est-à-dire on a bien, au niveau des degrés, que $\deg(UP + VQ) \leq n + m - 1$.

Lue dans les bases $\{1, X, \ldots, X^{m-1}; 1, X, \ldots, X^{n-1}\}$ de l'espace vectoriel $k[X]_{m-1} \times k[X]_{n-1}$ et de $\{1, X, \ldots, X^{n+m-1}\}$ de $k[X]_{n+m-1}$, la matrice de ρ est la suivante :

$$R = \begin{pmatrix}
a_0 & & & 0 & b_0 & & & & 0 \\
a_1 & a_0 & & & b_1 & b_0 & & & \\
\vdots & & \ddots & & \vdots & & \ddots & & \\
a_{m-1} & & & a_0 & b_{m-1} & & & b_0 & \\
\vdots & & & \vdots & b_m & & & & \ddots \\
\vdots & & & \vdots & & \ddots & & & b_0 \\
a_n & a_{n-1} & & a_{n-m+1} & & & b_m & & \vdots \\
 & a_n & & \vdots & & & & \ddots & \vdots \\
 & & \ddots & \vdots & & & & & \ddots \\
0 & & & a_n & 0 & & & & b_m
\end{pmatrix}$$

où le vecteur colonne $(a_0, \ldots, a_n)$ est recopié m fois en décalant vers le bas, puis le vecteur colonne $(b_0, \ldots, b_m)$ est recopié n fois en décalant vers le bas. On appelle *résultant* de P et de Q est on note $\mathrm{Res}_{n,m}(P, Q)$ le déterminant de R.

Le fait que le résultant est la transposée et non la matrice des exemples du début provient du point de vue pris : pour chercher le pgcd il est plus naturel de considérer l'application $(U, V) \mapsto UP + VQ$. Bien entendu, au niveau du déterminant, le résultat est le même. La proposition suivante répond à la question du début. Sa démonstration est simple avec ce que nous savons déjà.

Proposition 9.1.1. — Soit k un corps et $P, Q \in k[X]$ deux polynômes de degrés inférieurs ou égaux à n et m respectivement. Alors, $\mathrm{Res}_{n,m}(P, Q)$ est nul si et seulement si

– ou bien P et Q ne sont pas premiers entre eux ;

– ou bien $a_n = b_m = 0$.

Démonstration. Si $P = Q = 0$, alors $m = n = 0$ et par définition du déterminant on a $\mathrm{Res}_{n,m}(P, Q) = 0$. Supposons qu'ils ne sont

pas tous deux nuls. On cherche à traduire que le déterminant est nul exactement quand le noyau de ρ est non trivial. Soit $D = \mathrm{pgcd}(P, Q)$. Alors on peut écrire $P = DP'$ et $Q = DQ'$ où P' et Q' sont premiers entre eux. Si U et V sont tels que $UP + VQ = 0$, nous avons aussi $UP' + VQ' = 0$. Par suite, Q' divise U et P' divise V. On a donc $U = Q'S$ et $V = P'T$. Par construction, on doit avoir $T = -S$, d'où $U = Q'S$ et $V = -P'S$. Ainsi $U \in k[X]_{m-1}$ si et seulement si $\deg S \leq m - 1 - \deg Q'$, tandis que $V \in k[X]_{n-1}$ si et seulement si $\deg S \leq n - 1 - \deg P'$. Maintenant on a

$$m - 1 - \deg Q' = (m - \deg Q) + \deg D - 1$$

et donc aussi $n - 1 - \deg P' = (n - \deg P) + \deg D - 1$. Posons $s = \max(n - \deg P, m - \deg Q)$. L'application $S \mapsto (Q'S, -P'T)$ où S vérifie $\deg S \leq s + \deg D - 1$ est un isomorphisme de k-espaces vectoriels de $k[X]_{s+deg(D)-1}$ sur le noyau de ρ. Ce noyau est donc de dimension $s + \deg D$. Il en résulte que $\mathrm{Res}_{n,m}(P, Q)$ est nul si et seulement si $s + \deg D > 0$, donc si $a_n = b_m = 0$ ou si D est de degré non nul. □

Corollaire 9.1.2. — Soient $P, Q \in \mathbb{C}[X, Y]$. Soit $A = \mathbb{C}[Y]$. Dans $A[X] = \mathbb{C}[X, Y]$ on écrit

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

où les P_i et les Q_j sont des éléments de $\mathbb{C}[Y]$. Soit $R = Res_{m,n}(P, Q)$. Alors $R \in \mathbb{C}[Y]$. Un élément $y \in \mathbb{C}$ est racine de R si et seulement si

- ou bien $P(X, y)$ et $Q(X, y)$ ont une racine commune dans $\mathbb{C}$;
- ou bien $P_n(y) = Q_m(y) = 0$.

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

$$R(y) = Res_{m,n}(P, Q)(y) = Res_{m,n}(P(X, y), Q(X, y))$$

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

9.2. Le théorème de Bézout

Théorème 9.2.1. — 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 $pq=1$.

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.*

$$\mathbb{A}^n_k:=\{(x_1,\dots,x_n)\,|\,x_i\in k\quad\forall i=1,\dots,n\},$$

Soient $P_1,\dots,P_\ell\in k[X_1,\dots,X_n]$ des polynômes en n indéterminées. On note :

$$V(P_1,\dots,P_\ell)=\{(x_1,\dots,x_n)\in\mathbb{A}^n_k;P_i(x_1,\dots,x_n)=0,i=1,\dots,\ell\}.$$

La notation V est un anglicisme (V pour *vanishing*). Commençons avec un exemple. 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 :

$$\begin{aligned} V(P, Q) &= \{(x, y) \in \mathbb{A}^2_{\mathbb{C}} \,|\, x^2 + y^2 = 1 \text{ et } x = -2\} \\ &= \left\{\left(-2, i\sqrt{3}\right)\right\} \cup \left\{\left(-2, -i\sqrt{3}\right)\right\}. \end{aligned}$$

Soit $J = \langle P_1, \ldots, P_\ell \rangle$ l'idéal de $k[X_1, \ldots, X_n]$ engendré par les polynômes $P_1, \ldots, P_\ell$. Alors pour tout $P \in J$ on a :

$$P(x_1, \ldots, x_n) = 0 \text{ pour } (x_1, \ldots, x_n) \in V(P_1, \ldots, P_\ell).$$

En effet, on peut écrire $P = \sum_{i=1}^{\ell} Q_i P_i$ pour certains $Q_i \in k[X_1, \ldots, X_n]$ d'où :

$$P(x_1, \ldots, x_n) = \sum_{i=1}^{\ell} Q_i(x_1, \ldots, x_n) P_i(x_1, \ldots, x_n) = 0.$$

Généralement, nous définissons pour un idéal $J \subset k[X_1, \ldots, X_n]$ *le sous-ensemble algébrique déterminé par l'idéal* J par :

$$V(J) := \{(x_1, \ldots, x_n) \in \mathbb{A}^n_k \,|\, P(x_1, \ldots, x_n) = 0 \quad \forall P \in J\}.$$

Lemme 9.2.2. — Si $J = \langle P_1, \ldots, P_\ell \rangle$, alors $V(J) = V(P_1, \ldots, P_\ell)$.

Démonstration. Nous venons de voir que $V(P_1, \ldots, P_\ell) \subset V(J)$. L'inclusion inverse est claire car $P_i \in J$ pour tout $i \in \{1, \ldots, \ell\}$. □

Proposition 9.2.3. — On a les propriétés suivantes :

a) $V(\langle 0 \rangle) = \mathbb{A}^n_k$ et $V(k[X_1, \ldots, X_n]) = \emptyset$;

b) $\bigcup_{j=1}^{\ell} V(I_j) = V(\bigcap_{j=1}^{\ell} I_j)$;

c) $\bigcap_{\lambda \in \Lambda} V(I_\lambda) = V\left(\sum_{\lambda \in \Lambda} I_\lambda\right)$.

On en déduit que l'ensemble :

$$\tau(\mathbb{A}_k^n) := \{V(J)^c \mid J \text{ idéal de } k[X_1, \ldots, X_n]\}$$

forme une topologie sur $\mathbb{A}_k^n$ ou autrement dit : les sous-ensembles algébriques de $\mathbb{A}_k^n$ forment les fermés d'une topologie sur $\mathbb{A}_k^n$ qu'on appelle la *topologie de Zariski* de $\mathbb{A}_k^n$. On dira donc parfois *fermé de Zariski* au lieu de *sous-ensemble algébrique*.

Démonstration.

a) Clair.

b) On observe que si $J_1 \subset J_2$ alors $V(J_1) \supset V(J_2)$: l'opération $V(\cdot)$ renverse les inclusions. Ainsi $V(I) \subset V(I \cap J)$ et $V(J) \subset V(I \cap J)$, donc $V(I) \cup V(J) \subset V(I \cap J)$. Réciproquement, soit $(x_1, \ldots, x_n) \in V(I \cap J)$. Si $(x_1, \ldots, x_n) \notin V(I)$, il existe un polynôme $P \in I$ tel que $P(x_1, \ldots, x_n) \neq 0$. Pour tout $Q \in J$ on a $P \cdot Q \in I \cap J$ donc $Q(x_1, \ldots, x_n)P(x_1, \ldots, x_n) = 0$, ce qui donne $Q(x_1, \ldots, x_n) = 0$ pour tout $Q \in J$, donc $(x_1, \ldots, x_n) \in V(J)$. Ainsi, on a obtenu $V(I \cap J) \subset V(I) \cup V(J)$, d'où finalement l'égalité. Par récurrence, l'énoncé analogue pour un nombre *fini* d'idéaux est encore valable.

c) Pour $\mu \in \Lambda$ on a $I_\mu \subset \sum_{\lambda \in \Lambda} I_\lambda$ donc $V(I_\mu) \supset V\left(\sum_{\lambda \in \Lambda} I_\lambda\right)$, d'où : $\bigcap_{\mu \in \Lambda} V(I_\mu) \supset V\left(\sum_{\lambda \in \Lambda} I_\lambda\right)$. Inversement si $(x_1, \ldots, x_n) \in \bigcap_{\mu \in \Lambda} V(I_\mu)$

$$\forall \lambda \in \Lambda, \quad \forall P_\lambda \in I_\lambda, \quad P_\lambda(x_1, \ldots, x_n) = 0.$$

Puisque l'idéal $\sum_{\lambda \in \Lambda} I_\lambda$ est engendré par les polynômes $P_\lambda \in I_\lambda$ pour tout λ, il en résulte que $(x_1, \ldots, x_n) \in V\left(\sum_{\lambda \in \Lambda} I_\lambda\right)$.

□

Exemple 9.2.4. — Soit k un corps infini. Alors $Z \subset \mathbb{A}_k^1$ est un fermé de Zariski si et seulement si $Z = \emptyset$, ou $Z = \mathbb{A}_k^1$, ou Z est un sous-ensemble fini de $\mathbb{A}_k^1$. En effet, si Z est un fermé distinct de $\emptyset$ et de $\mathbb{A}_k^1$, alors $Z = V(I)$ avec $I \neq 0$ et $I \neq k[X]$. Puisque $k[X]$

est un anneau principal, on a $I = \langle P \rangle$ donc $V(I) = V(P)$ et P n'a qu'un nombre fini de zéros. Inversement, si $Z = \{a_1, \ldots, a_n\}$ est un sous-ensemble fini de $\mathbb{A}^1_k$ on voit que Z est de la forme $Z = V(I)$ avec $I = \langle P \rangle$ et $P(X) = \prod_{i=1}^{n}(X - a_i)$.

Remarque 9.2.5. — Par récurrence on a vu que :

$$\bigcup_{j=1}^{n} V(I_j) = V\left(\bigcap_{j=1}^{n} I_j\right).$$

Cependant ceci n'est valable que pour des réunions *finies*. En effet, supposons k infini et $a_1, a_2, \ldots \in k$ distincts tels que $Z = \{a_1, a_2, \ldots\} \neq \mathbb{A}^1_k$. Alors $Z = \bigcup_{n\in\mathbb{N}} V(\langle X - a_n \rangle)$ mais ne peut pas être de la forme $V(J)$ car les seuls fermés de Zariski de $\mathbb{A}^1_k$ distincts de $\mathbb{A}^1_k$ et non vides sont les ensembles finis.

Démonstration. Démontrons maintenant le théorème de Bézout. Il s'agit de montrer que si $P, Q \in \mathbb{C}[X, Y]$ sont premiers entre eux, alors l'ensemble $V(P, Q) \subset \mathbb{A}^2_{\mathbb{C}}$ est fini de cardinal au plus pq. 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 R par rapport à X est un polynôme non nul R_Y de $\mathbb{C}[Y]$. Ainsi, les racines communes à P et Q n'ont qu'un nombre fini d'ordonnées y possibles. De même il n'y qu'un nombre fini d'abscisses possibles. Ainsi $V(P, Q)$ est fini.

Montrons que $\#V(P, Q) \leq pq$. Quitte à faire un changement de variables linéaire on peut supposer qu'une droite horizontale ne contienne au plus qu'un point de $V(P, Q)$ (Il n'y a qu'un nombre fini de directions est à éviter, donc c'est possible.) Cela change les polynômes P et Q mais non leurs degrés. Il suffit donc de montrer que l'ensemble des ordonnées des points de $V(P, Q)$ est de cardinal au plus pq. Pour cela on écrit

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

où P_n et Q_m sont non nuls. Soit $R = Res_{n,m}(P,Q)$ le résultant par rapport à X. Si $y \in \mathbb{C}$ 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 $1 \leq j \leq m$, on a $R_{ij} = P_{i-j}$ si $0 \leq i-j \leq n$ et $R_{ij} = 0$ sinon
- pour $m+1 \leq j \leq m+n$, on a $R_{ij} = Q_{i-j+m}$ si $0 \leq i-j+m \leq m$ et $R_{ij} = 0$ sinon

Le degré de R_{ij} est donc majoré par $p-i+j$ si $1 \leq j \leq m$ et par $q-m-i+j$ si $m+1 \leq j \leq m+n$. Maintenant le déterminant de R est une somme de produits de la forme

$$\prod_{j=1}^{m+n} R_{\sigma(j)j}$$

où σ est une permutation de l'ensemble $\{1,\ldots,n\}$. Au niveau des degrés, on voit alors que nous avons

$$\begin{aligned}
\sum_{j=1}^{m+n} \deg R_{\sigma(j)j} &\leq \sum_{j=1}^{m}(p-\sigma(j)+j) + \sum_{j=m+1}^{m+n}(q-m-\sigma(j)+j) \\
&\leq pm + (q-m)n - \sum_{j=1}^{n+m}\sigma(j) + \sum_{j=1}^{n+m} j \\
&\leq pq - (p-n)(q-m) \\
&\leq pq
\end{aligned}$$

□

10. Polynômes symétriques

10.1. Définitions, premières propriétés

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

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

Un polynôme constant est symétrique ; si P et Q sont symétriques, alors $P + Q$ et PQ sont encore symétriques. L'ensemble des polynômes symétriques est donc un sous-anneau, noté $A[X_1, \ldots, X_n]^{S_n}$, dans l'anneau des polynômes. Les polynômes symétriques élémentaires $s_k := \sum_{i_1 < \ldots < i_k} X_{i_1} \cdots X_{i_k}$ sont symétriques pour $0 < k \leq n$. Explicitement, pour $n = 4$ on a

$$\begin{aligned} s_1 &= X_1 + X_2 + X_3 + X_4 \\ s_2 &= X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 \\ s_3 &= X_1X_2X_3 + X_1X_2X_4 + X_1X_3X_4 + X_2X_3X_4 \\ s_4 &= X_1X_2X_3X_4 \end{aligned}$$

La notation s_k pour les polynômes symétriques élémentaires n'est pas tout à fait satisfaisant, puisque le nombre de variables en jeux dépend du contexte et non des notations. Mais ajouter des indices supplémentaires aurait alourdi les notations.

Un autre exemple de polynômes symétriques sont les sommes de puissances $t_k := X_1^k + \ldots + X_n^k$ pour $k > 0$.

Remarque 10.1.1. — (formules de Girard) Nous avons la relation suivante dans $A[X_1, \ldots, X_n, t]$

$$(t - X_1) \cdot \ldots \cdot (t - X_n) = t^n - s_1 t^{n-1} + s_2 t^{n-2} + \ldots + (-1)^n s_n. \tag{10.1}$$

C'est la formule de Girard et Viète sur la relation entre coefficients et zéros d'un polynôme : si $\lambda_1, \ldots, \lambda_n \in A$ sont les zéros du polynômes

$P = X^n + a_1X^{n-1} + a_2X^{n-2} + \ldots + a_{n-1}X + a_n$, alors on a

$$a_k = (-1)^k s_k(\lambda_1, \ldots, \lambda_n).$$

10.2. **Théorème fondamental sur les polynômes symétriques**

Théorème 10.2.1. — Soit A un anneau. Alors le morphisme

$$f : A[Y_1, \ldots, Y_n] \to A[X_1, \ldots, X_n]^{S_n} \ , \ Y_i \mapsto s_i,$$

est un isomorphisme d'anneaux.

Autrement dit, tout polynôme symétrique est un polynômes en les polynômes symétriques s_k, $k = 1, \ldots, n$ et ceci de manière unique.

Démonstration. Remarquons d'abord que $Y_i \mapsto s_i$ définit, grâce à la propriété universelle des anneaux des polynômes, un morphisme d'anneaux $A[Y_1, \ldots, Y_n] \to A[X_1, \ldots, A_n]$. Et puisque l'évaluation d'un polynôme quelconque en des polynômes symétriques est encore symétrique, on sait que l'image est dans le sous-anneau des polynômes symétriques.

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

Algorithme 1 : Soit $q : A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_{n-1}]$ 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 et que l'on a $q(s_n) = 0$ et $q(s_i) = s'_i$, le $i^{\text{ème}}$ polynôme symétrique élémentaire en les variables $X_1, \ldots, X_{n-1}$, pour $i < n$.

Soit $f' : A[Y_1, \ldots, Y_{n-1}] \to A[X_1, \ldots, X_{n-1}]$ le morphisme d'anneau défini par $Y_i \mapsto s'_i$. Par récurrence, on peut supposer que f' est un isomorphisme sur le sous-anneau des polynômes symétriques. Nous avons un diagramme commutatif de suites exactes (cela signifie

ici que q est surjectif et de noyau (Y_n) et (X_n) respectivement)

$$\begin{array}{ccccccccc} 0 & \to & (Y_n) & \to & A[Y_1,\ldots,Y_n] & \stackrel{q}{\to} & A[Y_1,\ldots,Y_{n-1}] & \to & 0 \\ & & \downarrow & & \downarrow f & & \downarrow f' & & \\ 0 & \to & (X_n) & \to & A[X_1,\ldots,X_n] & \stackrel{q}{\to} & A[X_1,\ldots,X_{n-1}] & \to & 0 \end{array}$$

Soit $P \in A[X_1,\ldots,X_n]$ symétrique et $P' = q(P)$. Alors P' est encore symétrique (en les variables $X_1,\ldots,X_{n-1}$). Par récurrence il existe un polynôme $Q' \in A[Y_1,\ldots,Y_{n-1}]$ tel que $f'(Q') = P'$. Soit Q tel que $q(Q) = Q'$. La différence $R := P - f(Q)$ est alors un polynôme avec $q(R) = 0$, d'où $X_n|R$. Grâce à la symétrie de R, on a également $X_i|R$ pour $i = 1,\ldots,n-1$ et par la suite $s_n|R$. On pose $\tilde{P} := R/s_n$. Alors le degré de $\tilde{P}$ est strictement plus petit que celui de P. On peut donc supposer, par récurrence sur le degré, que $\tilde{P}$ est dans l'image de f. Il existe donc un polynôme $\tilde{Q} \in A[Y_1,\ldots,Y_n]$ avec $f(\tilde{Q}) = \tilde{P}$. On a alors $P = s_n f(\tilde{Q}) + f(Q)$.

L'injectivité se montre de manière analogue : Supposons $Q \in \mathrm{Ker}(f)$. Alors $q(Q)$ est dans le noyau de f'. Par récurrence, $q(Q)$ est trivial. Par conséquent on a $Q = Y_n\tilde{Q}$ avec $\tilde{Q}$ un polynôme de degré strictement plus petit. Puisque $0 = f(Q) = X_n \cdot f(\tilde{Q})$ on a $\tilde{Q} \in \mathrm{Ker}(f)$. Par récurrence sur le degré de Q on voit que $\tilde{Q} = 0$ et donc que $Q = Y_n\tilde{Q} = 0$.

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

L'idée est de mettre un ordre lexicographique sur les monômes $X^d = X_1^{d_1}\cdots X_n^{d_n}$: on pose $X^d > X^{d'}$ s'il existe i avec la propriété $d_j = d'_j$ pour tout $j < i$ et $d_i > d'_i$. Soit maintenant $P = \sum P_t X^t$ un polynôme symétrique. Pour le monôme principal X^d de P, c'est-à-dire le monôme le plus grand de P pour l'ordre ci-dessus, on a par symétrie de P que $d_1 \geq d_2 \geq \ldots \geq d_n$. Si l'on considère le polynôme

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

on observe que Q a le même monôme principal que P. La différence $P - Q$ a donc un monôme principal strictement plus petit que celui de P. Le théorème suit par récurrence.

De même, on démontre l'injectivité : le polynôme $s_1^{\nu_1} \cdots s_n^{\nu_n}$ a comme monôme principal $x_1^{\nu_1+\ldots+\nu_n} x_2^{\nu_2+\ldots+\nu_n} \cdots x_n^{\nu_n}$. Maintenant, les images de monômes différents $Y_1^{\nu_1} \cdots Y_n^{\nu_n}$ sous f ont des monômes principaux différents. Ainsi, dans $f(\sum_\nu a_\nu Y^\nu)$ on ne peut pas avoir l'annulation complète de tous les monômes en les variables X_i. □

Le deuxième algorithme est facile à mettre en œuvre. On cherche d'abord le monôme principal de P. Ensuite on considère le polynôme Q comme dans la démonstration ci-dessus, puis on continue avec le polynôme $P - Q$.

10.3. **Applications**

Une conséquence importante du théorème est le principe suivant

Corollaire 10.3.1. — Soient A, B deux anneaux tels que $A \subset B$ et $P = X^n + a_1 X^{n-1} + \ldots + a_n \in A[X]$ un polynôme qui se décompose sur B en facteurs linéaires :

$$f(X) = (X - \lambda_1) \cdot \ldots \cdot (X - \lambda_n).$$

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

Démonstration. Soit $f : A[X_1, \ldots, X_n] \to B$ le morphisme d'anneau tel que $f : X_i \mapsto \lambda_i$. L'hypothèse sur b dit qu'il existe un polynôme symétrique P avec $f(P) = b$. D'après les formules de Girard und Viète, on a $f(s_i) = (-1)^i a_i \in A$. D'après le théorème ci-dessus, il existe donc un polynôme $Q \in A[Y_1, \ldots, Y_n]$ avec $P = Q(s_1, \ldots, s_n)$. Mais alors, $b = f(P) = Q(f(s_1), \ldots, f(s_n)) \in A$. □

Que se passe-t-il pour les sommes des puissance $t_k := x_1^k + \ldots + x_n^k$? D'après le théorème, ils doivent s'exprimer en fonction des s_i. On voit

facilement

$$\begin{aligned} t_1 &= s_1 \\ t_2 &= s_1^2 - 2s_2 \\ t_3 &= s_1^3 - 3s_1s_2 + 3s_3 \end{aligned}$$

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 :

Lemme 10.3.2. — (Newton) Nous avons

$$s_0t_n - s_1t_{n-1} + s_2t_{n-2} - \ldots + (-1)^n t_0 s_n = 0. \tag{10.2}$$

Démonstration. On remarque que par définition $s_0 = 1$ et que $t_0 = n$. Si l'on évalue l'équation (10.1) en les X_i on obtient

$$0 = X_i^n - s_1X_i^{n-1} + \ldots + (-1)^n s_n.$$

Le lemme s'en suit 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 10.2.1 Remarquons que le facteur devant s_n est égal à $n = t_0$ dans l'identité (10.2). Ainsi, si l'on résout dans le sens inverse, on doit prendre des dénominateurs : les formules

$$\begin{aligned} s_1 &= t_1 \\ s_2 &= \frac{1}{2}(t_1^2 - t_2) \\ s_3 &= \frac{1}{6}t_1^3 - \frac{1}{2}t_1t_2 + \frac{1}{3}t_3 \end{aligned}$$

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

11. Compléments sur les groupes

Dans les sections qui suivent nous allons étudier davantage la notion de groupe, particulièrement dans le cas où les groupes en question ne sont pas supposés abéliens.

11.1. Rappels sur les sous-groupes

Soit G un groupe. Rappelons qu'un ensemble $H \subset G$ est un sous-groupe, si H est non vide, si le produit de deux éléments de H est encore dans H et si H est lui-même un groupe pour la restriction du produit dans G. Pour qu'un sous-ensemble non-vide $H \subset G$ est un sous-groupe il suffit que $gh^{-1} \in H$ pour tout $g, h \in H$. On écrit souvent $H < G$, pour exprimer que H est un sous-groupe de G.

Un sous-groupe $H < G$ est *distingué* ou *normal* si $ghg^{-1} \in H$ pour tout $h \in H$ et $g \in G$. Nous écrivons $H \lhd G$ pour exprimer que H est distingué dans G. Le *centre* d'un groupe

$$Z(G) := \{g \in G \mid hg = gh \text{ pour tout } h \in G\}.$$

est distingué.

Pour un sou-groupe $H < G$ et un élément $a \in G$ on note $aH = \{ah \mid h \in H\}$ la *classe à gauche* de H engendré par a. De manière analogue, $Ha = \{ha \mid h \in H\}$ est la classe à droite de H. L'ensemble des classes à gauches est noté par G/H ; l'ensemble des classes à droite est noté par $H\backslash G$. Les classes à gauche (ou à droite) ont clairement le même cardinal que H (l'application $G \to G, g \mapsto ax$ est une bijection, a étant inversible). De plus deux classes à gauche (ou à droite) sont ou bien disjoints ou bien égal : ainsi G est la réunion disjoint des classes à gauche (ou à droite) sous H. Par conséquent, nous avons le

Théorème 11.1.1. — (Lagrange) Pour tous sous-groupe $H < G$

$$|G| = |H| \cdot |G/H| = |H| \cdot |H\backslash G|.$$

Un sous-groupe H est distingué exactement quand $aH = Ha$ pour tout $a \in G$. Dans ce cas, les classes à gauche sont les classes à droite et les ensembles G/H et $H\backslash G$ sont les mêmes.

Proposition 11.1.2. — Soit $N \lhd G$. Il existe exactement une structure de groupe sur G/N, pour laquelle la projection canonique $\pi : G \to G/N$ est un groupe.

On appelle G/N avec cette structure de groupe le groupe quotient de G par rapport au sous-groupe distingué N.

Démonstration. Si $\pi : G \to G/N$ est un morphisme de groupes

$$g_1N \cdot g_2N = \pi(g_1) \cdot \pi(g_2) = \pi(g_1g_2) = g_1g_2N.$$

La structure de groupe sur G/N est donc définie de manière unique. Réciproquement, si l'on pose la multiplication sur G/N de cette manière, alors il faut d'abord montrer qu'elle est bien définie : si $g_1N = g_1'N$ et $g_2N = g_2'N$, alors il existe $n_1, n_2 \in N$ avec $g_1' = g_1n_1$ et $g_2' = g_2n_2$. Il suit

$$g_1'g_2' = g_1n_1g_2n_2 = g_1g_2(g_2^{-1}n_1g_2)n_2.$$

Comme N est distingué, on a bien$(g_2^{-1}n_1g_2)n_2 \in N$. Maintenant il est facile de voir que ce produit définit une structure de groupe sur G/N et que π est un morphisme de groupes. □

Proposition 11.1.3. — Soit $\varphi : G \to G'$ un morphisme de groupes. Alors φ induit un isomorphisme de groupes

$$G/\operatorname{Ker}(\varphi) \to \operatorname{Im}(\varphi).$$

Démonstration. En remplaçant G' par $\varphi(G)$, on peut supposer que φ est surjectif. Soit $N = \operatorname{Ker}(\varphi)$. On a $\varphi(g_1) = \varphi(g_2)$ si et seulement si $g_1^{-1}g_2 \in N$, *i.e.* $g_1N = g_2N$. Ainsi $\bar{\varphi} : G/N \to G'$, $g_1N \mapsto \varphi(g_1)$, est bien défini, un morphisme de groupes, et bijectif. □

Théorème 11.1.4. — (Propriété universelle de G/N) Soit G un groupe, $N \lhd G$ un sous-groupe distingué de G et $\pi : G \to G/N$

la projection canonique. Un morphisme de groupes $\varphi : G \to G'$ se factorise à travers G/N, *i.e.* il existe un morphisme de groupes $\bar{\varphi} : G/N \to G'$ avec $\varphi = \bar{\varphi} \circ \pi$, si et seulement si $N \subset \mathrm{Ker}(\varphi)$.

Démonstration. Si $\bar{\varphi}$ existe, on a $\varphi(N) = \bar{\varphi}(\pi(N)) = \bar{\varphi}(\bar{e}) = e'$, *i.e.* $N \subset \mathrm{Ker}(\varphi)$. Réciproquement, supposons $N \subset \mathrm{Ker}(\varphi)$. Alors on a pour deux représentants g_1, g_2 de la même classe, *i.e.* $g_1 N = g_2 N \in G/N$, que $g_1^{-1} g_2 \in N$, d'où $\varphi(g_1)^{-1}\varphi(g_2) = e'$ ou $\varphi(g_1) = \varphi(g_2)$. Ainsi $\bar{\varphi}(g_1 N) := \varphi(g_1)$ est bien défini. Il vérifie ensuite que $\bar{\varphi}$ est un morphisme de groupes, et d'après construction $\bar{\varphi} \circ \pi = \varphi$. □

11.2. **Actions de groupe**

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 S_X l'ensemble des bijections de X. Si G opère sur X, on peut définir une application

$$\rho : G \to S_X, g \mapsto (x \mapsto g.x).$$

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 $\rho : G \to S_X$, alors $g.x := \rho(g)(x)$ définit une action de groupes de G sur X.

De manière analogue on définit une action à droite. Un ensemble X muni d'une action d'un groupe G sera appelé un $G - ensemble$.

Soit X un G-ensemble. *L'orbite* de $x \in X$ est le sous-ensemble $Gx := Orb^G(x) := \{gx \,|g \in G\}$ de X. Le *stabilisateur* de $x \in X$ est le sous-groupe $G_x := Stab^G(x) := \{g \in G \mid gx = x\}$ de G.

L'espace des orbites est l'ensemble des orbites et sera noté pour une action à gauche par $G\backslash X$ et pour une action à droite par X/G. La projection canonique $\pi : X \to G\backslash X$ 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. — (Équation des orbites) Soit G un groupe fini et X un G-ensemble. Alors

a) $|X| = \sum_{B \in G\backslash X} |B|$;
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 S_n des bijections de $[n] = \{1, \ldots, n\}$ opère sur l'ensmeble $[n]$ par $(\pi, k) \mapsto \pi(k)$. L'opération est transitive : si $x, y \in [n]$ 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 $x \in [n]$ est isomorphe au groupe symétrique S_{n-1}.

Exemple 11.2.3. — Soit $H < G$ un sous-groupe. Alors H opère sur G à gauche par multiplication à gauche : $h.g := hg$ et à droite par multiplication à droite : $g.h = gh$. Les orbites sont exactement les classes à droite et à gauche respectivement. On remarque l'échange de gauche et droite : la classe à droite de H par rapport à a est l'ensemble $Ha = \{ha \mid h \in H\}$, donc l'orbite pour l'action à gauche. L'action est libre et l'équation des orbites n'est autre que le théorème de Lagrange.

11.3. **Calculer dans le groupe symétrique**

Le calcul dans le groupe symétrique est supposé connu des années de licence. Nous rappelons cependant les règles les plus importantes pour fixer les notations.

Soit $n \in \mathbb{N}$. Le groupe symétrique S_n est l'ensemble des bijections de l'ensemble $[n] = \{1, \ldots, n\}$ avec pour structure de groupe la composition des bijections. Ses éléments sont appelés des *permutations*.

Pour toute suite $(n_1, \ldots, n_k)$ d'éléments deux à deux différents de $[n]$ on note $\pi = (n_1 \ \ldots \ n_k) \in S_n$ la permutation définie par

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

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 $[n]$). 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 $[n]$. Finalement, si l'inverse du cycle $(n_1 \ldots n_k)$ est donné par le cycle $(n_k \ldots n_1)$.

Soit $\pi \in S_n$ une permutation quelconque. On va montrer comment on peut écrire π de manière unique (à ordre près) comme produit de cycles disjoints. Pour cela, on considère le groupe cyclique engendré par π, *i.e.* $\langle \pi \rangle = \{\pi^k; k \in \mathbb{Z}\} \subset S_n$ et son action sur $[n]$. Sous cette action $[n]$ se décompose en orbites $B_1, \ldots, B_s$ que l'on suppose numérotées de telle manière que $|B_1| \geq |B_2| \geq \ldots \geq |B_s|$.

Soit $\lambda_i = |B_i|$ pour $i = 1, \ldots, s$. D'après l'équation des orbites on a $\sum \lambda_i = n$; par hypothèse $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_s \geq 1$. On appelle une telle suite de nombre naturels une *partition* de n et on notera souvent $[\lambda_1, \ldots, \lambda_s]$.

Nous associons ainsi une partition $\lambda(\pi)$ de n à toute permutation $\pi \in S_n$ qu'on appellera le *type de cycle* de π. Toute orbite B de longueur ℓ définit dé manière unique un ℓ-cycle ζ comme suit : pour $x \in B$ quelconque on pose $\zeta = (x\, \pi(x)\, \pi^2(x) \ldots \pi^{\ell-1}(x))$. On observe qu'une orbite de longueur 1, qui ne comporte donc uniquement un point fixe sous $\langle \pi \rangle$, définit bien entendu l'identité. Si l'on associe de cette manière à toute orbite B_i un cycle de longueur λ_i un λ_i-cycle ζ_i, alors les cycles $\zeta_1, \zeta_2, \ldots, \zeta_s$ sont deux à deux disjoints et nous avons $\pi = \zeta_1 \zeta_2 \ldots \zeta_s$. Dans cette écriture nous pouvons et allons bien entendu oublier les cycles de longueur 1. Dans le cas $\pi = \mathrm{Id}_{[n]}$ il n'y a pas d'orbite de longueur ≥ 2, et π et donc le produit vide. De cette manière nous pouvons donc écrire toute permutation en tant que produit de cycles disjoints et ceci de manière unique, à l'ordre de facteurs près bien entendu.

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 $(145)(27) \in S_8$

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 est facile à démontrer par calcul direct pour le premier énoncé ; le second énoncé suit du premier. Il est laissé en exercice (ou regardez dans vos cours de licence)

Lemme 11.3.1. — Soit π une permutation et $(n_1 \ \dots \ n_k)$ un k-cycle de S_n. Alors on a

$$\pi \cdot (n_1 \ \dots \ n_k) \cdot \pi^{-1} = (\pi(n_1) \ \dots \ \pi(n_k)).$$

Deux permutations $\pi, \pi' \in S_n$ sont conjuguées si et seulement si ils ont le même type de cycle. En particulier, l'application

$$\begin{array}{rcl} \{\text{classes de conjugaisons de } S_n\} & \to & \{\text{partitions de } n\} \\ \pi & \mapsto & \lambda(\pi), \end{array}$$

est une bijection.

Proposition 11.3.2. — Soit $n \geq 3$. Alors le centre de S_n est trivial.

Démonstration. Rappelons que le centre $Z(S_n)$ est le sous-groupe de S_n des éléments de S_n qui commutent avec tous les éléments de S_n. Soit $\pi \in S_n$ non trivial (*i.e.* différent de l'identité). Il existe donc $a \in [n]$ tel que $\pi(a) = b \neq a$. Comme $n \geq 3$, il existe $c \in [n]$ avec $c \neq a$ et $c \neq b$. D'après le lemme précédent,

$$\pi \cdot (ac)\pi^{-1} = (b\pi(c))$$

Cette transposition est différente de (ac) puisque $b \neq a, b \neq c$. Ainsi, π ne commute pas avec (ac) et ne peut donc pas être dans le centre de S_n. □

Proposition 11.3.3. — Soit $n \geq 2$. Alors S_n est engendré par les transpositions.

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

Soit π une permutation et $\lambda(\pi) = [\lambda_1, \ldots, \lambda_s]$ le type de cycle de π. On appelle *longueur* de π l'entier $\ell(\pi) = \sum(\lambda_i - 1)$. Ainsi la longueur d'un k-cycle est $k-1$. En particulier, la longueur d'une transposition est 1. On dira qu'une permutation est *paire* (respectivement *impaire*) si sa longueur est paire (respectivement impaire). La proposition suivante est supposé connue de la licence :

Proposition 11.3.4. — L'application $S_n \to \{\pm 1\}, \pi \mapsto (-1)^{\ell(\pi)}$ est un morphisme de groupes.

En particulier, l'ensemble des éléments pairs de S_n est un sous-groupe distingué de S_n, appelé le groupe alterné et noté A_n. Par construction, ce groupe a $\frac{1}{2}n!$ éléments. Observons aussi que si π est le produit de s transpositions, alors π est pair si et seulement si s est pair.

Proposition 11.3.5. — Soit $n \geq 3$. Le groupe alterné A_n est engendré par les 3-cycles.

Démonstration. Nous savons déjà que tout élément de 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 $(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)$. □

11.4. **Groupes simples**

Définition 11.4.1. — Un groupe G est *simple*, si $G \neq \{e\}$ et si $\{e\}$ sont G les seuls sous-groupes distingués dans G.

Exemple 11.4.2. — Un groupe abélien est simple si et seulement s'il est cyclique d'ordre premier. En effet, si G est un groupe simple abélien et g un élément non trivial de G, alors g engendre un sous-groupe obligatoirement distingué (G est abélien) de G donc G entier. Si g est d'ordre infini, $\langle g^2 \rangle$ serait un sous-groupe propre distingué non

trivial en contradiction avec la simplicité de G. Par conséquent G est fini, cyclique : $G \simeq \mathbb{Z}/n$. Pour tout diviseur propre $d|n$ il existe un sous-groupe $H \subset \mathbb{Z}/n$, et on a $H \simeq \mathbb{Z}/d$. Puisque G est simple, n doit donc être un nombre premier. Réciproquement, si p est un nombre premier, alors tout élément $x \neq 0$ est inversible dans le corps $\mathbb{Z}/p\mathbb{Z}$ et engendre donc additivement le groupe entier.

Exemple 11.4.3. — Le groupe S_n n'est pas simple pour $n \geq 3$: le groupe alterné A_n est un sous-groupe distingué de S_n et nous avons donc $\{(1)\} \lhd A_n \lhd S_n$. On peut donc se poser la question si A_n est simple. Si $n = 3$, le groupe A_n a $\frac{1}{2}3! = 3$ éléments. Il est donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$ et par conséquent simple. Pour $n \geq 4$, le groupe A_n n'est plus abélien. Par exemple nous avons $(124)\cdot(123)\cdot(124)^{-1} = (243)$. Mais A_4 admet un sous-groupe distingué propre non trivial : soit

$$V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}.$$

Que V_4 est effectivement un sous-groupe se voit par calcul direct. Que V_4 est distingué se voit en remarquant que deux permutations sont conjugués exactement s'ils ont le même type de cycle. Un sous-groupe de S_n est donc distingué dans S_n si avec une permutation π il contient aussi toutes les permutations du même type de cycle que π, ce qui est le cas pour V_4. Ainsi V_4 est distingué dans S_4 et donc aussi dans A_4. Le groupe alterné A_4 n'est donc pas simple.

Théorème 11.4.4. — Le groupe A_n est simple pour $n \geq 5$.

Démonstration. Observons d'abord que tous les 3-cycles sont conjugués dans A_n. En effet, soient $\zeta_1 = (abc)$ et $\zeta_2 = (def)$ deux 3-cycles. Comme ils ont le même type de cycle, ils sont conjugués vus dans S_n, c'est-à-dire il existe une permutation $\pi \in S_n$ telle que $\zeta_2 = \pi\zeta_1\pi^{-1}$. Puisque $n \geq 5$, il existe une transposition (xy) qui commute avec ζ_1. Soit $\mu = \pi(xy)$. Alors nous avons aussi $\zeta_2 = \pi\mu\zeta_1\mu^{-1}\pi^{-1}$. Une des deux permutations π ou $\pi(xy)$ est paire. Ainsi ζ_1 et ζ_2 sont aussi conjugués dans A_n.

Soit maintenant $N \subset A_n$ un sous-groupe distingué $\neq \{(1)\}$. Supposons que N contient un 3-cycle. Alors, d'après le remarque précédente, N doit contenir tous les 3-cycles puisque N est distingué. Mais nous avons vu dans la proposition 11.3.5 que A_n est engendré par les 3-cycles. Ainsi $N = A_n$ et A_n est donc bien simple. Pour démontrer la proposition, il reste donc de montrer que N contient nécessairement un 3-cycle. Pour cela on choisit parmi tous les éléments de $N \setminus \{(1)\}$ une permutation π ayant le plus de points fixes sur l'ensemble $[n] = \{1, \ldots, n\}$. Nous allons montrer par une étude de cas par cas, que π est nécessairement un 3-cycle.

Supposons d'abord que π contient un cycle de longueur $m \geq 4$. On peut supposer que π contient le cycle $z = (12 \cdots m)$. Alors N contient aussi l'élément $(123)\pi(123)^{-1}\pi^{-1} = (124)$, en contradiction avec le choix de π (supposé ayant le plus de points fixes).

Supposons maintenant que π contient un 3-cycle ainsi qu'un cycle disjoint de longueur 2 ou 3, par exemple $\pi = (123)(45\cdots)\cdots$. Alors N contient aussi $(124)\pi(421)\pi^{-1} = (12534)$. Si nous avons $\pi = (123)(456)\cdots$ ou $(123)(34)(56)\cdots$, alors (12534) contredit le choix de π. Si $\pi = (123)(45)$, alors (12534) a lui même un nombre maximal de points fixes. Mais ceci contredit le cas précédent.

Supposons π contient trois transpositions disjoints, par exemple $\pi = (12)(34)(56)\cdots$. Alors N contient nécessairement aussi l'élément $(123)\pi(321)\pi^{-1} = (13)(24)$, contradiction.

Supposons π contient deux transposition disjoints, par exemple $\pi = (12)(34)$. Alors N contient aussi $(125)\pi(521)\pi^{-1} = (152)$, contradiction.

Finalement, π est nécessairement un 3-cycle et nous avons donc démontré que A_n est simple. □

Remarque 11.4.5. — Les groupes finis simples sont complètement classifiés. Il y a, comme nous avons vu

– les groupes cycliques $\mathbb{Z}/p$, avec p premier ;

– les groupes alternés 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

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

éléments. Il y a des relations bizarres 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.

11.5. **Groupes résolubles**

Définition 11.5.1. — Soit G un groupe. Une suite $(G_0, \ldots, G_n)$ de sous-groupes de G est une *suite distinguée* si $G_0 = G$, $G_n = \{e\}$ et si pour tout $i = 1, \ldots, n$ le groupe G_i est un sous-groupe distingué propre de G_{i-1}. Les groupes G_{i-1}/G_i, $i = 1, \ldots, n$, s'appellent les facteurs de la série.

Nous notons une suite distinguée comme suit

$$\{e\} = G_n \lhd G_{n-1} \lhd \ldots \lhd G_0 = G.$$

Exemple 11.5.2. — Nous avons déjà vu que $\{(1)\} \lhd A_n \lhd S_n$ est une suite distinguée pour $n \geq 3$. Pour $n = 4$, nous savons aussi que A_4 admet le sous-groupe distingué V_4. Par la suite, on obtient dans ce cas la suite distinguée

$$\{(1)\} \lhd V_4 \lhd A_4 \lhd S_4.$$

Définition 11.5.3. — Un groupe G est dit *résoluble*, s'il admet une suite distingué avec des facteurs abéliens.

Soit G un groupe et $a, b \in G$. Le *commutateur* de $a, b \in G$ est $[a, b] = aba^{-1}b^{-1}$. D'après la définition, nous avons

$$[a, b]^{-1} = [b, a] \quad \text{et} \quad c[a, b]c^{-1} = [cac^{-1}, cbc^{-1}].$$

Ainsi l'ensemble $[G, G] \subset G$ de tous le produits finis de commutateurs est un sous-groupe distingué de G. La proposition suivante est laissé en exercice.

Proposition 11.5.4. — Soit G un groupe. Le quotient $G^{ab} = G/[G, G]$ est abélien et tout morphisme de groupes $f : G \to A$ dans un groupe abélien A factorise à travers G^{ab}, *i.e.* il existe un morphisme $f^{ab} : G^{ab} \to A$ tel que $f = f^{ab}\pi$ où $\pi : G \to G^{ab}$ est la projection canonique.

Dans ce sens, G^{ab} est le plus grand quotient abélien de G.

Définition 11.5.5. — Le quotient G^{ab} s'appelle *l'abélianisé* de G. Un groupe G est dit *parfait*, si $G^{ab} = \{1\}$ ou autrement dit si $[G, G] = G$.

Par exemple, tout groupe simple qui n'est pas abélien est parfait.

Soit G un groupe. Alors nous pouvons définir récursivement les sous-groupes suivants : $K^0(G) = G$, $K^1(G) = [G, G]$ et $K^{n+1}(G) = [K^n(G), K^n(G)]$. D'après la construction $K^{n+1}(G)$ est un sous-groupe distingué dans $K^n(G)$, et les facteurs de la suite

$$G = K^0(G) \rhd K^1(G) \rhd K^2(G) \rhd \dots$$

sont abéliens.

Proposition 11.5.6. — Un groupe est résoluble si et seulement si $K^n G = \{e\}$ pour un $n \in \mathbb{N}$.

Démonstration. Si $K^n(G) = \{e\}$ pour un $n \in \mathbb{N}$, alors la suite

$$G = K^0(G) \rhd \dots \rhd K^n(G) = \{e\}$$

est distinguée avec des facteurs abéliens et G est donc résoluble.

Réciproquement, supposons que

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_m = \{e\}$$

soit une suite distinguée avec des facteurs abéliens. Montrons par récurrence que $K^n(G) \subset G_n$ pour tout $n = 0, \ldots, m$. Pour $n = 0$, il n'y a rien à montrer. Supposons que l'on le sache pour n et raisonnons comme suit : l'image de l'application composée $G_n \to G_n/G_{n+1}$ est abélien. Par conséquent nous avons

$$K^{n+1}(G) = [K^n(G), K^n(G)] \subset [G_n, G_n] \subset G_{n+1}$$

et donc aussi $K^m(G) \subset G_m = \{e\}$. □

Corollaire 11.5.7. — Le groupe S_n est résoluble si et seulement si $n \leq 4$.

Démonstration. Pour $n \leq 4$ nous avons déjà vu des suites distingués avec facteurs abéliens dans les exemples ci-dessus. Pour $n \geq 5$ nous avons $[S_n, S_n] = A_n$, mais A_n est parfait (puisque simple d'après la proposition 11.4.4 et non abélien). □

12. Théorèmes de Sylow

Les théorèmes Sylow donnent beaucoup d'informations sur les sous-groupes d'un groupe fini.

12.1. p-groupes

Définition 12.1.1. — Soit p un nombre premier. Un groupe fini G est un *p-groupe*, si $|G| = p^n$ pour un $n \in \mathbb{N}$.

L'observation centrale, qui est le point de départ pour beaucoup d'informations sur la structure des p-groupes, est le lemme suivant :

Lemme 12.1.2. — Soit G un p-groupe opérant sur un ensemble fini X. Alors nous avons $|X| \equiv |X^G| \bmod p$, où X^G désigne l'ensemble des points fixes de X sous l'action de G.

Démonstration. Soient $B_i \subset X$, $i = 1, \ldots, n$, 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. □

Proposition 12.1.3. — Soit G un p-groupe. Alors le centre $Z(G)$ est non trivial. En particulier, il existe un élément central d'ordre p.

Démonstration. On va faire opérer G sur lui même par conjugaison : $h.g := hgh^{-1}$, puis on va appliquer le lemme 12.1.2. Un élément $g \in G$ est un point fixe exactement s'il commute avec tous les éléments de G ou autrement dit s'il est dans le centre. Par conséquent, nous avons $|Z(G)| \equiv |G| \equiv 0 \bmod p$. Puisque le centre contient au moins l'élément neutre, on doit avoir $|Z(G)| \geq p$. Maintenant, si $x \in Z(G)$ est un élément quelconque non trivial alors il est d'ordre p^m pour un $m \geq 1$. Ainsi $y = x^{p^{m-1}}$ est un élément central d'ordre p. □

Corollaire 12.1.4. — Soit G un groupe d'ordre p^2 où p est premier. Alors G est abélien.

Démonstration. D'après le théorème 12.1.3 on sait que $|Z(G)| = p$ ou p^2. Si $|Z(G)| = p^2$, alors G est abélien. Supposons donc que $|Z(G)| = p$. Alors $Z(G)$ et $G/Z(G)$ sont tous les deux d'ordre p et donc cycliques. Soit $[a] \in G/Z(G)$ un générateur. Alors tout élément $[g] \in G/Z(G)$ s'écrit de la forme $[g] = [a]^m$. Il suit que $g = a^m x$ pour un $x \in Z(G)$. De même, pour $[h] \in G/Z(G)$, il existe $y \in Z(G)$ tel que $h = a^n y$ pour un entier n. Comme x et y sont centraux, ils commutent avec tous les éléments de G d'où

$$gh = a^m x a^n y = a^{m+n} xy = a^n y a^m x = hg,$$

Ainsi, G doit être abélien □

Proposition 12.1.5. — Soit G un p-groupe. Alors il existe une suite de sous-groupes $G_0 = \{e\} < G_1 < \cdots < G_n = G$ d'ordre $|G_i| = p^i$ avec la propriété que G_i est distingué dans G.

Démonstration. Soit $x \in Z(G)$ un élément d'ordre p. Le sous-groupe cyclique $G_1 = \langle x \rangle$ engendré par x est central et donc un sous-groupe distingué dans G. Le groupe quotient G/G_1 est aussi un p-groupe. Par récurrence, il existe donc une suite de sous-groupes distingués $\{1\} < \overline{G}_2 < \ldots < \overline{G}_n = G/G_1$ avec $|\overline{G}_k| = p^{k-1}$. Soit G_k l'image réciproque sous $\overline{G}_k$ sous la projection canonique $G \to G/G_1$. Comme images réciproques de sous-groupes distingués, les G_k sont encore distingués et leur ordre est $|G_k| = |G_1| \cdot |\overline{G}_k| = p^k$. □

12.2. Sous-groupes de Sylow

Définition 12.2.1. — Soit G un groupe fini, p un nombre premier et m la multiplicité de p dans l'ordre de G. Un p-sous-groupe $S \subset G$ est appelé un *p-sous-groupe de Sylow* de G si $|S| = p^m$.

Dans la suite, on dira simplement *p-Sylow*.

Théorème 12.2.2. — (Sylow) Soit G un groupe d'ordre $p^m u$ où p est un nombre premier et où p ne divise pas u. Alors

a) Il existe un p-Sylow de G et si s_p est le nombre des p-Sylow, alors $s_p \,|\, |G|$ et $s_p \equiv 1 \bmod p$;
b) Tout p-sous-groupe de G est contenu dans un p-Sylow ;
c) Tous les p-Sylow de G sont conjugués ;

Démonstration. L'idée est de produire des sous-groupes de G en tant que stabilisateurs pour des actions de G sur des ensembles appropriés.

Considérons donc l'ensemble X des sous-ensembles de G ayant p^m éléments, *i.e.*

$$X = \{Y \subset G; |Y| = p^m\}$$

Le groupe G opère sur X par translation à gauche, c'est-à-dire pour $Y = \{y_1, \ldots, y_{p^m}\} \in X$ et $g \in G$ on a $g.Y = \{gy_1, \ldots, gy_{p^m}\}$.

Soit $Y \in X$ et soit $H = G_Y$ le stabilisateur de Y. Cela signifie que $h.Y = Y$ pour tout $h \in H$. En particulier, nous avons une opération de H sur Y : $(h, y) \mapsto hy$. L'action de H sur Y est libre (puisque $h.y = y$ implique $h = e$) et Y se décompose en une réunion disjointe de classes à droites de H. En particulier, l'ordre de H est un diviseur de $|Y| = p^m$ ou autrement dit H est un p-groupe d'ordre $p^{m'}$ avec $m' \leq m$. De plus, H sera un p-Sylow exactement si Y est formée d'une seule orbite, c'est-à-dire de la forme $Y = Hy$.

En revenant à l'action de G sur X, cela signifie que que la longueur de l'orbite de Y est $|G|/|H| = up^{m-m'}$. Ce nombre *n'est pas* divisible par p, exactement si $Y = Hy$ pour p-Sylow. Soit $X_0 \subset X$ l'ensemble des sous-ensembles de la forme $Y = Hy$ pour un p-Sylow H et $y \in G$. D'après l'équation des orbites, il on a donc $|X| \equiv |X_0| \bmod p$.

Maintenant nous avons

$$|X| = \binom{p^m u}{p^m} \equiv u \bmod p \not\equiv 0 \bmod p.$$

Ainsi $|X_0| \not\equiv 0 \bmod p$ et X_0 est donc non-vide, c'est-à-dire il existe des p-Sylow.

De plus, pour tout p-Sylow H il existe exactement $u = |G/H|$ classes à droite différentes Hy dans X_0. Par ailleurs, H est bien définie en tant que stabilisateur de la classe à droite Hy, *i.e.* un élément de X_0 correspond exactement à un p-Sylow. Ceci montre que $|X_0| = us_p$, d'où $u \equiv us_p \bmod p$, et donc $s_p \equiv 1 \bmod p$.

Pour démontrer le second énoncé, soit $S < G$ un p-Sylow et $H < G$ un p-sous-groupe quelconque. Nous allons appliquer le lemme 12.1.2 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 $y^{-1}Hy \subset S$ ou autrement dit $H \subset ySy^{-1}$. Ainsi H est contenu dans le p-Sylow ySy^{-1}.

Cet argument donne dans le cas particulier où H est déjà un p-Sylow une inclusion $H \subset ySy^{-1}$ entre groupes de même cardinal donc en particulier une égalité. Par conséquent, deux p-Sylow sont conjugués, d'où le troisième énoncé.

Finalement, il reste la première relation sur s_p du premier énoncé à démontrer. Pour cela on considère l'action de G sur l'ensemble X_1 des p-Sylow par conjugaison : $(g, S) \mapsto gSg^{-1}$. Nous venons de voir que tous les p-Sylow sont conjugués. Par conséquent il n'existe qu'une seule orbite. Si K est de le stabilisateur de $S \in X_1$, alors : $|G| = |K| \cdot |X_1|$, d'où $s_p = |X_1|$ est un diviseur de $|G|$. □

Dans la démonstration nous avons utilisé que pour tout nombre premier et tout nombre naturel u premier avec p :

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

En fait, un résultat plus général est vrai :

Lemme 12.2.3. — 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. Dans l'anneau des polynômes $\mathbb{F}_p[x, y]$ nous avons $(x + y)^p = x^p + y^p$. Par récurrence, nous avons donc $(x + y)^{p^m} = x^{p^m} + y^{p^m}$ et finalement

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

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

12.3. **Applications**

Le théorèmes de Sylow permettent de démontrer de nombreux résultats utiles sur les groupes finis d'un ordre particulier.

Exemple 12.3.1. — L'ordre de A_5 est égal à $60 = 2^2 \cdot 3 \cdot 5$. D'après les théorèmes de Sylow, A_5 admet donc des 2, 3 et 5-Sylow d'ordre respectivement 4, 3 et 5. Quel est le nombre de 5-Sylow ? Toujours d'après les théorèmes de Sylow, ce nombre doit diviser 60 et être congruent à 1 mod 5. Par conséquent, il peut en avoir un ou six. S'il y en avait qu'un seul, alors ce sous-groupe serait conjugué à lui même et donc un sous-groupe distingué propre et non trivial de A_5. Comme nous savons déjà que A_5 est simple, ce n'est pas possible. Par conséquent, A_5 a exactement six 5-Sylow distincts.

Exemple 12.3.2. — Si p et q sont des nombres premiers distincts avec $p < q$, alors tout groupe G d'ordre pq a un sous-groupe distingué d'ordre q. En particulier, G ne peut pas être simple. En effet, d'après les théorèmes de Sylow, G admet un q-Sylow H, d'ordre q. Le nombre de ces q-Sylow divise pq et doit être égal à $1 + kq$, pour $k = 0, 1, \ldots$. Mais déjà $1 + q$ est trop grand pour pouvoir diviser pq d'où $k = 0$. Ainsi, H est conjugué à lui même, et donc un sous-groupe distingué propre et non trivial de G. Par exemple, un groupe d'ordre $15 = 3 \cdot 5$ n'est donc jamais simple. On verra plus loin qu'un tel groupe est en fait toujours cyclique.

Exemple 12.3.3. — Aucun groupe G d'ordre $20 = 2^2 \cdot 5$ ne peut être simple. En effet, G contient un 5-Sylow. Comme le nombre des 5-Sylow doit diviser 20 et doit être congruent à 1 mod 5 il doit être égale à 1. Ainsi G contient un sous-groupe distingué d'ordre 5.

Exemple 12.3.4. — Aucun groupe G d'ordre $56 = 2^3 \cdot 7$ ne peut être simple. Regardons d'abord les 7-Sylow. Il peut en avoir 1 ou 8. S'il y en a qu'un alors il est distingué. Supposons donc qu'il y en ait 8. Un tel sous-groupe est d'ordre 7 donc cyclique. Ainsi l'intersection de deux 7-Sylow distincts est réduit à l'élément neutre. Cela nous donne $8 \cdot 6 = 48$ éléments différents d'ordre 7. Comptons maintenant les 2-Sylow. Il peut en avoir 1 ou 7. Tout élément d'un 2-Sylow doit être différent des 48 éléments d'ordre 7, puisque son ordre est une

puissance de 2. Comme un 2-Sylow de G est d'ordre 8 cela ne laisse donc que la place pour un seul 2-Sylow, qui doit donc être distingué.

Pour d'autres groupes il est plus difficile de montrer que G n'est pas simple. Par exemple si $|G| = 48$ le technique de l'exemple précédent ne fonctionne pas. On peut cependant s'en sortir dans ce cas en utilisant le lemme suivant.

Lemme 12.3.5. — Soient H et K deux sous-groupes finis de G. Alors

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

Démonstration. Par définition, nous avons

$$HK = \{hk : h \in H, k \in K\}.$$

Nous avons certainement $|HK| \leq |H| \cdot |K|$ puisque tout élément de HK est produit de deux éléments différents de H et K.

Supposons $h_1k_1 = h_2k_2$ pour $h_1, h_2 \in H$ et $k_1, k_2 \in K$. Soit

$$a = (h_1)^{-1}h_2 = k_1(k_2)^{-1}.$$

Alors $a \in H \cap K$, puisque $(h_1)^{-1}h_2$ est dans H et $k_2(k_1)^{-1}$ est dans K. Ainsi, nous avons $h_2 = h_1a^{-1}$ et $k_2 = ak_1$.

Réciproquement, soit $h = h_1b^{-1}$ et $k = bk_1$ pour $b \in H \cap K$. Alors $hk = h_1k_1$, avec $h \in H$ et $k \in K$. Ainsi, tout élément $hk \in HK$ est de la forme h_ik_i pour $h_i \in H$ et $k_i \in K$, autuant de fois qu'il y a d'éléments dans $H \cap K$, *i.e.* $|H \cap K|$ fois. Par conséquent, nous avons bien $|HK| = (|H| \cdot |K|)/|H \cap K|$. □

Exemple 12.3.6. — Montrons qu'un groupe G d'ordre $48 = 2^4 \cdot 3$ n'est pas simple : on va montrer qu'il contient ou bien un sous-groupe distingué d'ordre 8 ou bien un sous-groupe distingué d'ordre 16.

D'après les théorèmes de Sylow, on sait que G a un ou trois 2-Sylow. Le premier cas correspond à l'existence d'un sous-groupe distingué d'ordre 16. Supposons donc que nous sommes dans le deuxième

cas. Soient H et K deux de ces 2-Sylow. Alors nous avons $|H \cap K| = 8$. En effet, si $|H \cap K| \leq 4$, on aurait d'après le lemme

$$|HK| = \frac{16 \cdot 16}{4} = 64,$$

ce qui est impossible. Ainsi $H \cap K$ est distingué dans H et dans K puisqu'il est d'indice 2 (exercice : tout sous-groupe d'indice 2 d'un groupe est obligatoirement distingué). Le normalisateur $N(H \cap K)$ de $H \cap K$ contient donc H et K. Son cardinal est donc strictement plus grand que 16. Comme par ailleurs il doit diviser 48, seul $|N(H \cap K)| = 48$ est possible. Ainsi $H \cap K$ est distingué dans G.

13. Produit semi-direct

Nous avons vu dans les exemples d'application des théorèmes des Sylow qu'il est souvent utile d'étudier le sous-ensemble $HK \subset G$ pour H et K deux sous-groupes de G. Nous allons étudier cette situation en détail maintenant.

13.1. Produits de sous-groupes

Soient G un groupe et H et K deux sous-groupes de G.
Considérons l'ensemble

$$HK = \{hk : h \in H, k \in K\} \subset G.$$

Nous avons bien entendu, que $H \subset HK$ et $K \subset HK$. On dira que K *normalise* H si pour tout $k \in K$ on a $kHk^{-1} \subset H$.

Lemme 13.1.1. — Soient G un groupe et H, K deux sous-groupes de G. Si K normalise H alors HK est un sous-groupe de G.

Démonstration. Il est clair que $e \in HK$. Si $x = hk \in HK$ et $x' = h'k' \in HK$ alors nous avons

$$xx' = hkh'k' = hkh'(k^{-1}k)k' = h(kh'k^{-1})kk' = hh''kk'$$

puisque K normalise H. Ainsi HK est clos par multiplication. Pour le passage à l'inverse, observons

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

Ainsi HK est un sous-groupe de G. □

En particulier, si H est distingué dans G, le produit HK est un sous-groupe pour tout sous-groupe K puisque dans ce cas là, tout sous-groupe de G normalise H.

Remarque 13.1.2. — Si K normalise H alors le sous-groupe HK n'est autre que le sous-groupe engendré par $H \cup K$. En effet, comme $H \subset HK$ et $K \subset HK$, on sait que $H \cup K \subset HK$. Comme HK est un sous-groupe de G, on a donc $\langle H \cup K \rangle \subset HK$. Réciproquement, un élément de la forme hk est bien entendu dans $\langle H \cup K \rangle$ d'où l'inclusion dans l'autre sens et finalement l'égalité $\langle H \cup K \rangle = HK$

Lemme 13.1.3. — Soient G un groupe et H, K deux sous-groupes distingués de G. Alors HK est un sous-groupe distingué de G.

Démonstration. Comme H est distingué, on sait déjà que HK est un sous-groupe de G. Soit $g \in G$ et $hk \in HK$. Alors nous avons

$$ghkg^{-1} = ghg^{-1}gkg^{-1} = h'k' \in HK$$

puisque H et K sont distingués dans G. Ainsi HK est distingué. □

Proposition 13.1.4. — Soient G un groupe et H, K deux sous-groupes de G. On suppose

- $H \cap K = \{e\}$;
- $hk = kh$ pour tout $h \in H$ et $k \in K$

Alors l'application $\varphi : H \times K \to HK, (h, k) \mapsto hk$ est un isomorphisme de groupes.

Démonstration. On observe d'abord que la deuxième condition implique que φ est bien un morphisme de groupes :

$$\varphi(hh', kk') = hh'kk' = hkh'k = \varphi(h, k)\varphi(h', k')$$

Ce morphisme est surjectif par définition. Montrons qu'il est injectif : si $hk = e$ nous avons $h = k^{-1}$ donc h appartient aussi à K. Mais alors la première condition dit que $h = e$ d'où la proposition. □

En particulier, si dans le conditions de la proposition, nous avons en plus que

– $HK = G$,

alors nous savons que $H \times K \simeq G$. Parfois on dit dans ce cas que G est le *produit direct interne* des sous-groupes H et K (pour distinguer du *produit direct externe* obtenu en prenant deux groupes H et K quelconques et en formant le groupe $G = H \times K$).