Algèbre

Johannes Huisman

Table des matières

Chapitre 1

Anneaux

1. Anneaux et morphismes

Rappelons la définition d'un anneau. Soit A un ensemble. Soient $+$ et $\cdot$ deux lois de composition internes sur A, c-à-d, $+$ et $\cdot$ sont des applications de $A \times A$ dans A. On notera $a + b$ au lieu de $+(a, b)$ et $a \cdot b$, voir ab, au lieu de $\cdot(a, b)$. On va considérer les conditions suivantes :

A1: $\forall a, b, c \in A : (a + b) + c = a + (b + c)$ (l'associativité de $+$)

A2: $\exists z \in A : \forall a \in A : a + z = z + a = a$ (l'existence élément neutre additif)

Lorsque **A2** est satisfaite, l'élément neutre additif z de A est unique. En effet, si $z' \in A$ satisfait aussi $a + z' = z' + a = a$ quel que soit $a \in A$, on aura en particulier $z' = z' + z = z$. Cela montre l'unicité de l'élément neutre additif. Désormais, on lui réserve la notation 0.

A3: $\forall a \in A : \exists b \in A : a + b = b + a = 0$ (l'existence d'opposé, sous l'hypothèse de **A2**)

Lorsque **A1**–**A3** sont satisfaites, l'opposé d'un élément $a \in A$ est uniquement déterminé. En effet, si b' est aussi un opposé de a, on aura $b' = b' + 0 = b' + (a + b) = (b' + a) + b = 0 + b = b$. Cela montre l'unicité de l'opposé d'un élément $a \in A$. On le notera $-a$. On écrira $a - b$ au lieu de $a + (-b)$.

Rappelons que les conditions A1–A3 expriment que A est un groupe sous la loi de composition interne $+$.

A4: $\forall a, b \in A : a + b = b + a$ (la commutativité de $+$)

Les conditions A1–A4 expriment que A est un groupe abélien sous la loi de composition interne $+$.

A5: $\forall a, b, c \in A : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ et $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (la distributivité)

A6: $\forall a, b, c \in A : (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (l'associativité de $\cdot$)

A7: $\exists u \in A \forall a \in A : a \cdot u = u \cdot a = a$ (l'existence élément neutre multiplicatif)

On peut montrer l'unicité de u comme l'on a fait pour l'élément neutre additif. On le désignera par 1.

A8: $\forall a, b \in A : a \cdot b = b \cdot a$ (la commutativité de $\cdot$)

Définition 1.1. Soit A un ensemble muni de deux lois internes $+$ et $\cdot$. Le triplet $(A, +, \cdot)$ est un *anneau* si les conditions **A1**–**A6** sont satisfaites. Le triplet $(A, +, \cdot)$ est un *anneau unitaire* si de plus **A7** est satisfaite. Le triplet $(A, +, \cdot)$ est un *anneau unitaire commutatif* si toutes les conditions **A1**–**A8** sont satisfaites. Par abus de langage, on dira aussi que A au lieu du triplet $(A, +, \cdot)$ est un anneau, anneau unitaire ou un anneau unitaire commutatif.

Comme on ne considérera essentiellement que des anneaux unitaires commutatifs, on dira «anneau» au lieu «d'anneau unitair commutatif» pour simplifier. Lorsqu'on considère des anneaux non commutatifs ou non unitairs, on l'explicitera.

Observons encore que l'ensemble A muni de sa loi additive $+$ est un groupe abélien lorsque $(A, +, \cdot)$ est un anneau.

Exemple 1.2. (1) Tous les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ munis de leurs lois internes habituelles sont des anneaux.

(2) Pour un entier n non nul, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des entiers modulo n muni de ses lois internes habituelles est un anneau.

(3) Soient A et B des anneaux. Le produit cartésien $A \times B$ est un anneau si on définit

$$(a, b) + (a', b') = (a + a', b + b') \quad \text{et} \quad (a, b) \cdot (a', b') = (a \cdot a', b \cdot b')$$

quels que soient $(a, b), (a', b') \in A \times B$. C'est l'anneau produit de A et B. Il est unitaire si A et B le sont ; il est commutatif si A et B le sont.

Voici quelques conséquences de la définition d'un anneau :

PROPOSITION 1.3. *Soit A un anneau unitaire. On a*

(1) $(-a)\cdot b = -(ab)$ *et* $a\cdot(-b) = -(ab)$ *quels que soient* $a, b \in A$.

(2) $(-1)\cdot a = -a$ *et* $a\cdot(-1) = -a$ *quel que soit* $a \in A$.

(3) $0\cdot b = 0$ *et* $a\cdot 0 = 0$ *quels que soient* $a, b \in A$ *(*0 *est absorbant pour la loi multiplicative).*

DÉMONSTRATION. Le 2 est un cas particulier du 1. Pour montrer le 1 et 3, soit $b \in A$ quelconque, et soit $f\colon A \to A$ la multiplication à droite par b :

$$f(a) = a\cdot b$$

quel que soit $a \in A$. Comme la loi multiplicative $\cdot$ est distributive par rapport à la loi additive $+$ sur A, l'application f est un morphisme de groupes additifs. Pour un tel morphisme, on sait que $f(-a) = -f(a)$ et que $f(0) = 0$. Cela montre que $(-a)\cdot b = -(a\cdot b)$ et que $0\cdot b = 0$. Les deux autres assertions à savoir $a\cdot(-b) = -(a\cdot b)$ et $a\cdot 0 = 0$ s'obtiennent de manière analogue en considérant l'application $g\colon A \to A$ de multiplication à gauche par a, pour $a \in A$ quelconque. □

EXEMPLE 1.4. Un singleton $A = \{a\}$ admet exactement une structure d'anneau à savoir celle définie par $a + a = a$ et $a\cdot a = a$. Dans cet anneau on a $0 = a$, $1 = a$, et en particulier $0 = 1$. C'est l'anneau nul, noté 0. Réciproquement si dans un anneau unitaire A on a $0 = 1$, alors $A = \{0\}$. On en avait vu déjà ci-dessus, des anneaux nuls : $\mathbb{Z}/1\mathbb{Z}$ et $\mathbb{Z}/(-1)\mathbb{Z}$!

Morphismes d'anneaux

DÉFINITION 1.5. Soient A et B des anneaux et $f\colon A \to B$ une application. L'application f est un *morphisme d'anneaux*, ou par abus de langage un *morphisme*, lorsque

M1: $f(a + b) = f(a) + f(b)$;

M2: $f(ab) = f(a)f(b)$;

M3: $f(1) = 1$;

quels que soient $a, b \in A$. Si de plus il existe un morphisme $g\colon B \to A$ tel que $g\circ f = \mathrm{id}$ et $f\circ g = \mathrm{id}$ alors f est un isomorphisme d'anneaux. Deux anneaux A et B sont isomorphes, notés $A \cong B$ s'il existe un isomorphisme de A vers B. On morphisme d'anneaux d'un anneau A dans lui-même est un endomorphisme. Un endomorphisme qui est un isomorphisme est un automorphisme.

Notons qu'un morphisme d'anneaux est en particulier un morphisme des groupes additifs sous-jacents. En particulier, si $f\colon A \to B$ est un morphisme d'anneaux, alors $f(0) = 0$ et $f(-a) = -f(a)$ quel que soit $a \in A$. On peut donc aussi considérer le noyau $\ker(f)$ et l'image $\mathrm{im}(f)$ d'un morphisme d'anneaux $f\colon A \to B$; ce sont des sous-groupes additifs de A et de B, respectivement.

EXEMPLE 1.6.

(1) L'identité $\mathrm{id}_A\colon A \to A$ est un morphisme d'anneaux pour tout anneau A, un iso, un endo et un auto.

(2) Quel que soit l'anneau A, l'unique application de A dans l'anneau nul est un morphisme d'anneaux. C'est le *morphisme nul*.

(3) Si A est un anneau non nul, il n'y a aucun morphisme d'anneaux de l'anneau nul dans A.

(4) Les inclusions $\mathbb{Z} \to \mathbb{Q}$, $\mathbb{Z} \to \mathbb{R}$, $\mathbb{Z} \to \mathbb{C}$, $\mathbb{Q} \to \mathbb{R}$, $\mathbb{Q} \to \mathbb{C}$ et $\mathbb{R} \to \mathbb{C}$ sont toutes des morphismes d'anneaux.

(5) Soit $n \in \mathbb{Z}$ un entier non nul. L'application $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ de réduction modulo n est un morphisme d'anneaux.

(6) La conjugaison complexe est un endo et automorphisme de $\mathbb{C}$.

(7) Soient A et B des anneaux. Soit $p\colon A\times B \to A$ l'application définie par $p(a, b) = a$. ALors p est un morphisme d'anneaux. De même pour $q\colon A\times B \to B$ définie par $q(a, b) = b$.

(8) Soient A et B des anneaux. Soit $i\colon A \to A\times B$ définie par $i(a) = (a, 0)$. Alors i n'est pas un morphisme d'anneaux à moins que B est l'anneau nul. De même pour $j\colon B \to A\times B$ définie par $j(b) = (0, b)$.

PROPOSITION 1.7. *Soient A, B et C des anneaux. Soient $f\colon A \to B$ et $g\colon B \to C$ des morphismes d'anneaux. Alors, $g\circ f\colon A \to C$ est un morphisme d'anneaux.*

DÉMONSTRATION. Exercice. □

PROPOSITION 1.8. *Un morphisme est un isomorphisme si et seulement s'il est bijectif.*

DÉMONSTRATION. Exercice. □

2. Sous-anneaux

Parmi les sous-ensembles d'un anneau A, ceux qui héritent de A la structure d'un anneau nous intéressent particulièrement.

DÉFINITION 2.1. Soit $(A, +, \cdot)$ un anneau. Un sous-ensemble B de A est un *sous-anneau* de A lorsque

SA1: $b + b'$, bb' et $-b$ appartiennent à B pour tous les $b, b' \in B$;

SA2: 1 appartient à B.

Notons qu'un sous-anneaux est en particulier un sous-groupe additif. En particulier, il en contient l'élément neutre additif.

EXEMPLE 2.2. (1) $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, de $\mathbb{R}$ et de $\mathbb{C}$. $\mathbb{Q}$ est un sous-anneau de $\mathbb{R}$ et de $\mathbb{C}$. $\mathbb{R}$ est un sous-anneau de $\mathbb{C}$.

(2) Soit $\mathbb{D} \subseteq \mathbb{Q}$ le sous-ensemble des nombre décimaux, i.e.,

$$\mathbb{D} = \{\frac{a}{10^n} \mid a \in \mathbb{Z} \text{ et } n \in \mathbb{N}\}.$$

Alors, $\mathbb{D}$ est un sous-anneaux de $\mathbb{Q}$.

La terminologie de sous-anneau est justifiée par la proposition suivante :

PROPOSITION 2.3. *Soit A un anneau et $B \subseteq A$ un sous-anneau de A. Les lois internes $+$ et $\cdot$ sur A induisent des lois internes sur B par restriction. L'ensemble B muni de ces lois internes est un anneau. De plus, l'application d'inclusion $i\colon B \to A$ définie par $i(b) = b$ pour tout $b \in B$, est un morphisme d'anneaux.*

DÉMONSTRATION. Exercice. □

PROPOSITION 2.4. *Soit $f\colon A \to B$ un morphisme d'anneaux.*

(1) Si C est un sous-anneau, son image directe $f(C)$ est un sous-anneau de B.

(2) Si C est un sous-anneau de B, son image réciproque $f^{-1}(C)$ est un sous-anneau de A.

En particulier, l'image $\mathrm{im}(f)$ *de f est un sous-anneau de B.*

DÉMONSTRATION. Exercice. □

La proposition précédente permet de considérer un morphisme d'anneaux $f\colon A \to B$ comme morphisme d'anneaux de A dans son image $f(A)$. L'intérêt en est qu'on peut décomposer tout morphisme d'anneaux f comme une composition $i \circ s$ d'un morphisme d'anneaux injectif i avec un morphisme d'anneaux surjectif s. En effet, on pose i le morphisme d'inclusion de $f(A)$ dans B, et s le morphisme f vu comme morphisme de A dans $f(A)$.

COROLLAIRE 2.5. *Soit $f\colon A \to B$ un morphisme d'anneaux injectif. Alors f est un isomorphisme d'anneaux de A sur son image $f(A)$.*

Remarquons que le noyau d'un morphisme d'anneaux n'est en généneral pas un sous-anneaux. En effet, dès que $f\colon A \to B$ est un morphisme à valeurs dans un anneau B non nul, on a $1 \notin \ker(f)$.

La réunion de deux sous-anneaux n'a aucune raison d'être un sous-anneau [1]. Par contre, l'intersection de deux sous-anneau d'un anneau donné en est encore un, comme on montre facilement. En fait, l'intersection d'une collection arbitraire de sous-anneaux en est encore un, comme on verra ci-dessous.

Soit $\mathcal{C}$ une collection de sous-ensembles d'un ensemble E, c-à-d, $\mathcal{C} \subseteq \mathcal{P}(E)$. Rappelons que l'intersection $\bigcap \mathcal{C}$ de $\mathcal{C}$ est par définition

$$\bigcap \mathcal{C} = \{x \in E \mid x \in X \text{ pour tout } X \in \mathcal{C}\}.$$

1. On verra un exemple ci-dessous d'une réunion de sous-anneaux qui n'est pas un sous-anneau

LEMME 2.6. *Soit A un anneau. Soit $\mathcal{C}$ une collection de sous-anneaux de A. Alors l'intersection $\bigcap \mathcal{C}$ est un sous-anneau de A.*

DÉMONSTRATION. Exercice. □

PROPOSITION 2.7. *Soit A un anneau et S un sous-ensemble de A. Alors, le plus petit sous-anneau de A contenant S existe.*

DÉMONSTRATION. Soit $\mathcal{C}$ la collection des sous-anneaux de A contenant S. D'après Lemme 2.6, $\bigcap \mathcal{C}$ est un sous-anneau de A. Evidemment, $\bigcap \mathcal{C}$ contient S. Il reste à montrer que $\bigcap \mathcal{C}$ est le plus petit sous-anneau de A contenant S. Soit alors B un sous-anneau de A contenant S. Comme $B \in \mathcal{C}$, on a $\bigcap \mathcal{C} \subseteq B$. □

COROLLAIRE 2.8. *Tout anneau contient un plus petit sous-anneaux.*

DÉFINITION 2.9. Le plus petit sous-anneau d'un anneau est son *sous-anneau premier*.

Soit A un anneau. Soit B un sous-anneau de A et s un élément de A. Le plus petit sous-anneau de A contenant $B \cup \{s\}$ est noté par $B[s]$. C'est le sous-anneau de A obtenu de B en adjoignant s. Afin d'en avoir une description explicite, on rappelle la notation suivante.

Soit A un anneau et $a \in A$. On définit $a^0 = 1$, et par récurrence $a^n = a^{n-1} \cdot a$ pour $n > 0$. En particulier $a^1 = a$ et $a^2 = a \cdot a$ etc. On ne définit pas a^n pour $n < 0$. On a les règles de calcul suivants :

(1) $a^{m+n} = a^m \cdot a^n$
(2) $(ab)^n = a^n b^n$
(3) $a^{mn} = (a^m)^n$.

Observons encore que si $f\colon A \to B$ est un morphisme d'anneaux, alors $f(a^n) = f(a)^n$ pour tout $a \in A$ et tout $n \in \mathbb{N}$.

Voici la description explicite du sous-anneaux $A[s]$ de B. On peut vérifier que

$$B[s] = \{a \in A \mid \exists n \in \mathbb{N} \exists b_i \in B : a = \sum_{i=0}^{n} b_i s^i\}.$$

EXEMPLE 2.10. (1) L'anneau de Gauss $\mathbb{Z}[i]$ est le sous-anneau de $\mathbb{C}$ obtenu de $\mathbb{Z}$ en adjoignant i. On a $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

(2) L'anneau des décimaux $\mathbb{D}$ est égal au sous-anneau de $\mathbb{Q}$ obtenu de $\mathbb{Z}$ en adjoignant $\frac{1}{10}$, i.e., $\mathbb{D} = \mathbb{Z}[\frac{1}{10}]$.

Voici un exemple de deux sous-anneaux dont la réunion n'en est pas un.

EXEMPLE 2.11. Considérons les sous-anneaux $\mathbb{Z}[\frac{1}{2}]$ et $\mathbb{Z}[\frac{1}{3}]$ de $\mathbb{Q}$. La réunion $S = \mathbb{Z}[\frac{1}{2}] \cup \mathbb{Z}[\frac{1}{3}]$ n'est pas un sous-anneau de $\mathbb{Q}$. En effet, $\frac{1}{2} + \frac{1}{3} \notin S$. On laisse la vérification à titre d'exercice.

3. La propriété universelle de l'anneau $\mathbb{Z}$

Rappelons que dans un groupe G, noté additivement, on a donné un sens à ng où $n \in \mathbb{Z}$ et $g \in G$. En effet, on pose $0g = 0$, et pour $n > 0$, on a

$$ng = g + g + \cdots + g \quad (n \text{ termes}).$$

Plus formellement on définit ng par récurrence par

$$ng = (n-1)g + g.$$

On définit encore $(-n)g = -(ng)$ pour $n > 0$, et on a les règles de calcul suivants :

(1) $1g = g$
(2) $(m+n)g = mg + ng$,
(3) $n(g + g') = ng + ng'$, et
(4) $(mn)g = m(ng)$,

quels que soient $g, g' \in G$ et $m, n \in \mathbb{Z}$. Notons de plus que si $f\colon G \to H$ est un morphisme de groupes notés additivement, alors $f(ng) = nf(g)$ quels que soient $g \in G$ et $n \in \mathbb{Z}$.

PROPOSITION 3.1. *Soit A un anneau. Alors $(na) \cdot b = n(a \cdot b)$ et $a \cdot (nb) = n(a \cdot b)$ quels que soient $a, b \in A$ et $n \in \mathbb{Z}$.*

DÉMONSTRATION. Soit $b \in A$ quelconque, et soit $f\colon A \to A$ l'application de multiplication à droite par b définie par $f(a) = a \cdot b$ pour tout $a \in A$. Comme on a vu précédemment, f est un endomorphisme du groupe additif A. En particulier, $f(na) = nf(a)$ pour tout $a \in A$ et pour tout $n \in \mathbb{Z}$. Il s'ensuit que $(na) \cdot b = n(a \cdot b)$. □

PROPOSITION 3.2 (La propriété universelle de l'anneau $\mathbb{Z}$). *Soit A un anneau. Il existe un et un seul morphisme d'anneaux de $\mathbb{Z}$ dans A.*

DÉMONSTRATION. Supposons que $f\colon \mathbb{Z} \to A$ est un morphisme d'anneaux. On a donc $f(1) = 1$. Par la suite, $f(n) = f(n1) = nf(1) = n1$ dans A. Cela montre l'unicité. Quant à l'existence, l'application $f\colon \mathbb{Z} \to A$ définie par $f(n) = n1$ est un morphisme d'anneaux car $f(m+n) = (m+n)1 = m1 + n1 = f(m) + f(n)$, $f(mn) = (mn)1 = m(n1) = mf(n) = m(1 \cdot f(n)) = (m1) \cdot f(n) = f(m) \cdot f(n)$, et $f(1) = 1$. □

EXEMPLE 3.3.
(1) L'identité de $\mathbb{Z}$ dans lui-même est le seul morphisme d'anneaux de $\mathbb{Z}$ dans lui-même !
(2) Les morphismes $\mathbb{Z} \to \mathbb{Q}$, $\mathbb{Z} \to \mathbb{R}$, $\mathbb{Z} \to \mathbb{C}$ et $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ci-dessus étaient donc les seuls morphismes partant de $\mathbb{Z}$!
(3) Déterminons l'unique morphisme f de $\mathbb{Z}$ dans $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. On peut écrire $f = (g, h)$. Comme $g = p \circ f$ et $h = q \circ f$, les applications g et h sont des morphismes d'anneaux. Donc g est nécessairement l'application de réduction modulo 4 et h celle de réduction modulo 6. Du coup $f(n) = (n \mod 4, n \mod 6)$.

PROPOSITION 3.4 (La propriété universelle de $\mathbb{Z}$ en tant qu'anneau). *Soit A un anneau et $f\colon \mathbb{Z} \to A$ l'unique morphisme d'anneaux. Alors $f(\mathbb{Z})$ est le sous-anneau premier de A.*

DÉMONSTRATION. Exercice. □

COROLLAIRE 3.5. *L'anneau premier de A est le sous-groupe additif de A engendré par 1.*

Soit A un anneau. Soit $f\colon \mathbb{Z} \to A$ l'unique morphisme d'anneaux de $\mathbb{Z}$ dans A. Pour un élément $n \in \mathbb{Z}$, on écrit aussi n_A, voire n tout court, pour son image $f(n)$ dans A [2]. Notons que le morphisme f de $\mathbb{Z}$ dans A n'est pas forcément injectif. On peut donc écrire $2 \in A$, $-36 \in A$ etc., mais on peut très bien avoir $2 = -36$ dans A !

Notons qu'on s'est alors débarrassé de la notation-à-barre des éléments de l'anneau $\mathbb{Z}/n\mathbb{Z}$. En effet, l'unique morphisme de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ étant le morphism de réduction modulo n, on a $2 = \bar{2}$, $3 = \bar{3}$, etc. dans $\mathbb{Z}/n\mathbb{Z}$.

EXEMPLE 3.6. Soit n et k des entiers naturels avec $k \leq n$. Rappelons que le coefficient binomiale $\binom{n}{k}$ est l'entier naturel défini par

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1}.$$

C'est un entier naturel, donc relatif. Cela a donc un sens le considérer comme élément d'un anneau A.

Pour donner un exemple explicite, on a $\binom{4}{2} \in \mathbb{Z}/6\mathbb{Z}$, et d'ailleurs, comme $\binom{4}{2} = 6$ dans $\mathbb{Z}$, on a $\binom{4}{2} = 0$ dans $\mathbb{Z}/6\mathbb{Z}$. Par contre, la définition de $\binom{4}{2}$ comme $(4 \cdot 3)/(2 \cdot 1)$ n'a pas de sens dans $\mathbb{Z}/6\mathbb{Z}$ car on ne sait diviser par 2 dans $\mathbb{Z}/6\mathbb{Z}$; en effet $2 \cdot 3 = 0$ dans $\mathbb{Z}/6\mathbb{Z}$, mais $3 \neq 0$ dans $\mathbb{Z}/6\mathbb{Z}$.

La notation n_A pour l'image dans l'anneau A de l'entier relatif n possède une certaine cohérence :

PROPOSITION 3.7. *Soit $f\colon A \to B$ un morphisme d'anneaux. Pour tout entier relatif n, on a $f(n_A) = n_B$* [3].

DÉMONSTRATION. Exercice. □

2. On le faisait déjà pour 0 et 1 !
3. Avec la notation quelque peu abusive de n aussi bien pour son image dans A que pour celle dans B, on aurait pu écrire ici $f(n) = n$. De là, il ne faut pas croire que f soit l'identité sur l'anneaux premier de A !

4. Anneaux de polynômes

Soient A un anneau et X une indéterminée. Un *polynôme* en X à coefficients dans A est une expression formelle de la forme

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$ [4]

où $a_0, \ldots, a_n \in A$ et n est un entier naturel. L'expression est formelle dans le sens que deux polynômes sont égaux

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = b_0 + b_1X + b_2X^2 + \cdots + b_mX^m$$

si et seulement si $a_i = b_i$ pour tout entier naturel i. Là et ci-dessous il est sous-entendu que $a_i = 0$ si $i > n$, et $b_i = 0$ si $i > m$. A titre d'exemple, les polynômes $1 + 4X^2 + 3X^3 + 0X^5$ et $1 + 0X + 4X^2 + 3X^3$ sont égaux. Un polynôme comme expression formelle n'a donc pas de représentation unique. Il faudrait donc veiller à ce que les définitions suivantes ne dépendent pas de la représentation choisie d'un polynôme. Comme ces vérifications sont faciles à faire, on les laissera au lecteur. D'ailleurs, on verra ci-dessous une définition alternative et équivalente d'un polynôme en X à coefficients dans A qui ne possède pas cet inconvénient.

L'ensemble des polynômes en X à coefficients dans A est noté par $A[X]$. On définit deux lois de composition interne $+$ et $\cdot$ sur $A[X]$. L'addition $+$ est définie par

$$(a_0 + a_1X + a_2X^2 + \cdots + a_nX^n) + (b_0 + b_1X + b_2X^2 + \cdots + b_mX^m) = \\ (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + \cdots + (a_\ell + b_\ell)X^\ell,$$

où $\ell = \max\{m, n\}$. Le produit $\cdot$ est défini par

$$(a_0 + a_1X + a_2X^2 + \cdots + a_nX^n) \cdot (b_0 + b_1X + b_2X^2 + \cdots + b_mX^m) = \\ c_0 + c_1X + c_2X^2 + \cdots + c_{m+n}X^{m+n},$$

où

$$c_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0$$

pour $k = 0, \ldots, m + n$. On peut vérifier que ces lois sont bien définies et que $A[X]$ est alors un anneau. On l'appelle *l'anneau de polynômes* en X à coefficients dans A. Comme l'élément neutre multiplicatif de $A[X]$ est le polynôme 1, il est justifié d'introduire la notation X^n pour $1X^n$, quel que soit l'entier naturel n [5]. Ce sont les *monômes* dans $A[X]$.

Insistons sur le fait que X est une indéterminée et non pas un élément de A. Par exemple, les polynômes X^2 et X^3 à coefficients dans $\mathbb{Z}/2$ sont des polynômes distincts, même s'ils prennent les mêmes valeurs dans $\mathbb{Z}/2$ si on substitue 0 or 1 pour X dans les deux. D'ailleurs, par définition, l'anneau $A[X]$ est infini lorsque A est non nul.

Observons encore que l'anneau $0[X]$ des polynômes en X à coefficients dans l'anneau 0 est l'anneau nul. Même le monôme X^n est égal à 0 dans $0[X]$. En effet, par définition $X^n = 1X^n$. Comme $1 = 0$ dans l'anneau nul, on obtient $X^n = 1X^n = 0X^n = 0$.

Remarquons que A est naturellement un sous-ensemble de $A[X]$ et en tant que tel il en est un sous-anneau.

L'intérêt principal de l'anneau des polynômes $A[X]$ est sans doute la facilité de construire des morphismes d'anneaux de $A[X]$ dans d'autres anneaux. Le cas le plus simple est le morphisme d'évaluation.

DÉFINITION 4.1. Soit A un anneau et $a \in A$. Soit $P \in A[X]$ et écrivons $P = a_0 + a_1X + \cdots + a_nX^n$. L'*évaluation de P en a* est l'élément $P(a)$ de A défini par

$$P(a) = a_0 + a_1a + \cdots + a_na^n.$$

L'application $\mathrm{ev}_a \colon A[X] \to A$ définie par $\mathrm{ev}_a(P) = P(a)$ pour tout $P \in A[X]$ est l'*application d'évaluation en a*.

PROPOSITION 4.2. *Soit A un anneau et $a \in A$. L'application $\mathrm{ev}_a \colon A[X] \to A$ d'évaluation en a est un morphisme d'anneaux. Il satisfait*

(1) $(\mathrm{ev}_a)_{|A} = \mathrm{id}_A$, *et*

(2) $\mathrm{ev}_a(X) = a$.

4. ou mieux : $a_0X^0 + a_1X^1 + \cdots + a_nX^n$, mais on s'éloignerait sans doute trop des habitudes notationnelles...

5. sand cette notation X^n ne serait même pas un polynôme en X à coefficients dans A dans le sens précédent

C'est l'unique morphisme d'anneaux de $A[X]$ dans A ayant ces deux propriétés-là.

DÉMONSTRATION. Exercice. □

On peut généraliser ce morphisme dans le sens suivant. D'abord un énoncé préliminaire.

PROPOSITION 4.3. *Soit $f\colon A \to B$ un morphisme d'anneaux. Soit $F\colon A[X] \to B[X]$ l'application définie par*

$$F(a_0 + a_1X + \cdots + a_nX^n) = f(a_0) + f(a_1)X + \cdots + f(a_n)X^n$$

quels que soient $a_0, \ldots, a_n \in A$ et $n \in \mathbb{N}$. Alors F est un morphisme d'anneau. Il satisfait

(1) $F_{|A} = f$, et

(2) $F(X) = X$.

C'est l'unique morphisme d'anneaux de $A[X]$ dans $B[X]$ ayant ces deux propriétés-là.

DÉMONSTRATION. Exercice. □

Voici la généralisation du morphisme d'évaluation de la Proposition 4.1.

PROPOSITION 4.4. *Soit $f\colon A \to B$ un morphisme d'anneaux et soit $b \in B$. Soit $\varphi\colon A[X] \to B[X]$ l'application définie par*

$$\varphi(a_0 + a_1X + \cdots + a_nX^n) = f(a_0) + f(a_1)b + \cdots + f(a_n)b^n$$

quels que soient $a_0, \ldots, a_n \in A$ et $n \in \mathbb{N}$. Alors φ est un morphisme d'anneau. Il satisfait

(1) $\varphi_{|A} = f$, et

(2) $\varphi(X) = b$.

C'est l'unique morphisme d'anneaux de $A[X]$ dans B ayant ces deux propriétés-là.

DÉMONSTRATION. Observons que $\varphi = \mathrm{ev}_b \circ F$ avec les notations ci-dessus. Comme ev_b et F sont des morphismes d'anneaux, φ en est un. Il est clair que $\varphi_{|A} = f$ et que $\varphi(X) = b$. L'unicité est laissé comme exercice. □

Notons que la proposition précédente est effectivement une généralisation de la Proposition 4.1. Si on prend $A = B$, et $f = \mathrm{id}_A$, on a $\varphi = \mathrm{ev}_b$.

Par abus de notation, on écris encore $P(b)$ pour l'image $\varphi(P)$ dans B pour $P \in A[X]$. On l'appelle même parfois l'évaluation de P en b.

La proposition précédente permet d'obtenir des sous anneaux de la forme $A[s]$ comme image d'un morphisme.

PROPOSITION 4.5. *Soit B un anneau et A un sous-anneau de B. Soit $s \in B$. Soit $f\colon A[X] \to B$ l'unique morphisme avec $f(X) = s$ et dont la restriction à A est égale au morphisme d'inclusion de A dans B. Alors* $\mathrm{im}(f) = A[s]$.

DÉMONSTRATION. Exercice. □

D'un point de vue formel la définition de l'ensemble $A[X]$ n'est pas très satisfaisante. Au fond, qu'est-ce qu'une indéterminée si ce n'est pas un élément de A ? Et qu'est-ce qu'une expression formelle ? C'est pourquoi on explique comment définir $A[X]$ de manière alternative, équivalente et surtout satisfaisante.

Comme un polynôme ci-dessus est uniquement déterminé par la suite de ses coefficients, qu'on peut penser infinie en prolongeant par 0, on n'a qu'à définir un polynôme comme une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A dont les termes sont tous nuls à partir de certain rang. Notons temporairement $A[X]'$ l'ensembles de telles suites. On définit deux lois internes binaire $+$ et $\cdot$ sur $A[X]'$ par

$$(a+b)_i = a_i + b_i \quad \text{et} \quad (a \cdot b)(k) = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0$$

pour tous $a, b \in A[X]'$. On vérifie facilement que $A[X]'$ est un anneau. Observons que $A[X]'$ contient l'anneau A comme sous-anneau en considérant un élément a de A comme la suite $a, 0, 0, 0, \ldots$ dans $A[X]'$.

Maintenant on peut préciser ce que c'est l'indéterminée X dans $A[X]'$. Soit X la suite $0, 1, 0, 0, 0, \ldots$ dans $A[X]'$. Le produit $b \cdot X$ dans $A[X]'$, où $b \in A$, est égal à la suite $0, b, 0, 0, 0, \ldots$. L'élément $a + bX$ de $A[X]'$ est la suite $a, b, 0, 0, 0, \ldots$. Notons que X^n est la suite égale à la suite nulle sauf en son n-ième terme qui est égal à 1, quel que soit l'entier naturel n. L'élément $a_0 + a_1X + \cdots + a_nX^n$

de $A[X]'$ est la suite $a_0, a_1, \ldots, a_n, 0, 0, 0, \ldots$. Donc tout élément de $A[X]'$ s'écrit sous la forme $a_0 + a_1X + \cdots + a_nX^n$ où $a_0, \ldots, a_n \in A$ et $n \in \mathbb{N}$. On a

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = b_0 + b_1X + b_2X^2 + \cdots + b_mX^m$$

dans $A[X]'$ si et seulement si $a_i = b_i$ pour tout entier naturel i, tout comme dans $A[X]$. Les ensembles $A[X]$ et $A[X']$ sont donc en bijection. De plus, les lois se correspondent, ainsi que les éléments neutres multiplicatifs, c-à-d que les anneaux $A[X]$ et $A[X]'$ sont isomorphes ! L'anneau $A[X]'$ n'est donc rien d'autre que l'anneau des polynômes $A[X]$ introduit ci-dessus, mais sa définition est bien plus précise que celle de $A[X]$. C'est la bonne définition de l'anneau des polynômes en X à coefficients dans A.

DÉFINITION 4.6. Soit $P \in A[X]$ un polynôme. Si $P \neq 0$, on peut écrire

$$P = a_0 + a_1X + \cdots + a_nX^n$$

où n est l'unique entier naturel tel que $a_n \neq 0$. On appelle a_n le *coefficient dominant* de P. On le note $\mathrm{cd}(P)$. Le *degré* de P est l'entier naturel n. Lorsque $a_n = 1$ dans A, on dit que le polynôme P est *unitaire*. Si $P = 0$, le *degré* de P est égal à $-\infty$. On note $\deg(P)$ pour le degré de P.

Notons que $\deg(P)$ est un élément de l'ensemble $\mathbb{N} \cup \{-\infty\}$. Ce dernier est naturellement totalement ordonné, et muni d'une loi de composition interne d'addition $+$ qui étend l'addition sur $\mathbb{N}$ par $-\infty + x = -\infty$ et $x + (-\infty) = -\infty$ pour tout $x \in \mathbb{N} \cup \{-\infty\}$. Avec ces définitions, le degré d'un polynôme possède les propriétés suivantes :

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

Ces propriétés se démontrent facilement. On peut les améliorer sous certaines conditions sur P et Q.

(1) $\deg(P + Q) = \max\{\deg(P), \deg(Q)\}$ sauf si P et Q sont non nuls, $\deg(P) = \deg(Q)$ et $\mathrm{cd}(P) + \mathrm{cd}(Q) = 0$.
(2) $\deg(PQ) = \deg(P) + \deg(Q)$ sauf si P et Q sont non nuls et $\mathrm{cd}(P) \cdot \mathrm{cd}(Q) = 0$ dans A.

EXEMPLE 4.7. (1) Dans $\mathbb{Z}[X]$ on a

$$(1 + 2X - 3X^2) + (1 + 2X + 3X^2) = 2 + 4X,$$

ce qui montre qu'on peut avoir $\deg(P + Q) < \max\{\deg(P), \deg(Q)\}$.

(2) Dans $\mathbb{Z}/6\mathbb{Z}[X]$ on a

$$(1 + 2X) \cdot (2 + 3X^2) = 2 + 4X + 3X^2 + 6X^3 = 2 + 4X + 3X^2,$$

ce qui montre que $\deg(PQ)$ peut être strictement inférieur à $\deg(P) + \deg(Q)$.

Maintenant que l'anneau de polynômes en une variable à coefficients dans A est bien défini, on peut définir par récurrence les anneaux de polynômes en plusieurs variables à coefficients dans A par

$$A[X_1, \ldots, X_n] = (A[X_1, \ldots, X_{n-1}])[X_n]$$

quel que soit $n \geq 2$.

Pour $n = 2$, on écrit habituellement Y pour X_2, et on a

$$A[X, Y] = (A[X])[Y].$$

C'est l'anneau des polynômes en Y à coefficients dans $A[X]$, c-à-d, leurs coefficients sont des polynôme à leur tour en X à coefficients dans A. Il n'empêche qu'on peut écrire un élément de $A[X, Y]$ sous la forme

$$\sum_{i,j=0}^{m,n} a_{i,j}X^iY^j,$$

où $a_{i,j} \in A$ et $m, n \in \mathbb{N}$.

Pour $n = 3$, on écrit habituellement Y pour X_2 et Z pour X_3, et on a

$$A[X, Y, Z] = ((A[X])[Y])[Z].$$

C'est l'anneau des polynômes en Z à coefficients dans l'anneau $A[X,Y]$. On préfère écrire un élément de $A[X,Y,Z]$ sous la forme

$$\sum_{i,j,k=0}^{\ell,m,n} a_{i,j,k}X^iY^jZ^k,$$

où $a_{i,j,k} \in A$ et $\ell, m, n \in \mathbb{N}$.

5. La propriété universelle de l'anneau $\mathbb{Z}[X]$

Soit A un anneau et $a \in A$. D'après la propriété universelle de $\mathbb{Z}$, il n'y a qu'un morphisme de $\mathbb{Z}$ dans A. Soit $P \in \mathbb{Z}[X]$. Ecrire $P = a_0 + a_1X + \cdots + a_X^n$ avec $a_1, \ldots, a_n \in \mathbb{Z}$. L'évaluation de P en X est alors égal à

$$P(a) = a_0 + a_1a + a_2a^2 + \cdots + a_na^n \in A.$$

On a vu qu'en l'occurence l'application d'évaluation en a est un morphisme

$$\mathrm{ev}_a \colon \mathbb{Z}[X] \to A$$

défini par $\mathrm{ev}_a = P(a)$. Il a la propriété que $f(X) = a$. C'est donc l'unique morphisme de $\mathbb{Z}[X]$ dans A avec cette dernière propriété.

Proposition 5.1. *Soit A un anneau et $a \in A$. Alors il existe un et un seul morphisme $f \colon \mathbb{Z}[X] \to A$ tel que $f(X) = a$.* □

On interprète ce dernier énoncé en disant que l'anneau $\mathbb{Z}[X]$ muni de son élément X est universel. Toutes les identités dans l'anneau $\mathbb{Z}[X]$ ne faisant intervenir que les opérations $+, -, \cdot$ sont valables dans tout anneau A lorsqu'on remplace X par un élément a de A.

Exemple 5.2. Rappelons que

$$(1+X)^n = \sum_{i=0}^{n} \binom{n}{i} X^i$$

dans $\mathbb{Z}[X]$ où $n \in \mathbb{N}$. Soit A un anneau quelconque et $a \in A$. On a alors

$$(1+a)^n = \sum_{i=0}^{n} \binom{n}{i} a^i$$

dans A.

De même, on a la propriété universelle de $\mathbb{Z}[X,Y]$.

Proposition 5.3. *Soit A un anneau et $a, b \in A$. Alors il existe un et un seul morphisme $f \colon \mathbb{Z}[X,Y] \to A$ tel que $f(X) = a$ et $f(Y) = b$.* □

Démonstration. Exercice. □

On interprète ce dernier énoncé en disant que l'anneau $\mathbb{Z}[X,Y]$ muni de ses éléments X, Y est universel. Toutes les identités dans l'anneau $\mathbb{Z}[X,Y]$ ne faisant intervenir que les opérations $+, -, \cdot$ sont valables dans tout anneau A lorsqu'on remplace X par un élément a et Y par un élément b de A.

Exemple 5.4. Rappelons que

$$(X+Y)^n = \sum_{i=0}^{n} \binom{n}{i} X^{n-i}Y^i$$

dans $\mathbb{Z}[X,Y]$ où $n \in \mathbb{N}$. Soit A un anneau quelconque et $a, b \in A$. On a alors

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

dans A.

6. Idéaux

Soit $f\colon A \to B$ un morphisme d'anneaux. On a vu que l'image $f(A)$ de f est un sous-anneaux de B. On aimerait construire l'anneau $f(A)$, à isomorphisme près, à partir des données intrinsèques à l'anneau A, i.e., sans avoir recours à B ou f. Observons que $f(a) = f(a')$ si et seulement si $a - a' \in \ker(f)$ quels que soient $a, a' \in A$. De ce fait il suffit de connaître le noyau $I = \ker(f)$ de f pour pouvoir construire l'ensemble $f(A)$. En effet, $f(A)$, en tant qu'ensemble, est en bijection avec quotient de l'ensemble A par la relation d'équivalence $\sim$ définie par

$$a \sim a' \iff a - a' \in I.$$

Le fait que f soit un morphisme d'anneaux implique que le sous-ensemble I de A vérifient les conditions suivantes :

I1: $0 \in I$;

I2: $x, y \in I \Longrightarrow x + y \in I$;

I3: $a \in A$ et $x \in I \Longrightarrow ax \in I$.

Réciproquement, soit $I \subseteq A$ un sous-ensemble vérifiant **I1**, **I2** et **I3**. On verra dans le paragraphe suivant que la relation $\sim$ définie sur A par $a \sim a' \Leftrightarrow a - a' \in I$ est alors une relation d'équivalence et que le quotient de l'ensemble A par $\sim$ admet une structure d'anneau induite par celle de A.

Définition 6.1. Soit A un anneau. Un sous-ensemble I de A est un *idéal* de A lorsque les conditions **I1**, **I2** et **I3** sont satisfaites.

Notons qu'un idéal est en particulier un sous-groupe de l'anneau.

Exemple 6.2.
(1) Les sous-ensembles $\{0\}$ et A sont des idéaux de A.
(2) Les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$.
(3) Si I est un idéal de A et J de B, alors $I \times J$ est un idéal de $A \times B$. Tout idéal de $A \times B$ est de la forme $I \times J$ où I est un idéal de A et J un idéal de B.

Rappelons la notion de somme de sous-groupes d'un groupe abélien. Soit G un groupe abélien et H et K deux sous-groupes. La somme de H et K est le sous-groupe

$$H + K = \{h + k \,|\, h \in H, k \in K\}.$$

Plus généralement, soit $H_1, \ldots, H_n$ une famille finie de sous-groupes de G. Alors la somme

$$H_1 + \cdots + H_n = \{h_1 + \cdots + h_n \,|\, h_1 \in H_1, \ldots, h_n \in H_n\}$$

est un sous-groupe de G.

Proposition 6.3. *Soit A un anneau et $I_1, \ldots, I_n$ une famille finie d'idéaux de A. Alors la somme $I_1 + \cdots + I_n$ est un idéal de A.*

Démonstration. Exercice. □

Exemple 6.4. $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$.

Lemme 6.5. *Soit A un anneau. Soit $\mathcal{C}$ une collection d'idéaux de A. Alors l'intersection $\bigcap \mathcal{C}$ est un idéal de A.*

Démonstration. Exercice. □

Exemple 6.6. $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$.

Proposition 6.7. *Soit A un anneau et S un sous-ensemble de A. Alors, le plus petit idéal de A contenant S existe.*

Démonstration. Soit $\mathcal{C}$ la collection des idéaux de A contenant S. D'après Lemme, $\bigcap \mathcal{C}$ est un idéal de A. Evidemment, $\bigcap \mathcal{C}$ contient S. Il reste à montrer que $\bigcap \mathcal{C}$ est le plus petit idéal de A contenant S. Soit alors I un sous-anneau de A contenant S. Comme $I \in \mathcal{C}$, on a $\bigcap \mathcal{C} \subseteq I$. □

Proposition 6.8. *Soient A un anneau et S un sous-ensemble de A. Alors le plus petit idéal de A contenant S est égal à*

$$(S) = \{\sum_{i=1}^{n} a_i s_i \,|\, a_i \in A, s_i \in S \text{ et } n \in \mathbb{N}\}.$$

Démonstration. On voit bien que (S) est un idéal de A. De plus, si I est un idéal de A contenant S, $\sum_{i=1}^{n} a_i s_i \in I$ pour tout $a_i \in A$, $s_i \in S$ et $n \in \mathbb{N}$. D'où $(S) \subseteq I$ et (S). □

Définition 6.9. Soit A un anneau et S un sous-ensemble de A. Alors, l'idéal (S) de A est *l'idéal engendré par S*.

Soit S un sous-ensemble de A. On rencontrera une multitude de notations pour l'idéal engendré par S : (S), AS ou aussi SA ; $(s_1, \ldots, s_n)$ lorsque $S = \{s_1, \ldots, s_n\}$; sA ou aussi As lorsque $S = \{s\}$.
Notons que

$$(s_1, \ldots, s_n) = (s_1) + \cdots + (s_n).$$

Exemple 6.10. (1) L'idéal $n\mathbb{Z}$ dans $\mathbb{Z}$, n un entier.

(2) L'idéal (X, Y) dans $A[X, Y]$. C'est l'idéal des polynômes en X et Y sans terme constant.

Définition 6.11. Soit A un anneau, I un idéal de A et S un sous-ensemble de A. L'idéal I est *engendré* par le sous-ensemble S lorsque $I = (S)$. L'idéal I de A est *de type fini* s'il existe un sous-ensemble fini de A engendrant I, i.e., s'il existe un entier n et $s_1, \ldots, s_n \in A$ tels que $I = (s_1, \ldots, s_n)$. L'idéal I est *principal* lorsque I est engendré par un singleton, i.e., lorsque $I = As$, pour certain $s \in A$.

Proposition 6.12. *Soit $f \colon A \to B$ un morphisme d'anneaux. Soit I un idéal de A et J un idéal de B.*

(1) $f^{-1}(J)$ est un idéal de A.

(2) Si f est surjectif alors $f(I)$ est un idéal de B.

Démonstration. Exercice. □

L'exemple suivant montre que la surjectivité est nécessaire.

Exemple 6.13. Soit f le morphisme d'inclusion de $\mathbb{Z}$ dans $\mathbb{Q}$. L'image directe $f(\mathbb{Z})$ de l'idéal $\mathbb{Z}$ n'est pas un idéal dans $\mathbb{Q}$. En effet, $\frac{1}{2} \cdot 1 = \frac{1}{2} \notin f(\mathbb{Z}) = \mathbb{Z}$ dans $\mathbb{Q}$.

Proposition 6.14. *Soit $f \colon A \to B$ un morphisme surjectif. Soit S un sous-ensemble de A, alors $f((S)) = (f(S))$.*

Démonstration. Exercice. □

Proposition 6.15. *Soit $f \colon A \to B$ un morphisme d'anneaux surjectif. Soit $I = \ker(f)$. Soient $\mathcal{I}$ l'ensemble des idéaux de A contenant I, et soit $\mathcal{J}$ l'ensemble des idéaux de B. Définisson deux applications :*

$$\begin{aligned} \varphi \colon \mathcal{I} &\to \mathcal{J} \\ I &\mapsto f(I) \end{aligned}$$

and

$$\begin{aligned} \psi \colon \mathcal{J} &\to \mathcal{I} \\ J &\mapsto f^{-1}(J) \end{aligned}$$

Alors $\psi \circ \varphi = \mathrm{id}$ et $\varphi \circ \psi = \mathrm{id}$. En particulier, l'ensembles des idéaux de B son en bijection avec l'ensembles des idéaux de A contenant I.

Démonstration. Exercice. □

Exemple 6.16. Déterminons les idéaux de l'anneau $\mathbb{Z}/36\mathbb{Z}$. Soit $\pi \colon \mathbb{Z} \to \mathbb{Z}/36\mathbb{Z}$ le morphisme de reduction modulo 36. Comme π est surjectif et son noyau est egal à lidéal $36\mathbb{Z}$ dans $\mathbb{Z}$, l'ensemble des idéaux est en bijection avec les idéaux I de $\mathbb{Z}$ contenant $36\mathbb{Z}$. Or les idéaux de $\mathbb{Z}$ sont tous de la forme $n\mathbb{Z}$, pour un certain entier naturel n. L'idéal $n\mathbb{Z}$ contient $36\mathbb{Z}$ si et seulement si $n|36$. Les diviseurs naturels de $36 = 2^2 3^2$ sont $1, 3, 2, 6, 18, 4, 12, 36$. Les idéaux de $\mathbb{Z}$ contenant $36\mathbb{Z}$ sont donc les idéaux $1\mathbb{Z}, 3\mathbb{Z}, 2\mathbb{Z}, 6\mathbb{Z}, 18\mathbb{Z}, 4\mathbb{Z}, 12\mathbb{Z}, 36\mathbb{Z}$. Les idéaux correpsondants de $\mathbb{Z}/36\mathbb{Z}$ sont $(1), (3), (2), (6), (18), (4), (12), (36)$.

7. Anneaux quotients

Soient A un anneau et I un idéal de A. On va construire *l'anneau quotient* A/I de A par I : Soit $\sim$ la relation sur A définie par

$$a \sim b \Longleftrightarrow a - b \in I.$$

Cette relation est une relation d'équivalence. Soit A/I le quotient de l'ensemble A par $\sim$, c-à-d, A/I est l'ensemble des classes d'équivalences de $\sim$. Pour $a \in A$ on notera sa classe d'équivalence par $\overline{a}$.

Ensuite on définit deux lois internes binaires $+$ et $\cdot$ sur A/I induites par celles de A. D'abord, soient

$$\alpha, \mu \colon A \times A \longrightarrow A/I$$

les applications définies par $\alpha(a,b) = \overline{a+b}$ et $\mu(a,b) = \overline{ab}$. On vérifie que $\alpha(a,b)$ et $\mu(a,b)$ ne dépendent que des classes d'équivalence de a et b. En effet, si $a \sim c$ et $b \sim d$, $(a+b)-(c+d) = (a-c)+(b-d) \in I$ et $ab - cd = b(a-c) + c(b-d) \in I$. D'où, $a+b \sim c+d$ et $ab \sim cd$, c-à-d, $\alpha(a,b) = \alpha(c,d)$ et $\mu(a,b) = \mu(c,d)$. Par conséquent, α et μ induisent deux lois internes binaires $+$ et $\cdot$ sur A/I définies par

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{et} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Il est facile de vérifier que A/I muni de ces lois internes est un anneau. On a $0 = \overline{0}$, $1 = \overline{1}$ et $-\overline{a} = \overline{-a}$ dans A/I. De plus, l'application

$$\pi \colon A \longrightarrow A/I$$

qui envoie $a \in A$ sur sa classe d'équivalence $\overline{a}$ est un morphisme d'anneaux.

Définition 7.1. Soient A un anneau et I un idéal de A. Le *quotient* de A par I est la paire $(A/I, \pi)$ consistant de *l'anneau quotient* A/I et du *morphisme de passage au quotient* $\pi \colon A \to A/I$. Parfois on dira par abus de langage que A/I est le quotient.

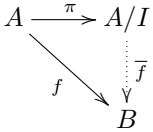
Exemple 7.2. (1) $\mathbb{Z}/n\mathbb{Z}$

(2) Notons α la classe de X dans le quotient $A = \mathbb{Z}[X]/(X^2-2)$. On a alors $\alpha^2 = 2$ dans A. On a adjoint abstraitement une racine carré de 2. On peut démontrer qu'ici A est isomorphe avec le sous-anneau $\mathbb{Z}[\sqrt{2}]$ de $\mathbb{R}$.

La définition du quotient comme l'anneau quotient muni du morphisme de passage au quotient est d'une subtilité que l'on va expliquer : Le morphisme de passage au quotient établit le lien entre l'anneau et son anneau quotient. Sans ce morphisme il n'y aurait eu aucun rapport entre A et A/I. Ils auraient été tout simplement deux anneau flottant dans l'univers. Par contre, c'est le morphisme, lui, qui les met en rapport. La propriété suivante en est une illustration.

Propriété universelle du quotient. *Soient A un anneau et I un idéal de A. Soit $\pi \colon A \to A/I$ le passage au quotient. Alors, on a $\pi(I) = \{0\}$ et π est le morphisme universel ayant cette propriété, c-à-d, pour tout anneau B et tout morphisme $f \colon A \to B$ avec $f(I) = \{0\}$ il existe un et un seul morphisme $\overline{f} \colon A/I \to B$ tel que le diagramme commute :*

(1)

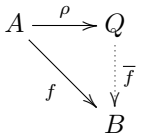


Démonstration. Soient $a, b \in A$ tels que $a - b \in I$. Comme $f(I) = 0$, on a $f(a) = f(b)$. Cela montre que l'application $\overline{f} \colon A/I \to B$ définie par $\overline{f}(\overline{a}) = f(a)$ est bien définie. Comme $\overline{f} \circ \pi = f$ est un morphisme d'anneaux et π est un morphisme d'anneaux surjectif, $\overline{f}$ est un morphisme d'anneaux. L'unicité de $\overline{f}$ s'ensuit de la surjectivité de π. □

On ne veut pas favoriser la construction ci-dessus du quotient d'un anneau et on appelle un quotient de A par I tout morphisme $\rho \colon A \to Q$ étant universel parmi les morphismes d'anneaux $f \colon A \to B$ tels que $f(I) = \{0\}$. Plus précisément :

Définition 7.3. Soit A un anneau et $I \subseteq A$ un idéal. Un morphisme d'anneaux $\rho \colon A \to Q$ est *un quotient de A par I* si $\rho(I) = \{0\}$ et pour tout anneau B et tout morphisme d'anneaux

$f\colon A \to B$ avec $f(I) = \{0\}$, il existe un et un seul morphisme d'anneaux $\overline{f}\colon Q \to B$ tel que le diagramme suivant commute :



PROPOSITION 7.4. *Soit A un anneau et $I \subseteq A$ un idéal. Soit $\pi\colon A \to A/I$ le passage au quotient. Lorsque $\rho\colon A \to Q$ est un quotient de A par I, il existe un isomorphisme $f\colon A/I \to Q$ tel que $f \circ \pi = \rho$. En particulier, A/I et Q sont isomorphes.*

DÉMONSTRATION. Il existe un morphisme d'anneaux $f\colon A/I \to Q$ tel que $f \circ \pi = \rho$, d'après la propriété universelle de π. De même, il existe un morphisme d'anneaux $g\colon Q \to A/I$ tel que $g \circ \rho = \pi$, d'après la propriété universelle de ρ. On a alors le morphisme $g \circ f$ de A/I dans lui-même satisfaisant $(g \circ f) \circ \pi = \pi$. Or, l'identité $\mathrm{id}_{A/I}$ sur A/I satisfait lui aussi $\mathrm{id}_{A/I} \circ \pi = \pi$. D'après l'unicité, $g \circ f = \mathrm{id}_{A/I}$. De même, en utilisant la propriété universelle de ρ cette fois-ci, on montre $f \circ g = \mathrm{id}_Q$, c-à-d, $f\colon A/I \to Q$ est un isomorphisme. □

PROPOSITION 7.5. *Soit A un anneau, $I \subseteq A$ un idéal et $\rho\colon A \to Q$ un morphisme d'anneaux. Le morphisme ρ est un quotient de A par I si et seulement si ρ est surjectif et $\ker(\rho) = I$.*

DÉMONSTRATION. Supposons que ρ est un quotient de A par I. Soit $\pi\colon A \to A/I$ le quotient de A par I. D'après Proposition 7.4, il existe un isomorphisme $f\colon A/I \to Q$ tel que $f \circ \pi = \rho$. On a alors $\ker(\rho) = \ker(\pi)$. Or $\ker(\pi) = I$, donc $\ker(\rho) = I$. De plus, comme f et π sont surjectifs, ρ est surjectif.

Pour montrer l'autre implication, supposons que $\ker(\rho) = I$ et que ρ est surjectif. Il faut montrer que ρ est universel. Soit $f\colon A \to B$ un morphisme d'anneaux tel que $f(I) = \{0\}$. En utilisant la surjectivité de ρ, définissons une application $\overline{f}\colon Q \to B$ par $\overline{f}(q) = f(a)$ où $a \in A$ est tel que $\rho(a) = q$. Observez que $\overline{f}(q)$ ne dépend pas du choix de $a \in A$ tel que $\rho(a) = q$. En effet, si $a' \in A$ satisfait $\rho(a') = q$ lui aussi, alors $a - a' \in \ker(\rho) = I$. D'où $f(a) - f(a') = f(a - a') = 0$. Par conséquent, on a $\overline{f} \circ \rho = f$. Comme f est un morphisme et ρ est un morphisme surjectif, $\overline{f}$ est un morphisme. Il est clair que la surjectivité de ρ implique l'unicité de $\overline{f}$. On conclut que ρ est universel. □

EXEMPLE 7.6. Soit A un anneau et $a \in A$. Soit $f\colon A[X] \to A$ le morphisme d'évaluation en a, c-à-d, $f(P) = P(a)$, où

$$P(a) = a_n a^n + \cdots + a_1 a + a_0$$

lorsque $P = a_n X^n + \cdots + a_1 X + a_0$. Alors, f est un quotient de $A[X]$ par l'idéal $(X - a)$. Effectivement, f est surjectif et on a $(X - a) \subseteq \ker(f)$. Pour montrer l'inclusion $\ker(f) \subseteq (X - a)$ on utilise la division euclidienne dans $A[X]$ par un polynôme unitaire : Soit $P \in \ker(f)$. Alors, il existe $Q, R \in A[X]$ tels que $P = (X - a)Q + R$ où $\deg(R) < \deg(X - a) = 1$. D'où $R \in A$ et l'évaluation en a donne $0 = P(a) = 0 \cdot Q(a) + R(a) = R$, i.e., $R = 0$ et donc $P \in (X - a)$.

Le quotient permet de construire des anneaux universels ayant certaines propriétés.

EXEMPLE 7.7.

(1) Soit $A = \mathbb{Z}[X, Y]/(XY)$ et notons x et y les classes de X et Y respectivement. On a $xy = 0$ dans A mais $x \neq 0$, $y \neq 0$. Cet anneau A est l'exemple universel d'un anneau muni de deux éléments de produit nul. En effet, soit B un anneau ayant deux éléments b, c avec $bc = 0$. Alors il existe un morphisme d'anneaux $f\colon \mathbb{Z}[X, Y] \to B$ avec $f(X) = b$ et $f(Y) = c$. Comme $f(XY) = bc = 0$, $f((XY)) = \{0\}$ et f induit un morphisme $\overline{f}$ de A dans B avec $f(x) = b$ et $f(y) = c$.

(2) Soit $A = \mathbb{Z}[X, Y]/(XY - 2)$. C'est l'anneau universel où 2 possède une décomposition comme produit de deux éléments.

(3) Soit $\mathbb{Z}[X, Y]/(XY - 6)$. C'est l'anneau universel où 6 possède au moins 2 décomposition essentiellement distinctes $6 = 2 \cdot 3$ et $6 = xy$ car $x, y \neq \pm 1, \pm 2, \pm 3, \pm 6$.

8. Inversibles dans un anneau

DÉFINITION 8.1. Soit A un anneau et $a \in A$. L'élément a de A est *inversible* s'il existe $b \in A$ tel que $ab = 1$ et $ba = 1$. Si un tel élément b existe, il est unique. On le note a^{-1}.

Exemple 8.2. (1) L'élément neutre multiplicatif 1 est inversible dans n'importe quel anneau.

(2) L'élément neutre additif 0 est inversible dans un anneau A si et seulement si A est l'anneau nul.

(3) 2 n'est pas inversible comme élément de l'anneau $\mathbb{Z}$; il l'est comme élément de l'anneau $\mathbb{Q}$.

(4) X n'est pas inversible dans $\mathbb{Z}[X]$; sa classe dans le quotient $\mathbb{Z}[X,Y]/(XY-1)$ l'est.

On a la règle de simplification pour un élément inversible : si dans un anneau A on a $ab = ac$ avec a inversible, alors $b = c$.

Proposition 8.3. *Soit $f\colon A \to B$ un morphisme d'anneaux. Si $a \in A$ est inversible, $f(a)$ l'est et $f(a)^{-1} = f(a^{-1})$.*

Proposition 8.4. *Soit A un anneau et $a \in A$. Alors a est inversible si et seulement si $(a) = A$.*

Proposition 8.5. *Soit A un anneau et $a, b \in A$. Si a est inversible, $(ab) = (b)$.*

Proposition 8.6. *Soit A un anneau.*

(1) Soit $a \in A$. Si a est inversible, $-a$ l'est et $(-a)^{-1} = -(a^{-1})$.

(2) Soient $a, b \in A$. Si a et b sont inversibles, ab l'est et $(ab)^{-1} = b^{-1}a^{-1}$.

(3) Soit $a \in A$ et $n \in \mathbb{N}$. Si a est inversible, a^n l'est et $(a^n)^{-1} = (a^{-1})^n$.

(4) Soit $a \in A$ si a est inversible, a^{-1} l'est et $(a^{-1})^{-1} = a$.

(5) Soient $a, b \in A$. Si ab est inversible, a et b le sont, et $a^{-1} = b(ab)^{-1}$ et $b^{-1} = (ab)^{-1}a$.

(6) Soient $a \in A$ et $n \in \mathbb{N} \setminus \{0\}$. Si a^n est inversible, a l'est et $a^{-1} = (a^n)^{-1}a^{n-1}$.

Définition 8.7. Soit A un anneau. On note $A^\times$ le sous-ensemble des inversibles de A. Il suit de la proposition précédente que $A^\times$ est un groupe pour la multiplication, c'est le *groupe multiplicatif* de A. Il est commutatif si A l'est.

On voit aussi la notation $A^\star$ pour le groupe multiplicatif d'un anneau. Dans ce cours $A^\star$ désignera toujours le sous-ensemble $A \setminus \{0\}$ de A.

Exemple 8.8. (1) Le groupe multiplicatif de l'anneau $\mathbb{Z}$ est $\{\pm 1\}$, muni de la multiplication.

(2) Le groupe multiplicatif de l'anneau $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont $\mathbb{Q}\setminus\{0\}$, $\mathbb{R}\setminus\{0\}$ et $\mathbb{C}\setminus\{0\}$, respectivement.

(3) Le groupe multiplicatif de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est $\{\overline{x} \mid \mathrm{pgcd}(x,n) = 1\}$, muni de la multiplication. On laisse la vérification au lecteur.

Comme dans tout groupe noté multiplicativement, l'expression a^n possède un sens lorsque $n \in \mathbb{Z}$ pour tout élément inversible a d'un anneau A. De plus, on a les règles de calcul habituelles :

(1) $a^1 = a$

(2) $a^{m+n} = a^m \cdot a^n$,

(3) $(ab)^n = a^n b^n$, et

(4) $a^{mn} = (a^m)^n$,

quels que soient $a, b \in A^\times$ et $m, n \in \mathbb{Z}$.

Proposition 8.9. *Soient A et B des anneaux. Le groupe multiplicatif $(A \times B)^\times$ est égal à $A^\times \times B^\times$.*

Proposition 8.10. *Soit $f\colon A \to B$ un morphisme d'anneaux. Alors $f(A^\times) \subseteq B^\times$ et la restriction de f à $A^\times$, considérée comme application dans $B^\times$, est un morphisme de groupes. En particulier, on a $f(a^n) = f(a)^n$ pour tout $a \in A^\times$ et $n \in \mathbb{Z}$.*

Exemple 8.11. Soit $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ le morphisme quotient, où n est un entier naturel non nul. Il induit un morphisme de groupe multiplicatif $\pi^\times\colon \mathbb{Z}^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$. Rappelons que le groupe $\mathbb{Z}^\times$ est le groupe multiplicatif $\{\pm 1\}$. Le morphisme $\pi^\times$ est défini par $\pi^\times(1) = \overline{1}$ et $\pi^\times(-1) = -\overline{1}$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Le cardinal de ce dernier groupe est égal à $\varphi(n)$, où φ est la fonction totient d'Euler. Comme $\varphi(n) > 2$ lorsque $n \neq 1, 2, 3, 4, 6$. Le morphisme de groupes $\pi^\times$ n'est pas surjectif lorsque $n \neq 1, 2, 3, 4, 6$. C'est remarquable car le morphisme π, il est bien surjectif !

COROLLAIRE 8.12. *Si A et B sont des anneaux isomorphes, leurs groupes multiplicatifs $A^\times$ et $B^\times$ sont des groupes isomorphes.*

Notons que dans la démonstration de la proposition précédente, on a utilisé seulement les conditions M2 et M3 de la définition d'un morphisme d'anneaux. On a donc plus généralement :

PROPOSITION 8.13. *Soient A et B des anneaux. Soit $f\colon A \to B$ une application telle que $f(1) = 1$ et $f(aa') = f(a)f(a')$ quels que soient $a, a' \in A$. Alors $f(A^\times) \subseteq B^\times$ et la restriction de f à $A^\times$, considérée comme application dans $B^\times$, est un morphisme de groupes.*

EXEMPLE 8.14. Le groupe multiplicatif de l'anneau de Gauss $\mathbb{Z}[i]$ est $\{\pm 1, \pm i\}$, muni de la multiplication. En effet, il est clair que $\pm 1, \pm i$ sont des inversibles dans $\mathbb{Z}[i]$. On a donc $\{\pm 1, \pm i\} \subseteq \mathbb{Z}[i]^\times$. Afin de montrer l'inclusion réciproque, soit $N\colon \mathbb{Z}[i] \to \mathbb{Z}$ l'application définie par $N(z) = z\bar{z}$. On a bien $N(wz) = N(w)N(z)$ et $N(1) = 1$. Il suit de la proposition précédente que $N(\mathbb{Z}[i]^\times) \subseteq \mathbb{Z}^\times = \{\pm 1\}$. Comme $N(a + bi) = a^2 + b^2 \geq 0$, quels que soient $a, b \in \mathbb{Z}$, on a forcément $N(\mathbb{Z}[i]^\times) = \{1\}$. Les seules solutions dans $\mathbb{Z}$ de l'équation $a^2 + b^2 = 1$ étant $(a, b) = (\pm 1, 0), (0, \pm 1)$, on a $\mathbb{Z}[i]^\times \subseteq \{\pm 1, \pm i\}$. Par conséquent, $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

9. La localisation d'un anneau

La localisation d'un anneau A va permettre de considérer un anneau de fractions $\frac{a}{s}$ où a est un élément de A et s est un élément d'un sous-ensemble de dénominateurs S de A. Pour que l'ensemble de tels fractions soit un anneau il va falloir que S soit une partie multiplicative de A :

DÉFINITION 9.1. Soit A un anneau. Un sous-ensemble S de A est une *partie multiplicative* lorsque $1 \in S$ et $st \in S$ pour tout $s, t \in S$.

EXEMPLE 9.2. (1) Le sous-ensemble $\mathbb{Z} \setminus \{0\}$ de $\mathbb{Z}$ est une partie multiplicative de $\mathbb{Z}$.

(2) Le sous-ensemble $\{1, 10, 10^2, \ldots\}$ de $\mathbb{Z}$ est une partie multiplicative de l'anneau $\mathbb{Z}$.

(3) $\{1, X, X^2, \ldots\} \subseteq A[X]$ est une partie multplicative de $A[X]$

Soit A un anneau et $S \subseteq A$ une partie multiplicative. On définira la localisation de A par S. Tout d'abord, on définit sur $A \times S$ une relation $\sim$ par

$$(a, s) \sim (b, t) \iff \exists r \in S : rta = rsb.$$

LEMME 9.3. *La relation $\sim$ sur l'ensemble $A \times S$ est une relation d'équivalence.*

DÉMONSTRATION. La reflexivité et la symétrie de $\sim$ sont évidentes. Pour la transitivité supposons que $(a, s) \sim (b, t)$ et $(b, t) \sim (c, r)$. Alors il existe $u, v \in S$ tels que $uta = usb$ et $vrb = vtc$. Multiplier la première équation par vr et la deuxième par us :

$$vruta = vrusb = usvrb = usvtc.$$

Ou encore,

$$(vut)ra = (vut)sc.$$

Comme $vut \in S$ on a $(a, s) \sim (c, r)$. □

Soit $S^{-1}A$ le quotient de $A \times S$ par la relation d'équivalence $\sim$. La classe d'équivalence d'un élément (a, s) de $A \times S$ sera notée par $\frac{a}{s}$. Observons que l'on a $\frac{at}{st} = \frac{a}{s}$ dans $S^{-1}A$ quel que soit $t \in S$.

Ensuite on définira deux lois internes binaires $+$ et $\cdot$ sur $S^{-1}A$. On se laisse guider par la somme et le produit de deux fractions rationelles. Soient

$$\alpha, \mu\colon (A \times S) \times (A \times S) \to S^{-1}A$$

les applications définies par

$$\alpha((a, s), (b, t)) = \frac{at + bs}{st} \quad \text{et} \quad \mu((a, s), (b, t)) = \frac{ab}{st}.$$

C'est un exercice de montrer que $\alpha((a, s), (b, t))$ et $\mu((a, s), (b, t))$ ne dépendent que des classes d'équivalence de (a, s) et (b, t). Les applications α et μ induisent alors des lois internes sur $S^{-1}A$:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \quad \text{et} \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

On vérifie sans peine que $S^{-1}A$ est un anneau. On a dans $S^{-1}A$

$$0 = \frac{0}{1}, \quad 1 = \frac{1}{1}, \quad \text{et} \quad -\frac{a}{s} = \frac{-a}{s}.$$

De plus, on a une application

$$\iota\colon A \to S^{-1}A$$

définie par $\iota(a) = \frac{a}{1}$. Il est clair que ι est un morphisme d'anneaux.

DÉFINITION 9.4. Soit A un ensemble et $S \subseteq A$ une partie multiplicative. La *localisation* de A par S est l'anneau $S^{-1}A$ muni du morphisme $\iota\colon A \to S^{-1}A$. Parfois on appelle $S^{-1}A$ lui-même la localisation de A par S.

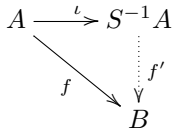
EXEMPLE 9.5.
(1) Soit S le sous-ensemble $\mathbb{Z} \setminus \{0\}$ de $\mathbb{Z}$. Alors, $\frac{a}{s} = \frac{b}{t}$ dans $S^{-1}\mathbb{Z}$ si et seulement si $ta = sb$. Par conséquent, $S^{-1}\mathbb{Z}$ *est* l'anneau $\mathbb{Q}$, et le morphisme $\iota\colon \mathbb{Z} \to S^{-1}\mathbb{Z}$ est l'inclusion de $\mathbb{Z}$ dans $\mathbb{Q}$.
(2) Soit $S = \{1, 10, 10^2, 10^3, \ldots\} \subseteq \mathbb{Z}$. Alors, la localisation $S^{-1}\mathbb{Z}$ de $\mathbb{Z}$ par S est isomorphe à l'anneau des nombres décimaux $\mathbb{D}$.
(3) Soit $S = \{1, X, X^2, \ldots\} \subseteq A[X]$. Alors, la localisation $S^{-1}A[X]$ est l'anneau des polynômes de Laurent en X à coefficients dans A.
(4) Soit S la partie multiplicative $\{1\}$ d'un anneau A. Alors $S^{-1}A$ est isomorphe à A.
(5) Soit S la partie multiplicative $\{0, 1\}$ dans un anneau A. Alors $S^{-1}A$ est l'anneau nul.

Soit $S \subseteq A$ une partie multiplicative et $\iota\colon A \to S^{-1}A$ le morphisme de localisation. L'image par ι d'un élément $s \in S$ est inversible dans $S^{-1}A$. En effet,

$$\frac{s}{1} \cdot \frac{s}{1} = 1 \quad \text{et} \quad \frac{s}{1} \cdot \frac{1}{s} = 1.$$

En fait, l'anneau $S^{-1}A$, ou plus précisément, le morphisme de localisation $\iota\colon A \to S^{-1}A$, est universel avec cette propriété :

PROPRIÉTÉ UNIVERSELLE DE LA LOCALISATION. *Soit A un anneau et $S \subseteq A$ une partie multiplicative. Soit $\iota\colon A \to S^{-1}A$ le morphisme de localisation. Alors, $\iota(s)$ est inversible dans $S^{-1}A$ quel que soit $s \in S$ et ι est universel ayant cette propriété, c-à-d, pour tout anneau B et pour tout morphisme d'anneaux $f\colon A \to B$ avec $f(s)$ inversible quel que soit $s \in S$, il existe un et un seul morphisme d'anneaux $f'\colon S^{-1}A \to B$ rendant commutatif le diagramme suivant :*



DÉMONSTRATION. On a déjà vu que $\iota(s) = s/1$ est inversible dans $S^{-1}A$. Montrons donc que ι est universel, et supposons que $f\colon A \to B$ est un morphisme d'anneaux tel que $f(s)$ est inversible quel que soit $s \in S$.

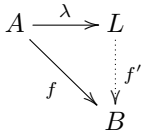
Soit $g\colon A \times S \to B$ définie par $g(a, s) = f(s)^{-1}f(a)$. Lorsque $(a, s) \sim (b, t)$ dans $A \times S$, il existe $u \in S$ tel que $uta = usb$. On a alors $f(u)f(t)f(a) = f(u)f(s)f(b)$ dans B. Comme $f(u)$, $f(t)$ et $f(s)$ sont inversibles dans B, on a $g(a, s) = f(s)^{-1}f(a) = f(t)^{-1}f(b) = g(b, t)$. Cela montre que g induit une application f' de $S^{-1}A$ dans B. On a alors $f'(\frac{a}{s}) = f(s)^{-1}f(a)$. On vérifie facilement que f' est un morphisme d'anneaux. De plus, on a $f' \circ \iota = f$. Cela montre l'existence de f'.

Pour montrer l'unicité de f', supposons que f'' est aussi un morphisme de $S^{-1}A$ dans B tel que $f'' \circ \iota = f$. En particulier, on a $f''(\frac{s}{1}) = f(s) = f'(\frac{s}{1})$ pour tout $s \in S$. Comme $\frac{s}{1}$ est inversible dans $S^{-1}A$ et son inverse est $\frac{1}{s}$, $f''(\frac{1}{s}) = f'(\frac{1}{s})$. D'où $f''(\frac{a}{s}) = f''(\frac{a}{1})f''(\frac{1}{s}) = f'(\frac{a}{1})f'(\frac{1}{s}) = f'(\frac{a}{s})$ pour tout $\frac{a}{s} \in S^{-1}A$. Cela montre l'unicité de f'. □

Comme pour les anneaux quotients, on ne veut pas favoriser la construction particulière de $S^{-1}A$:

DÉFINITION 9.6. Soit A un anneau et $S \subseteq A$ une partie multipicative. Soit $\lambda\colon A \to L$ un morphisme d'anneaux avec $\lambda(s)$ inversible quel que soit $s \in S$. On appelle λ une *localisation de A par S* lorsque pour λ satisfait la propriété universelle suivante. Pour tout anneau B et pour tout

morphisme $f\colon A \to B$ avec $f(s)$ inversible pour tout $s \in S$, il existe un et un seul morphisme d'anneaux $f'\colon L \to B$ tel que le diagramme suivant commute :



Comme pour les quotients, lorsque L est une localisation de A par S, L est isomorphe à $S^{-1}A$.

PROPOSITION 9.7. *Soit A un anneau et S une partie multiplicative de A. Supposons que tous les éléments de S sont inversibles dans A. Alors, $S^{-1}A$ est isomorphe à A. Plus précisément, le morphisme d'identité* $\mathrm{id}\colon A \to A$ *est une localisation de A par S.*

DÉMONSTRATION. L'image par id de tout élément $s \in S$ est bien inversible pour tout $s \in S$.

Soit $f\colon A \to B$ un morphisme d'anneaux tels que $f(s)$ est inversible pour tout $s \in S$. Il est clair qu'il existe un et un seul morphisme $f'\colon A \to A$ tel que $f' \circ \mathrm{id} = f$. En effet, C'est le morphisme f lui-même. □

Si $S \subseteq A^\times$, on peut donc identifier A avec $S^{-1}A$ par ι. En particulier, on a $\frac{1}{s} = s^{-1}$, ou plus généralement $\frac{a}{s} = s^{-1}a$ dans ce cas.

EXEMPLE 9.8. Soit n un entier naturel non nul. Soit S l'ensemble des éléments inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$. Du coup, le morphisme de localisation ι de $\mathbb{Z}/n\mathbb{Z}$ dans $S^{-1}(\mathbb{Z}/n\mathbb{Z})$ est un isomorphisme. La fraction de la forme $\frac{\bar{a}}{\bar{s}}$ avec $a, s \in \mathbb{Z}$ et $\mathrm{pgcd}(s, n) = 1$ a donc un sensdans $S^{-1}(\mathbb{Z}/n\mathbb{Z})$ et est égale à $\bar{s}^{-1}\bar{a}$ dans $\mathbb{Z}/n\mathbb{Z}$.

DÉFINITION 9.9. Soient A un anneau et s un élément de A. Soit S la plus petite partie multiplicative de A contenant s, i.e., $S = \{1, s, s^2, s^3, \ldots\}$. On notera A_s au lieu de $S^{-1}A$. La *localisation* de A par s est l'anneau A_s, ou plus précisément, l'anneau A_s muni du morphisme $\iota\colon A \to A_s$, défini par $\iota(a) = \frac{a}{1}$.

PROPOSITION 9.10. *Soit A un anneau et $s \in A$. Soit $S = \{1, s, s^2, \ldots\}$. Soit $\lambda\colon A \to A[X]/(sX-1)$ le morphisme définie par $\lambda(a) = \bar{a}$. Alors, λ est une localisation de A par S. En particulier, les anneaux $A[X]/(sX-1)$ et A_s sont isomorphes.*

DÉMONSTRATION. On montre que λ vérifie la propriété universelle de la localisation $\iota\colon A \to S^{-1}A$ de A par S.

Tout d'abord, il fait vrifier que $\lambda(s')$ est inversible pour tout $s' \in S$. Dans $A[X]/(sX-1)$ on a $\bar{s} \cdot \bar{X} - 1 = 0$, i.e., $\bar{s} \cdot \bar{X} = 1$. Autrement dit, $\bar{s} = \lambda(s)$ est inversible dans $A[X]/(sX-1)$. Du coup, $\lambda(s^n) = \lambda(s)^n$ est inversible pour tout $n \in \mathbb{N}$.

Puis on montre que λ est universel. Soit $f\colon A \to B$ un morphisme d'anneaux avec $f(s')$ inversible pour tout $s' \in S$. On montre qu'il existe un et un seul morphisme $f'\colon A[X]/(sX-1) \to B$ tel que $f' \circ \lambda = f$.

Supposons qu'un tel f' existe. On a donc

$$0 = f'(0) = f'(\bar{s}\bar{X} - \bar{1}) = f'(\lambda(s)) \cdot f'(\bar{X}) - 1 = f(s) \cdot f'(\bar{X}) - 1$$

dans B. Autrement dit, $f'(\bar{X}) \cdot f(s) = 1$ et $f'(\bar{X}) = f(s)^{-1}$ dans B. Notons $\pi\colon A[X] \to A[X]/(sX-1)$ le passage au quotient. On a donc $f' \circ \pi(X) = f(s)^{-1}$ et $f' \circ \pi_{|A} = f' \circ \lambda = f$. Du coup, $f' \circ \pi$ est le morphisme d'évaluation en $f(s)^{-1}$ de $A[X]$ vers B. Comme π est surjectif, f' est unique.

SOit $g\colon A[X] \to B$ le morphisme d'évaluation en $f(s)^{-1}$. On a $g(sX-1) = 0$ et g induit un morphisme $f'\colon A[X]/(sX-1) \to B$ avec $f' \circ \pi = g$. Il s'ensuit que $f' \circ \lambda = f$. □

EXEMPLE 9.11. L'anneau $\mathbb{Z}_{10}$ est isomorphe à $\mathbb{Z}[X]/(10X-1)$. En particulier, l'anneau des nombres décimaux $\mathbb{D}$ est isomorphe à $\mathbb{Z}[X]/(10X-1)$.

Soit $S \subseteq A$ une partie multiplicative et $I \subseteq A$ un idéal de A. L'idéal de $S^{-1}A$ engendré par l'image de I dans $S^{-1}A$ est noté par $S^{-1}I$. On a

$$S^{-1}I = \{\frac{x}{s} \mid x \in I, s \in S\}.$$

Bien que I ne soit pas un sous-ensemble de $S^{-1}A$, on note l'idéal $S^{-1}I$ de $S^{-1}A$ engendré par $\iota(I)$ aussi par $(S^{-1}A)I$ ou bien par $I(S^{-1}A)$.

PROPOSITION 9.12. *Soit $S \subseteq A$ une partie multiplicative et $I \subseteq A$ un idéal de A. Soit $\overline{S}$ l'image de S dans le quotient A/I. Alors, $\overline{S}$ est une partie multiplicative et on a un isomorphisme*

$$\overline{S}^{-1}(A/I) \cong (S^{-1}A)/(S^{-1}I).$$

Il y a plusieurs façons de démontrer cet énoncé. Par exemple, le premier membre est la localisation de A/I par $\overline{S}$. On pourra montrer l'isomorphisme en montrant que le deuxième en est une aussi.

DÉMONSTRATION. Soit $\rho\colon S^{-1}A \to S^{-1}A/S^{-1}I$ le morphisme de passage au quotient. Le morphisme $\rho \circ \iota$ de A dans $S^{-1}A/S^{-1}I$ envoie I sur $\{0\}$. Il existe donc un morphisme λ de A/I dans $S^{-1}A/S^{-1}I$ tel que $\lambda \circ \pi = \rho \circ \iota$, d'apr'es la propriété universelle du quotient de A par I.

Montrons que λ est une localisation de A/I par $\overline{S}$. Tout d'abord, comme $\iota(S) \subseteq (S^{-1}A)^\times$ et $\rho((S^{-1}A)^\times) \subseteq (S^{-1}A/S^{-1}I)^\times$, on a

$$\lambda(\bar{S}) = \lambda(\pi(S)) = \lambda \circ \pi(S) = \rho \circ \iota(S) = \rho(\iota(S)) \subseteq (S^{-1}A/S^{-1}I)^\times$$

ce qui montre que $\lambda(\bar{s})$ est inversible quel que soit $\bar{s} \in \bar{S}$.

Montrons ensuite que λ satisfait la propriété universelle de la localisation de A/I par $\bar{S}$. Soit $f\colon A/I \to B$ un morphisme d'anneaux avec $f(\bar{s})$ inversible pour tout $s \in S$. L'application $\hat{f}$ de A dans B définie par $\hat{f} = f \circ \pi$ est un morphisme d'anneaux. De plus, $\hat{f}(s) = f(\bar{s})$ est inversible pour tout $s \in S$. Il induit donc un morphisme $\hat{f}'$ de $S^{-1}A$ dans B, i.e, $\hat{f}'$ est le morphisme de $S^{-1}A$ dans B défini par $\hat{f}'(\frac{a}{s}) = \hat{f}(s)^{-1}\hat{f}(a) = f(\bar{s})-1f(\bar{a})$. Il est clair que $\hat{f}'(S^{-1}I) = \{0\}$. Il existe donc un morphisme f' de $S^{-1}A/S^{-1}I$ dans B tel que $f' \circ \rho = \hat{f}'$. En particulier, on a

$$f' \circ \lambda \circ \pi = f' \circ \rho \circ \iota = \hat{f}' \circ \iota = \hat{f} = f \circ \pi.$$

Comme π est surjectif, on en déduit que $f' \circ \lambda = f$. Cela montre l'existence du morphisme f' de $S^{-1}A/S^{-1}I$ dans B tel que $f' \circ \lambda = f$.

Quant à l'unicité, supposons que $f''\colon S^{-1}A/S^{-1}I \to B$ est aussi un morphisme tel que $f'' \circ \lambda = f$. On a alors

$$f'' \circ \lambda \circ \pi = f \circ \pi = \hat{f}.$$

Du coup,

$$f'' \circ \rho \circ \iota = f''\lambda \circ \pi = \hat{f}.$$

D'après l'unicité de $\hat{f}'$, on a alors

$$f'' \circ \rho = \hat{f}'.$$

D'après l'unicité de f', on a $f'' = f'$. □

Voici une deuxième démonstration, dont la stratgie est de démontrer que le premier membre est un quotient de $S^{-1}A$ par $S^{-1}I$.

DÉMONSTRATION. □

REMARQUE 9.13. Notons que l'isomorphisme φ de $\bar{S}^{-1}(A/I)$ vers $S^{-1}A/S^{-1}I$ ainsi obtenu est l'unique isomorphisme tel que $\varphi \circ \bar{\iota} \circ \pi = \rho \circ \iota$. Il permet donc d'identifier de manière non ambigue les éléments de l'un avec les éléments de l'autre. Cela justifie d'écrire $\bar{S}^{-1}(A/I) = S^{-1}A/S^{-1}I$ au lieu de $\bar{S}^{-1}(A/I) \cong S^{-1}A/S^{-1}I$. On le fera désormais dans toutes les situations où l'isomorphisme est unique.

EXEMPLE 9.14. Déterminons la localisation $(\mathbb{Z}/6\mathbb{Z})_2$ de l'anneau $\mathbb{Z}/6\mathbb{Z}$ par 2. D'après la proposition précédente,

$$(\mathbb{Z}/6\mathbb{Z})_2 = \mathbb{Z}_2/6\mathbb{Z}_2.$$

Comme 2 est inversible dans $\mathbb{Z}_2$, l'idéal de $\mathbb{Z}_2$ engendré par 6 est égal à l'idéal engendré par $\frac{1}{2}\cdot 6 = 3$. Du coup,

$$\mathbb{Z}_2/6\mathbb{Z}_2 = \mathbb{Z}_2/3\mathbb{Z}_2.$$

En appliquant encore la proposition précédente, on obtient

$$\mathbb{Z}_2/3\mathbb{Z}_2 = (\mathbb{Z}/3\mathbb{Z})_2.$$

Or, 2 est inversible dans $\mathbb{Z}/3\mathbb{Z}$, et donc

$$(\mathbb{Z}/3\mathbb{Z})_2 = \mathbb{Z}/3\mathbb{Z}.$$

Au final, l'anneau $(\mathbb{Z}/6Z)_2$ est donc canoniquement isomorphe à l'anneau $\mathbb{Z}/3\mathbb{Z}$!

10. Corps et idéaux maximaux

On a vu que, dans un anneau A non nul, on a l'inclusion $A^\times \subseteq A^\star$. Lorsqu'on a égalité on dira que A est un corps. Plus précisément :

DÉFINITION 10.1. Un anneau A est un *corps* si A n'est pas l'anneau nul et tout élément non nul de A est inversible.

EXEMPLE 10.2. (1) Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.

(2) L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

(3) Les anneaux $A[X]$ et $\mathbb{Z}$ ne sont pas de corps.

PROPOSITION 10.3. *Soit A un anneau. Alors A est un corps si A possède exactement 2 idéaux. Dans ce cas les deux idéaux sont (0) et A.*

DÉMONSTRATION. Supposons que A est un corps. Comme A et non nul, les idéaux (0) et A de A sont déjà deux idéaux distincts de A. Montrons qu'il n'y a pas d'autres idaux. Soit I un idéal de A. On montre que si $I \neq (0)$ alors $I = A$. En effet, si $I \neq (0)$, l'idéal I contient un élément non nul a. Comme A est un corps, a est inversible. Du coup $1 = a^{-1}a \in I$, et $b = b1 \in I$ pour tout $b \in A$, c-à-d $A \subseteq I$ et $I = A$.

Réciproquement, si A contient exactement deux idéaux, ce sont obligatoirement (0) et A et ils sont distincts. En effet, si $(0) = A$, A est l'anneau nul qui ne contient qu'un seul idéal. En particulier A est non nul. Montrons que tout élément non nul a de A est inversible. Considérons l'idéal (a) de A. Comme $(a) \neq (0)$, on a $(a) = A$. En particulier, il existe $b \in A$ tel que $ab = 1$, et a est inversible. □

Rappelons qu'un morphisme d'anneaux $f\colon A \to B$ est *nul* si $f(a) = 0$ quel que soit $a \in A$. Dans ce cas, $1 = f(1) = 0$ dans B, et B est l'anneau nul.

PROPOSITION 10.4. *Soit K un corps. Tout morphisme de K dans un anneau est soit nul, soit injectif.*

DÉMONSTRATION. Soit $f\colon K \to A$ un morphisme. Le noyau $\ker(f)$ est un idéal de K. D'après la proposition précédente, $\ker(f) = (0)$ ou $\ker(f) = A$. Dans le premier cas f est injectif. Dans le deuxième cas, f est nul. □

DÉFINITION 10.5. Soit A un anneau. Un idéal I de A est *maximal* s'il est maximal parmi les idéaux strictement contenus dans A, i.e., $I \neq A$ et si J est un idéal de A contenant I, alors $J = I$ ou $J = A$. On note $\mathrm{Max}(A)$ l'ensemble des idéaux maximaux de A.

PROPOSITION 10.6. *Soit A un anneau et I un idéal. Le quotient A/I est un corps si et seulement si l'idéal I est maximal.*

DÉMONSTRATION. On a vu qu'il y a correspondence bijective entre les idéaux de A/I est les idéaux de A contenant I. □

EXEMPLE 10.7. (1) On sait que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier. Du coup, les idéaux maximaux de $\mathbb{Z}$ sont les idéaux $p\mathbb{Z}$, où p est un nombre premier.

(2) Soit K un corps et $P \in K[X]$. On sait que $K[X]/(P)$ est un corps si et seulement si P est irréductible. Les idéaux maximaux de $K[X]$ sont les idéaux de la forme (P) avec P irréductible.

COROLLAIRE 10.8. *Soit A un anneau et $I \subseteq A$ un idéal. Alors I est maximal si et seulement si $I \neq A$ et pour tout $a \in A \setminus I$, il existe $b \in$ avec $ab - 1 \in I$.*

PROPOSITION 10.9. *Tout anneau non nul possède un idéal maximal.*

Rappelons le Lemme de Zorn. Soit $\mathcal{P}$ un ensemble partiellement ordonné. Une *chaîne* dans $\mathcal{P}$ est un sous-ensemble $\mathcal{C}$ de $\mathcal{P}$ qui est totalement ordonné par la relation d'ordre induite. Si $\mathcal{S}$ est un sous-ensemble de $\mathcal{P}$. Un *majorant* de $\mathcal{S}$ est un élément M de $\mathcal{P}$ tel que $x \leq M$ quel que soit $x \in \mathcal{S}$. Un *élément maximal* de $\mathcal{S}$ est un élément m de $\mathcal{S}$ tel que $x \geq m$ et $x \in \mathcal{S}$ implique $x = m$.

LEMME 10.10. *Soit $\mathcal{P}$ un ensemble partiellement ordonné. Supposons que toute chaîne de $\mathcal{P}$ possède un majorant. Alors $\mathcal{P}$ possède un maximum.*

PROPOSITION 10.11. *Soit A un anneau. Soit $\mathcal{C}$ une collection non vide d'idéaux de A telle que pour tout $I, J \in \mathcal{C}$ on a $I \subseteq J$ ou $J \subseteq I$. Alors $\bigcup \mathcal{C}$ est un idéal de A.*

La condition sur $\mathcal{C}$ revient à dire que $\mathcal{C}$ est une chaîne d'idéaux dans l'ensemble $\mathcal{P}(A)$ des parties de A, partiellement ordonnée par l'inclusion.

DÉMONSTRATION. On a $0 \in \bigcup \mathcal{C}$ car $\mathcal{C}$ est non vide, et $0 \in I$ pour un $I \in \mathcal{C}$.

Soit $x, y \in \bigcup \mathcal{C}$. Il existe $I \in \mathcal{C}$ et $J \in \mathcal{C}$ tels que $x \in I$ et $y \in J$. Comme $\mathcal{C}$ est une chaîne, on a $I \subseteq J$ ou $J \subseteq I$. Quitte à échanger x et y, on peut supposer que $I \subseteq J$. Du coup, $x, y \in J$ et $x + y \in J$ car J est un idéal. En particulier, $x + y \in \bigcup \mathcal{C}$.

Soit $x \in \bigcup \mathcal{C}$ et $a \in A$. Il existe donc $I \in \mathcal{C}$ tel que $x \in I$. Comme I est un idéal, $ax \in I$. En pariculier, $ax \in \bigcup \mathcal{C}$. □

Voici la démonstration de la proposition ci-dessus.

DÉMONSTRATION. Soit A un anneau non nul. Soit $\mathcal{P}$ l'ensemble des idéaux $I \neq A$ de A, partiellement ordonné par l'inclusion. Soit $\mathcal{C}$ une chaîne dans $\mathcal{P}$. Si $\mathcal{C} = \emptyset$, l'idéal (0) est un majorant de $\mathcal{C}$. Si $\mathcal{C}$ n'est pas vide, $\bigcup \mathcal{C}$ est un majorant de $\mathcal{C}$. D'apr'es Zorn, $\mathcal{P}$ possède un élément maximal, i.e. A possède un idéal maximal. □

COROLLAIRE 10.12. *Soit I un idéal de A avec $I \neq A$. Alors, il existe un idéal maximal m de A le contenant.*

COROLLAIRE 10.13. *Soit $a \in A$. Si $a \notin m$ pour tout idéal maximal m de A, alors a est inversible dans A.*

DÉMONSTRATION. Soit $I = Aa$ l'idéal de A engendré par a. Comme a n'appartient à aucun idéal maximal de A, $I = A$ d'après Proposition 10.12. Cela implique que $1 \in I = Aa$, i.e., il existe $b \in A$ tel que $ab = 1$. □

COROLLAIRE 10.14. *Chaque anneau A est la réunion disjointe de son groupe multiplicatif $A^\times$, d'une part, et l'union de tous ses idéaux maximaux, d'autre part, i.e.,*

$$A = A^\times \cup \bigcup_{m \in \mathrm{Max}(A)} m \quad \text{et} \quad A^\times \cap \Big(\bigcup_{m \in \mathrm{Max}(A)} m \Big) = \emptyset.$$

COROLLAIRE 10.15. *Soit A un anneau. Si A possède exactement un seul idéal maximal m, alors $A \setminus m = A^\times$. Réciproquement, si $A \setminus A^\times$ est un idéal de A, alors il est maximal et c'est le seul idéal maximal de A.*

DÉFINITION 10.16. Un anneau A possédant exactement un idéal maximal est un *anneau local*. Si A est un anneau local et m son idéal maximal, le quotient A/m est un corps, le *corps résiduel* de A, noté $\kappa(A)$.

EXEMPLE 10.17. Tout corps k est local et $\kappa(k) = k$.

11. Anneaux intègres et idéaux premiers

DÉFINITION 11.1. Soit A un anneau. Un élément $a \in A$ est *régulier* lorsque $ab = 0$ implique que $b = 0$. Un élément $a \in A$ est un *diviseur de zéro* si a n'est pas régulier, i.e., s'il existe $b \in A$, $b \neq 0$ et $ab = 0$.

EXEMPLE 11.2. (1) 1 et -1 sont réguliers dans tout anneau A.

(2) 0 est régulier dans un anneau A si et seulement si l'anneau A est nul.

(3) 2 n'est pas régulier dans $\mathbb{Z}/6\mathbb{Z}$. En effet $2 \cdot 3 = 0$, pourtant $3 \neq 0$ dans $\mathbb{Z}/6\mathbb{Z}$.

PROPOSITION 11.3. *Un élément inversible est régulier.*

DÉMONSTRATION. Exercice. □

Le réciproque n'est pas forcément vrai comme montre l'exemple de $2 \in \mathbb{Z}$. Sauf :

PROPOSITION 11.4. *Soit A un anneau fini. Alors tout élément régulier est inversible.*

DÉMONSTRATION. Exercice. □

On a vu que dans un anneau non nul, l'ensemble des éléments réguliers est contenu dans $A^\star$. Si on a égalité, on dira que A est intègre :

DÉFINITION 11.5. L'anneau A est *intègre* lorsque A est non nul et chaque élément non nul de A est régulier, autrement dit, A est non nul et n'a pas de diviseurs de zéro non nuls.

Voici quelques propriétés faciles à démontrer :

PROPOSITION 11.6. *(1) Tout sous-anneau d'un anneau intègre est intègre.*

(2) Tout corps est intègre.

(3) Tout anneau intègre fini est un corps.

(4) Tout sous-anneau d'un corps est intègre.

(5) Si A est intègre, $A[X]$ l'est.

(6) Si K un corps, $K[X_1, \ldots, X_n]$ est intègre.

DÉMONSTRATION. Exercice. □

EXEMPLE 11.7. (1) L'anneau des entiers $\mathbb{Z}$ est intègre.

(2) Les anneaux $\mathbb{Z}[X]$, $\mathbb{Z}[X, Y]$, ... sont intègres.

(3) Les anneaux $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ sont intègres.

(4) $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est nul ou premier.

(5) $K[X]/(P)$ est intègre si et seulement si P est nul ou irréductible.

Grace à la localisation, on peut généraliser la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$ et montrer que tout anneau intègre est isomorphe à un sous-anneau d'un corps, son corps de fractions. Plus généralement, tout anneau est isomorphe à un sous-anneau d'un anneau dans lequel tout élément régulier est inversible :

PROPOSITION 11.8. *Soit A un anneau et R l'ensemble de ces éléments réguliers. Alors R est une partie multiplicative de A. Le morphisme de localisation ι de A dans $R^{-1}A$ est injective. D'ailleurs, $a/s = b/t$ dans $R^{-1}A$ si et seulement si $ta = sb$. En particulier, $a/s = 0$ ssi $a = 0$.*

DÉMONSTRATION. Soit $a \in \ker(\iota)$. Il existe donc $s \in R$ tq $sa = 0$. Comme s est régulier, $a = 0$. Cela montre l'injectivité de ι. □

DÉFINITION 11.9. Soit A un anneau. Soit R la partie multiplicative des éléments réguliers A. *L'anneau total de fractions* de A est l'anneau $R^{-1}A$, noté par $\mathrm{Frac}(A)$. Si A est intègre, $\mathrm{Frac}(A)$ est un corps, appelé le *corps de fractions* de A.

EXEMPLE 11.10. (1) $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$.

(2) Soit K un corps. Le corps de fractions de $K[X]$ est le corps des fractions rationnelles, noté $K(X)$, i.e.,

$$K(X) = \{\frac{P}{Q} \mid P, Q \in K[X], Q \neq 0\}.$$

PROPOSITION 11.11. *Soit A un anneau et $I \subseteq A$ un idéal. L'anneau quotient A/I est intègre si et seulement si $A \setminus I$ est une partie multiplicative de A.*

DÉMONSTRATION. Supposons que A/I est intègre. Comme A/I est non nul, $1 \notin I$, c-à-d, $1 \in A \setminus I$. Soit $s, t \in A \setminus I$. On a $\bar{s}, \bar{t} \neq 0$ dans A/I. Comme A/I intègre, $\bar{s}\bar{t} \neq 0$ dans A/I, et $st \notin I$, i.e., $st \in A \setminus I$.

Réciproquement, supposons que $A \setminus I$ est multiplicative. Dans ce cas $1 \notin I$, i.e., $I \neq A$ et $A/I \neq 0$. De plus, si $\bar{a} \neq 0$ dans A/I, supposons $\bar{a}\bar{b} = 0$, i.e., $ab \in I$ comme $A \setminus I$ est multiplicative et $a \notin I$, on doit avoir $b \in I$, c-à-d $\bar{b} = 0$ dans A/I. □

DÉFINITION 11.12. Soit A un anneau. Un idéal I de A est *premier* si A/I est intègre. Plus explicitement, I est premier si $I \neq A$ et $a, b \notin I$ implique que $ab \notin I$ quels que soient $a, b \in A$. On note $\mathrm{Spec}(A)$ l'ensemble de tous les idéaux premiers de A. C'est le *spectre* de A. Par extension, on appelle le *spectre maximal* de A l'ensemble $\mathrm{Max}(A)$ des idéaux maximaux de A.

EXEMPLE 11.13. Les idéaux premiers de $\mathbb{Z}$ sont (0) et $p\mathbb{Z}$. Les idéaux premiers de $K[X]$ sont (0) et (P).

PROPOSITION 11.14. *Tout idéal maximal est premier.*

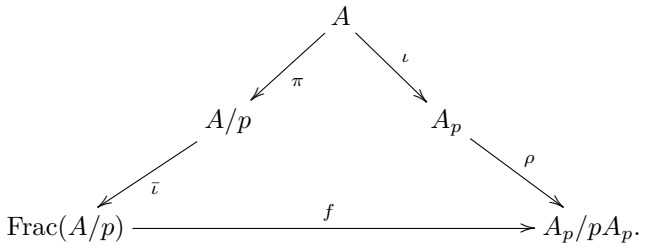
Le réciproque est faux comme montre l'exemple de l'idéal (0) dans $\mathbb{Z}$. Par contre, on peut rendre maximal tout idéal premier grâce à la localisation :

DÉFINITION 11.15. Soit A un anneau et p un idéal premier de A. D'après Proposition 11.11, le sous-ensemble $S = A\backslash p$ de A est une partie multiplicative de A. La localisation de A par $A\backslash p$ est la *localisation de A en p*, et est notée par A_p. On note pA_p l'idéal $S^{-1}p$ engendré par p dans A_p.

PROPOSITION 11.16. *Soit p un idéal premier de A. Alors, l'idéal pA_p est un idéal maximal de A_p. En fait, pA_p est le seul idéal maximal de A_p. En particulier, A_p est un anneau local. De plus, il y a un unique isomorphisme*

$$f\colon \mathrm{Frac}(A/p) \to A_p/pA_p$$

du corps des fractions de A/p sur le corps résiduel $\kappa(A_p)$ de l'anneau local A_p faisant commuter le diagramme



En fait, on a

$$f(\tfrac{\bar{a}}{\bar{b}}) = \overline{\tfrac{a}{b}},$$

ou encore

$$f^{-1}(\overline{\tfrac{a}{b}}) = \tfrac{\bar{a}}{\bar{b}}.$$

DÉMONSTRATION. D'abord, l'idéal pA_p n'est pas égal à A_p. En effet, si 1 appartenait à pA_p, il existerait $x \in p$ et $s, t \notin p$ tel que $tx = ts$. Or $tx \in p$, d'où $ts \in p$. Comme p est premier, on a $s \in p$ ou bien $t \in p$. Contradiction. D'où $pA_p \neq A_p$. En particulier $pA_p \subseteq A_p \setminus A_p^\times$.

On montre que A_p est un anneau local et que pA_p est un son idéal maximal en montrant que $pA_p = A_p \setminus A_p^\times$ (cf. Corollaire 10.16). On a déjà vu l'inclusion $pA_p \subseteq A_p \setminus A_p^\times$. Afin de montrer l'égalité des deux sous-ensemble de A_p, on montre quu tout élément $\frac{a}{s}$ de A_p n'appartenant pas à pA_p n'appartient pas à $A_p \setminus A_p^\times$, c-à-d, est inversible. Comme $\frac{a}{s} \notin pA_p$, on a nécessairement $a \notin p$. D'où $\frac{s}{a} \in A_p$, et bien-sûr $\frac{a}{s}\frac{s}{a} = 1$. Par conséquent $\frac{a}{s}$ est inversible. Cela montre bien que $pA_p = A_p \setminus A_p^\times$.

Pour montrer l'assertion sur le corps résiduel de A_p, soit S la partie multiplicative $A\backslash p$ de A. Soit $\overline{S}$ l'image de S dans le quotient A/p. En fait, $\overline{S} = (A/p)\backslash\{0\}$ si bien que

$$\overline{S}^{-1}(A/p) = \mathrm{Frac}(A/p).$$

On applique Proposition 9.12. Soit

$$\iota\colon A \to A_p$$

le morphisme de localisation de A par rapport à S. Soit

$$\rho\colon A_p \to A_p/pA_p$$

le morphisme de passage au quotient. Soit

$$\lambda\colon A/p \to A_p/pA_p$$

le morphisme induit par $\rho \circ \iota$, i.e., $\lambda \circ \pi = \rho \circ \iota$, où

$$\pi\colon A \to A/p$$

est le morphisme de passage au quotient. D'après Proposition 9.12, λ est un morphisme de localisation de A/p par $\overline{S}$. Du coup, Il existe un unique isomorphisme

$$f\colon \mathrm{Frac}(A/p) \to A_p/pA_p$$

tel que $f \circ \bar{\iota} = \lambda$, où

$$\bar{\iota}\colon A/p \to \mathrm{Frac}(A/p)$$

est le morphisme de localisation de A/p par $\overline{S}$. En particulier,

$$f \circ \bar{\iota} \circ \pi = \lambda \circ \pi = \rho \circ \iota.$$

On a donc bien

$$f(\tfrac{\bar{a}}{1}) = \overline{\tfrac{a}{1}}.$$

Du coup

$$f(\tfrac{\bar{a}}{\bar{b}}) = f(\tfrac{\bar{a}}{1} \cdot (\tfrac{\bar{b}}{1})^{-1}) = f(\tfrac{\bar{a}}{1}) \cdot f(\tfrac{\bar{b}}{1})^{-1}) = \overline{\tfrac{a}{1}} \cdot (\overline{\tfrac{b}{1}})^{-1} = \overline{\tfrac{a}{1}} \cdot (\overline{\tfrac{1}{b}}) = \overline{\tfrac{a}{b}}.$$

□

EXEMPLE 11.17. (1) Soit p un nombre premier et $(p) = p\mathbb{Z}$ l'idéal de $\mathbb{Z}$ engendré par p. C'est un idéal maximal de $\mathbb{Z}$, en particulier premier. Alors

$$\mathbb{Z}_{(p)} = \{\tfrac{a}{b} \mid a, b \in \mathbb{Z},\ p \not| b\}.$$

est un anneau local. C'est un sous-anneau de $\mathbb{Q}$. Notons que $\mathbb{Z}_p \cap \mathbb{Z}_{(p)} = \mathbb{Z}$. On a

$$Z_{(p)}/p\mathbb{Z}_{(p)} = \mathbb{Z}/p\mathbb{Z}.$$

(2) Soit K un corps et $a \in K$. L'idéal $(X - a)$ est un idéal maximal de $K[X]$; en particulier premier. Alors

$$K[X]_{(X-a)} = \{\tfrac{P}{Q} \mid P, Q \in K[X],\ Q(a) \neq 0\}$$

C'est donc le sous-anneau des fractions rationnelles définies en a. Cela explique le nom "anneau local". Notons que $K[X]_{X-a} \cap K[X]_{(X-a)} = K[X]$. On a

$$K[X]_{(X-a)}/(X-a)K[X]_{(X-a)} = K[X]/(X-a) = K.$$

PROPOSITION 11.18. *Soit $f\colon A \to B$ un morphisme d'anneaux. Si p est un idéal premier de B, alors $f^{-1}(p)$ est un idéal premier de A.*

DÉMONSTRATION. Soit $\pi\colon B \to B/p$ l'application quotient. On a $\ker(\pi \circ f) = f^{-1}(p)$. Du coup, $f \circ \pi$ induit un morphisme $\bar{f}\colon A/f^{-1}(p) \to B/p$. On vérifie aisément que le noyau de $\bar{f}$ est (0). Le morphisme $\bar{f}$ est donc injectif et $A/f^{-1}(p)$ est isomorphe à un sous-anneau de B/p. Comme B/p est intègre, ce sous-anneau l'est, et donc A/p aussi. Comme A/p est int'egre, p est premier. □

L'énoncé correspondant est faux pour les idéaux maximaux, comme montre l'exemple de $m = (0)$ dans $\mathbb{Q}$ et f l'inclusion de $\mathbb{Z}$ dans $\mathbb{Q}$. Par contre, comme tout idéal maximal est premier, on a du moins $f^{-1}(m)$ est premier pour tout idéal maximal m.

12. Anneaux noethériens

DÉFINITION 12.1. Un anneau A est *noethérien* lorsque tout idéal de A est de type fini.

EXEMPLE 12.2. Tout corps est noethérien. L'anneau $\mathbb{Z}$ est noethérien. Plus généralement, tout anneau principal est noethérien. En particulier, $K[X]$ est noethérien pour tout corps K. Tout anneau fini est noethérien.

Malheureusement, tout anneau n'est pas noethérien.

EXEMPLE 12.3. Soit $A = \mathbb{Z}[X_1, X_2, X_3, \ldots]$ l'anneau de polynômes en les indéterminées $X_1, X_2, X_3, \ldots$ à coefficients entiers. L'idéal $I = (X_1, X_2, X_3, \ldots)$ de A n'est pas de type fini. En particulier, l'anneau $\mathbb{Z}[X_1, X_2, X_3, \ldots]$ n'est pas noethérien. Pour le montrer on aura besoin du fait suivant.

Soit $n \in \mathbb{N}$. Soit A_n le sous-anneau $\mathbb{Z}[X_1, \ldots, X_n]$ de A et $I_n \subseteq A_n$ l'idéal de A_n engendré par $X_1, \ldots, X_n$. L'intersection $I \cap A_n$ est égale à l'idéal I_n de A_n. Effectivement, L'inclusion $I_n \subseteq I \cap A_n$ est évidente car $I_n \subseteq I$ et $I_n \subseteq A_n$. Pour montrer l'inclusion $I_n \supseteq I \cap A_n$, soit $P \in I \cap A_n$. Comme P appartient à I, il existe $m \in \mathbb{N}$ et $P_1, \ldots, P_m \in A$ tels que

$$P = \sum_{i=1}^{m} P_i X_i.$$

Quitte à augmenter m, on peut supposer que chaque P_i est un polynôme en $X_1, \ldots, X_i$ à coefficients entiers. Comme P appartient à A_n, on a $P_i = 0$ pour tout $i > n$. Comme $P_i \in A_n$ quel que soit $i \leq n$, on a $P \in I_n$. Cela montre que $I \cap A_n = I_n$.

Maintenant on montre que l'idéal I de A n'est pas de type fini. Supposons qu'il existe $P_1, \ldots, P_n \in A$ tels que

$$I = (P_1, \ldots, P_n).$$

Comme A est la réunion de ses sous-anneaux A_k, $k \in \mathbb{N}$. Il existe $k \in \mathbb{N}$ tel que $P_i \in A_k$ quel que soit $i = 1, \ldots, n$. Soit $f\colon A \to \mathbb{Z}$ le morphisme d'anneaux tel que $f(X_{k+1}) = 1$ et $f(X_i) = 0$ quel que soit $i \neq k$. D'après ce qui précède, chaque P_i appartient à l'idéal I_k de A_k engendré par $X_1, \ldots, X_k$. D'où, $P_i \in \ker(f)$ quel que soit i. Comme $\ker(f)$ est un idéal, l'idéal de A engendré par les P_i est contenu dans $\ker(f)$. D'où $I \subseteq \ker(f)$. Mais $X_{k+1} \in I$ et $f(X_{k+1}) = 1 \neq 0$. Contradiction.

PROPOSITION 12.4. *Soit $f\colon A \to B$ un morphisme d'anneaux surjectif. Si A est noethérien, alors B l'est.*

DÉMONSTRATION. Exercice. □

COROLLAIRE 12.5. *Soit A un anneau et I un idéal de A. Si A est noethérien, A/I l'est.*

PROPOSITION 12.6. *Soit A un anneau et $S \subseteq A$ une partie multiplicative de A. Si A est noethérien, alors $S^{-1}A$ l'est.*

DÉMONSTRATION. Exercice. □

On voit souvent la condition équivalente suivante comme définition d'un anneau noethérien :

PROPOSITION 12.7. *Soit A un anneau. Alors, A est noethérien si et seulement si chaque chaîne croissante d'idéaux de A*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

est stationnaire, c-à-d, il existe $N \in \mathbb{N}$ tel que $I_{N+k} = I_N$ quel que soit $k \in \mathbb{N}$.

DÉMONSTRATION. Supposons que A est noethérien. Soit $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ une chaîne croissante d'idéaux de A. L'union $I = \bigcup I_i$ est un idéal de A. Comme A est noethérien, il existe $a_1, \ldots, a_n \in I$ tels que $I = (a_1, \ldots, a_n)$. Puisque I est la réunion des idéaux I_i, $a_j \in I_{i_j}$ pour certain $i_j \in \mathbb{N}$, $j = 1, \ldots, n$. Soit $N = \max\{i_1, \ldots, i_n\}$. Comme $I_{i_j} \subseteq I_N$, on a $a_j \in I_N$ pour $j = 1, \ldots, n$. D'où $I_N \supseteq (a_1, \ldots, a_n) = I$ ce qui implique que la chaîne d'idéaux I_i est stationnaire à partir du rang N.

Supposons que A n'est pas noethérien, et soit I un idéal de A qui n'est pas de type fini. On peut choisir $a_1, a_2, a_3, \ldots \in I$ tels que $a_{n+1} \notin (a_1, \ldots, a_n)$. La chaîne croissante d'idéaux

$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \cdots$$

n'est alors pas stationnaire à partir d'un certain rang $N \in \mathbb{N}$. □

THÉORÈME DE LA BASE DE HILBERT. *Soit A un anneau noethérien. Alors, l'anneau de polynômes $A[X]$ est noethérien.*

DÉMONSTRATION. Par l'absurde : supposons I est un idéal de $A[X]$ qui n'est pas de type fini. Evidemment, $I \neq \{0\}$. On va construire, par récurrence, des éléments $P_1, P_2, P_3, \ldots$ de I. Soit $P_1 \in I\backslash\{0\}$ un polynôme de plus bas degré. Comme I n'est pas de type fini, $(P_1) \subsetneq I$. Soit $P_2 \in I\backslash(P_1)$ un polynôme de plus bas degré. Alors, $(P_1, P_2) \subsetneq I$. On continue ainsi et on construit une suite de polynômes $P_1, P_2, P_3, \ldots$ dans I telle que P_{n+1} appartient à $I\backslash(P_1, \ldots, P_n)$ et il est de plus bas degré parmi tous les polynômes de $I\backslash(P_1, \ldots, P_n)$.

Soit d_i le degré du polynôme P_i et $a_i \in A$ le coefficient dominant du polynôme P_i, $i = 1, 2, 3, \ldots$. Par construction, $d_{i+1} \geq d_i$ quel que soit $i \in \mathbb{N}$. Comme A est noethérien, la chaîne croissante d'idéaux de A

$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \cdots$$

est stationnaire à partir d'un certain rang n. En particulier, $a_{n+1} \in (a_1, \ldots, a_n)$, c-à-d, il existe $b_i \in A$ tels que $a_{n+1} = \sum_{i=1}^{n} b_i a_i$. On a alors

$$P_{n+1} - \sum_{i=1}^{n} b_i X^{d_{n+1}-d_i} P_i \ \in \ I\backslash(P_1, \ldots, P_n)$$

dont le degré est strictement inférieur à celui de P_{n+1}. Contradiction. □

COROLLAIRE 12.8. *Soit A un anneau noethérien. Alors, l'anneau de polynômes $A[X_1, \ldots, X_n]$ est noethérien. En particulier, les anneaux $\mathbb{Z}[X_1, \ldots, X_n]$ et $K[X_1, \ldots, X_n]$ sont noethériens. Et plus généralement des localisations et des quotients de ces anneaux sont noethériens.*

13. Anneaux factoriels

DÉFINITION 13.1. Soit A un anneau intègre et $a, b \in A$. On dit que a *divise* b, ou a est un *diviseur* de b s'il existe $c \in A$ tel que $ac = b$. On le note par $a|b$. Deux éléments $a, b \in A$ sont *associés* s'il existe $u \in A^\star$ tel que $a = ub$. Un élément $p \in A$, $p \neq 0$ et $p \notin A^\star$, est *premier* si $p|ab$ implique que $p|a$ ou $p|b$, quels que soient $a, b \in A$. L'élément $p \in A$, $p \neq 0$ et $p \notin A^\star$, est *irréductible* lorsque tout diviseur de p est soit inversible, soit associé à p.

Evidemment, $p \in A$, $p \neq 0$ est premier si et seulement si l'idéal (p) engendré par p est premier.

Soit A un sous-anneau de B et soient $a, b \in A$. Evidemment, si a divise b en tant qu'éléments de A, alors a divise b en tant qu'éléments de B. Par contre, la réciproque n'est pas valable en général : 2 divise 3 dans $\mathbb{Q}$, mais 2 ne divise pas 3 dans $\mathbb{Z}$. De même, si a et b sont associés dans A, ils le sont aussi dans B. Mais la réciproque n'est pas vraie : 2 et 3 sont associés dans $\mathbb{Q}$, mais ils ne le sont pas dans $\mathbb{Z}$.

Pour les éléments premiers ou irréductibles on n'a pas d'implications dans aucun sens : $X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$, mais il ne l'est pas dans son corps de fractions $\mathbb{Q}(X)$, et, le polynôme $2X^2 - 4$ est irréductible dans $\mathbb{Q}[X]$, mais il ne l'est pas dans le sous-anneau $\mathbb{Z}[X]$ de $\mathbb{Q}[X]$.

PROPOSITION 13.2. *Soit A un anneau intègre. Soient $a, b \in A$. Alors, a et b sont associés si et seulement si a et b se divisent.*

DÉMONSTRATION. Lorsque a et b sont associés, il existe $u \in A^\star$ tel que $a = ub$. En particulier a divise b. Et comme $b = u^{-1}a$, b divise a.

Pour montrer l'autre implication, on peut supposer que a est non nul. Lorsque a et b se divisent, il existe $c, d \in A$ tels que $ac = b$ et $bd = a$. Alors, $acd = bd = a$. D'où $a(cd - 1) = 0$. Comme $a \neq 0$, $cd = 1$, i.e., c et inversible et a et b sont alors associés. □

PROPOSITION 13.3. *Soit A un anneau intègre. Alors, tout élément premier est irréductible.*

DÉMONSTRATION. Soit $p \in A$ premier. Soit a un diviseur de p. Alors, il existe $b \in A$ tel que $ab = p$. En particulier, $p|ab$. Or p est premier, donc $p|a$ ou $p|b$. Si $p|a$, p et a sont associés. Sinon, il existe $c \in A$ tel que $cp = b$. D'où $acp = ab = p$ et $ac = 1$, c-à-d, a est inversible. □

La réciproque à la proposition précédente n'est pas vraie en général :

EXEMPLE 13.4. Soit A le sous-anneau $\mathbb{Z}[i\sqrt{5}]$ de $\mathbb{C}$. L'élément $2 \in A$ est irréductible. En effet, si $a + ib\sqrt{5}$, $a, b \in \mathbb{Z}$, divise 2 dans A, sa norme $a^2 + 5b^2$ divise 4 dans $\mathbb{Z}$. D'où $b = 0$ et $a = \pm 1, \pm 2$. Par conséquent, $2 \in A$ est irréductible. Cependant, 2 divise $6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ dans A, mais ne divise aucun des deux facteurs, c-à-d, $2 \in \mathbb{Z}[i\sqrt{5}]$ n'est pas premier.

DÉFINITION 13.5. Soit A un anneau intègre. Un *système de représentants des irréductibles* de A est un sous-ensemble $\mathcal{P}$ d'irréductibles de A tel que pour tout $p \in A$ irréductible il existe un et un seul $q \in P$ qui soit associé à p.

EXEMPLE 13.6.
(1) Le sous-ensemble de $\mathbb{Z}$ des premiers positifs est un système de représentants des premiers de $\mathbb{Z}$.
(2) Le sous-ensemble de $K[X]$ des polynômes irréductibles unitairs en est un de $K[X]$, où K est un corps.
(3) L'ensemble vide est un systéme de représentants des irréductibles d'un corps.

DÉFINITION 13.7. Soit A un anneau intègre. Soit $\mathcal{P}$ un systéme de représentants des irréductibles de A. On appelle A *factoriel* lorsque tout élément $a \in A$, $a \neq 0$, s'écrive de façon unique comme

$$a = u \cdot \prod_{p \in \mathcal{P}} p^{v_p},$$

où $u = u(a) \in A^\star$ et les $v_p = v_p(a) \in \mathbb{N}$ sont presque tous nuls. Lorsque A est factoriel, on appelle $v_p(a)$ la *valuation p-adique* de a, et $u(a)$ *l'inversible* de a.

EXEMPLE 13.8.
(1) L'anneau $\mathbb{Z}$ est factoriel (voir Corollaire 13.13).
(2) L'anneau $K[X]$, K un corps, est factoriel (voir Corollaire 13.14).
(3) Un corps est factoriel.

Soit A un anneau factoriel. On fixe un système $\mathcal{P}$ de représentants des irréductibles de A. Soient $a, b \in A$ non nuls. D'après la définition d'un anneau factoriel,

$$a = u(a) \cdot \prod_{p \in \mathcal{P}} p^{v_p(a)} \quad \text{et} \quad b = u(b) \cdot \prod_{p \in \mathcal{P}} p^{v_p(b)}.$$

On a que a divise b dans A si et seulement si $v_p(a) \leq v_p(b)$ quel que soit $p \in \mathcal{P}$.

Il en résulte que l'on peut définir le pgcd et le ppcm dans un anneau factoriel. Soient $a_1, \ldots, a_n \in A$ non nuls. Définissons

$$\operatorname{pgcd}(a_1, \ldots, a_n) = \prod_{p \in P} p^{\inf\{v_p(a_i) \,|\, i=1,\ldots,n\}}$$

et

$$\operatorname{ppcm}(a_1, \ldots, a_n) = \prod_{p \in P} p^{\max\{v_p(a_i) \,|\, i=1,\ldots,n\}}.$$

Observez que le pgcd et le ppcm dépendent du choix du système de représentants des irréductibles $\mathcal{P}$.

PROPOSITION 13.9. *Soit A un anneau factoriel et $p \in A$. Alors, p est premier si et seulement si p est irréductible.*

DÉMONSTRATION. D'après Proposition 13.3, p est irréductible lorsque p est premier. Supposons donc p irréductible. Soient $a, b \in A$ tels que $p|ab$. On a alors $v_p(ab) \geq 1$. Comme $v_p(ab) = v_p(a) + v_p(b)$, on a $v_p(a) \geq 1$ ou bien $v_p(b) \geq 1$, i.e., p divise a ou b. □

PROPOSITION 13.10. *Soit A un anneau intègre. Alors A est factoriel si*

(1) tout élément irréductible est premier, et

(2) toute chaîne croissante d'idéaux principaux est stationnaire.

DÉMONSTRATION. Soit $\mathcal{P}$ un système de représentants des irréductibles de A. Montrons que tout élément $a \in A$, $a \neq 0$, s'écrit comme $u \prod p^{e_p}$. Soit $S \subseteq A$ l'ensemble des élément de A ne s'écrivant pas sous cette forme-là. Supposons que S soit non vide. Considérer l'ensemble $\mathcal{I} = \{As \,|\, s \in S\}$ d'idéaux de A. L'ensemble $\mathcal{I}$ est ordonné par l'inclusion. D'après 2, toute chaîne dans $\mathcal{I}$ a une borne supérieure. D'après le Lemme de Zorn, $\mathcal{I}$ a un élément maximal, c-à-d, il existe $s \in S$ tel que As soit maximal dans $\mathcal{I}$. Comme s appartient à S, s n'est pas irréductible, i.e., s s'écrit comme $s_1 s_2$ où ni s_1 ni s_2 n'est inversible. On a alors $As \subsetneq As_1$ et $As \subsetneq As_2$. Par conséquent, $s_1, s_2 \notin S$, i.e.,

$$s_1 = u_1 \prod p^{e_p} \text{ et } s_2 = u_2 \prod p^{f_p},$$

et donc $s = u_1 u_2 \prod p^{e_p + f_p}$. Contradiction. Cela montre l'existence de l'écriture $a = u \prod p^{e_p}$. Pour en montrer l'unicité on utilise le fait que tout élément $p \in \mathcal{P}$ soit premier. □

COROLLAIRE 13.11. *Un anneau noetherien A est factoriel lorsque tout élément irréductible de A est premier.* □

COROLLAIRE 13.12. *Un anneau principal est factoriel.*

DÉMONSTRATION. Soit A un anneau principal. Il suffit de montrer que tout élément irréductible de A est premier. Soit $p \in A$ alors irréductible, et soient $a, b \in A$ tels que p divise ab. Supposons que p ne divise pas a. Considérer l'idéal (a, p) de A. Comme A est principal, il existe $c \in A$ engendrant (a, p). En particulier, c divise p. Or, p est irréductible. D'où, c est soit associé à p, soit c est inversible. Dans le premier cas, p divise a ce qui contredirait le fait que p ne divise pas a. Par conséquent, c est inversible. Du coup, $(a, p) = A$, i.e., il existe $x, y \in A$ tels que $xa + yp = 1$. On a alors, $xab + ypb = b$. Comme p divise ab, p divise xab et ypb, et donc aussi leur somme qui est égale à b. □

COROLLAIRE 13.13. *L'anneau des entiers $\mathbb{Z}$ est factoriel.* □

COROLLAIRE 13.14. *L'anneau $K[X]$ des polynômes à coefficients dans un corps K est factoriel.* □

Le résultat principal de ce paragraphe c'est que l'anneau de polynômes $A[X]$ sur A est factoriel lorsque A l'est. Avant de montrer ce résultat, il nous faut quelques définitions.

DÉFINITION 13.15. Soit A un anneau factoriel. Soit $P \in A[X]$. Alors, le *contenu* de P, noté par $\operatorname{cont}(P)$, est le pgcd de tous ses coefficients.

LEMME 13.16. *Soit A un anneau factoriel, $a \in A$ et $P \in A[X]$. Alors, $u(a) \cdot \mathrm{cont}(aP) = a \cdot \mathrm{cont}(P)$.*

DÉMONSTRATION. Soient a_i, $i = 0, \ldots, n$, les coefficients de P. Alors, $u(a) \cdot \mathrm{cont}(aP) = u(a) \cdot \mathrm{pgcd}(aa_1, \ldots, aa_n) = a \cdot \mathrm{pgcd}(a_1, \ldots, a_n) = a \cdot \mathrm{cont}(P)$. □

Lemme 13.16 nous permet d'étendre la définition du contenu aux polynômes à coefficients dans le corps de fractions K d'un anneau factoriel A : Soit $P \in K[X]$. Soit $a \in A$, $a \neq 0$ tel que $aP \in A[X]$. Définissons le contenue $\mathrm{cont}(P) \in K$ de P par

$$\mathrm{cont}(P) = \frac{u(a) \cdot \mathrm{cont}(aP)}{a}.$$

On vérifie facilement que cette définition ne dépend pas de a en utilisant Lemme 13.16.

LEMME 13.17. *Soit A un anneau factoriel, K son corps de fractions et $P \in K[X]$. Alors, $P \in A[X]$ si et seulement si $\mathrm{cont}(P) \in A$.*

DÉMONSTRATION. Evidemment, $P \in A[X]$ implique que $\mathrm{cont}(P) \in A$. Réciproquement, supposons que $\mathrm{cont}(P) \in A$. Montrons que $P \in A[X]$. Soit $P = a_n X^n + \cdots + a_1 X + a_0$, $a_i \in K$. Soit $a \in A$ non nul tel que $aP \in A[X]$. Soit $b_i = aa_i$, $i = 0, \ldots, n$. Alors, le contenu de P est par définition $u(a)\mathrm{pgcd}(b_0, \ldots, b_n)/a$. Lorsque ce contenu appartient à A, on a que a divise $\mathrm{pgcd}(b_0, \ldots, b_n)$, donc a divise b_i, quel que soit i. Par conséquent, $a_i = b_i/a$ appartient à A, c-à-d, P est dans $A[X]$. □

LEMME DE GAUSS. *Soit A un anneau factoriel et K son corps de fractions. Soient $P, Q \in K[X]$. Alors,*

$$\mathrm{cont}(PQ) = \mathrm{cont}(P) \cdot \mathrm{cont}(Q).$$

DÉMONSTRATION. Il suffit de montrer l'assertion pour $P, Q \in A[X]$. De plus, on peut supposer P et Q non nuls. Comme $\mathrm{cont}(P)$ divise tous les coefficients de P, il existe $P' \in A[X]$ tel que $\mathrm{cont}(P) \cdot P' = P$. De même, il existe $Q' \in A[X]$ tel que $\mathrm{cont}(Q) \cdot Q' = Q$. Evidemment, $\mathrm{cont}(P') = \mathrm{cont}(Q') = 1$. On va montrer que $\mathrm{cont}(P'Q') = 1$ également. Soit $P' = a_n X^n + \cdots + a_0$ et $Q' = b_m X^m + \cdots + b_0$. Alors $P'Q' = c_{n+m} X^{n+m} + \cdots + c_0$, où

$$c_k = \sum_{i+j=k} a_i b_j.$$

Supposons qu'il existe p premier divisant tous les coefficients c_k de $P'Q'$. Comme P' et Q' ont contenu égal à 1, il existe i_0 et j_0 tels que $p \not| a_{i_0}$ et $p \not| b_{j_0}$. De plus, on peut prendre i_0 et j_0 minimaux sous cette condition. Soit $k = i_0 + j_0$. Comme p divise a_i pour $i < i_0$ et p divise b_j pour $j < j_0$, p divise $a_i b_j$ pour $i + j = k$, $(i, j) \neq (i_0, j_0)$. Mais p divise aussi c_k, donc p divise $a_{i_0} b_{j_0}$. Or p est premier, donc p divise a_{i_0} ou p divise b_{j_0}. Contradiction. On a alors $\mathrm{cont}(P'Q') = 1$ et

$$\begin{aligned} \mathrm{cont}(PQ) &= \mathrm{cont}(\mathrm{cont}(P) \cdot P' \cdot \mathrm{cont}(Q) \cdot Q') = \\ &= \mathrm{cont}(P) \cdot \mathrm{cont}(Q) \cdot \mathrm{cont}(P'Q') = \\ &= \mathrm{cont}(P) \cdot \mathrm{cont}(Q) \end{aligned}$$

d'après Lemme 13.16. □

COROLLAIRE 13.18. *Soit A un anneau factoriel et K son corps de fractions. Soient $P, Q \in A[X]$. Alors Q divise P dans $A[X]$ lorsque Q divise P dans $K[X]$ et $\mathrm{cont}(Q)$ divise $\mathrm{cont}(P)$ dans A.* □

PROPOSITION 13.19. *Soit A un anneau factoriel et K son corps de fractions. Soit $P \in A[X]$ de degré strictement positif. Si P est irréductible dans $A[X]$ alors P est irréductible dans $K[X]$.*

DÉMONSTRATION. Comme P est de degré strictment positif, P n'est ni nul ni inversible dans $K[X]$. Soit $Q \in K[X]$ un diviseur de P dans $K[X]$. On veut montrer que Q est soit inversible dans $K[X]$, soit associé à P dans $K[X]$. On peut alors supposer Q de contenu 1. En particulier, $Q \in A[X]$, d'après Lemme 13.17. D'après Corollaire 13.18, Q divise P dans $A[X]$. Or P est irréductible dans $A[X]$, donc Q est soit inversible dans $A[X]$, soit associé à P dans $A[X]$. Dans le premier cas, Q est nécessairement inversible dans $K[X]$. Dans le deuxième cas, Q est forcément associé à P dans $K[X]$. □

THÉORÈME 13.20. *Soit A un anneau factoriel. Alors, l'anneau des polynômes $A[X]$ est factoriel.*

DÉMONSTRATION. Soit $P \in A[X]$ irréductible. Montrons qu'il est premier. Soient $F, G \in A[X]$ tels que P divise FG. Distinguer deux cas : le cas $\deg(P) = 0$ et le cas $\deg(P) \neq 0$.

Lorsque $\deg(P) = 0$, $P \in A$, P est irréductible dans A, et P divise $\mathrm{cont}(FG) = \mathrm{cont}(F)\mathrm{cont}(G)$. Or A est factoriel, donc P est même premier dans A. Alors, P divise $\mathrm{cont}(F)$ ou bien P divise $\mathrm{cont}(G)$. En particulier, P divise F ou P divise G.

Lorsque $\deg(P) \neq 0$, P est irréductible dans $K[X]$, d'après Proposition 13.19. Comme $K[X]$ est factoriel, P est premier dans $K[X]$. Par conséquent, P divise F ou P divise G dans $K[X]$. Or P est irréductible dans A et $\deg(P) \neq 0$, donc le contenu de P est égal à 1. D'après Corollaire 13.18, P divise alors F ou P divise G dans $A[X]$.

Cela montre qu'un élément irréductible de $A[X]$ est forcément premier. Ensuite, montrons que toute chaîne croissante d'idéaux principaux de $A[X]$ est stationnaire.

Soient $P_i \in A[X]$ tels que $A[X]P_i \subseteq A[X]P_{i+1}$. On en déduit deux chaînes d'idéaux principaux croissantes : la chaîne

$$K[X]P_0 \subseteq K[X]P_1 \subseteq K[X]P_2 \subseteq \cdots$$

dans $K[X]$, et la chaîne

$$A\mathrm{cont}(P_0) \subseteq A\mathrm{cont}(P_1) \subseteq A\mathrm{cont}(P_2) \subseteq \cdots$$

dans A. Or, les anneaux A et $K[X]$ sont factoriels donc ces deux suites sont stationnaires. Par conséquent, il existe un entier $n \in \mathbb{N}$ tel que

$$K[X]P_{n+k} = K[X]P_n \quad \text{et} \quad A\mathrm{cont}(P_{n+k}) = A\mathrm{cont}(P_n)$$

quel que soit $k \in \mathbb{N}$. Montrons alors que $A[X]P_{n+k} = A[X]P_n$ quel que soit $k \in \mathbb{N}$.

Soit $Q \in A[X]$ dans $A[X]P_{n+k}$. En particulier, $Q \in K[X]P_{n+k}$ et $\mathrm{cont}(Q) \in A\mathrm{cont}(P_{n+k})$. Comme $K[X]P_{n+k} = K[X]P_n$ et $A\mathrm{cont}(P_{n+k}) = A\mathrm{cont}(P_n)$, $Q \in K[X]P_n$ et $\mathrm{cont}(Q) \in A\mathrm{cont}(P_n)$. Autrement dit, P_n divise Q dans $K[X]$ et $\mathrm{cont}(P_n)$ divise $\mathrm{cont}(Q)$ dans A. D'après Corollaire 13.18, P_n divise Q dans $A[X]$, i.e, $Q \in A[X]P_n$. □

COROLLAIRE 13.21. *Soit A un anneau factoriel. Alors l'anneau de polynômes $A[X_1, \ldots, X_n]$ est factoriel. En particulier, $\mathbb{Z}[X_1, \ldots, X_n]$ et $K[X_1, \ldots, X_n]$, K un corps, sont factoriels.* □

EXEMPLE 13.22 (Paires de dés exotiques). Si on lance deux dés, la somme des valeurs des faces supérieures des dés est un entier entre $1 + 1 = 2$ et $6 + 6 = 12$. La probabilité d'obtenir une certaine somme s dépend bien-sûr du nombre de façon d'écrire s comme somme $i + j$ d'entiers $i, j \in \{1, \ldots, 6\}$. C'est donc le coefficient de X^s dans le produit des polynômes

$$P = (X^6 + X^5 + X^4 + X^3 + X^2 + X)(X^6 + X^5 + X^4 + X^3 + X^2 + X) = \\ X^{12} + 2X^{11} + 3X^{10} + 4X^9 + 5X^8 + 6X^7 + 5X^6 + 4X^5 + 3X^4 + 2X^3 + X^2.$$

Par exemple, le nombre de façon d'obtenir 8 avec deux dés est égal à 5. La probablilité d'obtenir une somme de 8 est donc de $\frac{5}{36}$, le dénominateur étant le nombre total de possibilités des valeurs des deux dés.

On souhaite savoir s'il est possible de mettre de manière différente des entiers naturels non nuls sur les faces de deux cubes, et de construire ainsi des paires de dés exotiques équivalentes à la paire de dés classique. Une paire de dés exotique est équivalente à la paire de dés classique si les sommes possibles sont les mêmes, à savoir de 2 à 12, et de plus que chaque somme possède la même probabilité par rapport à la paire de dés classique. Jouer un jeu avec une paire de dés exotique ou pas n'a donc aucune influence sur le jeu.

Supposons que sur les faces de l'un des dés exotiques figurent les entiers naturels non nuls a, b, c, d, e, f, non forcément distincts. Supposons que sur les faces de l'autre dé exotique figurent les entiers naturels non nuls a', b', c', d', e', f', non forcément distincts. Comme le nombre de façons d'obtenir une somme de s pour une lancée des deux dés exotiques est par hypothèse égal au nombre de façons d'obtenir une somme de s pour les deux dés classiques, on a

$$(X^a + X^b + X^c + X^d + X^e + X^f)(X^{a'} + X^{b'} + X^{c'} + X^{d'} + X^{e'} + X^{f'}) = P.$$

Soit Q le premier facteur du premier membre, et Q' le second. On a $QQ' = P$ dans $\mathbb{Z}[X]$. On s'appuie sur le fait que $\mathbb{Z}[X]$ soit un anneau factoriel, et on décompose P dans $\mathbb{Z}[X]$ en facteurs

irréductibles. Notons que

$$X^6+X^5+X^4+X^3+X^2+X = X(X^5+X^4+X^3+X^2+X+1) = X\frac{X^6-1}{X-1}.$$

On a

$$X^6-1 = (X^3-1)(X^3+1) = (X-1)(X^2+X+1)(X+1)(X^2-X+1)$$

Cette dernière est la décomposition en facteurs irréductibles de X^6-1 dans $\mathbb{Z}[X]$ car tous les facteurs sont de contenu 1 et irréductibles dans $\mathbb{Q}[X]$. Du coup,

$$X^6+X^5+X^4+X^3+X^2+X = X(X+1)(X^2+X+1)(X^2-X+1).$$

Comme P est le carré de celui-ci, on obtient la décomposition en facteurs irréductibles de P dans $\mathbb{Z}[X]$:

$$P = X^2(X+1)^2(X^2+X+1)^2(X^2-X+1)^2.$$

Comme $QQ' = P$ et P est unitaire, Q et Q' sont unitaires. Par unicité de la factorisation en irréductibles dans $\mathbb{Z}[X]$, on a alors

$$Q = X^\alpha(X+1)^\beta(X^2+X+1)^\gamma(X^2-X+1)^\delta$$

et

$$Q' = X^{2-\alpha}(X+1)^{2-\beta}(X^2+X+1)^{2-\gamma}(X^2-X+1)^{2-\delta},$$

où $\alpha,\beta,\gamma,\delta \in \{0,1,2\}$. Comme les faces des dés exotiques sont numérotées avec des entiers naturels non nuls, Q et Q' sont divisibles par X. Du coup, $\alpha = 1$. Comme chaque dé à 6 faces, on a $Q(1) = 6$ et $Q'(1) = 6$. Comme

$$X(1) = 1,\ (X+1)(1) = 2,\ (X^2+X+1)(1) = 3 \quad \text{et} \quad (X^2-X+1)(1) = 1,$$

on a forcément $\beta = 1$ et $\gamma = 1$. Il reste deux possibilités, $\delta = 0$ et $\delta = 1$, quitte à échanger Q et Q'. Si $\delta = 1$, on a bien-sûr

$$Q = Q' = X(X+1)(X^2+X+1)(X^2-X+1) = X^6+X^5+X^4+X^3+X^2+X,$$

et on retrouve les dés classiques. Si $\delta = 0$, on a

$$\begin{cases} Q &= X(X+1)(X^2+X+1) = X^4+X^3+X^3+X^2+X^2+X \quad \text{et} \\ Q' &= X(X+1)(X^2+X+1)(X^2-X+1)^2 = X^8+X^6+X^5+X^4+X^3+X. \end{cases}$$

Ce cas-là correspond donc à une paire de dés exotique où l'un des dés a les nombres $1,2,2,3,3,4$ sur ses faces, et l'autre les nombres $1,3,4,5,6,8$. C'est la paire de dés exotique dite *de Sicherman*. Il s'agit donc d'une paire de dés avec les mêmes probabilités d'obtenir une somme s que la paire classique, quel que soit s. De plus, notre calcul montre qu'il n'y a pas d'autre paire de dés exotique équivalente à la paire de dés classique, et tout ça grâce à la factorialité de l'anneau $\mathbb{Z}[X]$!

Chapitre 2

Polynômes symétriques, résultants et discriminants

1. Polynômes homogènes

Soit A un anneau et n un entier naturel. Rappelons que $A[X_1, \dots, X_n]$ est l'anneau des polynômes en $X_1, \dots, X_n$ à coefficients dans A. Un *monôme* dans $A[X_1, \dots, X_n]$ est un polynôme de la forme

$$aX_1^{e_1} X_2^{e_2} \cdots X_n^{e_n}$$

où $a \in A$, $a \neq 0$, et $e_1, \dots, e_n \in \mathbb{N}$. Le *degré* de ce monôme est $e_1 + e_2 + \cdots + e_n$. Tout polynôme est une somme finie de monômes. Le *degré (total)* d'un polynôme non nul est le maximum des degrés des monômes le constituant. Le polynôme nul est de degré $-\infty$. Un polynôme dans $A[X_1, \dots, X_n]$ est *homogène* de degré d s'il est une somme finie de monômes de degré d uniquement. On note $A[X_1, \dots, X_n]_d$ le sous-ensemble de $A[X_1, \dots, X_n]$ des polynômes homogènes de degré d, où d est un entier naturel.

Exemple 1.1. (1) Le polynôme nul est homogène de tout degré, car somme de zéro monômes de degré d, pour tout entier naturel d.

(2) Un polynôme constant non nul est homogène de degré 0.

(3) Le polynôme $a_1X_1 + \cdots + a_nX_n$ est homogène de degré 1, quels que soient $a_1, \dots, a_n \in A$. En fait,

$$A[X_1, \dots, X_n]_1 = \{a_1X_1 + \cdots + a_nX_n \mid a_1, \dots, a_n \in A\}.$$

(4) Le polynôme $X_1 \cdots X_n$ est homogène de degré n.

Proposition 1.2. *Soit d et n des entiers naturels. Soit A un anneau et $f \in A[X_1, \dots, X_n]$ homogène de degré d. Alors*

$$f(aX_1, aX_2, \dots, aX_n) = a^d f(X_1, X_2, \dots, X_n)$$

pour tout $a \in A$.

Démonstration. Si f est un monôme de degré d, on a

$$f = bX_1^{e_1} X_2^{e_2} \cdots X_n^{e_n},$$

où $b \in A$ et $e_1, \dots, e_n \in \mathbb{N}$. Du coup,

$$f(aX_1, \dots, aX_n) = b(aX_1)^{e_1}(aX_2)^{e_2} \cdots (aX_n)^{e_n} = a^{e_1+e_2+\cdots+e_n} bX_1^{e_1} X_2^{e_2} \cdots X_n^{e_n} = a^d bX_1^{e_1} X_2^{e_2} \cdots X_n^{e_n} = a^d f(X_1, \dots, X_n)$$

car $e_1 + e_2 + \cdots + e_n = d$.

Plus généralement, si f est une somme de monômes $f = m_1 + \cdots + m_k$, tous de degré d, on a

$$f(aX_1, aX_2, \dots, aX_n) = m_1(aX_1, aX_2, \dots, aX_n) + \cdots + m_k(aX_1, aX_2, \dots, aX_n) = a^d m_1(X_1, X_2, \dots, X_n) + \cdots + a^d m_k(X_1, X_2, \dots, X_n) = a^d f(X_1, X_2, \dots, X_n)$$

d'après ce qui précède. □

Le réciproque n'est pas vrai, comme montre l'exemple suivant.

Exemple 1.3. Soit $f \in \mathbb{Z}/2[X_1, X_2]$ n'importe quel polynôme avec $f(0,0) = 0$. Alors

$$f(aX_1, aX_2) = a^d f(X_1, X_2)$$

pour tout $a \in \mathbb{Z}/2$ et tout entier naturel non nul d. En effet, c'est évident si $a = 1$. Si $a \neq 1$, on a $a = 0$ et

$$f(aX_1, aX_2) = f(0,0) = 0 = 0^d f(X_1, X_2)$$

d'après l'hypothèse sur f. Pourtant, f n'est pas forcément homogène. Il suffit de prendre $f = X_1 + X_2^2$, par exemple.

PROPOSITION 1.4. *Soient f et g des polynômes homogènes. Soit $a \in A$.*

(1) Si $\deg(f) = \deg(g)$*, alors $f+g$ est homogène et* $\deg(f+g) = \deg(f) = \deg(g)$.

(2) af est homogène et $\deg(af) = \deg(f)$.

(3) fg est homogène et $\deg(fg) = \deg(f) + \deg(g)$.

DÉMONSTRATION. Exercice. □

PROPOSITION 1.5. *Soit A un anneau et n un entier naturel. Tout polynôme f de $A[X_1, \ldots, X_n]$ s'écrit sous la forme*

$$f = f_0 + f_1 + \cdots + f_d$$

où f_i est homogène de degré i. De plus, cette écriture est unique dans le sens que si

$$f = f'_0 + f'_1 + \cdots + f'_{d'}$$

où f'_i est homogène de degré i, alors $f'_i = f_i$ quel que soit i [1].

DÉMONSTRATION. Exercice. □

On appelle le polynôme homogène f_i la *composante homogène* de f de degré i, et l'écriture de f comme somme des f_i sa *décomposition en composantes homogènes*.

EXEMPLE 1.6. Soit $A = \mathbb{Z}$, $n = 2$ et $f = X_1^2 + X_2^2 + X_1^3 + X_2^3$. La décomposition en composantes homogènes de f est

$$f = (X_1^2 + X_2^2) + (X_1^3 + X_2^3),$$

Plus précisément, $f = f_2 + f_3$ où

$$f_2 = X_1^2 + X_2^2 \quad \text{et} \quad f_3 = X_1^3 + X_2^3,$$

f_2 étant homogène de degré 2, et f_3 homogène de degré 3.

PROPOSITION 1.7. *Soit A un anneau et n un entier naturel. Soient $f, g \in A[X_1, \ldots, X_n]$ et*

$$f = f_0 + \cdots + f_d \quad \text{et} \quad g = g_0 + \cdots + g_e$$

leurs décompositions en composantes homogènes. Alors, la composante homogène de $f+g$ de degré i est

$$(f+g)_i = f_i + g_i.$$

La composante homogène de fg de degré i est

$$(fg)_i = f_0 g_i + f_1 g_{i-1} + \cdots + f_i g_0.$$

DÉMONSTRATION. Exercice. □

EXEMPLE 1.8. Soit $A = \mathbb{Z}$, $n = 2$ et $f = X_1^2 + X_2^2 + X_1^3 + X_2^3$. La décomposition en composantes homogènes de f^2 est

$$f^2 = (f_2 + f_3)^2 = f_2^2 + 2f_2 f_3 + f_3^2,$$

où f_2 est la composante homogène de f de degré 2, et f_3 celle de degré 3. Comme f_2^2 est homogène de degré 4, $2f_2f_3$ est homogène de degré 5 et f_3^3 est homogène de degré 6, c'est bien la décomposition en composantes homogène de f_2^2.

Si A est un anneau intègre, il y a une réciproque à l'implication que fg est homogène si f et g le sont :

PROPOSITION 1.9. *Soit A un anneau intègre et n un entier naturel. Soit $f, g \in A[X_1, \ldots, X_n]$ non nuls. Si fg est homogene, alors f et g sont homogènes.*

DÉMONSTRATION. On montre la contraposée et on suppose que f ou g n'est pas homogène. On montre que fg n'est pas homogène. Quitte à échanger f et g, on peut supposer que f n'est pas homogène. La décomposition en composantes homogènes de f comprend au moins deux termes non nuls. Soit f_c la composante non nulle de f du plus bas degré, et f_d celle de plus haut degré. On a donc

$$f = f_c + f_{c+1} + \cdots + f_d$$

avec $f_c, f_d \neq 0$ et $c < d$. Soit

$$g = g_b + g_{b+1} + \cdots + g_e$$

1. où il est sous-entendu que $f_i = 0$ pour $i > d$ et $f'_i = 0$ pour $i > d'$

la décomposition en composantes homogènes de g avec $g_b, g_e \neq 0$ et $b \leq e$. La décomposition en composantes homogènes de fg est alors

$$fg = f_c g_b + \cdots + f_d g_e,$$

où $f_c g, f_d g_e \neq 0$. De plus, $f_c g_b$ est homogène de degré $c+b$, et $f_d g_e$ est de degré $d+e$. Comme $c < d$ et $b \leq e$, on a $c+b < d+e$. Il s'ensuit que fg n'est pas homogène. □

Soit A un anneau intègre. Soit $f, g \in A[X_1, \ldots, X_n]$ homogènes. On pourrait dire que f *divise* g *homogènement* s'il existe $h \in A[X_1, \ldots, X_n]$ homogène tel que $fh = g$. Cependant, la proposition précédente implique que cette relation coïncide avec la relation de divisibilité ordinare entre f et g.

De même, si $f \in A[X_1, \ldots, X_n]$ est homogène, non nul et non inversible. On pourrait dire que f est *homogènement irréductible* si tout diviseur homogène de f est soit inversible soit associé à f, mais cette propriété est équivalente à celle d'etre irréductible tout court d'après la proposition précédente.

On pourrait dire encore que f est *homogènement premier* si $f|gh$ avec g et h homogènes, implique que $f|g$ ou $f|h$, mais là encore cette propriété est équivalente à celle d'etre premier tout court.

Il s'ensuit que si A est factoriel, l'anneau $A[X_1, \ldots, X_n]$ n'est non seulement factoriel, mais même *factoriel homogènement*, c-à-d, tout polynôme homogène non nul de $A[X_1, \ldots, X_n]$ s'écrit de manière unique comme produit de polynômes homogènes irréductibles.

Exemple 1.10. Le polynôme $f = X^2 + Y^2$ dans $\mathbb{R}[X, Y]$ est irréductible. En effet, comme f est homogène, il suffit de vérifier que f est irréductible homogènement. Comme f n'est ni nul ni inversible, il suffit de montrer que tout diviseur homogène g de f est soit inversible soit associé à f. Supposons qu'il existe un diviseur homogène $g \in \mathbb{R}[X, Y]$ de f qui n'est ni inversible ni associé à f. Du coup, g est homogène de degré 1. Ecrivons $g = aX + bY$ avec $a, b \in \mathbb{R}$. Soit

$$\varphi \colon \mathbb{R}[X, Y] \to \mathbb{R}$$

le morphisme défini par $\varphi_{|\mathbb{R}} = \mathrm{id}_{\mathbb{R}}$, $\varphi(X) = b$ et $\varphi(Y) = -a$. On a $\varphi(g) = 0$. Comme $g|f$, on a $\varphi(f) = 0$. Or, $\varphi(f) = (-b)^2 + a^2$. Comme $a, b \in \mathbb{R}$, on en déduit que $a = b = 0$ et $g = 0$. Du coup, $f = 0$. Contradiction.

2. Polynômes symétriques

Soit A un anneau et n un entier naturel. Rappelons que S_n est le groupe symétrique sur l'ensemble $\{1, \ldots, n\}$. Si $f \in A[X_1, \ldots, X_n]$, on définit un nouveau polynôme πf par

$$\pi f = f(X_{\pi(1)}, X_{\pi(2)}, \ldots, X_{\pi(n)})$$

On dit que f est *symétrique* si $\pi f = f$ pour tout $\pi \in S_n$. On note

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

le sous-ensemble de $A[X_1, \ldots, X_n]$ des polynômes symétriques.

Exemple 2.1. (1) Tous les polynômes constants sont symétriques.

(2) $X_1 + \cdots + X_n$ est symétrique.

(3) $X_1^d + \cdots + X_n^d$ est symétrique.

(4) $X_1 \cdots X_n$ est symétrique

(5) Le polynôme X_1 n'est pas symétrique si $n > 1$.

Proposition 2.2. *Soit A un anneau et n un entier naturel. Soit $f, g \in A[X_1, \ldots, X_n]$ et $\pi \in S_n$. Alors,*

$$\pi(f+g) = \pi f + \pi g \quad \text{et} \quad \pi(fg) = (\pi f)(\pi g).$$

En particulier, si f et g sont symétriques, $f+g$ et fg le sont également. Le sous-ensemble $A[X_1, \ldots, X_n]^{S_n}$ des polynômes symétriques est donc un sous-anneau de $A[X_1, \ldots, X_n]$.

Démonstration. Exercice. □

Proposition 2.3. *Soit A un anneau et n un entier naturel. Soit $f \in A[X_1, \ldots, X_n]$ homogène et $\pi \in S_n$. Alors πf est homogène de même degré que f.*

Démonstration. Exercice. □

COROLLAIRE 2.4. *Soit A un anneau et n un entier naturel. Soit $f \in A[X_1, \dots, X_n]$ et soit $f = f_0 + \cdots + f_d$ sa décomposition en composantes homogènes. Alors f est symétrique si et seulement si chaque f_i l'est.*

Considérons dans l'anneau $(A[T])[X_1, \dots, X_n]$ le polynôme f défini par

$$f = (T + X_1)(T + X_2) \cdots (T + X_n).$$

Il est clair que f est symétrique en tant que polynôme en $X_1, \dots, X_n$ à coefficients dans $A[T]$. Développons f comme polynôme en T :

$$f = T^n + \sigma_1 T^{n-1} + \cdots + \sigma_{n-1} T + \sigma_n,$$

où $\sigma_1, \dots, \sigma_n \in A[X_1, \dots, X_n]$. Comme $\pi T = T$, chacun des polynômes σ_i est symétrique dans $A[X_1, \dots, X_n]$. On a

$$\begin{aligned}
\sigma_1 &= X_1 + \cdots + X_n \\
\sigma_2 &= \sum_{i<j} X_i X_j \\
\sigma_3 &= \sum_{i<j<k} X_i X_j X_k \\
&\vdots \\
\sigma_d &= \sum_{i_1<i_2<\cdots<i_d} X_{i_1} X_{i_2} \cdots X_{i_d} \\
&\vdots \\
\sigma_n &= X_1 \cdots X_n.
\end{aligned}$$

Les polynômes $\sigma_1, \dots \sigma_n$ dans $A[X_1, \dots, X_n]$ sont *les polynômes symétriques élémentaires*. Notons que σ_i est homogène de degré i, pour $i = 1, \dots, n$, et que ses coefficients sont des entiers relatifs, vus comme éléments de A.

EXEMPLE 2.5. (1) Si $n = 1$, on a $\sigma_1 = X_1$.

(2) Si $n = 2$, on a $\sigma_1 = X_1 + X_2$ et $\sigma_2 = X_1 X_2$.

(3) Si $n = 3$, on a $\sigma_1 = X_1 + X_2 + X_3$, $\sigma_2 = X_1X_2 + X_1X_3 + X_2X_3$, et $\sigma_3 = X_1X_2X_3$.

L'un des intérêts des polynômes symétriques élémentaires est le fait qu'ils donnent une relation entre les racines d'un polynôme unitaire et ses coefficients. En effet, évaluons le polynôme f ci-dessus en $(-X_1, \dots, -X_n)$ pour obtenir

$$\begin{aligned}
f' = (T - X_1)(T - X_2) \cdots (T - X_n) = (T + (-X_1))(T + (-X_2)) \cdots (T + (-X_n)) = \\
T^n + \sigma_1(-X_1, \dots, -X_n) T^{n-1} + \sigma_2(-X_1, \dots, -X_n) T^{n-2} + \cdots + \sigma_n(-X_1, \dots, -X_n) = \\
T^n - \sigma_1 T^{n-1} + \sigma_2 T^{n-2} - \cdots + (-1)^n \sigma_n.
\end{aligned}$$

En posant

$$A_i = (-1)^i \sigma_i \in A[X_1, \dots, X_n],$$

on voit que les coefficients $A_1, \dots, A_n$ du polynôme unitaire universel complètement scindé de degré n à coefficients dans A s'expriment en fonctions des indéterminées $X_1, \dots, X_n$.

Plus concrètement, on a l'énoncé suivant.

PROPOSITION 2.6. *Soit A un anneau et n un entier naturel. Soit $g \in A[T]$ un polynôme unitaire de degré n et écrivons*

$$g = T^n + a_1 T + \cdots + a_n$$

où $a_1, \dots, a_n \in A$. Supposons que g est complètement scindé dans $A[T]$, c-à-d, il existe $x_1, \dots, x_n \in A$ tels que

$$g = (T - x_1)(T - x_2) \cdots (T - x_n).$$

Alors,

$$a_i = (-1)^i \sigma_i(x_1, \dots, x_n)$$

pour $i = 1, \dots, n$.

DÉMONSTRATION. Soit

$$\Psi\colon A[X_1,\dots,X_n][T]\to A[T]$$

le morphisme défini par $\Psi_{|A}=\mathrm{id}_A$, $\Psi(X_i)=x_i$ pour $i=1,\dots,n$, et $\Psi(T)=T$. On a $\Psi(f')=g$, où f' est le polynôme défini ci-dessus. Et donc aussi $\Psi(A_i)=a_i$. D'où

$$a_i=\Psi(A_i)=\Psi((-1)^i\sigma_i)=(-1)^i\sigma_i(x_1,\dots,X_n)$$

pour $i=1,\dots,n$. □

Le but de ce paragraphe est de démontrer l'énoncé suivant.

THÉORÈME 2.7. *Soit A un anneau et n un entier naturel. Pour tout polynôme symétrique f dans $A[X_1,\dots,X_n]$ il existe un et un seul polynôme $g\in A[Y_1,\dots,Y_n]$ tel que*

$$f=g(\sigma_1,\dots,\sigma_n).$$

DÉMONSTRATION. Montrons d'abord l'unicité. Pour cela, il suffit de montrer que $g=0$ si $g(\sigma_1,\dots,\sigma_n)=0$, quel que soit $g\in A[Y_1,\dots,Y_n]$. On le montre par l'absurde. Supposons qu'il existe un polynôme $g\neq 0$ avec $g(\sigma_1,\dots,\sigma_n)=0$. On peut supposer que c'est le polynôme g pour lequel n est le plus petit, c-à-d, on suppose que l'unicité de l'énoncé est vraie pour tout nombre d'indéterminées $<n$. Comme l'unicité est évidente pour $n=0$ et $n=1$, on a $n\geq 2$.

De plus, on peut supposer que le degré de g comme polynôme en Y_n est minimal.

On écrit

$$g=g_0+g_1Y_n+\cdots+g_dY_n^d$$

avec $g_i\in A[Y_1,\dots,Y_{n-1}]$ et $g_d\neq 0$. On a aussi $g_0\neq 0$. Sinon, $g=Y_ng'$ avec $g'\neq 0$ et $g'(\sigma_1,\dots,\sigma_n)=0$ ce qui contredirait le fait que g est de degré minimal en Y_n. Soit

$$\varphi\colon A[X_1,\dots,X_n]\to A[X_1,\dots,X_{n-1}]$$

le morphisme défini par $\varphi(X_i)=X_i$ pour $i=1,\dots,n-1$, $\varphi(X_n)=0$ et $\varphi_{|A}=\mathrm{id}_A$. Notons que $\varphi(\sigma_i)=\sigma_i$ pour $i=1,\dots,n-1$, et que $\varphi(\sigma_n)=0$. Du coup,

$$0=\varphi(g(\sigma_1,\dots,\sigma_n))=\varphi(g_0(\sigma_1,\dots,\sigma_{n-1}))=g_0(\sigma_1,\dots,\sigma_{n-1})$$

ce qui contredit la minimalité de n, et montre l'unicité de g.

Comme les composantes homogènes d'un polynôme symétrique sont symétriques, ils suffit de démontrer l'existence de g dans le cas où f est homogène. Ce cas-là fait l'objet d'un énoncé plus précis ci-dessous. □

Afin de pouvoir formuler l'énoncé plus précis pour les polynômes symétriques homogènes, introduisons le poids d'un polynôme en $Y_1,\dots,Y_n$ à coefficients dans A. Le *poids* d'un monôme

$$aY_1^{e_1}Y_2^{e_2}\cdots Y_n^{e_n},$$

où $a\in A$ et $e_1,\dots,e_n\in\mathbb{N}$, est l'entier naturel $e_1+2e_2+3e_3+\cdots+ne_n$. En particulier, l'indéterminée Y_i est de poids i, pour $i=1,\dots,n$. Le *poids* d'un polynôme non nul est le maximum des poids des monômes le constituant. Le polynôme nul est de poids $-\infty$. Un polynôme $g\in A[Y_1,\dots,Y_n]$ est *homogène de poids p* s'il est somme de monômes de poids p uniquement.

Le poids d'un polynôme nous intéresse pour la raison suivante. Si g est un polynôme homogène de poids p, alors $g(\sigma_1,\dots,\sigma_n)$ est homogène de degré p.

THÉORÈME 2.8. *Soit A un anneau et $d,n\in\mathbb{N}$. Pour tout polynôme symétrique homogène $f\in A[X_1,\dots,X_n]$ de degré d, il existe un et un seul polynôme homogène $g\in A[Y_1,\dots,Y_n]$ de poids d tel que*

$$f=g(\sigma_1,\dots,\sigma_n).$$

DÉMONSTRATION. L'unicité est une conséquence de l'unicité de la version non homogène ci-dessus. Il suffit donc de montrer l'existence de g. Ici encore, on peut supposer que $n\geq 2$.

Soit M l'ensemble des monômes unitaires de degré d en $X_1,\dots,X_n$. Ecrivons tout monôme appartenant à M «en toutes lettres» c-à-d

$$X_1^{e_1}\cdots X_n^{e_n}=X_1X_1\cdots X_1X_2X_2\cdots X_2\cdots X_nX_n\cdots X_n.$$

Considérons ensuite l'ordre lexicographique sur M pour lequel $X_1<X_2<\cdots<X_n$. L'ensemble M est fini et totalement ordonné par cette relation d'ordre. Le plus petit élément de M est X_1^d.

Le plus grand est X_n^d. Soit $M(f)$ le sous-ensemble de M des monômes figurant dans f avec un coefficient non nul. Soit $m = m(f)$ l'infimum de $M(f)$. Ecrivons

$$m = X_1^{e_1} \cdots X_n^{e_n}.$$

On démontre l'énoncé d'existence de g par récurrence descendante sur m. Si $m = X_n^d$, on a forcément $M(f) = \emptyset$. Dans ce cas $f = 0$ et on prend $g = 0$. Supposons maintenant que $m < X_n^d$ dans M et que tout polynôme homogène f' de degré d avec $m' = m(f') > m$ est de la forme $g'(\sigma_1, \ldots, \sigma_n)$ avec g' homogène de poids d.

On a $e_1 \geq e_2 \geq \cdots \geq e_n$. En effet, si ce n'était pas le cas, il y aurait un i tel que $e_i < e_{i+1}$. Soit π la transposition $(i\ i+1)$ dans S_n. Comme f est symétrique $\pi m \in M(f)$. Or, $\pi m < m$. Contradiction. Considérons le polynôme

$$f' = f - a\sigma_1^{e_1-e_2}\sigma_2^{e_2-e_3} \cdots \sigma_{n-1}^{e_{n-1}-e_n}\sigma_n^{e_n},$$

où a est le coefficient de m dans f. Le plus petit monôme dans

$$\sigma_1^{e_1-e_2}\sigma_2^{e_2-e_3} \cdots \sigma_{n-1}^{e_{n-1}-e_n}\sigma_n^{e_n}$$

est le produit des plus petits monômes de ses facteurs, c-à-d

$$X_1^{e_1-e_2}(X_1X_2)^{e_2-e_3}(X_1X_2X_3)^{e_3-e_4} \cdots (X_1 \cdots X_{n-1})^{e_{n-1}-e_n}(X_1 \cdots X_n)^{e_n} = X_1^{e_1} \cdots X_n^{e_n} = m,$$

On a donc $m' = m(f') > m$. Par hypothèse de récurrence,

$$f' = g'(\sigma_1, \ldots, \sigma_n),$$

où g' est homogène de poids d. Du coup,

$$f = f' + a\sigma_1^{e_1-e_2}\sigma_2^{e_2-e_3} \cdots \sigma_{n-1}^{e_{n-1}-e_n}\sigma_n^{e_n} = g(\sigma_1, \ldots, \sigma_n),$$

où

$$g = g' + aY_1^{e_1-e_2}Y_2^{e_2-e_3} \cdots Y_{n-1}^{e_{n-1}-e_n}Y_n^{e_n}$$

est homogène de poids d. Cela démontre l'existence de g. □

EXEMPLE 2.9. (1) Soit $A = \mathbb{Z}$, $n = 2$ et $f = X_1^2 + X_2^2$. Le polynôme f est symétrique homogène de degré 2. On a

$$M = \{X_1X_1, X_1X_2, X_2X_2\},\ M(f) = \{X_1X_1, X_2X_2\} \quad \text{et} \quad m = X_1^2.$$

On a $e_1 = 2$ et $e_2 = 0$ pour le monôme m. Le coefficient de m dans f est égal à 1. On pose

$$f' = f - 1 \cdot \sigma_1^{2-0}\sigma_2^0 = f - \sigma_1^2 = X_1^2 + X_2^2 - (X_1 + X_2)^2 = -X_1X_2 = -\sigma_2.$$

Du coup,

$$f = \sigma_1^2 - \sigma_2.$$

Le polynôme g tel que $f = g(\sigma_1, \sigma_2)$ est le polynôme $g = Y_1^2 - Y_2$ qui est bien homogène de poids 2.

(2) Soit $A = \mathbb{Z}$, $n = 2$ et $f = X_1^3 + X_2^3$. Le polynôme f est symétrique homogène de degré 3. On a

$$M = \{X_1^3, X_1^2X_2, X_1X_2^2, X_2^3\},\ M(f) = \{X_1^3, X_2^3\} \quad \text{et} \quad m = X_1^3.$$

On a $e_1 = 3$ et $e_2 = 0$ pour le monôme m. Le coefficient de m dans f est égal à 1. On pose

$$f' = f - 1 \cdot \sigma_1^{3-0}\sigma_2^0 = f - \sigma_1^3 = -3X_1^2X_2 - 3X_1X^2.$$

On a

$$M(f') = \{X_1^2X_2, X_1X_2^2\} \quad \text{et} \quad m' = X_1^2X_2.$$

On a $e_1 = 2$ et $e_2 = 1$ pour le monôme m'. Le coefficient de m' dans f' est égal à -3. On pose

$$f'' = f' = -(-3) \cdot \sigma_1^{2-1}\sigma_2^1 = f' + 3\sigma_1\sigma_2 = -3X_1^2X_2 - 3X_1X^2 + 3X_1^2X_2 + 3X_1X_2^2 = 0.$$

Du coup,

$$f = f' + \sigma_1^3 = -3\sigma_1\sigma_2 + \sigma_1^3.$$

Le polynôme g tel que $f = g(\sigma_1, \sigma_2)$ est le polynôme $g = -3Y_1Y_2 + Y_1^3$ qui est bien homogène de poids 3.

(3) Soit $A = \mathbb{Z}$, $n = 2$ et $f = X_1^2 + X_2^2 + X_1^3 + X_2^3$. Le polynôme f est bien symétrique. Sa décomposition en composantes homogènes est

$$f = (X_1^2 + X_2^2) + (X_1^3 + X_2^3).$$

D'après les exemples précédents, on a

$$f = \sigma_1^2 - \sigma_2 - 3\sigma_1\sigma_2 + \sigma_1^3.$$

On a donc $f = g(\sigma_1, \sigma_2)$, avec

$$g = Y_1^2 - Y_2 - 3Y_1Y_2 + Y_1^3.$$

COROLLAIRE 2.10. *Soit A un anneau et n un entier naturel. Soit*

$$\varphi\colon A[Y_1, \ldots, Y_n] \to A[X_1, \ldots, X_n]$$

défini par $\varphi_{|A} = \mathrm{id}_A$ et

$$\varphi(Y_i) = \sigma_i$$

pour $i = 1, \ldots, n$. Alors, φ est un isomorphisme de $A[Y_1, \ldots, Y_n]$ sur $A[X_1, \ldots, X_n]^{S_n}$. En particulier, l'anneau $A[X_1, \ldots, X_n]^{S_n}$ des polynômes symétriques en $X_1, \ldots, X_n$ à coefficients dans A est isomorphe à un anneau de polynômes à coefficients dans A en n indéterminées.

3. L'algèbre de décomposition d'un polynôme unitaire en une indéterminée

THÉORÈME 3.1. *Soit A un anneau et $g \in A[T]$ un polynôme unitaire. Soit $n = \deg(g)$. Alors, il existe un anneau B contenant A comme sous-anneau et des éléments $x_1, \ldots, x_n \in B$ tels que*

$$g = (T - x_1)(T - x_2)\cdots(T - x_n)$$

dans $B[T]$. De plus, il y en a un qui soit universel.

On appelle *B l'algèbre de décomposition* de g sur A.

DÉMONSTRATION. On démontre l'énoncé seulement dans le cas où A contient le corps des nombres rationnels $\mathbb{Q}$ comme sous-anneau. Ecrivons $g = T^n + a_1T^{n-1} + \cdots + a_n$. Soit f le polynôme unitaire universel de degré n à coefficients dans A :

$$f = T^n + A_1T^{n-1} + \cdots + A_n \in A[A_1, \ldots, A_n][T].$$

Soit

$$\pi\colon A[A_1, \ldots, A_n] \to A$$

défini par $\pi_{|A} = \mathrm{id}_A$ et $\pi(A_i) = a_i$, pour $i = 1, \ldots, n$. Soit I le noyau de π. Considérons $A[A_1, \ldots, A_n]$ comme sous-anneau de $A[X_1, \ldots, X_n]$ en identifiant A_i avec $(-1)^i\sigma_i$. Soit J l'idéal de $A[X_1, \ldots, X_n]$ engendré par I. On pose $B = A[X_1, \ldots, X_n]/J$ et on écrit x_i pour la classe modulo J de X_i, pour $i = 1, \ldots, n$. Il y a un unique morphisme d'anneau ρ de A dans B tel que le diagramme

$$\begin{array}{ccc} A[A_1, \ldots, A_n] & \longrightarrow & A[X_1, \ldots, X_n] \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} \\ A & \xrightarrow{\quad\rho\quad} & B \end{array}$$

commute, où les morphismes verticaux sont les morphismes de passage au quotient, et le morphisme horizontal du dessus est l'inclusion. Montrons que ρ est injectif. Soit $a \in A$ tel que $\rho(a) = 0$. On a donc aussi $\rho(\pi(a)) = 0$, ou encore $\pi'(a) = 0$. Cela veut dire que $a \in J$. Il existe donc $p_i \in A[X_1, \ldots, X_n]$ et $q_i \in I$, pour $i = 1, \ldots, m$, tels que

$$a = p_1q_1 + \cdots + p_mq_m$$

dans $A[X_1, \ldots, X_n]$. Soit $\pi \in S_n$, on a aussi

$$a = (\pi p_1)(\pi q_1) + \cdots + (\pi p_m)(\pi q_m) = (\pi p_1)q_1 + \cdots + (\pi p_m)q_m$$

car

$$a, q_1, \ldots, q_m \in I \subseteq A[A_1, \ldots, A_n] = A[X_1, \ldots, X_n]^{S_n}.$$

En faisant la somme sur $\pi \in S_n$, on obtient

$$n! \cdot a = (\sum \pi p_1)q_1 + \cdots + (\sum \pi p_m)q_m$$

dans $A[X_1, \ldots, A_n]$. Comme

$$\sum \pi p_i \in A[X_1, \ldots, X_n]^{S_n} = A[A_1, \ldots, A_n]$$

et comme $n! \in \mathbb{Q}$ est inversible dans A, on obtient que $a \in I$, et $a = \pi(a) = 0$ dans A. Cela montre que ρ est injectif.

On peut donc identifier A avec son image dans B, et B est alors un anneau contenant A comme sous-anneau. Comme

$$f = (T - X_1) \cdots (T - X_n)$$

dans $A[X_1, \ldots, X_n][T]$, on a

$$g = (T - x_1) \cdots (T - x_n)$$

dans $B[T]$.

On montre facilement que B est universel. En effet, soit C un anneau contenant A comme sous-anneau et dans lequel il existe $y_1, \ldots, y_n$ tels que

$$g = (T - y_1) \cdots (T - y_n).$$

On montre qu'il existe un et un seul morphisme

$$\varphi \colon B \to C$$

tel que $\varphi_{|A} = \mathrm{id}_A$ et $\varphi(x_i) = y_i$ pour $i = 1, \ldots, n$. □

4. Le discriminant d'un polynôme unitaire

Soit n un entier naturel. Soit f le polynôme unitaire universel en T de degré n complètement scindé, i.e.,

$$f = (T - X_1)(T - X_2) \cdots (T - X_n) \in \mathbb{Z}[X_1, \ldots, X_n][T].$$

En développant, on trouve

$$f = T^n - \sigma_1 T^{n-1} + \cdots + (-1)^n \sigma_n,$$

où $\sigma_1, \ldots, \sigma_n$ sont les polynômes symétriques élémentaires dans $\mathbb{Z}[X_1, \ldots, X_n]$. En posant

$$A_i = (-1)^i \sigma_i \in \mathbb{Z}[X_1, \ldots, X_n],$$

pour $i = 1, \ldots, n$, on a

$$f = T^n + A_1 T^{n-1} + \cdots + A_n.$$

D'après le théorème sur les polynômes symétriques élémentaires, tout polynôme symétrique en $X_1, \ldots, X_n$ peut s'écrire comme un polynôme en $\sigma_1, \ldots, \sigma_n$, ou encore en $A_1, \ldots, A_n$. De plus, s'il est homogène de degré d en $X_1, \ldots, X_n$, il est homogène de poids d en $A_1, \ldots, A_n$. Par exemple, le polynôme

$$\Delta = \prod_{i<j} (X_i - X_j)^2$$

est une polynôme symétrique en $X_1, \ldots, X_n$ homogène de degré $n(n-1)$, et s'exprime donc comme polynôme homogène de poids $n(n-1)$ en $A_1, \ldots, A_n$. On l'appelle le *discriminant* de f ou le *discriminant universel*. Il appartient au sous-anneau $\mathbb{Z}[A_1, \ldots, A_n]$ de $\mathbb{Z}[X_1, \ldots, X_n]$. Déterminons-le pour de petites valeurs de n :

Pour $n = 0$ ou $n = 1$, le discriminant universel est $\Delta = 1$. Pour $n = 2$, le discriminant universel est

$$\Delta = (X_1 - X_2)^2 = X_1^2 - 2X_1X_2 + X_2^2 = \sigma_1^2 - 4\sigma_2 = (-A_1)^2 - 4A_2 = A_1^2 - 4A_2.$$

C'est bien le discriminant du polyôme quadratique $T^2 + A_1 T + A_2$ tel qu'on le connaît. Observons qu'il est bien homogène de poids 2 en A_1, A_2.

PROPOSITION 4.1. *Le discriminant universel en* 3 *indéterminées est le polynôme homogène de poids* 6

$$\Delta = A_1^2 A_2^2 - 4A_1^3 A_3 - 4A_2^3 + 18A_1A_2A_3 - 27A_3^2.$$

DÉMONSTRATION. Le discriminant universel en 3 indéterminées est

$$\Delta = (X_1 - X_2)^2 (X_1 - X_3)^2 (X_2 - X_3)^2 = (X_1^2 - 2X_1X_2 + X_2^2)(X_1^2 - 2X_1X_3 + X_3^2)(X_2^2 - 2X_2X_3 + X_3^2).$$

C'est un polynôme homogène symétrique de degré 6 en X_1, X_2, X_3. On va l'écrire comme polynôme en $\sigma_1, \sigma_2, \sigma_3$ en suivant la procédure de la démonstration du théorème sur les polynômes symétriques élémentaires. Afin de simplifier les expressions, on n'écrira dans la suite que les monômes de la forme

$$X_1^{e_1} X_2^{e_2} X_3^{e_3}$$

pour lequel $e_1 \geq e_2 \geq e_3$ et $e_1 + e_2 + e_3 = 6$. Les autres termes sont des permutés de ceux-ci. Les triplets (e_1, e_2, e_3) vérifiant ces conditions et qui figurent a priori dans Δ sont

$$(4,2,0),\ (4,1,1),\ (3,3,0),\ (3,2,1) \text{ et } (2,2,2).$$

Les coefficients des monômes correspondants sont

$$1,\ -2,\ -2,\ 2 \text{ et } -6$$

respectivement. Les trois premiers sont clairs. Le coefficient du monôme correspondant à $(3,2,1)$ s'obtient ainsi. Il n'y a pas de contribution à ce monôme du terme de X_2^2 du premier facteur. La contribution de $-2X_1X_2$ est $-2 \times -2 = 4$. La contribution de X_1^2 est de $-2 \times 1 = -2$. Cela fait un total de $4 - 2 = 2$. En ce qui concerne le coefficient du monôme correspondant à $(2,2,2)$, chaque terme du premier facteur y contribue. Le terme X_1^2 avec un coefficient 1, le terme X_2^2 avec un 1 également, et le terme $-2X_1X_2$ avec $-2 \times -2 \times -2 = -8$. Au total le coefficient du monôme correspondant à $(2,2,2)$ est de $1 + 1 - 8 = -6$. On obtient donc

$$\Delta = X_1^4X_2^2 - 2X_1^4X_2X_3 - 2X_1^3X_2^3 + 2X_1^3X_2^2X_3 - 6X_1^2X_2^2X_3^2 + \text{permutés}.$$

Afin de l'écrire comme polynôme en les polynômes symétriques élementaires, on va soustraire $\sigma_1^{4-2}\sigma_2^{2-0}\sigma_3^0$. Or, en arguant comme pour Δ, on a

$$\sigma_1^2\sigma_2^2 = (X_1 + X_2 + X_3)^2(X_1X_2 + X_1X_3 + X_2X_3)^2 = \\ X_1^4X_2^2 + 2X_1^4X_2X_3 + 2X_1^3X_2^3 + 8X_1^3X_2^2X_3 + 15X_1^2X_2^2X_3^2 + \text{permutés}.$$

Du coup,

$$\Delta - \sigma_1^2\sigma_2^2 = -4X_1^4X_2X_3 - 4X_1^3X_2^3 - 6X_1^3X_2^2X_3 - 21X_1^2X_2^2X_3^2 + \text{permutés}$$

commence bien avec un monôme plus grand que Δ. On va y rajouter

$$4\sigma_1^3\sigma_3 = 4(X_1 + X_2 + X_3)^3X_1X_2X_3 = 4X_1^4X_2X_3 + 12X_1^3X_2^2X_3 + 24X_1^2X_2^2X_3^2 + \text{permutés},$$

et on obtient

$$\Delta - \sigma_1^2\sigma_2^2 + 4\sigma_1^3\sigma_3 = -4X_1^3X_2^3 + 6X_1^3X_2^2X_3 + 3X_1^2X_2^2X_3^2 + \text{permutés}.$$

On y rajoute

$$4\sigma_2^3 = 4(X_1X_2 + X_1X_3 + X_2X_3)^3 = 4X_1^3X_2^3 + 12X_1^3X_2^2X_3 + 24X_1^2X_2^2X_3^2 + \text{permutés},$$

et on obtient

$$\Delta - \sigma_1^2\sigma_2^2 + 4\sigma_1^3\sigma_3 + 4\sigma_2^3 = 18X_1^3X_2^2X_3 + 27X_1^2X_2^2X_3^2 + \text{permutés}.$$

On y soustrait

$$18\sigma_1\sigma_2\sigma_3 = 18(X_1 + X_2 + X_3)(X_1X_2 + X_1X_3 + X_2X_3)X_1X_2X_3 = \\ 18X_1^3X_2^2X_3 + 54X_1^2X_2^2X_3^2 + \text{permutés}$$

et on obtient

$$\Delta - \sigma_1^2\sigma_2^2 + 4\sigma_1^3\sigma_3 + 4\sigma_2^3 - 18\sigma_1\sigma_2\sigma_3 = -27X_1^2X_2^2X_3^2 = -27\sigma_3^2.$$

Au final, on obtient que le discriminant universel pour $n = 3$ vaut

$$\Delta = \sigma_1^2\sigma_2^2 - 4\sigma_1^3\sigma_3 - 4\sigma_2^3 + 18\sigma_1\sigma_2\sigma_3 - 27\sigma_3^2 = A_1^2A_2^2 - 4A_1^3A_3 - 4A_2^3 + 18A_1A_2A_3 - 27A_3^2. \quad \square$$

Exemple 4.2. A titre indicatif, le discriminant universel en 4 indéterminées est

$$\Delta = A_1^2A_2^2A_3^2 - 4A_1^3A_3^3 - 4A_1^2A_2^3A_4 + 18A_1^3A_2A_3A_4 - 27A_1^4A_4^2 - \\ 4A_2^3A_3^2 + 18A_1A_2A_3^3 + 16A_2^4A_4 - 80A_1A_2^2A_3A_4 - 6A_1^2A_3^2A_4 + \\ 144A_1^2A_2A_4^2 - 27A_3^4 + 144A_2A_3^2A_4 - 128A_2^2A_4^2 - 192A_1A_3A_4^2 + 256A_4^3.$$

Soit maintenant A un anneau et g un polynôme unitaire en T à coefficients dans A. On écrit

$$g = T^n + a_1 T^{n-1} + \cdots + a_n$$

où $a_1, \ldots, a_n \in A$. Soit

$$\varphi\colon \mathbb{Z}[A_1, \ldots, A_n] \to A$$

le morphisme défini par $\pi(A_i) = a_i$. Le *discriminant* de g est par définition l'image $\varphi(\Delta)$ dans A du discriminant universel Δ défini ci-dessus. On l'écrit $\Delta(g)$. On a $\Delta(f) = \Delta$ car $\varphi = \mathrm{id}$ dans ce cas. Cela justifie qu'on appelle le discriminant universel également le discriminant du polynôme universel f.

EXEMPLE 4.3. Le discriminant du polynôme $g = T^2 + a_1 T + a_2$ est

$$\Delta(g) = a_1^2 - 4a_2.$$

EXEMPLE 4.4. Le discriminant du polynôme $g = T^3 + a_1 T^2 + a_2 T + a_3$ est

$$\Delta(g) = a_1^2 a_2^2 - 4a_1^3 a_3 - 4a_2^3 + 18 a_1 a_2 a_3 - 27 a_3^2.$$

Par exemple, le discriminant du polynôme $g = T^3 + a_2 T + a_3$ est

$$\Delta(g) = -4a_2^3 - 27a_3^2.$$

Ou encore le discriminant du polynôme $g = T^3 + a_1 T^2 + a_2 T$ est

$$\Delta(g) = a_1^2 a_2^2 - 4a_2^3 = a_2^2(a_1^2 - 4a_2).$$

EXEMPLE 4.5. Le discriminant du polynôme $g = T^4 + a_2 T^2 + a_3 T + a_4$ est

$$\Delta = -4a_2^3 a_3^2 + 16 a_2^4 a_4 - 27 a_3^4 + 144 a_2 a_3^2 a_4 - 128 a_2^2 a_4^2 + 256 a_4^3.$$

Ou encore, le discriminant du polynôme $g = T^4 + a_1 T^3 + a_2 T^2 + a_3 T$ est

$$\Delta = a_1^2 a_2^2 a_3^2 - 4a_1^3 a_3^3 - 4a_2^3 a_3^2 + 18 a_1 a_2 a_3^3 - 27 a_3^4 = a_3^2(a_1^2 a_2^2 - 4a_1^3 a_3 - 4a_2^3 + 18 a_1 a_2 a_3 - 27 a_3^2).$$

PROPOSITION 4.6. *Soit $\psi\colon A \to B$ un morphisme d'anneaux et $\Psi\colon A[T] \to B[T]$ son extension par $\Psi(T) = T$. Soit g un polynôme unitaire dans $A[T]$. Alors $\Psi(g)$ est unitaire dans $B[T]$, et*

$$\Delta(\Psi(g)) = \psi(\Delta(g)).$$

DÉMONSTRATION. Ecrivons $g = T^n + a_1 T^{n-1} + \cdots + a_n$ avec $a_1, \ldots, a_n \in A$. Du coup,

$$\Psi(g) = T^n + \psi(a_1) T^{n-1} + \cdots + \psi(a_n).$$

Soit $\varphi\colon \mathbb{Z}[A_1, \ldots, A_n] \to A$ le morphisme définie ci-dessus qui vérifie $\varphi(A_i) = a_i$. Du coup, $\psi \circ \varphi$ est le morphisme de $\mathbb{Z}[A_1, \ldots, A_n]$ dans B satisfaisant $\psi \circ \varphi(A_i) = \psi(a_i)$. Il s'ensuit que

$$\Delta(\Psi(g)) = \psi \circ \varphi(\Delta) = \psi(\varphi(\Delta)) = \psi(\Delta(g)). \qquad \square$$

EXEMPLE 4.7. Soit $g \in \mathbb{Z}[T]$ un polynôme unitaire de degré 3 à coefficients dans $\mathbb{Z}$

$$g = T^3 + a_1 T^2 + a_2 T + a_3.$$

Si a_1 et a_2 sont impairs et a_3 est pair, alors $\Delta(g) \neq 0$ dans $\mathbb{Z}$. En effet, appliquons la proposition précédente au morphisme $\psi\colon \mathbb{Z} \to \mathbb{Z}/2$ de réduction modulo 2. On a

$$\psi(\Delta(g)) = \Delta(\Psi(g)) = \Delta(T^3 + T^2 + T) = 1^2 \cdot 1^2 - 4 \cdot 1^3 \cdot 0 - 4 \cdot 1^3 + 18 \cdot 1 \cdot 1 \cdot 1 - 27 \cdot 0^2 = 1$$

dans $\mathbb{Z}/2$. En particulier, $\psi(\Delta(g)) \neq 0$, et donc $\Delta(g) \neq 0$.

COROLLAIRE 4.8. *Soit A un sous-anneau de B et $g \in A[T]$ unitaire. Alors, le discriminant de g comme polynôme à coefficients dans B est égal au discriminant de g comme polynôme à coefficients dans A.*

PROPOSITION 4.9. *Soit A un anneau et $g \in A[T]$ un polynôme unitaire se décomposant complètement, c-à-d, il existe $x_1, \ldots, x_n \in A$ tel que*

$$g = (T - x_1)(T - x_2) \cdots (T - x_n).$$

Alors

$$\Delta(g) = \prod_{i<j} (x_i - x_j)^2.$$

DÉMONSTRATION. Soit

$$\varphi' \colon \mathbb{Z}[X_1, \dots, X_n] \to A$$

défini par $\varphi'(X_i) = x_i$ pour $i = 1, \dots, n$. Notons que φ' est une extension de φ défini ci-dessus. En effet,

$$\varphi'(A_i) = \varphi'((-1)^i \sigma_i) = (-1)^i \sigma_i(x_1, \dots, x_n) = a_i = \varphi(A_i)$$

pour $i = 1, \dots, n$. Du coup, la restriction de φ' à $\mathbb{Z}[A_1, \dots, A_n]$ est bien égale à φ. On en déduit que

$$\Delta(g) = \varphi(\Delta) = \varphi'(\Delta) = \varphi'(\prod_{i<j}(X_i - X_j)^2) = \prod_{i<j}(x_i - x_j)^2. \qquad \square$$

Soit $g \in A[T]$ unitaire. Une *racine* de g dans un anneau B contenent A comme sous-anneau est un élément $x \in B$ tel que $g(x) = 0$ dans B. Grâce à la division euclidienne dans $B[T]$ par le polynôme unitaire $T - x$, on voit que l'élément x est une racine de g dans B si et seulement si $T - x$ divise g dans $B[T]$. Une racine x de g dans un anneau B contenant A comme sous-anneau est *multiple* si $(T - x)^2$ divise g dans $B[T]$.

PROPOSITION 4.10. *Soit A un anneau et $g \in A[T]$ un polynôme unitaire.*

(1) Si g possède une racine multiple dans un anneau B contenant A comme sous-anneau, alors $\Delta(g) = 0$.

(2) Supposons que B est une algèbre de décomposition intègre de g sur A. Si $\Delta(g) = 0$, alors g possède une racine multiple dans B.

DÉMONSTRATION. On suppose que g possède une racine multiple x dans B. Soit $h \in B[T]$ tel que $g = (T - x)^2 h$. Soit C une algèbre de décomposition de h. Du coup, $h = (T - x_3) \cdots (T - x_n)$. En posant $x_1 = x_2 = x$, on a

$$g = (T - x_1) \cdots (T - x_n)$$

et $\Delta(g) = 0$ car $x_1 - x_2 = 0$. Cela montre le 1.

Quant au 2, si $\Delta(g) = 0$ dans une algèbre de décomposition intègre B de g sur A, on a

$$\prod_{i<j}(x_i - x_j)^2 = 0$$

dans B. Comme B est intègre, il existe $i < j$ tels que $x_i = x_j$. Du coup, g possède une racine multiple dans B. $\square$

EXEMPLE 4.11. Le polynôme réel $T^3 - \frac{1}{3}T + \frac{2}{27}$ a une racine multiple dans $\mathbb{C}$. En effet, il est complètement décomposé dans $\mathbb{C}[T]$ d'après le théorème fondamental de l'algèbre, et

$$\Delta = -4(-\tfrac{1}{3})^3 - 27(\tfrac{2}{27})^2 = 0.$$

On sait que le discriminant d'un polynôme de degré 2 est strictement positif si et seulement si ses racines dans $\mathbb{C}$ sont toutes réelles et distinctes. Voici la généralisation à un polynôme réel unitaire de degré quelconque :

PROPOSITION 4.12. *Soit $g \in \mathbb{R}[T]$ unitaire. Soit n le degré de g. Soit r le nombre de racines réelles de g, et s le nombre de paires de racines complexes conjugués de g, comptés avec multiplicité, de sorte que $s = \frac{1}{2}(n - r)$.*

(1) $\Delta(g) = 0$ si et seulement si g possède une racine multiple dans $\mathbb{C}$,

(2) Si $\Delta(g) > 0$, l'entier naturel s est pair, et

(3) Si $\Delta(g) < 0$, l'entier naturel s est impair.

Autrement dit, si g est à racines simples dans $\mathbb{C}$, on a

$$\operatorname{sign}(\Delta(g)) = (-1)^s.$$

DÉMONSTRATION. Le 1 est une conséquence de la proposition précédente car $\mathbb{C}$ est une algèbre de décomposition de g sur $\mathbb{R}$, d'après le Théorème fondamental de l'algèbre.

Supposons maintenant que $\Delta(g) \neq 0$ et donc que g est à racines simples dans $\mathbb{C}$. On peut supposer que les racines $x_1, \dots, x_{r+2s}$ de g dans $\mathbb{C}$ sont numérotées de telle façon que

(1) les racines $x_1, \dots, x_r$ sont réelles et $x_1 < x_2 < \cdots < x_r$, et

(2) les racines $x_{r+1}, \dots, x_{r+2s}$ sont non réelles et $x_{r+2k} = \overline{x_{r+2k-1}}$ pour $k = 1, \dots, s$.

Rappelons que

$$\Delta(g) = \prod_{i<j}(x_i - x_j)^2.$$

Soit $K_<$ l'ensemble des couples d'entiers (i,j) avec $1 \leq i,j \leq n$ et $i < j$. Soit $K_>$ l'ensemble des couples d'entiers (i,j) avec $1 \leq i,j \leq n$ et $i > j$. Soit $K_>$. On pose $K = K_< \cup K_>$. Cette réunion est bien-sûr disjointe, c-à-d, $K_< \cap K_> = \emptyset$. L'ensemble K est l'ensemble des couples d'entiers (i,j) avec $1 \leq i,j \leq n$ et $i \neq j$. Comme $K_<$ et $K_>$ on le même cardinal, et comme le cardinal de K est $n^2 - n$, le cardinal de $K_<$ est égal à $\frac{1}{2}n(n-1)$. Du coup,

$$\Delta(g) = \prod_{(i,j)\in K_<}(x_i - x_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{(i,j)\in K_<}(x_i - x_j)(x_j - x_i) = (-1)^{\frac{n(n-1)}{2}} \prod_{(i,j)\in K}(x_i - x_j).$$

Comme toutes les racines de g sont distinctes, il existe, pour tout $(i,j) \in K$, un unique couple $(i',j') \in K$ tel que

$$x_{i'} = \overline{x_i} \quad \text{et} \quad x_{j'} = \overline{x_j}.$$

On peut donc définir une application ensembliste π de K dans lui-même par $\pi(i,j) = (i',j')$. Comme $\overline{\overline{z}} = z$ pour $z \in \mathbb{C}$, on a $\pi \circ \pi = \mathrm{id}$. En particulier, l'application π est une permutation de K dont les orbites ont 1 ou 2 éléments. En fait, les orbites à 1 élément sont les couples $(i,j) \in K$ pour lesquels x_i et x_j sont réels. Les couples $(i,j) \in K$ pour lesquels x_i ou x_j est non réel appartiennent tous à une orbite à 2 éléments. Comme K est la réunion disjointes des π-orbites, on a

$$\Delta(g) = (-1)^{\frac{n(n-1)}{2}} \prod_{O} \prod_{(i,j)\in O}(x_i - x_j),$$

où O parcourt l'ensemble des π-orbites dans K. Pour une orbite O à 2 éléments, le facteur $\prod_{(i,j)\in O}(x_i - x_j)$ est un produit d'un nombre complexe non nul avec son conjugué et est donc strictement positif. Les π-orbites dans K à un seul élément sont $\{(i,j)\}$ avec x_i et x_j réel. Comme $x_i < x_j$ si et seulement si $i < j$, le facteur $\prod_{(i,j)\in O}(x_i - x_j)$ est négatif si et seulement si $i < j$, pour une orbite O à un seul élément (i,j). Du coup,

$$\mathrm{sign}\left(\prod_{O} \prod_{(i,j)\in O}(x_i - x_j)\right) = (-1)^{\frac{r(r-1)}{2}},$$

et

$$\mathrm{sign}(\Delta(g)) = (-1)^{\frac{n(n-1)}{2}} \cdot (-1)^{\frac{r(r-1)}{2}} = (-1)^{\frac{1}{2}(n(n-1)-r(r-1))}.$$

Comme

$$n(n-1) - r(r-1) = (r+2s)((r-1)+2s) - r(r-1) = 2rs + 2(r-1)s + 4s^2 = 4rs - 2s + 4s^2,$$

on obtient

$$\mathrm{sign}(\Delta(g)) = (-1)^{-s} = (-1)^s. \qquad \square$$

COROLLAIRE 4.13. *Le discriminant Δ d'un polynôme unitaire réel g de degré 3 est > 0 si et seulement si toutes ses racines sont réelles et distinctes. Le discriminant $\Delta = 0$ si et seulement si toutes ses racines sont réelles et non toutes distinctes. Le discriminant $\Delta < 0$ si et seulement si g possède exactement une seul racine réelle ; les deux autres étant non réelles complexes conjugués.*

5. Le résultant

Soient m et n des entiers naturels. Soit A un anneau et $f, g \in A[T]$ des polynômes de degré m et n respectivement. Ecrivons

$$f = a_0T^m + a_1T^{m-1} + \cdots + a_m \quad \text{et} \quad g = b_0T^n + b_1T^{n-1} + \cdots + b_n,$$

où $a_0, \ldots, a_m, b_0, \ldots, b_n \in A$, $a_0 \neq 0$, $b_0 \neq 0$. Supposons que f et g ont une racine x en commun dans A. On a donc

$$\begin{cases} a_0x^m + a_1x^{m-1} + \cdots + a_m = 0 & (1) \\ b_0x^n + b_1x^{n-1} + \cdots + b_n = 0 & (2) \end{cases}$$

dans A. Les puissances $x^{\max\{m,n\}}, \dots, x^0$ sont des solutions d'un système de deux équations linéaires à coefficients dans A en un nombre d'inconnues égal à $\max\{m,n\}+1$. Cela semble en soi pas grand chose pour seulement deux équations, mais en les multipliant par des puissances de x on va réussir à en faire un système carré. Commençons par multiplier l'équation (1) par x^j, pour $j = 0, \dots, k-1$, disons, où k est un entier naturel. On obtient, en commençant par $j = k-1$ et en écrivant sous forme matricielle,

$$\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_m & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_{m-1} & a_m & 0 & \cdots & 0 \\ 0 & 0 & a_0 & \cdots & a_{m-2} & a_{m-1} & a_m & \cdots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & a_0 & a_1 & a_2 & \cdots & a_m \end{pmatrix} \cdot \begin{pmatrix} x^{m+k-1} \\ x^{m+k-2} \\ x^{m+k-3} \\ \\ \vdots \\ x^{k-1} \\ x^{k-2} \\ x^{k-3} \\ \\ \vdots \\ x^0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Puis, multiplions l'équation (2) par x^j, pour $j = 0, \dots, x^{\ell-1}$, où ℓ est un entier naturel. On obtient

$$\begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_n & 0 & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{n-1} & b_n & 0 & \cdots & 0 \\ 0 & 0 & b_0 & \cdots & b_{n-2} & b_{n-1} & b_n & \cdots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & b_0 & b_1 & b_2 & \cdots & b_n \end{pmatrix} \cdot \begin{pmatrix} x^{n+\ell-1} \\ x^{n+\ell-2} \\ x^{n+\ell-3} \\ \\ \vdots \\ x^{\ell-1} \\ x^{\ell-2} \\ x^{\ell-3} \\ \\ \vdots \\ x^0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Pour en faire un seul système d'équations carré à partir de ces deux systèmes, il faut que le nombre de colonnes de la matrice du premier système, $m+k$, soit égal au nombre de colonnes de la deuxième matrice, $n+\ell$, et que ce nombre de colonnes soit égal au nombre total d'équations, c-à-d $k+\ell$. On a donc $k = n$ et $\ell = m$. Le système carré obtenu est, sous forme matricielle,

$$\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_m & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_{m-1} & a_m & 0 & \cdots & 0 \\ 0 & 0 & a_0 & \cdots & a_{m-2} & a_{m-1} & a_m & \cdots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & a_0 & a_1 & a_2 & \cdots & a_m \\ b_0 & b_1 & b_2 & \cdots & b_{n-1} & b_n & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{n-2} & b_{n-1} & b_n & \cdots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & b_0 & b_1 & b_2 & \cdots & b_n \end{pmatrix} \cdot \begin{pmatrix} x^{m+n-1} \\ x^{m+n-2} \\ x^{m+n-3} \\ \\ \vdots \\ x^{m-1} \\ x^{m-2} \\ x^{m-3} \\ \\ \vdots \\ x^0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Soit $r = r(f,g)$ la matrice $(m+n) \times (m+n)$ des coefficients. Cette matrice a un sens que f et g possède une racine commune dans A ou pas. Soit $\tilde{r}$ sa matrice des cofacteurs de sorte que

$$\tilde{r} \cdot r = \det(r) \cdot I_{m+n},$$

où $\det(r) \in A$ est le déterminant de la matrice r, et I_{m+n} est la matrice identité de taile $m+n$. On a vu ci-dessus que si f et g ont une racine x en commun dans A, le vecteur colonne $v = (x^{m+n-1}, \dots, x^0)$ des puissances de x est tel que $rv = 0$. Multiplier par $\tilde{r}$ donne

$$0 = \tilde{r} \cdot rv = \det(r)v.$$

Comme la dernière coordonnée de v est égal à $x^0 = 1$ dans A, on en déduit que $\det(r) = 0$ dans A.

On appelle $\det(r)$ le *résultant* des polynômes f et g, et on le note $\mathrm{Res}(f,g)$, que f et g possède une racine commun dans A ou pas. On a montré l'énoncé suivant.

PROPOSITION 5.1. *Soit A un anneau et $f, g \in A[T]$ des polynômes non nuls. Si f et g ont une racine commune dans A, alors* $\mathrm{Res}(f,g) = 0$ *dans A.*

EXEMPLE 5.2. Soit $A = \mathbb{Z}/2$ et

$$f = T^2 + T + 1 \quad \text{et} \quad g = T^3 + T + 1$$

dans $\mathbb{Z}/2[T]$. Le résultant de f et g est

$$\mathrm{Res}(f,g) = \det \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} =,$$

en développant suivant la première colonne,

$$\det \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix} + \det \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} =,$$

en développant suivant la première colonne, respectivement, la première ligne,

$$\det \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} + \det \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} + \det \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} + \det \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} =,$$

en remarquant que les premier et quatrième déterminants sont identiques, et que le deuxième est nul, et en développant le troisième suivant la première ligne,

$$\det \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \det \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = 1 \neq 0$$

Donc $\mathrm{Res}(f,g) \neq 0$. Il s'ensuit que f et g n'ont pas de racine en commun dans aucun anneau contenant $\mathbb{Z}/2$ comme sous-anneau.

Afin d'étudier le résultant, on introduit le résultant universel. Soient

$$F = A_0 T^m + A_1 T^{m-1} + \cdots + A_m \quad \text{et} \quad G = B_0 T^n + B_1 T^{n-1} + \cdots + B_n$$

deux polynômes universel en T de degré m et n respectivement. Ce sont des éléments de l'anneau polynomial

$$\mathbb{Z}[A_0, \ldots, A_m, B_0, \ldots, B_n][T]$$

en $(m+1)(n+1)+1$ indéterminées sur $\mathbb{Z}$. On pose $R = R(F,G)$ la matrice obtenue à partir de la matrice r ci-dessus en remplaçant les lettres miniscules a et b par les majuscules A et B, respectivement. Plus précisément,

$$R = \begin{pmatrix} A_0 & A_1 & A_2 & \cdots & A_m & 0 & 0 & \cdots & 0 \\ 0 & A_0 & A_1 & \cdots & A_{m-1} & A_m & 0 & \cdots & 0 \\ 0 & 0 & A_0 & \cdots & A_{m-2} & A_{m-1} & A_m & \cdots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & A_0 & A_1 & A_2 & \cdots & A_m \\ B_0 & B_1 & B_2 & \cdots & B_{n-1} & B_n & 0 & \cdots & 0 \\ 0 & B_0 & B_1 & \cdots & B_{n-2} & B_{n-1} & B_n & \cdots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & B_0 & B_1 & B_2 & \cdots & B_n \end{pmatrix}.$$

C'est une matrice carré de taille $m+n$ à coefficients dans $\mathbb{Z}[A_0, \ldots, B_n]$. Le *résultant universel* Res est le déterminnant $\det(R)$ de la matrice R. C'est un élément de l'anneau $\mathbb{Z}[A_0, \ldots, B_n]$. En fait, le résultant universel est le résultant dans le sens précédent des polynômes universels F et G. On a donc $\mathrm{Res} = \mathrm{Res}(F,G)$.

Notons que Res est un polynôme homogène en $A_0, \ldots, A_m$ de degré n, et homogène en $B_0, \ldots, B_n$ de degré m. De plus, il est non nul car le monôme $A_0^n B_n^m$ y apparaît avec coefficient égal à 1.

Le résultant universel est universel dans le sens suivant.

PROPOSITION 5.3. *Soit A un anneau et $f, g \in A[T]$ de degré m et n respectivement. Ecrivons*

$$f = a_0T^m + a_1T^{m-1} + \cdots + a_m \quad \text{et} \quad g = b_0T^n + b_1T^{n-1} + \cdots + b_n,$$

où $a_0, \ldots, a_m, b_0, \ldots, b_n \in A$. Soient

$$\varphi\colon \mathbb{Z}[A_0, \ldots, A_m, B_0, \ldots, B_n] \to A$$

le morphisme déterminé par $\varphi(A_i) = a_i$, pour $i = 0, \ldots, m$, et $\varphi(B_i) = b_i$, pour $i = 0, \ldots, n$. Alors, le résultant de f et g est égal à l'image par φ du résultant universel, c-à-d,

$$\mathrm{Res}(f, g) = \varphi(\mathrm{Res}).$$

DÉMONSTRATION. On note encore par φ le morphisme d'anneaux non commutatifs induit

$$M_{m+n}(\mathbb{Z}[A_0, \ldots, B_n]) \to M_{m+n}(A).$$

On a bien-sûr $\varphi(R) = r$. Du coup,

$$\varphi(\mathrm{Res}) = \varphi(\det(R)) = \det(\varphi(R)) = \det(r) = \mathrm{Res}(f, g). \qquad \square$$

Voici une conséquence qu'on a déjà utilisée dans un exemple ci-dessus.

COROLLAIRE 5.4. *Soit A un anneau et B un anneau contenant A comme sous-anneau. Soient $f, g \in A[T]$ non nuls. Alors, le résultant de f et g comme polynômes à coefficients dans A est égal au résultant de f et g comme polynômes à coefficients dans B.*

Soient encore F et G les polynômes universels de degré m et n, et $R = r(F, G)$ la matrice comme ci-dessus. Soit v le vecteur colonne défini par

$${}^t v = \begin{pmatrix} T^{m+n-1} & T^{m+n-2} & \cdots & 1 \end{pmatrix}$$

Calculons le produit matriciel $w = Rv$:

On a $Rv = w$ où w est le vecteur

$$\begin{pmatrix} A_0 & A_1 & A_2 & \cdots & A_m & 0 & 0 & \cdots & 0 \\ 0 & A_0 & A_1 & \cdots & A_{m-1} & A_m & 0 & \cdots & 0 \\ 0 & 0 & A_0 & \cdots & A_{m-2} & A_{m-1} & A_m & \cdots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & A_0 & A_1 & A_2 & \cdots & A_m \\ B_0 & B_1 & B_2 & \cdots & B_{n-1} & B_n & 0 & \cdots & 0 \\ 0 & B_0 & B_1 & \cdots & B_{n-2} & B_{n-1} & B_n & \cdots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & B_0 & B_1 & B_2 & \cdots & B_n \end{pmatrix} \cdot \begin{pmatrix} T^{m+n-1} \\ T^{m+n-2} \\ T^{m+n-3} \\ \vdots \\ T^{m-1} \\ T^{m-2} \\ T^{m-3} \\ \vdots \\ T^0 \end{pmatrix} = \begin{pmatrix} T^{n-1}F \\ T^{n-2}F \\ T^{n-3}F \\ \vdots \\ F \\ T^{m-1}G \\ T^{m-2}G \\ \vdots \\ G \end{pmatrix}.$$

Comme $\det(R) \neq 0$, la règle de Cramer s'applique et donne pour la dernière coordonnée 1 de v :

$$1 = \frac{\det(v_1, \ldots, v_{m+n-1}, w)}{\det(R)},$$

dans le corps des fractions de l'anneau $\mathbb{Z}[A_0, \ldots, B_n, T]$, où $v_1, \ldots, v_{m+n}$ sont les colonnes de la matrice R. Multiplier par $\det(R)$ donne

$$\mathrm{Res} = \det(v_1, \ldots, v_{m+n-1}, w)$$

dans l'anneau $\mathbb{Z}[A_0, \ldots, B_n, T]$. Lorsqu'on calcule le dernier déterminant en développant suivant la dernière colonne on obtient l'énoncé suivant.

PROPOSITION 5.5. *Il existe des polynômes*

$$U, V \in \mathbb{Z}[A_0, \ldots, A_m, B_0, \ldots, B_n][T]$$

de degré au plus $n-1$ et $m-1$, respectivement, tels que

$$\mathrm{Res} = UF + VG$$

dans $\mathbb{Z}[A_0, \ldots, B_n][T]$. En particulier,

$$\mathrm{Res} \in (F, G) \cap \mathbb{Z}[A_0, \ldots, B_n].$$

On en déduit comme d'habitude un énoncé analogue pour le résultant de deux polynômes en T à coefficients dans un anneau A :

COROLLAIRE 5.6. *Soit A un anneau et $f, g \in A[T]$ de degré m et n, respectivement. Il existe des polynômes*

$$u, v \in A[T]$$

de degré au plus $n-1$ et $m-1$, respectivement, tels que

$$\mathrm{Res}(f,g) = uf + vg$$

dans $A[T]$. En particulier,

$$\mathrm{Res}(f,g) \in (f,g) \cap A.$$

Ce dernier énoncé fournit encore une démonstration du fait que le résultant $\mathrm{Res}(f,g)$ s'annule lorsque f et g ont une racine en commun. En effet, si $f(x) = g(x) = 0$, on a aussi

$$\mathrm{Res}(f,g)(x) = u(x)f(x) + v(x)g(x) = 0.$$

Or, $\mathrm{Res}(f,g)$ est un polynôme constant. Donc $\mathrm{Res}(f,g)(x) = \mathrm{Res}(f,g)$, et $\mathrm{Res}(f,g) = 0$ dans A.

Maintenant on va étudier la réciproque, et déterminer des conditions sous lesquelles f et g ont une racine en commun lorsque $\mathrm{Res}(f,g) = 0$.

Soient F et G de nouveau les polynômes universels de degré m et n, respectivement. Considérons la localisation

$$\mathbb{Z}[A_0, \ldots, A_n, B_0, \ldots, B_n]_{A_0B_0}$$

de $\mathbb{Z}[A_0, \ldots, B_n]$ où A_0B_0 est rendu inversible. Dans cette localisation A_0 et B_0 sont inversibles, et les polynômes

$$\tfrac{1}{A_0}F \quad \text{et} \quad \tfrac{1}{B_0}G \in \mathbb{Z}[A_0, \ldots, A_n, B_0, \ldots, B_n]_{A_0B_0}[T]$$

sont unitaires. L'anneau $\mathbb{Z}[A_0, \ldots, B_n]_{A_0B_0}$ est un anneau de polynômes en

$$\tfrac{A_1}{A_0}, \ldots, \tfrac{A_m}{A_0}, \tfrac{B_1}{B_0}, \ldots, \tfrac{B_n}{B_0}$$

a coefficients dans $\mathbb{Z}[A_0, B_0]_{A_0B_0}$. On peut donc l'identifier un sous anneau de l'anneau

$$\mathbb{Z}[A_0, B_0, X_1, \ldots, X_m, Y_1, \ldots, Y_n]_{A_0B_0}$$

en identifiant

$$\tfrac{A_i}{A_0} = (-1)^i\sigma_i(X_1, \ldots, X_m) \quad \text{et} \quad \tfrac{B_j}{B_0} = (-1)^j\sigma_j(Y_1, \ldots, Y_n)$$

pour $i = 1, \ldots, m$ et $j = 1, \ldots, n$. Du coup, on a

$$F = A_0(T - X_1)\cdots(T - X_m) \quad \text{et} \quad G = B_0(T - Y_1)\cdots(T - Y_n)$$

dans $\mathbb{Z}[A_0, X_1, \ldots, X_m, B_0, Y_1, \ldots, Y_n][T]$. On montre l'énoncé suivant :

PROPOSITION 5.7.

$$\mathrm{Res} = A_0^n B_0^m \prod_{i=1}^{m}\prod_{j=1}^{n}(X_i - Y_j)$$

dans $\mathbb{Z}[A_0, X_1, \ldots, X_m, B_0, Y_1, \ldots, Y_n]$. En particulier,

$$\mathrm{Res} = A_0^n \prod_{i=1}^{m} G(X_i) \quad \text{et} \quad \mathrm{Res} = (-1)^{mn} B_0^m \prod_{j=1}^{n} F(Y_i)$$

dans $\mathbb{Z}[A_0, X_1, \ldots, X_m, B_0, \ldots, B_n]$ et $\mathbb{Z}[A_0, \ldots, A_m, B_0, Y_1, \ldots, Y_n]$, respectivement.

DÉMONSTRATION. Soient i et j des entiers avec $1 \leq i \leq m$ et $1 \leq j \leq n$. Les images de F et G dans l'anneau quotient

$$\mathbb{Z}[A_0, X_1, \ldots, X_m, B_0, Y_1, \ldots, Y_n]/(X_i - Y_j)[T]$$

ont une racine commune à savoir $\overline{X}_i = \overline{Y}_j$. Du coup, l'image de Res dans

$$\mathbb{Z}[A_0, X_1, \ldots, X_m, B_0, Y_1, \ldots, Y_n]/(X_i - Y_j)$$

est égal à 0. Cela veut dire que $X_i - Y_j$ divise Res dans $\mathbb{Z}[A_0, X_1, \ldots, X_m, B_0, Y_1, \ldots, Y_n]$, quels que soient i et j. Comme les élments $X_i - Y_j$ de l'anneau de polynômes $\mathbb{Z}[A_0, X_1, \ldots, X_m, B_0, Y_1, \ldots, Y_n]$ sont irrductibles et deux-à-deux non associés, le produit

$$\prod_{i=1}^{m}\prod_{j=1}^{n}(X_i - Y_j)$$

divise Res dans $\mathbb{Z}[A_0, X_1, \ldots, X_m, B_0, Y_1, \ldots, Y_n]$. Comme

$$F = A_0T^m - A_0\sigma_1(X_1, \ldots, X_m)T^{m-1} + \cdots + (-1)^m A_0\sigma_m(X_1, \ldots, X_m)$$

et

$$G = B_0T^n - B_0\sigma_1(Y_1,\dots,Y_n)T^{n-1} + \cdots + (-1)^n B_0\sigma_n(Y_1,\dots,Y_n)$$

dans $\mathbb{Z}[A_0, X_1, \dots, X_m, B_0, Y_1, \dots, Y_n][T]$, on voit que $A_0^n B_0^m$ divise Res dans $\mathbb{Z}[A_0, X_1, \dots, X_m, B_0, Y_1, \dots, Y_n]$. Au final, le produit

$$P = A_0^n B_0^m \prod_{i=1}^{m}\prod_{j=1}^{n}(X_i - Y_j)$$

divise Res dans $\mathbb{Z}[A_0, X_1, \dots, X_m, B_0, Y_1, \dots, Y_n]$. On peut réécrire

$$P = A_0^n \prod_{i=1}^{m}\left(B_0\prod_{j=1}^{n}(X_i - Y_j)\right) = A_0^n\prod_{i=1}^{m}G(X_i).$$

Du coup,

$$P \in \mathbb{Z}[A_0, X_1, \dots, X_m, B_0, \dots, B_n][T],$$

et il est homogène en $B_0, \dots, B_n$ de degré m. De même manière on montre que

$$P = (-1)^{mn}B_0^n\prod_{j=1}^{n}F(Y_j)$$

de sorte que

$$P \in \mathbb{Z}[A_0, \dots, A_m, B_0, Y_1, \dots, Y_n][T]$$

est homogène en $A_0, \dots, A_n$ de degré n. Il s'ensuit que

$$P \in \mathbb{Z}[A_0, \dots, A_m, B_0, \dots, B_n][T]$$

est homogène en $A_0, \dots, A_m$ de degré n et homogène en $B_0, \dots, B_n$ de degré m. Comme Res possède exactement la même propriété d'homogénéité, il existe $\lambda \in \mathbb{Z}$ tel que $P = \lambda\,\mathrm{Res}$. Comme P et Res comportent tous les deux le monôme $A_0^n B_n^m$ avec coefficients 1, on a $\lambda = 1$. □

Corollaire 5.8. *Soit A un anneau et $f, g \in A[T]$ de degré m et n respectivement. Supposons qu'il existe un anneau B contenant A comme sous-anneau dans lequel f est g se décomposent complètement. Alors,*

$$\mathrm{Res}(f,g) = a_0^n b_0^m \prod_{i=1}^{m}\prod_{j=1}^{n}(x_i - y_j)$$

dans B.

Un tel anneau existe si a_0 et b_0 sont des éléments réguliers dans A.

Corollaire 5.9. *Soit A un anneau et $f, g \in A[T]$ de degré m et n respectivement. Supposons qu'il existe un anneau intègre B contenant A comme sous-anneau dans lequel f est g se décomposent complètement. Alors, f et g ont une racine commune dans B si et seulement si* $\mathrm{Res}(f,g) = 0$ *dans A.*

Avant de pouvoir donner le lien entre le résultant et le discriminant, on introduit la dérivée formelle d'un polynôme.

Soit A un anneau et

$$f = a_0T^m + a_1T^{m-1} + \cdots + a_{m-1}T + a_m$$

un polynôme dans $A[T]$. La *dérivée* de f est le polynôme

$$f' = ma_0T^{m-1} + (m-1)a_1T^{m-2} + a_{m-1}.$$

On a les règles de calcul plus ou moins habituelles :

(1) $(f+g)' = f' + g'$,
(2) $(fg)' = f'g + fg'$,
(3) $a' = 0$, et
(4) $\deg(f') \leq \deg(f) - 1$.

quels que soient $f, g \in A[T]$ et $a \in A$. Notons qu'on n'a pas forcément $\deg(f') = \deg(f) - 1$ même si $\deg(f) \geq 1$ comme montre l'exemple suivant.

Exemple 5.10. Soit $f = T^{2k}$ dans $\mathbb{Z}/2[T]$, où k est un entier naturel non nul. Alors, $f' = 2kT^{2k-1} = 0$ dans $\mathbb{Z}/2[T]$. Donc $\deg(f') = -\infty$, tandis que $\deg(f) = 2k$.

PROPOSITION 5.11. *Soit $f \in A[T]$ de degré $m \geq 1$. Soit a_0 le coefficient dominant de f. Alors $\deg(f') = \deg(f) - 1$ si et seulement si $ma_0 \neq 0$ dans A.*

DÉMONSTRATION. Exercice. □

PROPOSITION 5.12. *Soit*

$$F = A_0(T - X_1)\dots(T - X_m)$$

le polynôme universel complètement décomposé en T de degré $m \geq 1$. Soit F' sa dérivée. Alors,

$$\operatorname{Res}(F, F') = A_0^{2m-1} \prod_{\substack{i,j=1 \\ i\neq j}}^{m} (X_i - X_j).$$

DÉMONSTRATION. On a

$$F' = A_0 \sum_{j=1}^{m} (T - X_1)\cdots\widehat{(T - X_j)}\cdots(T - X_m),$$

où le chapeau au-dessus d'un facteur signifie que celui-ci est ôté. En particulier,

$$F'(X_i) = A_0(X_i - X_1)\cdots\widehat{(X_i - X_i)}\cdots(X_i - X_m).$$

Notons que F' est bien de degré $m - 1$. D'après un corollaire précédent, on a donc

$$\operatorname{Res}(F, F') = A_0^{m-1} \prod_{i=1}^{m} F'(X_i) = A_0^{2m-1} \prod_{\substack{i,j=1 \\ i\neq j}}^{m} (X_i - X_j). \qquad \square$$

COROLLAIRE 5.13. *Soit A un anneau et $f \in A[T]$ unitaire. Soit $m = \deg(f)$. Supposons que $m \neq 0$ dans A. Alors,*

$$\operatorname{Res}(f, f') = (-1)^{\frac{m(m-1)}{2}} \Delta(f).$$

Comme on a donc

$$\Delta(f) = (-1)^{\frac{m(m-1)}{2}} \operatorname{Res}(f, f')$$

pour un polynôme unitaire, on s'attendrait à ce qu'on définit le discriminant pour un polynôme non nécessairement unitaire par cette formule. Cependant, comme $\operatorname{Res}(F, F')$ est divisible par A_0 dans $\mathbb{Z}[A_0, \dots, A_m]$ pour le polynôme universel F de degré m dans $\mathbb{Z}[A_0, \dots, A_m][T]$, on définit

$$\Delta(F) = (-1)^{\frac{m(m-1)}{2}} \tfrac{1}{A_0} \operatorname{Res}(F, F')$$

dans $\mathbb{Z}[A_0, \dots, A_m]$. Du coup, si $f \in A[T]$ est de degré m non nécessairement unitaire mais tel que $\deg(f') = \deg(f) - 1$, on définit le *discriminant* de f par

$$\Delta(f) = \varphi(\Delta(F))$$

où

$$\varphi\colon \mathbb{Z}[A_0, \dots, A_m] \to A$$

est le morphisme défini par $\varphi(A_i) = a_i$ pour $i = 0, \dots, m$. Cela coïncide avec la définition du paragraphe précédent lorsque f est unitaire, d'après ce qu'on vient de voir.

EXEMPLE 5.14. Soit $F = AT^2 + BT + C$ le polynôme universel de degré 2 en T. Déterminons $\Delta(F)$. On a $F' = 2AT + B$. Du coup,

$$\Delta(F) = (-1)\tfrac{1}{A} \operatorname{Res}(F, F') = \det \begin{pmatrix} A & B & C \\ 2A & B & 0 \\ 0 & 2A & B \end{pmatrix} =,$$

en développant suivant la première colonne,

$$= -\det \begin{pmatrix} B & 0 \\ 2A & B \end{pmatrix} + 2\det \begin{pmatrix} B & C \\ 2A & B \end{pmatrix} = -B^2 + 2B^2 - 4AC = B^2 - 4AC.$$

Du coup, si $f = aT^2 + bT + c$ dans $A[T]$ avec $2a \neq 0$ dans A, on a

$$\Delta(f) = b^2 - 4ac,$$

comme il se doit.

Chapitre 3

Extensions de corps et Théorie de Galois

1. Sous-corps

Soient K et L des corps. Un *morphisme de corps* de K dans L est un morphisme d'anneaux de K dans L. De même pour un *isomorphisme*, *endomorphisme* et *automorphisme de corps*. Soit K un corps. Un *sous-corps* de K est un sous-anneau qui est un corps.

On a vu que tout morphisme de corps $f\colon K \to L$ est injectif. On pourra donc identifier K avec son image $f(K)$ dans L, et le considérer comme sous-corps de L. D'ailleurs, c'est ce qui s'est fait dans tous les exemples ci-dessous.

Exemple 1.1. 1. Le corps $\mathbb{Q}$ des nombres rationnels est un sous-corps du corps $\mathbb{R}$ des nombres réels.

2. Le corps $\mathbb{R}$ est un sous-corps du corps $\mathbb{C}$ des nombres complexes.

3. Soit K un corps. Le corps K est un sous-corps du corps $K(X)$ des fractions rationnelles en X sur K. Plus généralement, K est un sous-corps de $K(X_1, \ldots, X_n)$.

Proposition 1.2. *Soit $f\colon K \to L$ un morphisme de corps.*

(1) Si M est un sous-corps de K, alors $f(M)$ est un sous-corps de L.

(2) Si M est un sous-corps de L, alors $f^{-1}(M)$ est un sous-corps de K.

Démonstration. 1. La restriction $f_{|M}$ de f à M est un morphisme de corps de M dans L. Comme $f_{|M}$ est un isomorphisme sur son image, l'anneau image $f_{|M}(M) = f(M)$ est un corps. C'est donc un sous-corps de L.

2. L'image réciproque $f^{-1}(M)$ est un sous-anneau de K. La restriction $f_{|f^{-1}M}$ de f à $f^{-1}(M)$ est injectif car f l'est. C'est donc un isomorphisme d'anneaux sur son image. Or, l'image de $f_{|f^{-1}(M)}$ est égal à $M \cap f(K)$. Comme M et $f(K)$ sont des sous-corps de L, leur intersection $M \cap f(K)$ en est un d'après la proposition ci-dessous. Il s'ensuit que $f^{-1}(M)$ est un corps. C'est donc un sous-corps de K. □

Proposition 1.3. *Soit K un corps et $\mathcal{C}$ une collection de sous-corps de K. Alors, l'intersection $\bigcap \mathcal{C}$ est un sous-corps de K.*

Démonstration. Exercice. □

Corollaire 1.4. *Soit K un corps. Alors K contient un plus petit sous-corps.*

Définition 1.5. Ce plus petit sous-corps d'un corps s'appelle son *sous-corps premier*.

Proposition 1.6. *Soit K un corps. Soit $f\colon \mathbb{Z} \to K$ l'unique morphisme d'anneaux de $\mathbb{Z}$ dans K. Alors, de deux choses une, ou bien*

(1) f est injectif et induit un morphisme f' de $\mathbb{Q}$ dans K ; le sous-corps premier de K est l'image de f' et est donc isomorphe à $\mathbb{Q}$, ou bien

(2) f n'est pas injectif, son noyau est de la forme $p\mathbb{Z}$ avec p un nombre premier, et il induit un morphisme $\bar{f}$ de $\mathbb{Z}/p\mathbb{Z}$ dans K ; le sous-corps premier de K est l'image de $\bar{f}$ et est donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Démonstration. Si f est injectif, l'image de tout élément non nul de $\mathbb{Z}$ est inversible dans K. Le morphisme f induit donc un morphisme f' du corps des fractions $\mathbb{Q}$ de $\mathbb{Z}$ dans K. Le morphisme f' est forcément injectif et est donc un isomorphisme sur son image. Afin de montrer que $f'(\mathbb{Q})$ est le sous-corps premier de K, soit L un sous-corps de K. D'après la propriété universelle de $\mathbb{Z}$, on a $f(\mathbb{Z}) \subseteq L$. D'après la propriété universelle du corps des fractions, $f'(\mathbb{Q}) \subseteq L$. Cela montre bien que $f'(\mathbb{Q})$ est le sous-corps premier de K.

Si f n'est pas injectif, le morphisme induit $\bar{f}$ de $\mathbb{Z}/\ker(f)$ dans K est un isomorphisme sur son image. En particulier, $\mathbb{Z}/\ker(f)$ est intègre. Du coup $\ker(f)$ est premier. Comme $\ker(f) \neq \{0\}$, il existe un nombre premier p tel que $\ker(f) = p\mathbb{Z}$. Afin de montrer que $\bar{f}(\mathbb{Z}/p\mathbb{Z})$ est le sous-corps premier de K, soit L un sous-corps de K. D'après la propriét universelle de $\mathbb{Z}$, on a $f(\mathbb{Z}) \subseteq L$. Comme $\bar{f}(\mathbb{Z}/p\mathbb{Z}) = f(Z)$, l'image de $\bar{f}$ est contenu dans L. Cela montre bien que $\bar{f}(\mathbb{Z}/p\mathbb{Z})$ est le sous-corps premier de K. □

En théorie de corps, il est habituel de noter $\mathbb{F}_p$ au lieu de $\mathbb{Z}/p\mathbb{Z}$, pour p un nombre premier.

COROLLAIRE 1.7. *Soit K un corps. De deux chose une, ou bien son sous-corps premier est isomorphe à $\mathbb{Q}$, ou bien son sous-corps premier est isomorphe à $\mathbb{F}_p$, où p est un nombre premier. De plus, l'isomorphisme en question est unique.*

COROLLAIRE 1.8. *Le seul automorphisme du corps $\mathbb{Q}$ est l'identité. Le seul automorphisme du corps $\mathbb{F}_p$, où p est un nombre premier, est l'identité.*

Soit K un corps. Si son sous-corps premier est isomorphe à $\mathbb{Q}$, on dit que K est de *caractéristique nulle*. Si son sous-corps premier est isomorphe à $\mathbb{F}_p$, on dit K est de *caractristique p*. Comme l'isomorphisme est unique, on peut identifier de manière non ambigue $\mathbb{Q}$ avec son image dans K dans le premier cas, et $\mathbb{F}_p$ avec son image dans K dans le deuxième cas. Comme les corps $\mathbb{Q}$ et $\mathbb{F}_p$, avec p premier, sont deux-à-deux non isomorphes, la *caractéristique* d'un corps est bien défini. Il peut être 0 ou égal à un nombre premier. On le note $\mathrm{car}(K)$.

PROPOSITION 1.9. *Soit $f\colon K \to L$ un morphisme de corps. Alors $\mathrm{car}(K) = \mathrm{car}(L)$. Soit $\mathbb{F}$ le sous-corps premier commun de K et L. Alors, la restriction de f à $\mathbb{F}$ est égale à l'identité.*

DÉMONSTRATION. L'image réciproque $f^{-1}(\mathbb{F})$ du sous-corps $\mathbb{F}$ de L est un sous-corps de K, et contient donc le sous-corps premier de K. Du coup, $f(\mathbb{F}) \subseteq \mathbb{F}$. Comme $f(\mathbb{F})$ est un sous-corps de L, on a aussi $f(\mathbb{F}) \supseteq \mathbb{F}$. Du coup, la restrictin de f à $\mathbb{F}$ est un automorphisme de $\mathbb{F}$ et est égal à l'identité. □

Notons temporairement $\mathbb{F}_0$ pour $\mathbb{Q}$.

COROLLAIRE 1.10. *Le seul morphisme de corps de $\mathbb{F}_p$ vers $\mathbb{F}_{p'}$, où p et p' sont premiers ou nuls, est l'identité. En particulier, il n'y a aucun morphisme de $\mathbb{F}_p$ vers $\mathbb{F}_{p'}$ si $p \neq p'$.*

PROPOSITION 1.11. *Soit K un corps de caractéristique non nul. Soit $p = \mathrm{car}(K)$. Alors $p = 0$ dans K, et p est le plus petit entier strictement positif ayant cette propriété.*

DÉMONSTRATION. Comme K est de caractéristique $p \neq 0$, on peu supposer que K contient $\mathbb{F}_p$ comme sous-corps. On a bien sur $p = 0$ dans $\mathbb{F}_p$ et donc aussi $p = 0$ dans K. De plus, un entier n est égal à 0 dans K si et seulement s'il est 0 dans $\mathbb{F}_p$. Un entier n est égal à 0 dans $\mathbb{F}_p$ si et seulement s'il est divisible par p. Le plus petit entier n strictement positif tel que $n = 0$ dans K est donc bien égal à p. □

PROPOSITION 1.12. *Soit K un corps de caractéristique non nul. Soit $p = \mathrm{car}(K)$. Alors, l'application*

$$\varphi\colon K \to K$$

défini par $\varphi(x) = x^p$ est un endomorphisme de corps.

On l'appelle l'*endomorphisme de Frobenius*.

DÉMONSTRATION. C'est un cas particulier de l'endomorphisme d'anneaux de Frobenius d'un anneau A dans lequel $p = 0$. □

PROPOSITION 1.13. *Tout corps fini est de caractéristique non nulle.*

Le réciproque est bien-sûr faux :

EXEMPLE 1.14. Soit p un nombre premier. Le corps $\mathbb{F}_p(X)$ est un corps infini de caractéristique p.

2. Extensions de corps

Soit K un corps. Une *extension* de K est un corps L contenant K comme sous-corps. On écrit L/K pour dire que L est une extension de K. Il n'y aura pas de confusion avec le quotient de L par K en tant que groupes abéliens, par exemple, car on ne considérera jamais ce genre de quotient dans ce chapitre.

EXEMPLE 2.1. 1. Le corps $\mathbb{R}$ des nombres réels est une extension du corps $\mathbb{Q}$ des nombres rationnels.

2. Le corps $\mathbb{C}$ des nombres complexes est une extension du corps $\mathbb{R}$.

4. Si K est un corps, le corps $K(X)$ des fractions rationnelles en X à coefficients dans K est une extension de K. Plus généralement, $K(X_1, \dots, X_n)$ est une extension de K.

5. Soit K un corps et $P \in K[X]$ un polynôme irréductible. Comme l'idéal (P) est maximal, $L = K[X]/(P)$ est un corps. Du coup, L est une extension de K. Plus généralement, soit m un idéal maximal dans $K[X_1, \dots, X_n]$. Il en existe car $K[X_1, \dots, X_n]$ est un anneau non nul. Soit $L = K[X_1, \dots, X_n]/m$. Alors L est une extension de K.

6. Tout corps K est extension de son sous-corps premier. Autrement dit, tout corps K est sot extension de $\mathbb{Q}$, soit extension de $\mathbb{F}_p$, où p est un nombre premier.

Soit L/K et M/K deux extensions de K. Un *morphisme d'extensions de* K de L/K vers M/K est un morphisme d'anneaux $f\colon L \to M$ dont la restriction $f_{|K}$ à K est l'identité, c-à-d, on a $f(x) = x$ pour tout $x \in K$. Si f est un tel morphisme, on note $f\colon L/K \to M/K$. Un *isomorphisme d'extensions de* K de L/K vers M/K est un morphisme $f\colon L/K \to M/K$ pour lequel il existe un morphisme $g\colon M/K \to L/K$ avec $f \circ g = \mathrm{id}$ et $g \circ f = \mathrm{id}$. De manière équivalente, le morphisme d'extensions f est un isomorphisme de L/K vers M/K si $f\colon L \to M$ est bijectif. S'il existe un isomorphisme de L/K vers M/K on dit que les extensions L/K et M/K sont *isomorphes*, et on note $L/K \cong M/K$. En morphisme d'extensions de L/K dans elle-même est un *endomorphisme d'extensions*. Un isomorphisme de L/K dans elle-même est un *automorphisme d'extensions*.

EXEMPLE 2.2. 1. La conjugaison complexe $\sigma\colon \mathbb{C} \to \mathbb{C}$, définie par $\sigma(z) = \overline{z}$, est un morphisme de l'extension $\mathbb{C}/\mathbb{R}$ dans elle-même. C'est donc un endomorphisme de $\mathbb{C}/\mathbb{R}$. Comme $\sigma \circ \sigma = \mathrm{id}$, l'endomorphisme σ est un automorphisme de $\mathbb{C}/\mathbb{R}$.

2. Soit K un corps et $f\colon K[X] \to K[X]$ le morphisme défini par $f(P) = P(X^2)$ pour tout $P \in K[X]$. Comme f est injectif, f induit un morhisme $f'\colon K(X) \to K(X)$. En fait,

$$f'(\tfrac{P}{Q}) = \tfrac{P(X^2)}{Q(X^2)}$$

pour toute fraction $\frac{P}{Q}$ dans $K(X)$. Comme $f'(x) = x$ pour tout $x \in K$, l'application f' est un morphisme d'extensions de $K(X)/K$ dans elle-même. C'est donc un endomorphisme de $K(X)/K$. On pourra vérifier que f n'est pas un automorphisme d'extension.

3. Soit $f\colon K \to L$ un morphisme de corps. Soit $\mathbb{F}$ le sous-corps premier commun de K et L. Le morphisme f est automatiquement un morphisme d'extensions de $K/\mathbb{F}$ vers $L/\mathbb{F}$.

Soit L/K une extension. Une *sous-extension* ou *extension intermédiaire* de L/K est un sous-corps M de L contenant K. En particulier, M/K est une extension de K, mais L/M est également une extension de M. On appelle $L/M/K$ une *tour d'extensions*.

PROPOSITION 2.3. *Soit L/K une extension de corps. Soit S un sous-ensemble de L. Alors, il existe une plus petite sous-extension de L/K contenant S.*

DÉMONSTRATION. Soit $\mathcal{C}$ la collection de sous-extension M de L/K contenant S. L'intersection $\bigcap \mathcal{C}$ est alors la plus petite sous-extension de L/K contenant S. □

On le note $K(S)$ et on l'appelle la sous-extension de L/K *engendrée par* S ou encore la sous-extension de L/K obtenue à partir de K *en adjoignant* les éléments de S. Plus explicitement, on a

$$K(S) = \{\tfrac{P(s_1,\dots,s_n)}{Q(s_1,\dots,s_n)} \mid s_1, \dots, s_n \in S,\ P, Q \in K[X_1, \dots, X_n],\ Q(s_1, \dots, s_n) \neq 0,\ n \in \mathbb{N}\},$$

comme on montre facilement. Au cas où S est fini, disons $\{s_1, \dots, s_n\}$, on écrit $K(s_1, \dots, s_n)$ au lieu de $K(\{s_1, \dots, s_n\})$. On a donc

$$K(s_1, \dots, s_n) = \{\tfrac{P(s_1,\dots,s_n)}{Q(s_1,\dots,s_n)} \mid P, Q \in K[X_1, \dots, X_n],\ Q(s_1, \dots, s_n) \neq 0\}.$$

En particulier,

$$K(s) = \{\tfrac{P(s)}{Q(s)} \,|\, P, Q \in K[X],\ Q(s) \neq 0,\ n \in \mathbb{N}\}.$$

Observons que

$$K(s_1, \ldots, s_n) = K(s_1, \ldots, s_{n-1})(s_n)$$

pour tout entier naturel n.

Noter qu'il n'y a pas de confusion avec la notation $K(X)$ ou même $K(X_1, \ldots, X_n)$ pour les corps de fractions rationnelles. En effet, $K(X)$ est bien la plus petite sous-extension de $K(X)/K$ contenant X, et de même pour $K(X_1, \ldots, X_n)$.

On fera bien attention de distinguer entre $K[S]$ et $K(S)$. Le premier est le sous-anneau de L obtenu à partir de K en adjoignant les éléments de S, le dernier est le sous-corps de L obtenu à partir de K en adjoingnant les éléments de S. On a donc $K[S] \subseteq K(S)$. Qu'ils ne sont pas forcément égaux se voit dans l'exemple de l'anneau de polynômes $K[X]$ qui n'est pas égal à $K(X)$.

EXEMPLE 2.4. Le sous-anneau $\mathbb{Q}[i] = \{a + bi \,|\, a, b \in \mathbb{Q}\}$ et un sous-corps de $\mathbb{C}$, comme on vérifie facilement. On a donc $\mathbb{Q}(i) = \mathbb{Q}[i]$ ce qui montre qu'on peut avoir $K[s] = K(s)$. Notons de plus que le corps $\mathbb{Q}(i)$ n'est pas isomorphe à $\mathbb{Q}(X)$ en tant qu'anneau.

Soit L/K une extension de corps. La restriction de la loi de multiplication sur L à $K \times L$ donne une loi externe

$$\cdot : K \times L \to L.$$

Il est immédiat que L est un K-espace vectoriel sous cette loi externe.

DÉFINITION 2.5. Le *degré* de l'extension L/K est la dimension de L comme K-espace vectoriel. On le note $[L : K]$. Si L/K est une extension de degré fini, on dit que L/K est une *extension finie*.

Notons que le degré d'une extension est un entier naturel non nul.

EXEMPLE 2.6. 1. L'extension $\mathbb{C}/\mathbb{R}$ est une extension de degré fini. En effet, $1, i$ est une $\mathbb{R}$-base de $\mathbb{C}$. Donc $\mathbb{C}/\mathbb{R}$ est finie et $[\mathbb{C} : \mathbb{R}] = 2$.

2. L'extension $\mathbb{Q}(i)/\mathbb{Q}$ est une extension finie et son degré est égal à 2.

3. Soit K un corps. L'extension $K(X)/K$ est un extension infinie.

4. L'extension $\mathbb{R}/Q$ est infinie. En effet, $\mathbb{Q}$ étant dénombrable et $\mathbb{R}$ étant non dénombrable, le degré de $\mathbb{R}/\mathbb{Q}$ est même non dénombrable.

5. Soit K un corps et $P \in K[X]$ irréductible. Soit $L = K[X]/(P)$. Alors L est une extension finie de K et

$$[L : K] = \deg(P),$$

ce qui explique sans doute la terminologie de degré pour la dimension de L comme K-espace vectoriel.

PROPOSITION 2.7. *Soit $M/L/K$ une tour d'extensions telle que L/K et M/L sont des extensions finies. Alors M/K est une extension finie et*

$$[M : K] = [M : L] \cdot [L : K].$$

DÉMONSTRATION. Soit $x_1, \ldots, x_m$ une K-base de L, Soit $y_1, \ldots, y_n$ une L-base de M. Montrons que $x_i y_i$, $i = 1, \ldots, m$, $j = 1, \ldots, n$, est une K base de M.

Soit $y \in M$. Comme $y_1, \ldots, y_n$ est une L-base de M, il existe $\lambda_1, \ldots, \lambda_n \in L$ tels que

$$y = \lambda_1 y_1 + \cdots + \lambda_n y_n.$$

Comme $x_1, \ldots, x_m$ est une K-base de L, il existe $\mu_{ij} \in K$ tels que

$$\lambda_j = \mu 1 j x_1 + \cdots + \mu_{mj} x_m$$

pour $j = 1, \ldots, n$. Du coup,

$$y = \sum_{j=1}^{n} \lambda_j y_j = \sum j = 1^n (\sum_{i=1}^{n} \mu_{ij} x_i) y_j = \sum_{i,j=1}^{m,n} \mu_{ij} x_i y_j.$$

Cela montre bien que la famille $x_i y_j$, $i = 1, \ldots, m$, $j = 1, \ldots, n$, est bien génératrice du K-espace vectoriel M.

Montrons qu'elle est libre. Soient $\mu_{ij} \in K$ tels que

$$\sum_{i,j=1}^{m,n} \mu_{ij} x_i y_j = 0$$

dans M. Récrivons-la comme

$$\sum_{j=1}^{n}(\sum_{i=1}^{n}\mu_{ij}x_i)y_j = 0.$$

Comme $\sum_i \mu_{ij}x_i \in L$ pour tout j, et comme $y_1, \ldots, y_n$ est L-libre, on a

$$\sum_{i=1}^{n}\mu_{ij}x_i = 0$$

pour tout j. Comme $\mu_{ij} \in K$ et $x_1, \ldots, x_m$ est K-libre, on a $\mu_{ij} = 0$ pour tout i et pour tout j. Cela montre bien que la famille x_iy_j, $i = 1, \ldots, m$, $j = 1, \ldots, n$, est K-libre. C'est donc une K-base de M.

On en déduit que M/K est une extension finie et que

$$[M : K] = \dim_K(M) = mn = \dim_K(L) \cdot \dim_L(M) = [L : K] \cdot [M : L]. \qquad \square$$

COROLLAIRE 2.8. *Soit L/K une extension finie. Alors toute sous-extension M/K de L/K est finie et $[M : K]$ divise $[L : K]$. En particulier, lorsque $[L : K]$ est un nombre premier, les seules sous-extensions M/K de L/K sont les triviales : $M = K$ ou $M = L$.*

THÉORÈME 2.9. *Soit K un corps fini. Soit $p = \mathrm{car}(K)$ de sorte que K soit une extension de son sous-corps premier $\mathbb{F}_p$. Alors, l'extension $K/\mathbb{F}_p$ est finie. En particulier, il existe un entier non nul n tel que K est isomorphe comme $\mathbb{F}_p$ espace vectoriel à $\mathbb{F}_p^n$. Du coup,*

$$|K| = p^n.$$

DÉMONSTRATION. L'espace vectoriel K sur $\mathbb{F}_p$ est de dimensions finie car K et possède une famille génératrice finie sur $\mathbb{F}_p$ à savoir K lui-même. Du coup, l'extension $K/\mathbb{F}_p$ est finie. Soit $n = [K : \mathbb{F}_p]$. Comme tout espace vectoriel de dimension n sur $\mathbb{F}_p$, le corps K est isomorphe à $\mathbb{F}_p^n$ comme espace vectoriel. $\square$

On verra qu'il existe, pour tout entier naturel non nul et pour tout nombre premier p, un corps K de cardinal p^n. Il est très important de bien réaliser que ce corps K est donc seulement isomorphe à $\mathbb{F}_p^n$ comme $\mathbb{F}_p$-espace vectoriel. Il n'est pas isomorphe à l'anneau $\mathbb{F}_p^n = \mathbb{F}_p \times \cdots \times \mathbb{F}_p$, sauf si $n = 1$ bien-sûr.

COROLLAIRE 2.10. *Le cardinal d'un corps fini est une puissance d'un nombre premier.*

EXEMPLE 2.11. Il n'existe pas de corps à 6 éléments. Il est très instructif de vérifier cet énoncé directement à partir de la définition d'un corps.

3. Eléments algébriques

PROPOSITION 3.1. *Soit L/K un extension et soit $x \in L$. Soit*

$$f\colon K[X] \to L$$

le morphisme défini par $f(P) = P(x)$ dans L. De deux choses une, ou bien

1. *f est injectif, et induit donc un morphisme $f'\colon K(X) \to L$ d'extensions de K qui est un isomorphisme de $K(X)/K$ sur la sous-extension $K(x)/K$ de L/K, ou bien*
2. *f n'est pas injectif, et il existe un polynôme irréductible $P \in K[X]$ tel que $\ker(f) = (P)$; le morphisme d'extensions induit $\bar{f}$ de $K[X]/(P)$ dans L est un isomorphismes de $K[X]/(P)$ sur la sous-extension $K(x)/K$ de L/K. En particulier, $K[x] = K(x)$.*

DÉMONSTRATION. Si f est injectif, il induit un morphisme f' du corps des fractions $K(X)$ de $K[X]$ dans L. En fait,

$$f'(\tfrac{P}{Q}) = \tfrac{P(x)}{Q(x)}$$

pour toute fraction $\frac{P}{Q}$ dans $K(X)$. Il s'ensuit que f' est un isomorphisme du corps $K(X)$ sur le sous-corps $K(x)$ de L. Comme la restriction de f' à K est l'identité, le morphisme f' est bien un isomorphisme d'extension de $K(X)/K$ sur la sous-extension $K(x)/K$ de L/K.

Si f n'est pas surjectif, il induit un isomorphisme $\bar{f}$ de $K[X]/\ker(f)$ sur $f(K[X]) = K[x]$. Comme $K[x]$ est un sous-anneau d'un anneau intègre, il est intègre. Il s'ensuit que $\ker(f)$ est un idéal premier. Comme il n'est pas nul, il existe un polynôme irréductible $P \in K[X]$ tel que $\ker(f) = (P)$. Du coup, $K[X]/(P)$ est un corps, et $\mathrm{im}(\bar{f}) = \mathrm{im}(f) = K[x]$ est un corps. D'où

$K[x] = K(x)$. Comme la restriction de $\bar{f}$ à K est l'identité, $\bar{f}$ est un isomorphisme d'extensions de $K[X]/(P)$ sur la sous-extension $K(x)/K$ de L/K. □

Si on est dans le premier cas, on dit que x est *transcendent sur* K. Explicitement, $x \in L$ est *transcendent sur* K si $P(x) = 0$ implique que $P = 0$ quel que soit $P \in K[X]$. Si on est dans le deuxième cas, on dit que x est algébrique sur K. Explicitement, $x \in L$ est *algébrique sur* K s'il existe $P \in K[X]$ non nul tel que $P(x) = 0$ dans L. Dans ce cas il existe même un et un seul polynôme irréductible unitaire P ayant cette propriété d'après la proposition précédente. On l'appelle le *polynôme minimal de* x *sur* K. Il est minimal dans le sens que tout $Q \in K[X]$ avec $Q(x) = 0$ dans L est un multiple de P. On appelle *degré de* x *sur* K le degré du polynôme minimal de x sur K. On a

$$[K(x) : K] = \deg(P)$$

d'après la proposition précédente, toujours sous la condition d'algébricité de x sur K.

EXEMPLE 3.2. 1. Le nombre réel $\sqrt{2}$ est algébrique sur $\mathbb{Q}$. En effet, $\sqrt{2}$ est racine du polynôme $X^2-2 \in \mathbb{Q}[X]$. D'ailleurs, X^2-2 est le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$, comme on vérifie facilement en utilisant le fait que $\sqrt{2} \notin \mathbb{Q}$. Ou alors, on remarque que $X^2 - 2$ satisfait le critère d'Eisenstein pour le nombre premier 2. Il s'ensuit que $\sqrt{2}$ est de degré 2 sur $\mathbb{Q}$, ou encore que l'extension $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ est de degré 2.

2. Le nombre réel $\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$. En effet, $\sqrt[3]{2}$ est racine du polynôme $X^3-2 \in \mathbb{Q}[X]$. Le polynôme X^3-2 est son polynôme minimal sur $\mathbb{Q}$ car il est unitaire, irréductible (par Eisenstein encore) et s'annule en $\sqrt[3]{2}$. Il s'ensuit que $\sqrt[3]{2}$ est de degré 3 sur $\mathbb{Q}$, ou encore que l'extension $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ est de degré 3.

3. Le cardinal de l'ensemble des nombres réels algébriques sur $\mathbb{Q}$ est dénombrable. Comme $\mathbb{R}$ lui-même est non dénombrable, il y a une infinité non dénombrable de nombres réels transcendents sur $\mathbb{Q}$. Par contre, démontrer qu'un nombre réel explicite est transcendent sur $\mathbb{Q}$ n'est souvent pas facile.

Hermite a démontré en 1873 que le nombre réel e est transcendent sur $\mathbb{Q}$, et Lindemann a démontré en 1882 que le nombre réel π est transcendent sur $\mathbb{Q}$. Cela implique que le morphisme

$$f' : \mathbb{Q}(X) \to \mathbb{R}$$

d'évaluation en e, respectivement en π, est bien défini et injectif.

Voici un énoncé d'une grande utilité théorique :

PROPOSITION 3.3. *Soit L/K une extension et soit $x \in L$. Alors x est algébrique sur K si et seulement s'il existe une sous-extension finie M/K de L/K contenant x.*

DÉMONSTRATION. Si x est algébrique, $K(x) = K[x]$ est une sous-extension finie de L/K contenant x.

Réciproquement, s'il existe une sous-extension finie M/K de L/K contenant x, soit $f : K[X] \to M$ le morphisme d"evaluation en x, c-à-d-, $f(P) = P(x)$ quel que soit $P \in K[X]$. Comme f est K-linéaire, M est de K-dimension finie et $K[X]$ n'est pas de K-dimension finie, f ne peut être injectif. Il s'ensuit que x est algébrique sur K. □

Soit L/K un extension. L'extension L/K est *algébrique* si tout élément x de L est algébrique sur K.

COROLLAIRE 3.4. *Soit L/K une extension. L'extension L/K est algébrique si et seulement s'il est réunion de ses sous-extension finies.*

DÉMONSTRATION. Supposons que L/K est algébrique. Soit $x \in L$. Comme x est algébrique sur K, l'élément x de L appartient à la sousextension finie $K[x]/K$ de L/K.

Réciproquement, si L est la réunion de ses sous-extensions finie, tout élément de L est algébrique sur K. □

COROLLAIRE 3.5. *Soit L/K une extension finie. Alors L/K est algébrique. De plus, le degré de x sur K divise $[L : K]$.*

COROLLAIRE 3.6. *Soit L/K une extension et $x \in L$ algébrique sur K. Alors, l'extension $K(x)/K$ est algébrique.*

Voici la transitivité de l'algébricité :

PROPOSITION 3.7. *Soit $M/L/K$ une tour d'extensions. Supposons que M/K est algébrique et que $x \in M$ est algébrique sur L. Alors, x est algébrique sur K. En particulier, si M/L et L/K sont algébriques, M/K est algébrique.*

DÉMONSTRATION. Comme $x \in M$ est algébrique sur L, il existe un polynôme $P \in L[X]$ non nul tel que $P(x) = 0$ dans M. Soient $a_0, \ldots, a_n$ les coefficients de P. Comme L/K est algébrique, les éléments $a_0, \ldots, a_n$ de L sont tous algébriques sur L. La sous-extension $K(a_0, \ldots, a_n)/K$ de L est alors une extension finie. Comme $P \in K(a_0, \ldots, a_n)[X]$ est non nul et $P(x) = 0$ dans M, l'élément x est algébrique sur $K(a_0, \ldots, a_n)$. Du coup, $K(a_0, \ldots, a_n, x)/K$ est une extension finie et x est algébrique sur K. □

PROPOSITION 3.8. *Soit L/K une extension. Soit M le sous-ensemble des éléments de L algébriques sur K. Alors, M est un sous-corps de L contenant K.*

DÉMONSTRATION. Il est clair que $K \subseteq M$. Montrons d'abord que M est stable pour $+$ et $\cdot$. Soient $x, y \in M$. Du coup, la sous-extension $K(x)/K$ de L/K est une extension finie de K. Comme y est algébrique sur K il l'est a foriori sur $K(x)$. En particulier, la sous-extension $K(x)(y)/K(x)$ de $L/K(x)$ est une extension finie de $K(x)$. On a donc une tour $K(x, y)/K(x)/K$ d'extensions finies. Il s'ensuit que la sous-extension $K(x, y)/K$ de L/K est une extension finie. D'après la proposition précédente, tous les éléments de $K(x, y)$ sont algébrique sur K. en particulier, $x + y$ et xy le sont. Cela montre que M est un sous-anneau de L contenant K.

Afin de montrer que M est un sous-corps de L, soit $x \in M$ non nul. Comme x est algébrique sur K, l'extensions $K(x)/K$ est algébrique. Du coup, $K(x) \subseteq M$. Comme $x^{-1} \in K(x)$, on a $x^{-1} \in M$. □

Soit L/K une extension. Soit $\overline{K}$ l'ensemble des éléments de L qui sont algébriques sur K. On appelle $\overline{K}$ la *clôture algébrique de K dans L*. C'est une sous-extension de L/K. C'est une vraie clôture dans le sens suivant :

PROPOSITION 3.9. *Soit L/K une extension. Alors, $\overline{K}/K$ est la plus grande sous-extension algébrique de L/K. De plus, toute sous-extension algébrique $M/\overline{K}$ de $L/\overline{K}$ est égale à $\overline{K}/\overline{K}$. En particulier, $\overline{\overline{K}} = \overline{K}$.*

DÉMONSTRATION. Soit M/K une sous-extension algébrique de K. Comme tous les éléments de M sont algébriques sur K, on a $M \subseteq \overline{K}$. Cela montre bien que $\overline{K}/K$ est la plus grande sous-extension algébrique de L/K.

Soit $M/\overline{K}$ une sous-extension algébrique de $L/\overline{K}$. Par transitivité, M/K est algébrique. D'après ce qui précède, $M \subseteq \overline{K}$, et donc $M = \overline{K}$. □

Un corps K est *algébriquement clos* si toute extension algébrique L/K est de degré 1, c-à-d, $L = K$. Une *clôture algébrique* de K est une extension algébrique $\bar{K}/K$ avec $\bar{K}$ algébriquement clos.

PROPOSITION 3.10. *Soit K un corps et supposons que $\bar{K}$ est une clôture algébrique de K. Soit L/K une sous-extension de $\bar{K}/K$. Alors, $\bar{K}$ est une clôture algébrique de L.*

DÉMONSTRATION. Exercice. □

PROPOSITION 3.11. *Soit K un corps. Alors, les conditions suivantes sont équivalentes :*

(1) K est algébriquement clos,

(2) Tout polynôme non constant dans $K[X]$ possède une racine dans K,

(3) Les seuls polynômes irréductibles de $K[X]$ sont les polynômes de degré 1,

(4) Tout polynôme non nul dans $K[X]$ est complètement décomposé, c-à-d-, s'écrit sous la forme

$$a_0(X - x_1)(X - x_2) \cdots (X - x_n),$$

où $a_0, x_1, \ldots, x_n \in K$, et

(5) Lorsqu'on les compte avec multiplicités, le nombre de racines dans K d'un polynôme dans $K[X]$ est égal au degré du polynôme.

DÉMONSTRATION. Il suffit de démontrer l'équivalence $1 \Leftrightarrow 2$; les autres sont claires. Par contraposée, supposons qu'il existe un polynôme non constant P dans $K[X]$ ne possèdant pas de racine dans K. Dans ce cas, il en existe également un qui soit irréductible. On peut donc supposer que P le soit. Comme tout polynôme de degré 1 possède une racine, $\deg(P) \geq 2$ et $K[X]/(P)$ est une extension algébrique non triviale de K.

R'eciproquement, supposons que K possède une extension algébrique non triviale L/K. Soit $x \in L$, $x \notin K$. Soit P le polynôme minimal de x sur K. Le polynôme $P \in K[X]$ est irréductible et de degré ≥ 2. En particulier, il n'a pas de racine dans K. □

EXEMPLE 3.12. Une formulation courante du Théorème Fondamental de l'Algèbre consiste à dire que tout polynôme complex non constant en une indéterminée possède une racine complexe [1]. D'après la proposition précédente, le corps des nombres complexes $\mathbb{C}$ est donc algébriquement clos. Une clôture algébrique de $\mathbb{R}$ est $\mathbb{C}$.

COROLLAIRE 3.13. *Soit K un corps et Ω un corps algébriquement clos le contenant comme sous-corps. Soit $\bar{K}$ la clôture algébrique de K dans Ω. Alors, $\bar{K}$ est une clôture algébrique de K.*

EXEMPLE 3.14. Soit $\bar{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$. Alors $\bar{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$.

On montre que tout corps possède une clôture algébrique.

PROPOSITION 3.15. *Soit K un corps. Alors il existe une extension algébrique K' de K dans laquelle tout polynôme non constant $P \in K[X]$ possède une racine.*

DÉMONSTRATION. On va adjoindre à K une racine pour chaque polynôme non constant $P \in K[X]$. Pour ce faire, soit

$$\mathcal{P} = \{P \in K[X] \mid \deg(P) \geq 1\}.$$

Soit encore X_P une indéterminée distincte pour chaque $P \in \mathcal{P}$. Considérons l'idéal

$$I = (P(X_P) \mid P \in \mathcal{P})$$

dans l'anneau de polynômes $A = K[X_p \mid P \in \mathcal{P}]$. On montrera que $I \neq A$. Avant de le montrer, montrons comment cela permet de construire une extension K' ayant les propriétés requises. Comme $I \neq A$, l'anneau A possède un idéal maximal m contenant I. Soit $K' = A/m$. L'anneau K' est un corps car m est maximal, et il contient K comme sous-corps. Notons x_p la classe de X_p dans K'. On a

$$P(x_p) = P(\overline{X_P}) = \overline{P(X_P)} = 0,$$

dans K' quel que soit $P \in \mathcal{P}$, car $P(X_P) \in I \subseteq m$. Par conséquent, tout polynôme non constant dans $K[X]$ possède une racine dans K'. De plus, tout élément x_p de K' est algébrique sur K. Comme $K' = K(x_P \mid P \in \mathcal{P})$, l'extension K'/K est algébrique.

Il nous reste à montrer que $I \neq A$. Par l'absurde, supposons que $I = A$. On a donc

$$1 \in (P(X_P) \mid P \in \mathcal{P}).$$

Il existe $P_1, \ldots$ □

THÉORÈME 3.16. *Tout corps possède une clôture algébrique.*

DÉMONSTRATION. Soit K un corps. Posons $K_0 = K$ et $K_{n+1} = K'_n$ pour $n \in \mathbb{N}$, où K'_n est une extension algébrique de K_n dans laquelle tout polyn6ome non constant de $K_n[X]$ possède une racine. On obtient ainsi une chaîne d'extensions algébriques

$$K_0 = K \subseteq K_1 \subseteq K_2 \subseteq \cdots$$

Soit

$$\bar{K} = \bigcup_{n \in \mathbb{N}} K_n.$$

Alors, $\bar{K}$ est un corps, contenant K comme sous-corps. L'extension $\bar{K}/K$ est algébrique.

Montrons que $\bar{K}$ est algébriquement clos. Soit L une extension de $\bar{K}$, et soit $x \in L$ algébrique sur $\bar{K}$. On montre que $x \in \bar{K}$. Soit P le polynôme minimal de x sur $\bar{K}$. Il existe $n \in \mathbb{N}$ tel que $P \in K_n[X]$. Comme P possède une racine dans $K_{n+1} = K'_n$, le polynôme irréductible $P \in \bar{K}[X]$ possède une racine dans $\bar{K}$. Il s'ensuit que p est de degré 1 et $x \in \bar{K}$. □

1. La démonstration de cet énoncé se fait habituellement en théorie de variable complexe comme application du Théorème de Liouville et relève donc plutôt de l'analyse.

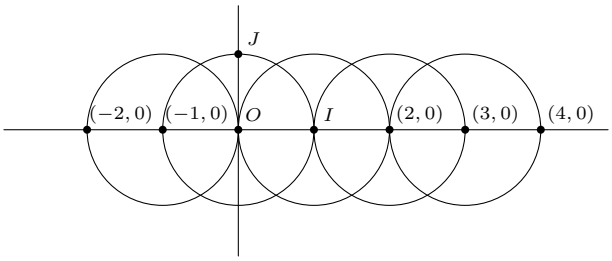


FIGURE 1. Construction des points $(n, 0)$ où $n \in \mathbb{Z}$.

4. Constructions à la règle et au compas

Soit P le plan euclidien de repère orthonormé direct (O, I, J). Chaque point p de P est déterminé de manière unique par son abscisse x et ordonée y dans ce repère. On identifiera p avec la paire de nombres réels (x, y).

Soit S un sous-ensemble de P. Une droite D dans P est *directement constructible à la règle à partir de* S si elle passe par deux points distincts de S. Un cercle C dans P est *directement constructible au compas à partir de* S si son centre appartient à S et son rayon est égal à la distance entre deux points de S. Soit $p \in P$. On dira que p est *directement constructible à la règle et au compas à partir de* S si p est soit un point de S, soit le point d'intersection de deux droites distinctes directement constructibles à partir de S, soit un point d'intersection d'une droite et d'un cercle directement constructibles à partir de S, soit un point d'intersection de deux cercles distincts directement constructibles à partir de S. Un point p de P est *constructible à la règle et au compas à partir de* S s'il existe une suite finie de points

$$p_1, p_2, p_3, \ldots, p_n = p$$

de P telle que p_i est constructible à la règle et au compas à partir du sous-ensemble

$$S_i = S \cup \{p_1, \ldots, p_{i-1}\}$$

quel que soit $i = 1, \ldots, n$. Un point p de P est *constructible à la règle et au compas* tout court si p est constructible à la règle et au compas à partir de l'ensemble $\{0, I, J\}$.

EXEMPLE 4.1. 1. Les points $O = (0, 0), I = (1, 0), J = (0, 1)$ sont constructibles car O, I, J appartiennent à $\{O, I, J\}$.

2. Les points $(n, 0)$ avec $n \in \mathbb{Z}$ sont constructibles à la règle et au compas. En effet, on trace la droite OI. On trace le cercle de centre I et de rayon IO. Ce cercle intersect la droite OI en O et en $(2, 0)$. Le point $(2, 0)$ est donc bien constructible. Pour construire le point $(3, 0)$, on trace le cercle de même rayon et de centre le point $(2, 0)$ qu'on vient de construire. Ce cercle intersecte la droite OI en le point I et le point $(3, 0)$. Ainsi de suite pour les points $(n, 0)$ avec $n \in \mathbb{N}$, $n \geq 2$. Pour construire le point $(-1, 0)$, on trace le cercle de centre O et de rayon OI. Ce cercle intersecte la droite OI en I et en $(-1, 0)$. Pour construire le point $(-2, 0)$, on trace le cercle de même rayon et de centre le point $(-1, 0)$ qu'on vient de construire. Ce cercle intersecte la droite OI en le point O en en $(-2, 0)$. Ainsi de suite pour construire les points $(n, 0)$ avec $n \in \mathbb{Z}$, $n \leq 3$. (Voir Figure 1.)

PROPOSITION 4.2. *Soit $S \subseteq P$ contenant $\{O, I, J\}$.*

(1) Si le point (x, y) est constructible à partir de S, les points $(x, 0)$ et $(0, y)$ le sont, et réciproquement.

(2) Si le point $(x, 0)$ est constructible à partir de S, le point $(0, x)$ l'est également, et réciproquement.

(3) Si $(x, 0)$ et $(y, 0)$ sont constructibles à partir de S, alors $(x + y, 0)$ l'est.

(4) Si $(x, 0)$ est constructible à partir de S, alors $(-x, 0)$ l'est.

(5) Si $(x, 0)$ et $(y, 0)$ sont constructibles à partir de S, alors $(xy, 0)$ l'est.

(6) Si $(x, 0)$ est constructible à partir de S, avec $x \neq 0$, alors $(x^{-1}, 0)$ l'est.

(7) Si $(x, 0)$ est constructible à partir de S, avec $x \geq 0$, alors $(\sqrt{x}, 0)$ l'est.

DÉMONSTRATION. 1. Supposons que le point (x, y) est constructible à partir de S. Si $y = 0$, l'énoncé est évident. De même si $x = 0$. On peut donc supposer que $x, y \neq 0$. On construit la

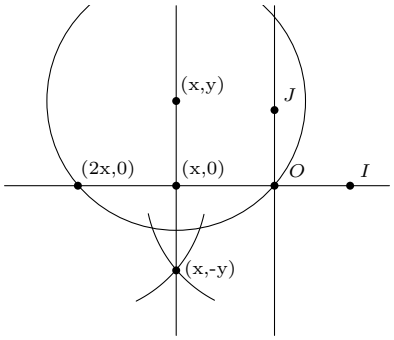


FIGURE 2. La construction du point $(x, 0)$ à partir de $S \cup \{(x, y)\}$.

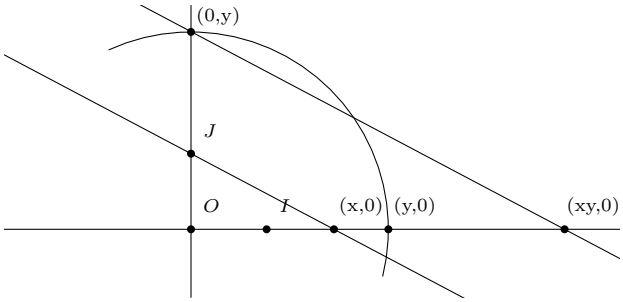


FIGURE 3. Construction du point $(xy, 0)$ à partir de $S \cup \{(x, 0), (y, 0)\}$

projection orthogonale du point (x, y) sur l'axe des abscisses. Tracer le cercle de centre (x, y) et passant par O, c-à-d, de rayon égal à la distance du point (x, y) au point O. Ce cercle intersecte l'axe des abscisses en deux points distincts, le point O et le point $(2x, 0)$. Tracer les cercles de centres O et $(2x, 0)$ et de même rayon que le premier. Ces deux cercles s'intersectent en deux points, (x, y) et $(x, -y)$. La droite par ces deux points intersecte l'axe des abscissesen le point $(x, 0)$. (Voir Figure 2.) La construction du point $(0, y)$ est analogue.

Réciproquement, si $(x, 0)$ et $(0, y)$ sont constructibles à partir de S, on peut construire le point (x, y) comme point d'intersection des droites passant par $(x, 0)$ et $(0, y)$ perpendiculaires à l'axe des abscisses et l'axe des ordonnées, respectivement.

2. Supposons que $(x, 0)$ est constructible à partir de S. On peut construire la droite IJ. Puis, on peut construire en quelques étapes la droite parallèle à la droite IJ passant par $(x, 0)$. Cette droite-ci intersecte l'axe des ordonnées en le point $(0, x)$. Le réciproque se fait de manière analogue.

3. Supposons que $(x, 0)$ et $(y, 0)$ sont constructibles à partir de S. Pour montrer que $(x + y, 0)$ l'est, on peut supposer que $y \neq 0$. Tracer le cercle de centre $(x, 0)$ et de rayon $|y|$, c-à-d, la distance de O à $(y, 0)$. Ce cercle intersecte la droites des abscisse en deux points, $(x + |y|, 0)$ et $(x - |y|, 0)$. L'un de sdeux points est le points $(x + y, 0)$.

4. Supposons que $(x, 0)$ est constructible à partir de S. Pour montrer que $(-x, 0)$ l'est, on peut supposer que $x \neq 0$. Tracer le cercle de centre O et passant par $(x, 0)$. Ce cercle intersecte l'axe des abscisses en un autre point, $(-x, 0)$.

5. Grâce au 4, on peut supposer que $x, y \geq$. Puis, on peut supposer que $x, y \neq 0$. On trace le cercle de centre O et de rayon y pour obtenir le point $(0, y)$. Puis, on trace la droite D passant par J et $(x, 0)$. Ensuite, on trace la droite parallèle à la droite D passant par $(0, y)$. Cette dernière droite intersecte l'axe des abscisses en le point $(xy, 0)$ par Thalès. (Voir Figure 3)

6. On peut suposer que $x > 0$. Voir Figure 4.

7. Soit $x \geq 0$ et supposons que le point $(x, 0)$ est constructible à partir de S. Construisons le point $(\sqrt{x}, 0)$. On peut supposer que $x > 0$. On peut construire le point $(x + 1, 0)$ d'après le 3. On peut construire le point $(\frac{x+1}{2}, 0)$ d'après les 5 et 6. Tracer le cercle C de centre $(\frac{x+1}{2}, 0)$ passant par $(x + 1, 0)$. Il est de rayon $\frac{x+1}{2}$. Construire le point $(x, 1)$ à l'aide du 1. Tracer la droite D passant par les points $(x, 0)$ et $(x, 1)$. Soit (x, y) le point d'intersection du cercle C avec la droite D ayant

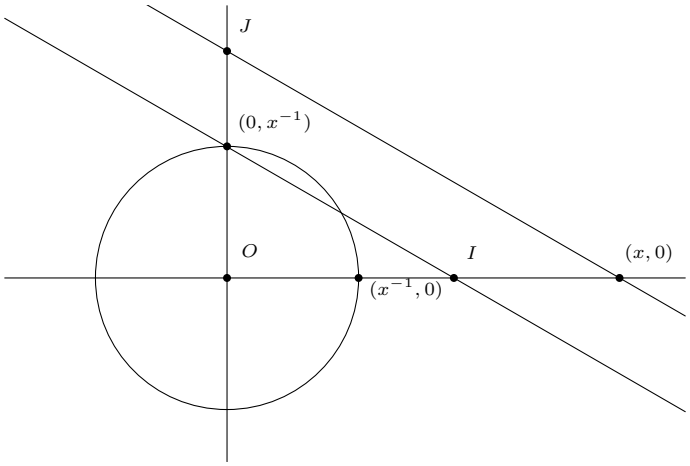


FIGURE 4. Construction de $(x^{-1}, 0)$ à partir de $S \cup \{(x, 0)\}$.

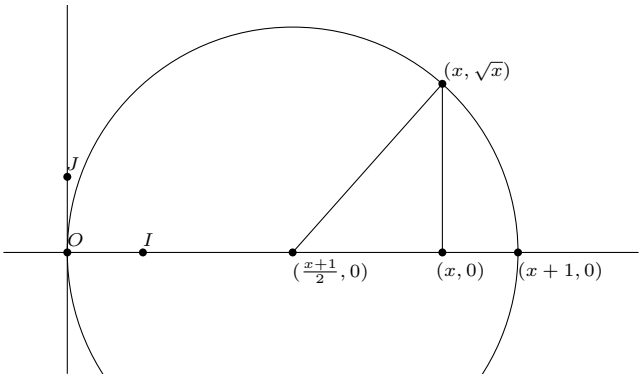


FIGURE 5. Construction du point $(\sqrt{x}, 0)$ à partir de $(x, 0)$.

$y \geq 0$. Le triangle de sommets $(\frac{x+1}{2}, 0)$, $(x, 0)$, (x, y) est rectangle. Par Pythagore

$$y = \sqrt{(\tfrac{x+1}{2})^2 - (\tfrac{x-1}{2})^2} = \sqrt{x}.$$

Du coup, $(\sqrt{x}, 0)$ est constructible, d'après les 1 et 2. (Voir Figure 5.) □

Soit $S \subseteq P$. On note $\mathbb{Q}(S)$ le sous-corps de $\mathbb{R}$ engendré par les coordonnées des points appartenant à S. Plus précisément

$$\mathbb{Q}(S) = \mathbb{Q}(\{x, y \,|\, (x, y) \in S\}).$$

Si $S \subseteq T$, on a bien-sûr $\mathbb{Q}(S) \subseteq \mathbb{Q}(T)$. A titre d'exemple, $\mathbb{Q}(\{O, I, J\}) = \mathbb{Q}$.

On note $\overline{S}$ l'ensemble de tous les points du plan P constructibles à partir de S. Notons que $\overline{S}$ est une sorte de clôture de S car $\overline{\overline{S}} = \overline{S}$. Proposition 4.2 implique alors qu'un point $(x, y) \in \overline{S}$ si et seulement si $(x, 0)$ et $(y, 0)$ appartiennent à $\overline{S}$. On notera $\overline{S} \cap \mathbb{R}$ ce sous-ensemble de $\mathbb{R}$:

$$\overline{S} \cap \mathbb{R} = \{x \in \mathbb{R} \,|\, (x, 0) \in \overline{S}\}.$$

Cette notation est justifié si on identifie la droite réelle $\mathbb{R}$ avec l'axe des abscisse en faisant correspondre un nombre réel x avec le point $(x, 0)$ du plan. Comme on vient de dire, un point (x, y) est constructible à partir de S si et seulement si $x, y \in \overline{S} \cap \mathbb{R}$. On peut le dire encore différemment, l'ensemble $\overline{S}$ des points constructibles à partir de S vérifie

$$\overline{S} = (\overline{S} \cap \mathbb{R}) \times (\overline{S} \cap \mathbb{R}).$$

L'ensemble $\overline{S}$ est donc complètement déterminé par $\overline{S} \cap \mathbb{R}$.

Proposition 4.2 a la conséquence suivante :

COROLLAIRE 4.3. *Soit $S \subseteq P$ contenant $\{O, I, J\}$. Alors*

$$\overline{S} \cap \mathbb{R} = \mathbb{Q}(\overline{S}).$$

En particulier, $\overline{S} \cap \mathbb{R}$ est un sous-corps de $\mathbb{R}$, et on a

$$\mathbb{Q}(S) \subseteq \overline{S} \cap \mathbb{R}.$$

De plus, supposons que $x_1, \ldots, x_n$ est une suite finie de nombre réels positifs telle que

$$x_i^2 \in \mathbb{Q}(S)(x_1, \ldots, x_{i-1})$$

pour tout $i = 1, \ldots, n$. Alors $x_n \in \overline{S} \cap \mathbb{R}$.

Cette dernière condition on peut la reformuler en termes de tour de sous-extensions de $\mathbb{R}/\mathbb{Q}$: Supposons que K est un sous-corps de $\mathbb{R}$ pour lequel il existe une suite croissante de sous-corps

$$K_0 = \mathbb{Q}(S) \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n = K$$

telle que K_i/K_{i-1} est de degré 1 ou 2, pour $i = 1, \ldots, n$. Alors

$$K \subseteq \overline{S} \cap \mathbb{R}.$$

Il se trouve que $\overline{S} \cap \mathbb{R}$ est la réunion des sous-corps K de $\mathbb{R}$ ayant cette propriété :

THÉORÈME 4.4. *Soit $S \subseteq P$ contenant $\{O, I, J\}$. Soit x un nombre réel. Alors, $x \in \overline{S} \cap \mathbb{R}$ si et seulement si x appartient à un sous-corps K de $\mathbb{R}$ pour lequel il existe une suite croissante de sous-corps*

$$K_0 = \mathbb{Q}(S) \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n = K$$

telle que K_i/K_{i-1} est de degré 1 ou 2, pour $i = 1, \ldots, n$.

DÉMONSTRATION. On a vu que la condition est suffisante. On montre qu'elle est nécessaire et on suppose que $x \in \overline{S} \cap \mathbb{R}$. cela veut dire que le point $p = (x, 0)$ est constructible à partir de S. Il existe donc une suite finie de points $p_1, \ldots, p_n = p$ de P telle que p_i est constructible à partir de $S \cup \{p_1, \ldots, p_{i-1}\}$. Ecrivons $p_i = (x_i, y_i)$, pour $i = 1, \ldots, n$, et posons

$$K_i = \mathbb{Q}(S \cup \{p_1, \ldots, p_i\}) = \mathbb{Q}(S)(x_1, y_1, \ldots, x_i, y_i),$$

pour $i = 0, \ldots, n$. On pose $K = K_n$. On a bien $K_0 = \mathbb{Q}(S)$, $K_i = K_{i-1}(x_i, y_i)$ et $x \in K \subseteq \mathbb{R}$. On montre que chaque extensions K_i/K_{i-1} est de degré 1 ou 2.

Rappelons que p_i est directement constructible a partir de $S \cup \{p_1, \ldots, p_{i-1}\}$. Il y a donc quatre possibilités :

On peut avoir $p_i \in S \cup \{p_1, \ldots, p_{i-1}\}$, au quel cas $x_i, y_i \in K_{i-1}$ et donc $K_i = K_{i-1}$.

Le point p_i peut être point intersection de deux droites D et D' distinctes directement constructibles à partir de $S \cup \{p_1, \ldots, p_{i-1}\}$. Cela signifie que les droites peuvent être données par des équations

$$ax + by = c \quad \text{et} \quad a'x + b'y = c',$$

respectivement, où a, b, c, a', b', c' appartiennent à K_{i-1}. En appliquant la règle de Cramer, par exemple, on obtient que x_i, y_i appartiennent également à K_{i-1}. On a encore $K_i = K_{i-1}$.

Si le point p_i est un point d'intersection d'une droite D et un cercle C directement constructibles à partir de $S \cup \{p_1, \ldots, p_{i-1}\}$, les nombres réels x_i et y_i sont solutions d'un système d'équations

$$\begin{cases} ax + by = c \\ (x-u)^2 + (y-v)^2 = r^2 \end{cases}$$

où $a, b, c, u, v, r^2 \in K_{i-1}$ avec $r > 0$. Si $b = 0$, on a $a \neq 0$, $x_i = c/a \in K_{i-1}$ et

$$(\tfrac{c}{a} - u)^2 + (y_i - v)^2 = r^2,$$

ce qui montre que y_i est algébrique sur K_{i-1} de degré ≤ 2. Donc, si $b = 0$, l'extension K_i/K_{i-1} est bien de degré 1 ou 2.

Si $b \neq 0$, on peut écrire $y_i = c/b - a/bx_i$ et on a $y_i \in K_{i-1}(x_i)$. Comme, de plus,

$$(x_i - u)^2 + (\tfrac{c}{b} - \tfrac{a}{b}x_i - v)^2 = r^2,$$

on voit que $K_i = K_{i-1}(x_i)$ est algébrique sur K_{i-1} de degré au plus 2 dans le cas $b \neq 0$ également.

Le dernier cas à traiter est lorsque p_i est un point d'intersection de deux cercles distincts C et C' directement constructibles à partir de $S \cup \{p_1, \ldots, p_{i-1}\}$. Dans ce cas, x_i et y_i sont solutions du système d'équations

$$\begin{cases} (x-u)^2 + (y-v)^2 = r^2 \\ (x-u')^2 + (y-v')^2 = (r')^2 \end{cases}$$

où $u, v, r^2, u', v', (r')^2 \in K_{i-1}$ avec $r, r' > 0$. La différence de ces deux équations est l'équation

$$2(u'-u)x + u^2 - (u')^2 + 2(v'-v)y + v^2 - (v')^2 = r^2 - (r')^2,$$

ce qui est l'équation d'une droite D à coefficients dans K_{i-1} [2]. En raisonnant comme ci-dessus, on obtient que l'extension K_i/K_{i-1} est de degré au plus 2 dans ce cas également. □

COROLLAIRE 4.5. *Soit $p = (x, y)$ un point constructible du plan P. Alors, x et y sont algébriques sur $\mathbb{Q}$ de degré une puissance de 2.*

On en tire de nombreux résultats d'impossibilité de construction à la règle et au compas :

THÉORÈME 4.6 (La quadrature du cercle). *Il est impossible de construire un carré Q dont l'aire est égal à celle du cercle unité de centre O et de rayon 1.*

DÉMONSTRATION. En effet, cela impliquerait que le nombre $\sqrt{\pi}$ serait constructible. Or, il n'en est rien. D'après le Théorème de Lindemann, π est transcendent sur $\mathbb{Q}$, donc $\sqrt{\pi}$ aussi. □

THÉORÈME 4.7 (La duplication du cube). *Etant donné une projection orthogonale sur le plan P d'un cube de côtés 1 dans l'espace, il est impossible d'en construire une dont le volume est double.*

DÉMONSTRATION. En effet, cela impliquerait que $\sqrt[3]{2}$ serait constructible. Or, $\sqrt[3]{2}$ est de degré 3 sur $\mathbb{Q}$, et 3 n'est pas une puissance de 2. □

THÉORÈME 4.8 (La trisection d'un angle). *Il n'y a pas de constructin générale à la règle et au compas qui permet de diviser un angle en 3 angles égaux. Plus préciément, il existe un $\angle BAC$ pour lequel il est impossible de construire un angle $\angle B'A'C'$ avec*

$$\angle BAC = 3\angle B'A'C'.$$

DÉMONSTRATION. Soit $\angle ABC$ un angle de $\frac{\pi}{3}$. On montre qu'on ne peut pas construire un angle $\angle A'B'C'$ tel que $3\angle A'B'C' = \angle ABC$. Par l'absurde, s'il existait un tel angle $\angle A'B'C'$, on pourrait construire le nombre réel $a = 2\cos(\frac{\pi}{9})$. Comme

$$\cos(3x) = \Re(\cos(3x) + i\sin(3x) = \Re((\cos x + i\sin x)^3) = \cos^3 x - 3\cos x \sin^2 x = 4\cos^3 x - 3\cos x,$$

on aurait

$$a^3 - 3a - 1 = 0.$$

Or, le polynôme $X^3 - 3X - 1 \in \mathbb{Q}[X]$ est irréductible car il est de degré ≤ 3 et ne possède pas de racine dans $\mathbb{Q}$. Le nombre a est donc algébrique sur $\mathbb{Q}$ de degré 3 qui n'est pas une puissance de 2. Contradiction. □

Il y a bien-sûr des angles $\angle BAC$ qu'on sait trisecter. Le plus simple étant sans doute un angle de $\frac{3}{2}\pi$. Mais il y aussi les angles de 2π, π, $\frac{\pi}{2}$ qu'on peut trisecter à la règle et au compas.

Remarquons que l'opération inverse, à savoir de tripler un angle général donné ne pose aucun problème.

Rappelons qu'un nombre premier p est *de Fermat* s'il est de la forme $p = 2^n + 1$ pour un certain entier naturel n. Exemples de nombres premiers de Fermat sont

$$2,\ 3,\ 5,\ 17,\ 257,\ 65537.$$

En fait, ce sont les seuls nombres premiers de Fermat connus à ce jour.

THÉORÈME 4.9 (Constructions de polygones réguliers). *Soit n un entier naturel ≥ 3. Alors, il est possible de construire un n-gone régulier à la règle et au compas, si et seulement si n est de la forme*

$$n = 2^e p_1 \cdots p_k,$$

où e est un entier naturel et les p_i sont des nombres premiers de Fermat distincts ≥ 3.

---

2. Notons que la droite D n'est a priori pas constructible et encore moins directement constructible à partir de $S \cup \{p_1, \ldots, p_{i-1}\}$! Elle sera constructible a posteriori comme droite passant par les deux points d'intersection des cercles C et C'.

Il est donc possible de construire des polygones réguliers à n côtés où $n \geq 3$ est un entier de la forme

$$2^e \cdot 3^{e_1} \cdot 5^{e_2} \cdot 17^{e_3} \cdot 257^{e_4} \cdot 65537^{e_5}$$

avec $e \in \mathbb{N}$ et $e_1, \ldots, e_5 = 0, 1$. De plus, à ce jour, ce sont les seuls pour lesquels on sait que la construction est possible. Plus explicitement, il est possible de construire des n-gones réguliers pour

$$n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, \ldots$$

Il l'est impossible pour

$$n = 7, 9, 11, 13, 14, 18, 19, 21, 22, 23, 25, \ldots$$

La démonstration du théorème ci-dessus sera plus facile une fois qu'on a vu la théorie de Galois...

5. Morphismes d'extensions

Soient L/K et M/K des extensions de K. On note

$$\mathrm{Hom}(L/K, M/K)$$

l'ensemble des morphismes d'extensions de L/K dans M/K. C'est un sous-ensemble du K-espace vectoriel

$$\mathrm{Hom}_K(L, M)$$

de toutes les applications K-linéaires de L dans M. Ce K-espace vectoriel $\mathrm{Hom}_K(L, M)$ sera même considéré comme M-espace vectoriel pour la multiplication externe définie par

$$(\mu \cdot f)(x) = \mu f(x),$$

quels que soient $\mu \in M$, $f \in \mathrm{Hom}_K(L, M)$ et $x \in L$. Il s'agit bien d'une extension de la structure de K-espace vectoriel sur $\mathrm{Hom}_K(L, M)$.

Proposition 5.1. *Soient L/K et M/K des extensions de K. Supposons que L/K est finie. Alors $\mathrm{Hom}_K(L, M)$ est un M-espace vectoriel de dimension finie et*

$$\dim_M \mathrm{Hom}_K(L, M) = [L : K].$$

Démonstration. Soit $v_1, \ldots, v_n$ une K-base L. Soit $\varphi_1, \ldots, \varphi_n$ la K-base duale du K-espace vectoriel dual $\mathrm{Hom}_K(L, K)$. Cela veut dire que

$$\varphi_i \colon L \to K$$

est K-linéaire et déterminée par $\varphi_i(v_j) = 0$ si $j \neq i$, et $\varphi_i(v_i) = 1$. Montrons que $\varphi_1, \ldots, \varphi_n$ est une M-base de $\mathrm{Hom}_K(L, M)$.

La famille $\varphi_1, \ldots, \varphi_n$ est M-libre. En effet, soient $\mu_1, \ldots, \mu_n \in M$ tels que

$$\mu_1\varphi_1 + \cdots + \mu_n\varphi_n = 0$$

dans $\mathrm{Hom}_K(L, M)$. Cela veut dire que

$$\mu_1\varphi_1(x) + \cdots + \mu_n\varphi_n(x) = 0$$

dans M, quel que soit $x \in L$. En particulier, pour $x = v_i$, on obtient $\mu_i = 0$. Du coup, la famille $\varphi_1, \ldots, \varphi_n$ est bien M-libre.

Montrons que la famille $\varphi_1, \ldots, \varphi_n$ est M-génératrice de $\mathrm{Hom}_K(L, M)$. Soit $\varphi \colon L \to M$ une application K-linéaire. Soit $\mu_i = \varphi(v_i)$ pour $i = 1, \ldots, n$. On a $\mu_1, \ldots, \mu_n \in M$. Par construction, l'application K-linéaire

$$\varphi - (\mu_1\varphi_1 + \cdots + \mu_n\varphi_n) \colon L \to M$$

est 0 sur chaque v_i. Comme les v_i engendrent L comme K-espace vectoriel, on a

$$\varphi = \mu_1\varphi_1 + \cdots + \mu_n\varphi_n.$$

Cela montre que la famille $\varphi_1, \ldots, \varphi_n$ est M-génératrice de $\mathrm{Hom}_K(L, M)$. □

Lemme 5.2 (Lemme de Dedekind). *Soient L/K et M/K des extensions de K. Alors, le sous-ensemble $\mathrm{Hom}(L/K, M/K)$ du M-espace vectoriel $\mathrm{Hom}_K(L, M)$ est libre.*

DÉMONSTRATION. On montre par récurrence sur n que toute sous-famille de n éléments distincts de $\mathrm{Hom}(L/K, M/K)$ est M-libre. C'est trivialement vrai lorsque $n = 0$.

Supposons maintenant que toute sous-famille de $n-1$ éléments distincts de $\mathrm{Hom}(L/K, M/K)$ est M-libre, où $n \geq 1$. Soit $\sigma_1, \ldots, \sigma_n$ une sous-famille de n éléments distincts de $\mathrm{Hom}(L/K, M/K)$. Soient $\mu_1, \ldots, \mu_n \in M$ tels que

$$\mu_1\sigma_1 + \cdots + \mu_n\sigma_n = 0$$

dans $\mathrm{Hom}_K(L, M)$. Cela veut dire que

$$\mu_1\sigma_1(x) + \cdots + \mu_n\sigma_n(x) = 0$$

dans M, pour tout $x \in L$. On substitue yx pour x, où $x, y \in L$ sont des éléments quelconques. Comme les σ_i sont multiplicatifs, on obtient

$$\mu_1\sigma_1(y)\sigma_1(x) + \cdots + \mu_n\sigma_n(y)\sigma_n(x) = 0.$$

En soustrayant cette dernière de la précédente équation multipliée par $\sigma_n(y)$, le dernier terme s'en va et on obtient

$$\mu_1(\sigma_n(y) - \sigma_1(y))\sigma_1(x) + \cdots + \mu_{n-1}(\sigma_n(y) - \sigma_{n-1}(y))\sigma_{n-1}(x) = 0$$

quel que soit $x \in L$, et pour tout $y \in L$. Du coup,

$$\mu_1(\sigma_n(y) - \sigma_1(y))\sigma_1 + \cdots + \mu_{n-1}(\sigma_n(y) - \sigma_{n-1}(y))\sigma_{n-1} = 0$$

dans $\mathrm{Hom}_K(L, M)$, quel que soit $y \in L$. Par hypothèse de récurrence, $\sigma_1, \ldots, \sigma_{n-1}$ est M-libre. Il s'ensuit que

$$\mu_i(\sigma_n(y) - \sigma_i(y)) = 0$$

pour $i = 1, \ldots, n-1$, et pour tout $y \in L$. Comme $\sigma_n \neq \sigma_i$ lorsque $i < n$, il existe $y \in L$ tel que $\sigma_n(y) - \sigma_i(y) \neq 0$. Du coup, $\mu_i = 0$ pour tout $i < n$. En substituant dans la toute premère équation, on obtient $\mu_n\sigma_n(x) = 0$ quel que soit $x \in L$. En prenant $x = 1$, on obtient $\mu_n = 0$. Par conséquent, $\mu_i = 0$ quel que soit i, et la famille $\sigma_1, \ldots, \sigma_n$ est bien M-libre. □

Comme conséquence des deux dernièrs énoncés, on a le corollaire crucial suivant :

COROLLAIRE 5.3. *Soient L/K et M/K des extensions de K. Supposons que L/K est finie. Alors*

$$|\mathrm{Hom}(L/K, M/K)| \leq [L : K].$$

En particulier, le groupe $\mathrm{Aut}(L/K)$ *est fini et*

$$|\mathrm{Aut}(L/K)| \leq [L : K]$$

pour toute extension finie L/K.

EXEMPLE 5.4. On a vu que $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ contient deux éléments, à savoir l'identité id et la conjugaison complexe σ. Comme $[\mathbb{C} : \mathbb{R}] = 2$, il n'y a pas d'autres automorphismes de $\mathbb{C}/\mathbb{R}$, d'après le corollaire précédent.

On s'intéressera au cas où l'ordre du groupe $\mathrm{Aut}(L/K)$ est égal à $[L : K]$. On verra dans les paragraphes suivants qu'il peut y avoir deux raisons qui empêchent le groupe $\mathrm{Aut}(L/K)$ d'être d'ordre $[L : K]$; l'extension peut ne pas être normale ou ne pas être séparable.

6. Extensions normales

PROPOSITION 6.1. *Soit K un corps et $\bar{K}$ une clôture algébrique de celui-ci. Soit $P \in K[X]$ irréductible et soit $L = K[X]/(P)$. Alors, pour tout morphisme d'extensions σ de L/K dans $\bar{K}/K$, l'élément $\sigma(\bar{X})$ est une racine de P dans $\bar{K}$. De plus, pour toute racine x de P dans $\bar{K}$, il y a un et un seul morphisme d'extensions σ de L/K dans $\bar{K}/K$ tel que $\sigma(\bar{X}) = x$. En particulier, il existe un morphisme d'extensions de L/K dans $\bar{K}/K$.*

DÉMONSTRATION. Soit σ un morphisme de L/K dans $\bar{K}/K$. Comme P est à coefficients dans K et σ est l'identité sur K, on a

$$P(\sigma(\bar{X})) = \sigma(P(\bar{X})) = \sigma(0) = 0,$$

c-à-d, $\sigma(\bar{X})$ est une racine de P dans $\bar{K}$.

Soit x une racine de P dans $\bar{K}$. Soit

$$f\colon K[X] \to \bar{K}$$

le morphisme d'évaluation en x défini par $f(Q) = Q(x)$. Soit $\pi\colon K[X] \to K[X]/(P) = L$ le morphisme de passage au quotient. Comme $f(P) = P(x) = 0$, il existe un morphisme $\sigma\colon L \to \bar{K}$ tel que $\sigma \circ \pi = f$. Il est clair que σ est un morphisme d'extensions de K, et que $\sigma(\bar{X}) = x$. De plus, σ est unique ayant cette propriété. En effet, si τ est un morphisme de L/K dans $\bar{K}/K$ avec $\tau(\bar{X}) = x$, on a $(\tau \circ \pi)(X) = x = f(X)$ et $(\tau \circ \pi)_{|K} = \mathrm{id}$. Cela veut dire que $\tau \circ \pi = f$. Comme σ est l'unique morphisme tel que $\sigma \circ \pi = f$, on obtient $\tau = \sigma$. □

On dit qu'une extension L/K est *monogène* s'il existe $x \in L$ tel que $K[x] = L$. On appelle x *générateur* de l'extension L/K. Une telle extension est forcément algébrique et finie. En fait, elle est isomorphe à l'extension $K[X]/(P)$ de K, où P est le polynôme minimal de x sur K. L'énoncé précédent porte donc sur les extensions monogènes et peut se formuler ainsi :

COROLLAIRE 6.2. *Soit K un corps et $\bar{K}$ une clôture algébrique de celui-ci. Soit L/K une extension monogène. Soit $x \in L$ un générateur et P son polynôme minimal sur K. Soit $Z(P)$ l'ensemble des racines de P dans $\bar{K}$. Alors, l'application ensembliste d'évaluation en x*

$$\mathrm{ev}_x\colon \mathrm{Hom}(L/K, \bar{K}/K) \to Z(P)$$

définie par $\mathrm{ev}_x(\sigma) = \sigma(x)$ est bien définie et est une bijection. En particulier, il existe un morphisme d'extensions de L/K dans $\bar{K}/K$.

Remarquons qu'on peut en déduire encore le Lemme de Dedekind, ou plutôt son corollaire, dans le cas d'une extension monogène car le corollaire ci-dessus implique que

$$|\mathrm{Hom}(L/K, \bar{K}/K)| = |Z(P)| \leq \deg(P) = [L : K]$$

pour une extension monogène L/K.

Afin que le nombre d'automorphismes d'une extension finie L/K soit égal au degré de l'extension, on sera donc amené à

(1) adjoindre à L/K toutes les racines des polynômes minimaux sur K d'éléments de L, ce qu'on fera dans ce paragraphe dans un cadre plus général, et
(2) considérer des extensions algébriques dont les éléments ont des polynômes minimaux à racines simples dans $\bar{K}$, ce qu'on fera dans le paragraphe suivant.

Momtrons d'abord que toute extension algébrique d'un corps K est isomorphe à une sous-extension de $\bar{K}/K$.

PROPOSITION 6.3. *Soit K un corps et $\bar{K}$ une clôture algébrique de celui-ci. Soit L/K une extension algébrique. Alors, il existe un morphisme d'extensions de L/K dans $\bar{K}/K$. En particulier, toute extension algébrique de K est isomorphe à une sous-extension de $\bar{K}/K$.*

DÉMONSTRATION. Soit $\mathcal{P}$ l'ensemble des paires (M, σ) où M/K est une sous-extension de L/K et σ est un morphisme d'extensions de M/K dans $\bar{K}/K$. On définit un ordre partiel $\leq$ sur $\mathcal{P}$ par $(M, \sigma) \leq (N, \tau)$ si $M \subseteq N$ et $\tau_{|M} = \sigma$. Il est clair que toute chaîne dans $\mathcal{P}$ possède un majorant. D'après le Lemme de Zorn, $\mathcal{P}$ possède un élément maximal (M, σ). Montrons que $M = L$. Soit $x \in L$. Comme x est algébrique sur K, il l'est a fortiori sur M. En particulier, $M[x]$ est une extension monogène de M. Comme $\bar{K}$ est aussi une clôture algébrique de M à travers σ, il existe, d'après Corollaire 6.2, une extension τ de σ à $M[x]$. On a donc $(M, \sigma) \leq (M[x], \tau)$ dans $\mathcal{P}$. Par maximalité de (M, σ), on a $M[x] = M$, c-à-d, $x \in M$. Cela montre que $L = M$. □

COROLLAIRE 6.4. *Une clôture algébrique d'un corps K est unique à un isomorphisme d'extensions de K près.*

Soit K un corps et $\bar{K}$ une clôture algébrique de celui-ci. Soit L/K une extension algébrique. La *clôture normale de L dans $\bar{K}$* est la plus petite sous-extension L^{norm}/K de $\bar{K}/K$ tel que $\sigma(L) \subseteq L^{\mathrm{norm}}$ pour tout morphisme d'extensions σ de L/K dans $\bar{K}/K$. Cette clôture existe évidemment ; elle est égale à l'intersection de toutes les sous-extensions M/K de $\bar{K}/K$ contenant $\sigma(L)$ pour tout morphisme σ de L/K dans $\bar{K}/K$.

Si L/K est une sous-extension de $\bar{K}/K$, alors $L \subseteq L^{\mathrm{norm}}$.

PROPOSITION 6.5. *Soit K un corps et $\bar{K}$ une clôture algébrique de celui-ci. Soit L/K une sous-extension de $\bar{K}/K$. Les conditions suivantes sont équivalentes.*

(1) $L = L^{\mathrm{norm}}$, c-à-d, pour tout morphisme σ de L/K dans $\bar{K}/K$ on a $\sigma(L) \subseteq L$,

(2) Pour tout $x \in L$, le polynôme minimal de x sur K a toutes ces racines dans L,

(3) Tout polynôme $P \in K[X]$ irréductible ayant une racine dans L a toutes ses racines dans L,

(4) Pour tout $\sigma \in \mathrm{Aut}(\bar{K}/K)$ on a $\sigma(L) = L$,

(5) Pour tout morphisme σ de L/K dans $\bar{K}/K$ on a $\sigma(L) = L$, et

(6) Pour tout $\sigma \in \mathrm{Aut}(\bar{K}/K)$ on a $\sigma(L) \subseteq L$.

Démonstration. $1 \Rightarrow 2$: Soit $x \in L$ et soit P son polynôme minimal sur K. On montre que toutes les racines y de P dans $\bar{K}$ appartiennent à L. Soit y une racine de P dans $\bar{K}$. D'après Corollaire 6.2, il existe un morphisme d'extensions τ de $K[x]/K$ dans $\bar{K}/K$ avec $\tau(x) = y$. Comme $L/K[x]$ est algébrique et $\bar{K}$ est également clôture algébrique de $\tau(K[x])$, il existe une extension σ de τ à L dans $\bar{K}$, d'après Proposition 6.3. Comme $\tau_{|K} = \mathrm{id}$, on a $\sigma_{|K} = \mathrm{id}$, et σ est un morphisme d'extensions de L/K dans $\bar{K}/K$. D'après l'hypothèse, $\sigma(L) \subseteq L$. En particulier, $y = \sigma(x) \in L$.

$2 \Rightarrow 3$: Il suffit de montrer le 3 pour les polynômes unitaires. Si $P \in K[X]$ est irréductible et unitaire ayant une racine x dans L, le polynôme P est le polynôme minimal de x sur K. D'après l'hypothèse, toutes les racines de P dans $\bar{K}$ appartiennent à L.

$3 \Rightarrow 4$: Par contraposée, soit $\sigma \in \mathrm{Aut}(\bar{K}/K)$ et supposons que $\sigma(L) \neq L$. Quitte à remplacer σ par σ^{-1}, on peut supposer que $\sigma(L) \not\subseteq L$. Soit $x \in L$ tel que $y = \sigma(x) \notin L$. Soit P le polynôme minimal de x sur K. Comme $P \in K[X]$, on a

$$P(y) = P(\sigma(x)) = \sigma(P(x)) = \sigma(0) = 0.$$

Le polynôme $P \in K[X]$ est donc un polynôme irréductible ayant une racine dans L et une racine en dehors de L.

Les conditions 4 et 5 sont équivalentes. En effet, l'implication $5 \Rightarrow 4$ est triviale. Quant à l'implication $4 \Rightarrow 5$, soit σ un morphisme de L/K dans $\bar{K}/K$. Comme $\bar{K}/L$ est algébrique et $\bar{K}$ est une clôture algébrique de $\sigma(L)$, le morphisme σ s'étend à un morphisme τ de $\bar{K}$ dans $\bar{K}$, d'après Proposition 6.3. Comme $\bar{K}$ est algébriquement clos, on a $\tau \in \mathrm{Aut}(\bar{K}/K)$. D'après le 4, $\tau(L) = L$. Il s'ensuit que $\sigma(L) = L$.

L'implications $4 \Rightarrow 6$ est trivial. Quant à l'implication $6 \Rightarrow 1$, elle se montre de manière analogue à la démonstration de l'implication $4 \Rightarrow 5$. □

Une sous-extension L/K de $\bar{K}/K$ est *normale* si $L^{\mathrm{norm}} = L$ [3]. Grâce à Proposition 6.5, cela est équivalent à dire que tout polynôme irréductible $P \in K[X]$ possédant une racine dans L se décompose complètement dans $L[X]$. Cette dernière formulation ne fait plus référence à l'inclusion de L dans $\bar{K}$, et permet donc la définition plus générale suivante. Soit L/K une extension algébrique. L'extension L/K est *normale* si tout polynôme irréductible $P \in K[X]$ possédant une racine dans L se décompose complètement dans $L[X]$. Comme un tel polynôme, s'il est unitaire, est le polynôme mimimal de sa racine, on peut encore dire que L/K est normale si le polynôme minimal sur K de tout élément de L est complètement décomposé dans $L[X]$.

Soit L/K un extension algébrique normale. Soit $x \in L$ et P son polynôme minimal sur K. Une racine de P dans L est un *conjugué* de x sur K. Si $y \in L$ est un conjugué de x, alors x est aussi un conjugué de y. En effet, le polynôme minimal P de x sur K est nécessairement polynôme minimal de y sur K. On dira encore que x et y sont conjugués dans L/K, si y est un conjugué de x sur K.

Proposition 6.6. *Soit L/K une extension normale. Soient $x, y \in L$. Alors, x et y sont conjugués dans L si et seulement s'il existe un automorphisme σ de L/K tel que $\sigma(x) = y$.*

Démonstration. Pour l'implication directe, il est utile de choisir une clôture algébrique $\bar{K}$ de K, et de considérer L/K comme sous-extension de $\bar{K}/K$. Supposons donc que x et y sont conjugués. Soit P le polynôme minimal de x sur K. Comme y est un conjugué de x sur K, il est racine de P dans $\bar{K}$. d'après Corollaire 6.2, il existe un morphisme d'extensions τ de $K[x]/K$ dans $\bar{K}/K$ avec $\tau(x) = y$. Comme L/K est algébrique et $\bar{K}$ est une clôture algébrique de $\tau(K[x])$, il existe un morphisme d'extensions σ de L/K dans $\bar{K}/K$ tel que $\sigma_{|K[x]} = \tau$. Comme L/K est normale, on a $\sigma(L) = L$ d'après Proposition 6.5. Du coup, σ est un automorphisme de L/K avec $\sigma(x) = y$.

Réciproquement, supposons qu'il existe un automorphisme σ de L/K tel que $\sigma(x) = y$. Soit P le polynôme minimal de x sur K. On a alors $P(y) = P(\sigma(x)) = \sigma(P(x)) = \sigma(0) = 0$, c-à-d, y est un conjugué de x sur K. □

3. On aurait préféré dire *normalement close*...

D'après l'énoncé précédent, deux nombres complexes distincts sont conjugués sur $\mathbb{R}$ si et seulement s'ils sont complexes conjugués. Etre conjugué est donc une généralisation d'être complexe conjugué.

Soit $M/L/K$ une tour d'extensions algébriques. Si M/K est normale, L/K l'est trivialement. Si M/K est normale, alors M/L est normale. En effet, le poynôme minimal de $x \in M$ sur L divise celui de x sur K. Comme ce dernier a toutes ses racines dans M, le premier aussi.

Par contre, les autres implications sont fausses : L/K n'est pas forcément normale si M/K l'est, et M/K n'est pas forcément normale si M/L et L/K le sont.

EXEMPLE 6.7. 1. La sous-extension $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ de $\bar{\mathbb{Q}}/\mathbb{Q}$ est normale. En effet, le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$ est le polynôme $P = X^2 - 2$, car ce dernier est irréductible dans $\mathbb{Q}[X]$, unitaire et annule $\sqrt{2}$. Les racines de P dans $\bar{\mathbb{Q}}$ sont $\pm\sqrt{2}$. D'après Proposition 6.2, il y a deux morphismes de $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ dans $\bar{Q}/\mathbb{Q}$ à savoir, l'inclusion ι et le morphisme σ de $\mathbb{Q}[\sqrt{2}]$ dans $\bar{\mathbb{Q}}$ déterminé par $\sigma(\sqrt{2}) = -\sqrt{2}$. Comme $\sigma(\sqrt{2}) = -\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, on a $\sigma(Q[\sqrt{2}]) \subseteq \mathbb{Q}[\sqrt{2}]$. D'après Proposition 6.5, ou même par la première définition de normalité, l'extension $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ est normale.

2. La sous-extension $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ de $\bar{Q}/\mathbb{Q}$ n'est pas normale. D'après Exemple 3.2, le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}$ est $P = X^3 - 2$. Une autre racine de P dans $\bar{\mathbb{Q}}$ est $\xi\sqrt[3]{2}$, où ξ est une racine cubique primitive de 1 dans $\mathbb{C}$, et donc dans $\bar{\mathbb{Q}}$. Par exemple, on peut prendre $\xi = e^{2\pi i/3} = -\frac{1}{2} + \frac{1}{2}i\sqrt{3}$. Comme $\xi\sqrt[3]{2} \notin \mathbb{R}$ et $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$, on a $\xi\sqrt[3]{2} \notin \mathbb{Q}[\sqrt[3]{2}]$. L'extension $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ n'est donc pas normale.

On peut encore le voir par les morphismes d'extension. D'après Corollaire 6.2, il existe un morphisme σ de $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ dans $\bar{\mathbb{Q}}/\mathbb{Q}$ avec $\sigma(\sqrt[3]{2}) = \xi\sqrt[3]{2}$. Comme $\sigma(\sqrt[3]{2}]) \notin \mathbb{R}$ et $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$, on voit que

$$\sigma(\mathbb{Q}[\sqrt[3]{2}]) \not\subseteq \mathbb{Q}[\sqrt[3]{2}].$$

L'extension $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ n'est donc pas normale.

La clôture normale de $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ est $\mathbb{Q}[\sqrt[3]{2}, \xi]/\mathbb{Q}$. En effet, soit ι l'inclusion de $\mathbb{Q}[\sqrt[3]{2}]$ dans $\bar{\mathbb{Q}}$ et soit τ le morphisme de $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ dans $\bar{\mathbb{Q}}/\mathbb{Q}$ déterminé par $\tau(\sqrt[3]{2}) = \xi^2\sqrt[3]{2}$, la troisème racine de P dans $\bar{\mathbb{Q}}$. D'après Corollaire 6.2, les morphismes ι, σ, τ sont tous les morphismes de $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ dans $\bar{\mathbb{Q}}/\mathbb{Q}$. La plus petite sous-extension de $\bar{\mathbb{Q}}/\mathbb{Q}$ contenant

$$\iota(\mathbb{Q}[\sqrt[3]{2}]) = \mathbb{Q}[\sqrt[3]{2}],\ \sigma(\mathbb{Q}[\sqrt[3]{2}]) = \mathbb{Q}[\xi\sqrt[3]{2}] \quad \text{et} \quad \tau(\mathbb{Q}[\sqrt[3]{2}]) = \mathbb{Q}[\bar{\xi}\sqrt[3]{2}]$$

est

$$\mathbb{Q}[\sqrt[3]{2}, \xi\sqrt[3]{2}, \bar{\xi}\sqrt[3]{2}] = \mathbb{Q}[\sqrt[3]{2}, \xi, \bar{\xi}] = \mathbb{Q}[\sqrt[3]{2}, \xi].$$

En particulier, l'extension $\mathbb{Q}[\bar{\xi}\sqrt[3]{2}]/\mathbb{Q}$ est normale. Notons que cette extension est de degré 6. En effet, le polyn6ome minimal de ξ sur $\mathbb{Q}$ est $X^2 + X + 1$. Celui n'a pas de racine dans $\mathbb{R}$ et donc non plus dans $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$. Comme il est de degré ≤ 3, il est irréductible dans $\mathbb{Q}[\sqrt[3]{2}][X]$. C'est donc aussi le polyn 6ome minimal de ξ sur $\mathbb{Q}[\sqrt[3]{2}]$. Il s'ensuit que

$$[\mathbb{Q}[\sqrt[3]{2}, \xi] : \mathbb{Q}[\sqrt[3]{2}] = 2$$

et

$$[\mathbb{Q}[\sqrt[3]{2}, \xi] : \mathbb{Q}] = [\mathbb{Q}[\sqrt[3]{2}, \xi] : \mathbb{Q}[\sqrt[3]{2}] \cdot [\mathbb{Q}[\sqrt[3]{2} : \mathbb{Q}] = 2 \cdot 3 = 6.$$

Cela fournit également un exemple d'une extension M/K normale ayant une sous-extension L/K non normale.

3. Les extensions $\mathbb{Q}[\sqrt[4]{2}/\mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ sont normales, mais l'extension $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}$ n'est pas normale. La clôture normale de cette dernière est $\mathbb{Q}[\sqrt[4]{2}, i]$. Les détails sont laissés au lecteur. Il peut être utile de montrer de manière générale que toute extension de degré ≤ 2 est normale.

Cela fournit un exemple d'extensions normales M/L et L/K sans que M/K soit normale.

Voici une caractérisation explicite d'extensions normales finies d'un corps donné.

PROPOSITION 6.8. *Soit K un corps et $\bar{K}$ une clôture algébrique de celui-ci. Soit $P \in K[X]$ un polynôme non nul. Soient $x_1, \ldots, x_n$ ses racines dans $\bar{K}$. Alors, l'extension $K[x_1, \ldots, x_n]/K$ est finie et normale. De plus, toute extension finie et normale de K est isomorphe à une extension de cette forme-là.*

DÉMONSTRATION. Soit $L = K[x_1, \ldots, x_n]$. Comme $x_1, \ldots, x_n$ sont algébriques sur K, l'extension L/K est une extension finie. Soit σ un morphisme de L/K dans $\bar{K}/K$. Afin de montrer que L/K est normale, on montre que $\sigma(L) \subseteq L$. Il suffit de montrer que pour tout i il existe j tel que $\sigma(x_i) = x_j$. Or, soit Q le polynôme minimal de x_i sur K. Comme $Q \in K[X]$, l'élement $\sigma(x_i)$ de

$\bar{K}$ est encore racine de Q. Comme Q divise P, il est aussi racine de P. Il existe donc j tel que $\sigma(x_i) = x_j$. Cela montre la première assertion de l'énonce.

Soit L/K finie et normale. On peut supposer que L/K soit une sous-extension de $\bar{K}/K$. Comme L/K est finie, il existe $x_1, \dots, x_n \in L$ tel que $L = K[x_1, \dots, x_n]$. Soit Q_i le polynôme minimal de x_i sur K, et soit $P = Q_1 \cdots Q_n \in K[X]$. Comme Q_i est irréductible dans $K[X]$ et possède une racine dans l'extension normale L/K, toutes les racines de Q_i dans $\bar{K}$ appartiennent à L. Ainsi, toutes les racines $y_1, \dots, y_m$ de P appartiennent à L. On a donc

$$L = K[x_1, \dots, x_n] \subseteq K[y_1, \dots, y_m] \subseteq L.$$

Il s'ensuit que $L = K[y_1, \dots, y_m]$. □

Soit $P \in K[X]$ non nul. Soit $x_1, \dots, x_n$ les racines de P dans $\bar{K}$. On appelle *extension de rupture de P dans $\bar{K}/K$* la sous-extension $K[x_1, \dots, x_n]/K$ de $\bar{K}/K$. Le corps $K[x_1, \dots, x_n]$ est appelé *corps de rupture de P dans $\bar{K}/K$*.

D'après Proposition 6.8, l'extension de rupture sur K d'un polynôme à coefficients dans K est une extension normale. De plus, toute extension finie normale de K est le corps de rupture d'un polynôme dans $K[X]$.

Exemple 6.9. Soit $n \in \mathbb{N}$, $n \neq 0$. L'extension de rupture du polynôme $X^n - 1$ dans $\bar{Q}/\mathbb{Q}$ est l'extension

$$\mathbb{Q}[1, \xi, \xi^2, \dots, \xi^{n-1}] = \mathbb{Q}[\xi]$$

de $\mathbb{Q}$, où ξ est une racine n-ième primitive de l'unité. On peut par exemple prendre $\xi = e^{\frac{2\pi i}{n}}$. L'extension $\mathbb{Q}[\xi]/\mathbb{Q}$ est donc normale. On l'appelle *l'extension cyclotomique de $\mathbb{Q}$ d'ordre n.*

Soit $P \in K[X]$ non nul. L'extension de rupture de P sur K est une extension L/K telle que P se décompose complètement dans $L[X]$, et que L/K est engendré par les racines de P dans L. Comme cette dernière caractérisation ne fait plus référence à la clôture algébrique $\bar{K}$ de K, elle permet de définir une extension de rupture sur K d'un polynôme non nul $P \in K[X]$ sans s'appuyer sur une clôture algébrique de K : Une extension de rupture de P sur K est une extension L/K telle que

(1) P se décompose complètement dans $L[X]$, et
(2) $L = K[x_1, \dots, x_n]$ où $x_1, \dots, x_n$ sont les racines de P dans L.

Evidemment, une telle extension de rupture de P est isomorphe à une extension de rupture de P dans $\bar{K}/K$. L'avantage est qu'on n'a plus besoin de choisir une clôture algébrique de K avant de pouvoir considérer une extension de rupture. En fait, une extension de rupture se construit très facilement par récurrence :

Soit K un corps et $P \in K[X]$ non nul. Si $\deg(P) = 0$, l'extension triviale K/K est extension de rupture de P sur K. On peut donc supposer que $\deg(P) > 0$. L'hypothèse de récurrence est qu'on sait déjà construire des extensions de rupture pour les polynômes de degré $< \deg(P)$ sur tout corps. Soit Q un diviseur irréductible de P dans $K[X]$. Soit $L = K[X]/(Q)$. Le corps L est une extension de K dans laquelle Q possède une racine à savoir $x = \bar{X}$. Comme x est aussi racine de P, on peut factoriser $P = (X - x)R$ dans $L[X]$. Comme $\deg(R) < \deg(P)$, il existe une extension de rupture M/L de R sur L. Il est facile de vérifier que M/K est extension de rupture de P sur K.

Une autre possibilité de construction d'une extension de rupture d'un polynôme non nul sur un corps K repose sur l'algèbre de décomposition d'un polynôme unitaire. En effet, on peut supposer que $P \in K[X]$ est unitaire. Soit A l'algèbre de décomposition de P sur K. Rappelons que A est un anneau contenant K comme sous-anneau et dans lequel existe des éléments $x_1, \dots, x_n$ tels que

$$P = (X - x_1) \cdots (X - x_n).$$

De plus, $A = K[x_1, \dots, x_n]$. Comme A est un anneau non nul, il possède un idéal maximal m. En posant $L = A/m$, l'extension L/K est une extension de rupture de P sur K.

Il suit de chacune de deux constructions, ainsi que de la définition même d'une extension de rupture dans $\bar{K}/K$, qu'une extension de rupture L/K d'un polynôme $P \in K[X]$ est de degré $\leq \deg(P)!$. On laisse la vérification au lecteur à titre d'exercice.

Exemple 6.10. Soit P le polynôme unitaire universel de degré n :

$$P = X^n + A_1 X^{n-1} + \cdots + A_n$$

qu'on considère comme polynôme en X à coefficients dans le corps des fractions rationnelles $K = \mathbb{Q}(A_1, \ldots, A_n)$. Soit $L = \mathbb{Q}(X_1, \ldots, Q_n)$. D'après le Théorème sur les polynômes symétriques élémentaires, on peut identifier K avec un sous-corps de L en faisant

$$A_i = (-1)^i \sigma_i$$

pour $i = 1, \ldots, n$. Comme

$$P = (X - X_1) \cdots (X - X_n)$$

dans $L[X]$, on a $P(X_i) = 0$ pour tout i. En particuler, les X_i sont algébriques sur K. On a donc $L = K[X_1, \ldots, X_n]$, et l'extension L/K est une extension de rupture de P sur K. Le groupe symétrique S_n agit comme automorphismes de L/K. D'après le Lemme de Dedekind,

$$[L : K] \geq n!.$$

Comme on a aussi

$$[L : K] \leq \deg(P)! = n!,$$

l'extension L/K est de degré $n!$. Autrement dit

$$[\mathbb{Q}(X_1, \ldots, X_n) : \mathbb{Q}(A_1, \ldots, A_n)] = n!.$$

EXEMPLE 6.11. Soit p un nombre premier et $n \in \mathbb{N}$, $n \neq 0$. Soit $q = p^n$. Soit $\mathbb{F}_q$ le corps de rupture du polynôme $X^q - X$ sur $\mathbb{F}_p$. Soit F le sous-ensemble des racines de $X^q - X$ dans $\mathbb{F}_q$. Notons que F est l'ensemble des points fixes du morphisme de Frobenius itéré φ^n. Il s'ensuit que F est un sous-corps de $\mathbb{F}_q$. On a donc $\mathbb{F}_q = \mathbb{F}_p[F] = F$. Comme la dérivée de $X^q - X$ est le polynôme 1, toutes les racines de $X^q - X$ sont simples. Il s'ensuit que $|\mathbb{F}_q| = q$. On a démontré que, pour tout nombre premier p et pour tout entier naturel non nul n, il existe un corps de cardinal p^n. Notons que l'extension de rupture $\mathbb{F}_q/\mathbb{F}_p$ est de degré n, bien plus petit que $p^n!$.

7. Extensions séparables

Soit K un corps et $\bar{K}$ une clôture algébrique de celui-ci. Soit $P \in K[X]$ irréductible. On dit que P est *séparable* si P n'a que des racines simples dans $\bar{K}$.

PROPOSITION 7.1. *Soit K un corps et $\bar{K}$ une clôture algébrique de celui-ci. Soit $P \in K[X]$ irréductible. Les conditions suivantes sont équivalentes.*

(1) P est séparable,

(2) P et P' n'ont pas de racine en commun dans $\bar{K}$.

(3) P et P' sont premiers entre eux, et

(4) $P' \neq 0$ dans $K[X]$.

Il est plus facile de montrer l'équivalence des négations de toutes ces assertions, et étendre un peu la liste des conditions :

PROPOSITION 7.2. *Soit K un corps et $\bar{K}$ une clôture algébrique de celui-ci. Soit $P \in K[X]$ irréductible. Les conditions suivantes sont équivalentes.*

(1) P est inséparable,

(2) P et P' ont une racine en commun dans $\bar{K}$.

(3) P et P' ne sont pas premiers entre eux, et

(4) $P' = 0$ dans $K[X]$.

(5) La caractéristique de K est non nulle, et il existe $Q \in K[X]$ tel que $Q(X^p) = P$, où $p = \mathrm{car}(K)$.

(6) La caractéristique de K est non nulle, et il existe $R \in \bar{K}[X]$ tel que $R^p = P$, où $p = \mathrm{car}(K)$.

(7) Toutes les racines de P dans $\bar{K}$ sont multiples.

DÉMONSTRATION. $1 \Rightarrow 2$: Supposons que P n'est pas séparable. Il possède donc une racine multiple x dans $\bar{K}$. Cela veut dire que $(X - x)^2$ divise P dans $\bar{K}[X]$. Par Leibniz, $(X - x)$ divise P' dans $\bar{K}[X]$. Les polynômes P et P' ont donc une racine en commun dans $\bar{K}$.

$2 \Rightarrow 3$: Si P et P' ont une racine en commun dans $\bar{K}[X]$, ils ne sont pas premiers entre eux dans $\bar{K}[X]$, et donc pas non plus dans $K[X]$.

$3 \Rightarrow 4$: Supposons que P et P' ne sont pas premiers entre eux. Ils ont donc un diviseur irréductible commun dans $K[X]$. Comme P est lui-même irréductible, ce diviseur est associé à

P. Il s'ensuit que P est un diviseur commun de P et P'. En particulier, P divise P'. Comme $\deg(P') \leq \deg(P) - 1 < \deg(P)$, on a forcément $P' = 0$.

$4 \Rightarrow 5$: Supposons que $P' = 0$ dans $K[X]$. Comme $\deg(P') = -\infty < \deg(P) - 1$, le corps K est de caractéristique non nulle. Soit $p = \mathrm{car}(K)$. Ecrivons

$$P = a_n X^n + \cdots + a_0$$

avec $a_0, \ldots, a_n \in K$ et $n \in \mathbb{N}$. Comme $P' = 0$ dans $K[X]$, on a $ia_i = 0$ pour tout $i > 0$. Donc $a_i \neq 0$ seulement si $p|i$, et cela est vrai aussi pour $i = 0$. Du coup, P s'écrit sous la forme

$$b_m X^{mp} + b_{m-1} X^{(m-1)p} + \cdots + b_1 X^p + b_0$$

où $b_0, \ldots, b_m \in K$. Il s'ensuit que $P = Q(X^p)$ avec

$$Q = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0 \in K[X]$$

$5 \Rightarrow 6$: Supposons que $P = Q(X^p)$ avec $Q \in K[X]$. Ecrivons

$$Q = a_n X^n + \cdots + a_0$$

avec $a_0, \ldots, a_n \in K$ et $n \in \mathbb{N}$. Comme $\bar{K}$ est algébriquement clos, il existe $b_i \in \bar{K}$ tel que $b_i^p = a_i$, pour tout i. Du coup,

$$P = Q(X^p) = a_n X^{np} + a_{n-1} X^{(n-1)p} + \cdots + a_1 X^p + a_0 =$$
$$b_n^p X^{np} + b_{n-1}^p X^{(n-1)p} + \cdots + b_1^p X^p + b_0^p = (b_n X^n + b_{n-1} X^{n-1} + \cdots + b_1 X + b_0)^p,$$

car K est de caractéristique p et l'endomorphisme de Frobenius de $K[X]$ est additif. Il s'ensuit que $P = R^p$ avec $R \in \bar{K}[X]$.

$6 \Rightarrow 7$: Comme $P = R^p$ et $p \geq 2$, toutes les racines de P dans $\bar{K}$ sont multiples.

$7 \Rightarrow 1$: Si toutes les racine de P sont multiples dans $\bar{K}$, le polynôme P en possède au moins une car $\deg(P) \geq 1$. Donc P est inséparable. □

Un corps K est *parfait* s'il n'y a pas de polynôme irréductible inséparable dans $K[X]$. A titre d'exemple, un corps de caractéristique nulle est parfait, d'après Proposition 7.2.

Pour un corps K de caractéristique $p \neq 0$, on note K^p le sous-corps de K des puissances p-ièmes d'éléments de K. C'est effectivement un sous-corps, car l'endomorphisme de Frobenius de K est un isomorphisme de K sur son image K^p. Notons que $K^p = K$ si K est un corps fini. Le plus petit exemple de corps K avec $K^P \subsetneq K$ est $K = \mathbb{F}_p(X)$.

PROPOSITION 7.3. *Soit K un corps de caractéristique non nulle. Soit $p = \mathrm{car}(K)$. Si $K^p = K$ alors K est parfait. En particulier, parfaits sont : les corps finis et les corps algébriquement clos.*

DÉMONSTRATION. Par l'absurde, supposons K n'est pas parfait. Il existe donc un polynôme irréductible inséparable P dans $K[X]$. D'après Proposition 7.2, il existe $R \in \bar{K}[X]$ tel que $R^p = P$. Ecrivons

$$R = a_n X^n + \cdots + a_0$$

où $a_0, \ldots, a_n \in \bar{K}$. Comme

$$R^p = a_n^p X^{np} + \cdots + a_0^p = P \in K[X],$$

on a $a_i^p \in K$ pour tout i. L'endomorphisme de Frobenius φ de $\bar{K}$ est injectif et $\varphi(K) = K^p = K$ par hypothèse. Il s'ensuit que $a_i \in K$. Par conséquent $R \in K[X]$ avec $R^p = P$, et P est réductible. Contradiction. □

EXEMPLE 7.4. Soit p un nombre premier et soit $K = \mathbb{F}_p(T)$. C'est sans doute le corps de caractéristique p le plus simple pour lequel on a $K^P \subsetneq K$. En fait, on a $K^p = \mathbb{F}_p(T^p) \subsetneq \mathbb{F}_p(T) = K$.

Soit $P = X^p - T$ dans $K[X]$. Le polynôme P est irréductible car Eisenstein. Il est inséparable car de la forme $Q(X^p)$ pour $Q \in K[X]$.

On peut également voir que P a des racines multiples dans $\bar{K}$. Soit $L = K[X]/(P)$. L'extension L/K est algébrique et donc isomorphe à une sous-extension de $\bar{K}/K$. Notons $\sqrt[p]{T}$ pour $\bar{X}$. C'est justifié car

$$(\sqrt[p]{T})^p = \bar{X}^p = \overline{X^p} = \overline{T} = T$$

dans L. Dans $L[X]$ on a

$$P = X^p - T = X^p - (\sqrt[p]{T})^p = (X - \sqrt[p]{T})^p.$$

La racine $\sqrt[p]{T}$ de P dans L est donc une racine de multiplicité p. En particulier, le polynôme P a une racine multiple dans $\bar{K}$, comme il se doit. D'ailleurs, on voit également que $P = R^p$ pour un polynôme $R \in \bar{K}[X]$.

Soit L/K une extension algébrique. Un élément $x \in L$ est *séparable* sur K si son polynôme minimal sur K est séparable. L'extension L/K est *séparable* si tous les éléments de L sont séparables sur K.

Soit $M/L/K$ une tour d'extensions algébriques. Si M/K est séparable, L/K est bien-sûr séparable. Si M/K est séparable, M/L est séparable. En effet, le polynôme minimal de $x \in M$ sur L divise celui de x sur K. Comme ce dernier n'a que des racines simples dans $\bar{K}$, il en est de même pour le premier.

PROPOSITION 7.5. *Soit K un corps et $\bar{K}$ une clôture algébrique de celui-ci. Soit $M/L/K$ une tour d'extensions finies. Choisissons un morphisme d'extensions τ_0 de L/K dans $\bar{K}/K$. Alors, on a*

$$|\mathrm{Hom}(M/K, \bar{K}/K)| = [M : K]$$

si et seulement si

$$|\mathrm{Hom}(M/L, \bar{K}/L)| = [M : L] \quad \text{et} \quad |\mathrm{Hom}(L/K, \bar{K}/K)| = [L : K],$$

où $\bar{K}$ est vu comme extension de L via τ_0.

DÉMONSTRATION. Soit

$$\rho \colon \mathrm{Hom}(M/K, \bar{K}/K) \to \mathrm{Hom}(L/K, \bar{K}/K)$$

l'application de restriction définie par $\rho(\sigma) = \sigma_{|L}$. D'après Proposition 6.3, l'application ρ est surjective considérant $\bar{K}$ comme clôture algébrique de L via τ_0. Les fibres de ρ sont toutes de cardinal $\leq [M : L]$ d'après le Lemme de Dedekind.

Montrons maintenant les deux implications. Supposons que

$$|\mathrm{Hom}(M/K, \bar{K}/K)| = [M : K]$$

On a donc

$$[M : K] = |\mathrm{Hom}(M/K, \bar{K}/K)| \leq [M : L] \cdot |\mathrm{Hom}(L/K, \bar{K}/K)| \leq [M : L] \cdot [L : K] = [M : K].$$

Il s'ensuit que toute les inégalités sont des égalités. En particulier,

$$|\mathrm{Hom}(L/K, \bar{K}/K)| = [L : K],$$

et chaque fibre de ρ est de cardinal $[M : L]$. En particulier, la fibre au-dessus de τ_0 est de cardinal $[M : L]$, c-à-d,

$$|\mathrm{Hom}(M/L, \bar{K}/L)| = [M : L].$$

Réciproquement, supposons que

$$|\mathrm{Hom}(M/L, \bar{K}/L)| = [M : L] \quad \text{et} \quad |\mathrm{Hom}(L/K, \bar{K}/K)| = [L : K].$$

Cela veut dire que le cardinal de la fibre $\rho^{-1}(\tau_0)$ est égal à $[M : L]$. On montre que toutes les fibres de ρ ont ce cardinal. Pour ce faire, soit τ un morphisme quelconque de L/K dans $\bar{K}$. D'après Proposition 6.3, il existe un morphisme α de $\bar{K}/K$ dans $\bar{K}/K$ tel que $\alpha \circ \tau_0 = \tau$. Comme $\alpha(\bar{K})$ est algébriquement clos dans $\bar{K}/K$, il est surjectif. Le morphisme α est donc un automorphisme. Soit

$$\varphi \colon \rho^{-1}(\tau_0) \to \rho^{-1}(\tau)$$

définie par $\varphi(\sigma) = \alpha \circ \sigma$. Elle est bien définie. En effet, soit σ un morphisme de M/K das $\bar{K}/L$ dont la restriction à L est égal à τ_0. Du coup,

$$\rho(\alpha \circ \sigma) = (\alpha \circ \sigma)_{|L} = \alpha \circ \tau_0 = \tau.$$

Cela montre bien que φ envoie $\rho^{-1}(\tau_0)$ dans $\rho^{-1}(\tau)$. Comme l'application ψ définie par $\psi(\sigma) = \alpha^{-1} \circ \sigma$ est une application récriproque à φ, l'application φ est une bijection. Cela montre que toutes les fibres de ρ sont de cardinal $[M : L]$. Il s'ensuit que

$$|\mathrm{Hom}(M/K, \bar{K}/K)| \geq [M : L] \cdot [L : K] = [M : K].$$

D'après le Lemme de Dedekind, cette inégalité est une égalité. □

PROPOSITION 7.6. *Soit K un corps et $\bar{K}$ une clôture algébrique de celui-ci. Soit L/K une extension monogène, soit x un générateur et P son polynôme minimal sur K. Alors, les conditions suivantes sont équivalentes :*

(1) P est séparable,

(2) $|\mathrm{Hom}(L/K, \bar{K}/K)| = [L : K]$,

(3) L/K est séparable.

DÉMONSTRATION. $1 \Leftrightarrow 2$: C'est une conséquence immédiate du Corollaire 6.2.
$2 \Rightarrow 3$: Soit $y \in L$ et posons $M = K[y]$. D'après la proposition précédente, on a

$$|\mathrm{Hom}(M/K, \bar{K}/K)| = [M : K].$$

Il suit de l'implication $2 \Rightarrow 1$ appliquée à l'extension monogène M/K que y est séparable sur K.
L'implication $3 \Rightarrow 1$ est triviale. □

PROPOSITION 7.7. *Soit K un corps et $\bar{K}$ une clôture algébrique de celui-ci. Soit L/K une extension finie. Alors L/K est séparable si et seulement si*

$$|\mathrm{Hom}(L/K, \bar{K}/K)| = [L : K].$$

DÉMONSTRATION. Supposons que L/K est séparable et finie. Montrons par récurrence sur $[L : K]$ que

$$|\mathrm{Hom}(L/K, \bar{K}/K)| = [L : K].$$

Si $[L : K] = 1$, on a $L = K$ et l'énoncé est trivialement vrai. Supposons que l'énoncé est vérifié pour toutes les extensions finies séparables de degré $< [L : K]$. Soit $x \in L$, $x \notin K$. Si $K[x] = L$, l'énoncé découle de la proposition précédente. Si $K[x] \subsetneq L$, on a deux extensions finies séparables $L/K[x]$ et $K[x]/K$ de degré $< [L : K]$. Par récurrence,

$$|\mathrm{Hom}(L/K[x], \bar{K}/K[x])| = [L : K[x]] \quad \text{et} \quad |\mathrm{Hom}(K[x]/K, \bar{K}/K)| = [K[x] : K].$$

D'après Proposition 7.5, on a

$$|\mathrm{Hom}(L/K, \bar{K}/K)| = [L : K].$$

Réciproquement, supposons que

$$|\mathrm{Hom}(L/K, \bar{K}/K)| = [L : K].$$

Montrons que L/K est séparable. Soit $x \in L$. D'après Proposition 7.5,

$$|\mathrm{Hom}(K[x]/K, \bar{K}/K)| = [K[x] : K].$$

D'après Proposition 7.6, x est séparable sur K. □

On en déduit la transitivité d'extensions algébriques séparables :

PROPOSITION 7.8. *Soit $M/L/K$ une tour d'extensions algébriques séparables. Alors M/K est algébrique et séparable.*

DÉMONSTRATION. Soit $x \in M$. Soit P le polynôme minimal de x sur L. Soient $a_0, \ldots, a_n$ les coefficients de L. Soit $L' = K[a_0, \ldots, a_n]$. L'extension L'/K est finie et séparable car sous-extension de L/K. De plus, x est algébrique sur L' de polynôme minimal P. Soit $M' = L'[x]$. Comme P est séparable, l'extension M'/L' est séparable. On a donc

$$|\mathrm{Hom}(L'/K, \bar{K}/K)| = [L' : K] \quad \text{et} \quad |\mathrm{Hom}(M'/L', \bar{K}/L')| = [M' : L'].$$

Il s'ensuit que

$$|\mathrm{Hom}(M'/K, \bar{K}/K)| = [M' : K].$$

Du coup, M'/K est séparable, en particulier x est séparable sur K. □

PROPOSITION 7.9. *Soit K un corps et $\bar{K}$ une clôture algébrique de celui-ci. Soit*

$$K^{\mathrm{sep}} = \{x \in \bar{K} \mid x \text{ est séparable sur } K\}.$$

(1) K^{sep} est une sous-extension de $\bar{K}/K$.

(2) Pour tout morphisme σ d'une extension séparable L/K dans $\bar{K}/K$, on a $\sigma(L) \subseteq K^{\mathrm{sep}}$.

(3) Toute extension algébrique séparable L/K est isomorphe à une sous-extension de K^{sep}/K.

(4) Si L/K^{sep} est une extension algébrique séparable, alors $L = K^{\mathrm{sep}}$.

DÉMONSTRATION. 1. Il faut montrer que K^{sep} est un sous-corps de $\bar{K}$ contenant K. Comme tout élément x de K est nécessairement séparable sur K, on a bien $K \subseteq K^{\text{sep}}$. Il suffit donc de montrer que K^{sep} est stable pour $+$ et $\cdot$. Soient $x, y \in K^{\text{sep}}$. Comme x est séparable sur K, on a

$$|\text{Hom}(K[x]/K, \bar{K}/K)| = [K[x] : K].$$

Comme y est séparable sur K, il l'est aussi sur $K[x]$. On a donc

$$|\text{Hom}(K[x,y]/K[x], \bar{K}/K[x])| = [K[x,y] : K[x]].$$

Il s'ensuit que

$$|\text{Hom}(K[x,y]/K, \bar{K}/K)| = [K[x,y] : K]$$

ce qui implique que $K[x,y]/K$ est séparable. En particulier, $x+y, xy \in K^{\text{sep}}$.

Les autres énoncés sont laissé au lecteur à titre d'exercice. □

Soit $\bar{K}$ une clôture d'un corps K. La sous-extension K^{sep}/K de $\bar{K}/K$ est la *clôture séparable de K dans $\bar{K}$*. On dit que K est *séparablement clos* si $K = K^{\text{sep}}$.

Tout corps possède une clôture séparable. En effet, on n'a qu'à prendre la clôture séparable du corps dans l'une de ses clôtures algébriques. Une clôture séparable d'un corps est unique à isomorphisme près.

8. Extensions galoisiennes

Soit L/K une extension de corps. La théorie de Galois étudie le rapport entre les sous-groupes de $\text{Aut}(L/K)$ et les sous-extensions M/K de L/K.

Soit $\mathcal{G} = \mathcal{G}(L/K)$ l'ensemble des sous-groupes du groupe $\text{Aut}(L/K)$ des automorphismes de L/K. Soit $\mathcal{E} = \mathcal{E}(L/K)$ l'ensemble des sous-extensions de L/K. Ces deux ensembles sont partiellement ordonnés par l'inclusion, et possèdent tous les deux un plus grand et un plus petit élément. De plus, deux éléments de chacun de ces deux ensembles possèdent une borne inférieure et une borne supérieure. En effet, si G et H sont des sous-groupes de $\text{Aut}(L/K)$, on a

$$\inf\{G, H\} = G \cap H \quad \text{et} \quad \sup\{G, H\} = GH,$$

où GH désigne le sous-groupe de $\text{Aut}(L/K)$ engendré par les éléments de la forme gh, $g \in G$ et $h \in H$. Si M/K et N/K sont des sous-extensions de L/K, on a

$$\inf\{M/K, N/K\} = (M \cap N)/K \quad \text{et} \quad \sup\{M/K, N/K\} = K(M \cup N)/K.$$

D'ailleurs, on note MN pour $K(M \cup N)$, et on l'appelle le *compositum* des deux sous-extensions M/K et N/K de L/K. On peut vérifier que

$$MN = \{m_1 n_1 + \cdots + m_k n_k \,|\, m_1, \ldots, m_k \in M,\ n_1, \ldots, n_k \in N \quad \text{et} \quad k \in \mathbb{N}\},$$

si l'extension L/K est algébrique, ce qui justifie la notation MN dans ce cas.

Si G est un sous-groupe de $\text{Aut}(L/K)$, on note

$$L^G = \{x \in L \,|\, \sigma(x) = x \text{ quel que soit } \sigma \in G\}$$

l'ensemble des points fixes pour l'action de G sur L. C'est un sous-corps de L contenant K, comme on peut vérifier facilement. Autrement dit, L^G/K est une sous-extension de L/K.

Inversement, si M/K est une sous-extension de L/K, on dispose du groupe $\text{Aut}(L/M)$, entre autres. Ce groupe-ci nous intéresse car c'est un sous-groupe de $\text{Aut}(L/K)$ à savoir

$$\text{Aut}(L/M) = \{\sigma \in \text{Aut}(L/K) \,|\, \sigma(m) = m \text{ quel que soit } m \in M\}.$$

On obtient alors deux application ensemblistes, l'une de $\mathcal{G}$ dans $\mathcal{E}$, l'autre de $\mathcal{E}$ dans $\mathcal{G}$. On les définit par

$$F \colon \mathcal{G} \to \mathcal{E}, \qquad G \mapsto L^G$$

et

$$A \colon \mathcal{E} \to \mathcal{G}, \qquad M/K \mapsto \text{Aut}(L/M).$$

Notons que F et A sont toutes les deux décroissantes par rapport aux ordres partiels sur $\mathcal{E}$ et $\mathcal{G}$. En effet, si G et H sont des sous-groupes de $\text{Aut}(L/K)$, alors

$$G \subseteq H \Rightarrow L^G \supseteq L^H.$$

Si M/K et N/K sont des sous-extensions de L/K, alors

$$M \subseteq N \Rightarrow \text{Aut}(L/M) \supseteq \text{Aut}(L/N).$$

Il s'ensuit que les compositions

$$F \circ A \colon \mathcal{E} \to \mathcal{E}, \qquad M/K \mapsto L^{\mathrm{Aut}(L/M)}$$

et

$$A \circ F \colon \mathcal{G} \to \mathcal{G}, \qquad H \mapsto \mathrm{Aut}(L/L^H)$$

sont croissantes. Explicitement, si M/K et N/K sont des sous-extensions de L/K, alors

$$M \subseteq N \Rightarrow L^{\mathrm{Aut}(L/M)} \subseteq L^{\mathrm{Aut}(L/N)}.$$

Si G et H sont des sous-groupes de $\mathrm{Aut}(L/K)$, alors

$$G \subseteq H \Rightarrow \mathrm{Aut}(L/L^G) \subseteq \mathrm{Aut}(L/L^H).$$

De plus, F envoie le plus petit élément $\{\mathrm{id}\}$ de $\mathcal{G}$ sur le plus grand élément L/K de $\mathcal{E}$ car

$$L^{\{\mathrm{id}\}} = L.$$

Inversement, l'application A envoie le plus grand élément L/K de $\mathcal{E}$ sur le plus petit élément $\{\mathrm{id}\}$ de $\mathcal{G}$ car

$$\mathrm{Aut}(L/L) = \{\mathrm{id}\}.$$

Une exentension algébrique L/K est *galoisienne* si elle est normale et séparable. Si M/K est une sous-extension d'une extension galoisienne, l'extension L/M est galoisienne. Une sous-extension d'une extension galoisienne n'est pas forcément galoisienne. Lorsque L/K est une extension galoisienne, on écrit $\mathrm{Gal}(L/K)$ au lieu de $\mathrm{Aut}(L/K)$, i.e.,

$$\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K),$$

et on l'appelle *groupe de Galois* de L/K.

Si $P \in K[X]$ est un polynôme non nul et de facteurs irréductibles séparables, l'extension de rupture de P sur K est une extension galoisienne finie. Le *groupe de Galois* de P est le groupe de Galois de l'extension de rupture de P sur K. Comme toute extension galoisienne finie de K est l'extension de rupture sur K d'un tel polynôme P, tout groupe de Galois d'une extension galoisienne finie de K est le groupe de Galois d'un polynôme sur K.

Il est très facile de réaliser n'importe quel groupe fini comme groupe de Galois d'une extension finie, comme montre l'énoncé suivant, ou plutôt son corollaire. Ce qui est beaucoup plus difficile, est de réaliser un groupe fini G comme groupe de Galois d'une extension galoisienne finie d'un corps donné, comme du corps $\mathbb{Q}$ par exemple.

PROPOSITION 8.1. *Soit L un corps et G un sous-groupe fini du groupe $\mathrm{Aut}(L)$ de tous les automorphismes de L. Alors, l'extension L/L^G est une extension galoisienne finie de degré $|G|$ et*

$$G = \mathrm{Gal}(L/L^G).$$

DÉMONSTRATION. Montrons que L/L^G est algébrique, normale et séparable. Soit $x \in L$. L'orbite Gx de x sous l'action de G est finie. Soient $x_1, \ldots, x_n$ les éléments de Gx. Pour tout $\sigma \in G$, il existe une permutation $\pi = \pi(\sigma) \in S_n$ telle que

$$\sigma(x_i) = x_{\pi(i)}$$

quel que soit i. Soit

$$Q = (X - x_1) \cdots (X - x_n) = X^n - \sigma_1(x_1, \ldots, x_n)X^{n-1} + \cdots + (-1)^n \sigma_n(x_1, \ldots, x_n),$$

où $\sigma_1, \ldots, \sigma_n$ sont les polynômes symétriques élémentaires. Comme

$$\sigma(\sigma_i(x_1, \ldots, x_n)) = \sigma_i(\sigma(x_1), \ldots, \sigma(x_n)) = \sigma_i(x_{\pi(1)}, \ldots, x_{\pi(n)}) = \sigma_i(x_1, \ldots, x_n)$$

quel que soit i, on a $Q \in L^G[X]$. Comme $x \in Gx$, on a $Q(x) = 0$ et x est algébrique sur L^G. Comme Q est complètement décomposé dans $L[X]$, l'extension L/L^G est normale. Comme toutes les racines de Q sont simples, x est séparable sur L^G. Il s'ensuit que L/L^G est une extension galoisienne.

Pour finir, on montre que la dimension de L comme L^G-espace vectoriel est $\leq |G|$. D'après le Lemme de Dedekind, on aura que la L^G-dimension de L est égale à $|G|$ et que $G = \mathrm{Aut}(L/L^G)$. Afin de montrer que la L^G-dimension de L est $\leq |G|$, montrons que toute famille de $n+1$ éléments

$x_1, \ldots, x_{n+1}$ de L est L^G-liée, où $n = |G|$. Soient $\sigma_1, \ldots, \sigma_n$ les éléments de G. Considérons le système de n équations linéaires homogènes

$$\begin{aligned} \sigma_1(x_1)\lambda_1 + \cdots + \sigma_1(x_{n+1})\lambda_{n+1} &= 0 \\ \vdots \qquad\qquad & \qquad \vdots \\ \sigma_n(x_1)\lambda_1 + \cdots + \sigma_n(x_{n+1})\lambda_{n+1} &= 0 \end{aligned}$$

en les inconnues $\lambda_1, \ldots, \lambda_{n+1}$ à coefficients dans le corps L. Comme le nombre d'inconnues est strictement plus grand que le nombre d'équations, ce système possède une solution non triviale, c-à-d, il existe $\lambda_1, \ldots, \lambda_{n+1} \in L$, non tous nuls, tels que

$$\sigma_i(x_1)\lambda_1 + \cdots + \sigma_i(x_{n+1})\lambda_{n+1} = 0$$

quel que soit $i = 1, \ldots, n$. Quitte à renuméroter la famille $x_1, \ldots, x_{n+1}$, on peut supposer que $\lambda_{n+1} \neq 0$, et même que $\lambda_{n+1} = 1$:

$$\sigma_i(x_1)\lambda_1 + \cdots + \sigma_i(x_n)\lambda_n + \sigma_i(x_{n+1}) = 0 \tag{2}$$

quel que soit $i = 1, \ldots, n$.

D'après le Lemme de Dedekind, il existe $\lambda \in L$ tel que

$$\sigma_1(\lambda) + \cdots + \sigma_n(\lambda) \neq 0$$

dans L. En effet, s'il n'existe pas de tel λ, on aurait

$$\sigma_1(\lambda) + \cdots + \sigma_n(\lambda) = 0$$

quel que soit $\lambda \in L$, c-à-d,

$$\sigma_1 + \cdots + \sigma_n = 0$$

dans $\mathrm{Hom}_{L^G}(L, L)$, ce qui contredirait le Lemme de Dedekind qui dit que $\mathrm{Hom}(L/L^G, L/L^G)$ est libre dans le L-espace vectoriel $\mathrm{Hom}_{L^G}(L, L)$.

Multiplions toutes les équations 2 par λ pour obtenir

$$\sigma_i(x_1)\lambda\lambda_1 + \cdots + \sigma_i(x_n)\lambda\lambda_n + \sigma_i(x_{n+1})\lambda = 0$$

quel que soit $i = 1, \ldots, n$. En appliquant σ_i^{-1} à chaque i-ième équation, on obtient

$$x_1\sigma_i^{-1}(\lambda\lambda_1) + \cdots + x_n\sigma_i^{-1}(\lambda\lambda_n) + x_{n+1}\sigma_i^{-1}(\lambda) = 0$$

quel que soit $i = 1, \ldots, n$. Prenons la somme de ces équations pour obtenir

$$x_1\mu_1 + \cdots + x_n\mu_n + x_{n+1}\mu_{n+1} = 0$$

où

$$\mu_j = \sum_{i=1}^{n} \sigma_i^{-1}(\lambda\lambda_j) = \sum_{i=1}^{n} \sigma_i(\lambda\lambda_j)$$

pour $j = 1, \ldots, n$ et

$$\mu_{n+1} = \sum_{i=1}^{n} \sigma_i^{-1}(\lambda) = \sum_{i=1}^{n} \sigma_i(\lambda).$$

Il est clair que $\mu_j \in L^G$, pour $j = 1, \ldots, n+1$, et que $\mu_{n+1} \neq 0$ par choix de λ. Cela montre que $x_1, \ldots, x_{n+1}$ est L^G-liée. □

COROLLAIRE 8.2. *Soit G un groupe fini. Alors, il existe une extension galoisienne L/K dont le groupe de Galois* $\mathrm{Gal}(L/K)$ *est isomorphe à G.*

DÉMONSTRATION. Soit $n = |G|$. Faisant agir G sur lui-même par translation à gauche, on obtient un morphisme injectif

$$\alpha \colon G \to S_n$$

après avoir numéroté les éléments de G. Le groupe S_n agit fidèlement sur l'anneau $\mathbb{Z}[X_1, \ldots, X_n]$ en définissant $\pi(X_i) = X_{\pi(i)}$ pour toute permutation $\pi \in S_n$. Le groupe G agit donc également fidèlement sur cet anneau à travers le morphisme α. Comme cette action en est une par automorphismes, elle s'étend automatiquement au corps des fractions

$$L = \mathbb{Q}(X_1, \ldots, X_n)$$

de l'anneau $\mathbb{Z}[X_1, \ldots, X_n]$. En posant $K = L^G$, on a une extension galoisienne L/K de groupe de Galois isomorphe à G d'après la proposition précédente. □

EXEMPLE 8.3. Soit $n \in \mathbb{N}$. L'action du groupe symétrique S_n sur le corps $L = \mathbb{Q}(X_1, \ldots, X_n)$ laisse fixes tous les polynômes symétriques élémentaires $\sigma_1, \ldots, \sigma_n$. On a donc

$$K = \mathbb{Q}(\sigma_1, \ldots, \sigma_n) \subseteq \mathbb{Q}(X_1, \ldots, X_n)^{S_n} = L^{S_n}.$$

D'après Exemple 6.10, l'extension L/K est de degré $n!$. D'après Proposition 8.1, l'extension L/L^{S_n} est également de degré $n!$. Il s'ensuit que

$$\mathbb{Q}(\sigma_1, \ldots, \sigma_n) = \mathbb{Q}(X_1, \ldots, X_n)^{S_n} = L^{S_n},$$

et l'extension

$$\mathbb{Q}(X_1, \ldots, X_n)/\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$$

est galoisienne de groupe de Galois S_n.

Le résultat clé de la théorie de Galois est que toute extension galoisienne finie est de la forme L/L^G. Ensemble avec les résultats ci-dessous qui en découlent, ils constituent le Théorème Fondamental de la Théorie de Galois. On a découpé ce dernier en petits morceaux pour en faciliter la digestion.

THÉORÈME 8.4. *Soit L/K une extension finie galoisienne. Alors*

$$L^{\mathrm{Gal}(L/K)} = K.$$

Explicitement, un élément x de L appartient à K si et seulement si pour tout $\sigma \in \mathrm{Gal}(L/K)$ on a $\sigma(x) = x$.

DÉMONSTRATION. Ecrivons $G = \mathrm{Gal}(L/K)$ pour simplifier la notation. Comme L/K est finie, normale et séparable, on a

$$|G| = [L : K].$$

Comme $\sigma(x) = x$ pour tout $x \in K$, on a $K \subseteq L^G$. D'après Proposition 8.1, on a

$$[L : K] = [L : L^G] \cdot [L^G : K] = |G| \cdot [L^G : K] = [L : K] \cdot [L^G : K].$$

Il s'ensuit que $[L^G : K] = 1$, et $L^G = K$. □

Ce résultat généralise donc l'énoncé bien connu qu'un nombre complexe est réel si et seulement s'il est égal à son conjugué complexe. On peut encore dire sur ce résultat qu'il dit simplement que l'application $F \colon \mathcal{G} \to \mathcal{E}$ définie ci-dessus envoie le plus grand élément de $\mathcal{G}$ sur le plus petit de $\mathcal{E}$.

THÉORÈME 8.5. *Soit L/K une extension galoisienne finie. Soient*

$$\mathcal{E} = \{M/K \mid M/K \text{ est une sous-extension de } L/K\},$$

et

$$\mathcal{G} = \{H \mid H \text{ est un sous-groupe de } \mathrm{Gal}(L/K)\}.$$

Alors, les applications décroissantes

$$A \colon \mathcal{E} \to \mathcal{G}, \qquad M/K \mapsto \mathrm{Gal}(L/M)$$

et

$$F \colon \mathcal{G} \to \mathcal{E}, \qquad H \mapsto L^H$$

sont des bijections et des applications réciproques l'une de l'autre. Plus explicitement,

$$L^{\mathrm{Gal}(L/M)} = M \quad \text{et} \quad \mathrm{Gal}(L/L^H) = H$$

quels que soient la sous-extension M/K de L/K et le sous-groupe H de $\mathrm{Gal}(L/K)$. De plus,

$$|\mathrm{Gal}(L/M)| = [L : M] \quad \text{et} \quad [L : L^H] = |H|.$$

DÉMONSTRATION. Soit M/K une sous-extension de L/K. Comme L/K est galoisienne et finie, l'extension L/M est galoisienne et finie. D'après Théorème 8.4,

$$L^{\mathrm{Gal}(L/M)} = M.$$

Comme L/M est galoisienne et finie, on a bien $|\mathrm{Gal}(L/M)| = [L : M]$.

Soit H un sous-groupe de $\mathrm{Gal}(L/K)$. D'après Proposition8.1, on a

$$H = \mathrm{Gal}(L/L^H) \quad \text{et} \quad [L : L^H] = |H|.$$ □

On peut formuler l'énoncé précédent encore différemment. Soit $\mathcal{G}^{\mathrm{op}}$ l'ensemble $\mathcal{G}$, mais muni de l'ordre partiel opposé :

$$G \leq H \Leftrightarrow G \supseteq H.$$

L'énoncé précédent dit alors que l'application

$$A\colon \mathcal{E} \to \mathcal{G}^{\mathrm{op}}$$

est une isomorphisme d'ensembles partiellement ordonnés. Son morphisme réciproque est F. Comme conséquence, on a

$$\sup A(\mathcal{F}) = A(\sup \mathcal{F}) \quad \text{et} \quad \inf A(\mathcal{F}) = A(\inf \mathcal{F}),$$

quel que soit le sous-ensemble $\mathcal{F}$ de $\mathcal{E}$. Explicitement et plus concrètement, cela veut dire que

$$\mathrm{Gal}(L/M) \cap \mathrm{Gal}(L/N) = \mathrm{Gal}(L/MN) \quad \text{et} \quad \mathrm{Gal}(L/M) \cdot \mathrm{Gal}(L/N) = \mathrm{Gal}(L/(M \cap N),$$

lorsque M/K et N/K sont des sous-extensions d'une extension galoisienne finie L/K. Comme l'application F de $\mathcal{G}^{\mathrm{op}}$ vers $\mathcal{E}$ est également un isomorphisme d'ensembles partiellement ordonnés, on peut en tirer les énoncés analogues

$$L^G \cdot L^H = L^{G \cap H} \quad \text{et} \quad L^G \cap L^H = L^{GH}$$

lorsque G et H sont des sous-groupes de $\mathrm{Gal}(L/K)$.

THÉORÈME 8.6. *Soit L/K une extension galoisienne finie. Soit M/K une sous-extension. Alors, M/K est galoisienne si et seulement si le sous-groupe $\mathrm{Aut}(L/M)$ de $\mathrm{Aut}(L/K)$ est distingué. Dans ce cas, le morphisme de restriction*

$$\rho\colon \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$$

est bien défini, et est surjectif de noyau $\mathrm{Gal}(L/M)$. En particlier, le morphisme induit

$$\bar{\rho}\colon \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \to \mathrm{Gal}(M/K)$$

est un isomorphisme.

DÉMONSTRATION. Supposons que M/K est galoisienne. Montrons d'abord que $\sigma(M) = M$ pour tout $\sigma \in \mathrm{Gal}(L/K)$. En effet, soit $\bar{K}$ une clôture algébrique de L. C'est donc également une clôture algébrique de K contenant L/K comme sous-extension. Soit $\sigma \in \mathrm{Gal}(L/K)$. D'après Proposition 6.3, le morphisme σ s'étend à un endomorphisme σ' de l'extension $\bar{K}/K$. Comme M/K est normale, on a $\sigma'(M) = M$. Comme $M \subseteq L$, on a bien $\sigma(M) = \sigma'(M) = M$.

Il s'ensuit que l'application de restriction ρ est bien définie. C'est évidemment un morphisme de groupes. En particulier, son noyau, $\mathrm{Gal}(L/M)$, est un sous-groupe distingué de $\mathrm{Gal}(L/K)$.

Réciproquement, supposons que $\mathrm{Gal}(L/M)$ est distingué dans $\mathrm{Gal}(L/K)$. Montrons que M/K est galoisienne. Comme sous-extension d'une extension séparable, M/K est séparable. Il suffit donc de montrer que M/K est normale[4]. Soit $\sigma' \in \mathrm{Aut}(\bar{K}/K)$ et montrons que $\sigma'(M) \subseteq M$. Il suffit de montrer que $\tau(\sigma'(x)) = \sigma'(x)$ quel que soit $x \in M$ et $\tau \in \mathrm{Gal}(L/M)$, d'après le résultat clé de la Théorie de Galois. Soit $x \in M$ et $\tau \in \mathrm{Gal}(L/M)$. Comme L/K est normale, $\sigma'(L) = L$, et la restriction σ de σ' à L est un élément de $\mathrm{Gal}(L/K)$. Comme $\mathrm{Gal}(L/M)$ est distingué dans $\mathrm{Gal}(L/K)$, on a $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/M)$. En particulier,

$$\sigma^{-1}\tau\sigma(x) = x.$$

D'où $\tau(\sigma(x)) = \sigma(x)$, et donc aussi $\tau(\sigma'(x)) = \sigma'(x)$. Cela montre que M/K est normale.

Supposons maintenant que M/K est galoisienne. On a vu ci-dessus que le morphisme ρ est alors bien défini, et que son noyau est égal au sous-groupe $\mathrm{Gal}(L/M)$. L'image de ρ est donc d'ordre

$$\frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/M)|} = \frac{[L:K]}{[L:M]} = [M:K] = |\mathrm{Gal}(M/K)|.$$

Du coup, ρ est surjectif. □

EXEMPLE 8.7. Soit L l'extension de rupture du polynôme $X^3 - 2$ sur $K = \mathbb{Q}$. D'après Exemple 6.7,

$$L = \mathbb{Q}[\sqrt[3]{2}, \xi] \subseteq \mathbb{C}$$

où ξ est une racine cubique primitive de l'unité, et l'extension $L/\mathbb{Q}$ est une extension de degré 6. Elle est normale comme toute extension de rupture, et elle est séparable car $\mathrm{car}(\mathbb{Q}) = 0$. L'extension $L/\mathbb{Q}$ est donc une extension galoisienne finie.

4. Voilà qui explique la terminologie d'extension «normale», si $\mathrm{Gal}(L/M)$ est distingué, *normal* en anglais, l'extension M/K est normale, et réciproquement !

Déterminons les sous-extensions de $L/\mathbb{Q}$. Pour ce faire, on détermine le groupe de Galois de $L/\mathbb{Q}$. L'action du groupe de Galois $\mathrm{Gal}(L/\mathbb{Q})$ sur l'ensemble des racines du polynôme X^3-2 est fidèle car ces racines engendrent l'extension. Soient

$$z_i = \xi^i \sqrt[3]{2},$$

pour $i=1,2,3$, les racines de X^3-2 dans $\mathbb{C}$. On en déduit un morphisme de groupes

$$\alpha\colon \mathrm{Gal}(L/K) \to S_3$$

où $\alpha(\sigma)$ est l'unique permutation π dans S_3 telle que

$$\sigma(z_i) = z_{\pi(i)}$$

quel que soit i. Comme l'action est fidèle, α est injectif. Comme $|\mathrm{Gal}(L/K)| = [L:K] = 6 = |S_3|$, le morphisme α est un isomorphisme de groupes. Toute permutation π dans S_3 détermine donc un unique automorphisme σ de L/K. On identifiera $\mathrm{Gal}(L/K)$ avec S_3 à travers cet isomorphisme.

Les sous-groupes de S_3, autres que ses sous-groupes triviaux $\{\mathrm{id}\}$ et S_3, sont

$$\langle(1\,2)\rangle, \langle(1\,3)\rangle, \langle(2\,3)\rangle, \langle(1\,2\,3)\rangle$$

Ce dernier est l'unique sous-groupe distingué A_3 de S_3.

Déterminons les sous-extensions de $L/\mathbb{Q}$ correspondantes. La tranposition $(1\,2)$ fixe l'élément $z_3 = \sqrt[3]{2}$. On a donc

$$\mathbb{Q}[\sqrt[3]{2}] \subseteq L^{\langle(1\,2)\rangle}.$$

Comme $[L : L^{\langle(1\,2)\rangle}] = |\langle(1\,2)\rangle| = 2$ et $[L:\mathbb{Q}[\sqrt[3]{2}]] = 2$ également, on a

$$L^{\langle(1\,2)\rangle} = \mathbb{Q}[\sqrt[3]{2}].$$

De même,

$$L^{\langle(1\,3)\rangle} = \mathbb{Q}[\xi^2\sqrt[3]{2}]$$

et

$$L^{\langle(2\,3)\rangle} = \mathbb{Q}[\xi\sqrt[3]{2}].$$

En ce qui concerne la sous-extension $M/\mathbb{Q}$ correspondante au sous-groupe A_3 de S_3, si on ne la devine pas, on pourra avoir l'idée que

$$(1\,2\,3)\cdot\tfrac{z_2}{z_1} = \tfrac{z_3}{z_2} = \xi = \tfrac{z_2}{z_1}.$$

Ce qui montre que $(1\,2\,3)\cdot\xi = \xi$, et que

$$\mathbb{Q}[\xi] \subseteq L^{\langle(1\,2\,3)\rangle}.$$

Comme $[L : L^{\langle(1\,2\,3)\rangle}] = |\langle(1\,2\,3)\rangle| = 3$ et $[L:\mathbb{Q}[\xi]] = 3$ également, on a donc

$$L^{\langle(1\,2\,3)\rangle} = \mathbb{Q}[\xi].$$

Remarquons que l'extension $\mathbb{Q}[\xi]/\mathbb{Q}$ est effectivement galoisienne, comme toute extension de degré 2 en caractéristique $\neq 2$. De plus, son groupe de Galois $\{\mathrm{id}, \gamma\}$, où γ est la conjugaison complexe sur $\mathbb{Q}[\xi]$, est effectivement isomorphe au quotient

$$\tfrac{\mathrm{Gal}(L/\mathbb{Q})}{\mathrm{Gal}(L/\mathbb{Q}[\xi])} = \tfrac{S_3}{A_3} \cong \{\pm 1\}.$$

Si on n'a pas l'idée que z_2/z_1 est fixé par $(1\,2\,3)$, la méthode générale c'est de chercher les vecteurs propres pour la valeur propre de l'endomorphisme $\mathbb{Q}$-linéaire

$$(1\,2\,3)\colon L \to L.$$

On prend, par exemple, la $\mathbb{Q}$-base

$$1,\ \sqrt[3]{2},\ \sqrt[3]{4}, \xi\sqrt[3]{2}, \xi\sqrt[3]{4}$$

du $\mathbb{Q}$-espace vectoriel L. On écrit la matrice de l'endomorphisme $\mathbb{Q}$-linéaire $(1\,2\,3)$ dans cette base :

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \end{pmatrix}$$

Par exemple, la troisième colonne s'explique par le calcul

$$(1\,2\,3)\cdot\sqrt[3]{4} = (1\,2\,3)\cdot(\sqrt[3]{2})^2 = ((1\,2\,3)\cdot\sqrt[3]{2})^2 = (\xi\sqrt[3]{2})^2 =)(-\xi-1)\sqrt[3]{4} = -\sqrt[3]{4} - \xi\sqrt[3]{4}.$$

Puis on détermine les vecteurs propres pour la valeur propre 1 de cette matrice...

Au final, les sous-extension de l'extension

$$\mathbb{Q}[\sqrt[3]{2},\xi]/\mathbb{Q}$$

sont

$$\mathbb{Q}/\mathbb{Q},\ \mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q},\ \mathbb{Q}[\xi\sqrt[3]{2}]/\mathbb{Q},\ \mathbb{Q}[\xi^2\sqrt[3]{2}]/\mathbb{Q}\quad\text{et}\quad\mathbb{Q}[\sqrt[3]{2},\xi]/\mathbb{Q}.$$