Table des matières

Introduction

Ce travail tente de donner des idées sur la résolution des équations algébriques : partant d'un corps K, on se donne une équation algébrique à coefficient dans K, qui n'a pas toutes ses racines dans K (par exemple $X^n - d$), on ajoute à K toutes les combinaisons algébriques possibles d'une racine $\alpha \notin K$ de cette équation, on obtient un corps K_1 avec $(K \subset K_1)$ et puis généralité sur les fonctions symétriques.

D'après ce qu'on a vu, tous les résultats nécessaires pour commencer l'étude de la théorie de Galois ont bien été établis.

Ainsi, ce travail se compose de quatre parties :
Le premier chapitre
Nous rappelons certaines définitions et propriétés concernant les groupes, les anneaux, les corps, les extensions.
Le deuxième chapitre
Nous allons donner quelques définitions, exemples et théorèmes élémentaires.
Le troisième chapitre
Dans La troisième partie, les notions de corps de rupture seront présentées, ainsi que des propriétés sur les clôtures algébriques.
Le quatrième chapitre
Cette partie est réservé pour les fonctions symétriques.

1 Rappels

1.1 Groupe

Définition 1.1.1. *Une loi de composition interne (G, T) est dite un* ***groupe*** *si :*

i) *La loi T est associative*

ii) *Il existe un élément neutre*

iii) *Tout élément est symétrisable.*

Exemple 1.1.1. $(\mathbb{Z}, +)$, $(\mathbb{R}^*, \times)$ *sont deux groupes.*

1.2 Anneau

Définition 1.2.1. *On appelle* ***anneau*** *un ensemble A muni de deux lois de composition internes, une addition et une multiplication telles que :*

i) *A est un groupe commutatif pour l'addition*

ii) *La multiplication est associative*

iii) *La multiplication est distributive par rapport à l'addition.*

Exemple 1.2.1. $(\mathbb{Z}, +, .)$,$(\mathbb{Q}, +, .)$,$(\mathbb{R}, +, .)$,$(\mathbb{C}, +, .)$ *sont des anneaux commutatifs.*

Remarque 1.2.1.

• *Si en outre, la multiplication est commutatif, on dit que A est un* ***anneau commutatif****.*

• *Si A possède un élément neutre pour la multiplication, on note 1 cet élément unité et on dit que A est* ***anneau unitaire****.*

• *Un anneau A est dit* ***intègre*** *si pour tous $x, y \in A$, on a :*

$xy = 0 \Longrightarrow x = 0$ *ou* $y = 0$.

Exemple 1.2.2. *Les anneaux* $(\mathbb{Z}, +, .)$, $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$, $(\mathbb{C}, +, .)$ *sont commutatifs unitaires et intègres.*

Proposition 1.2.1. *Soient* A *un anneau unitaire et* $U(A) = \{x \in A$ *et* $xy = 1$ *et* $yx = 1$ *avec* $y \in A\}$ *l'ensemble des éléments inversibles. Alors* $(U(A), .)$ *est un groupe.*

Démonstration
- $U(A) \neq \varnothing$ car $1 \in U(A)$.
- Soit $x, y \in U(A)$. Alors $xy^{-1} \in U(A)$ car $xy^{-1}yx^{-1} = 1$. Donc $U(A)$ est un groupe pour la multiplication.

1.3 Idéal

La notion d'idéal joue un rôle central dans la théorie des anneaux.

Définition 1.3.1. *Un sous ensemble* I *d'un anneau* $(A, +, .)$ *est dit un idéal si :*

- $(I, +)$ *est un groupe*
- $\forall x \in I, \forall y \in A,$ *on a* $xy \in I$.

Exemple 1.3.1.
1. les seuls idéaux de l'anneau $(\mathbb{Z}, +, .)$ *sont de type* $n\mathbb{Z}$*, car les seuls sous-groupes de* $(\mathbb{Z}, +, .)$ *sont* $n\mathbb{Z}$.
2. Soit A *un anneau et* $a \in A$. *L'ensemble :* $< a >= Aa = \{xa \ / \ x \in A\}$ *est un idéal de* A.

Définition 1.3.2. *Idéaux premiers et idéaux maximaux*

Soient A *un anneau commutatif unitaire et* P *un idéal de* A *:*
1. P *est dit* ***premier*** *si* $\forall x, y \in A$, $xy \in P \Rightarrow x \in P$ *ou* $y \in P$.
2. P *est dit* ***maximal*** *si* $P \neq A$ *et si les seuls idéaux compris entre* P *et* A *sont* P *et* A.

1.4 polynôme irréductible

Définition 1.4.1. *Soient* A *un anneau,* a *et* b *deux éléments de* A. *On dit que* a *divise* b*, et on note* $a|b$*, s'il existe* $c \in A$ *tel que* $b = ac$*, autrement dit, cela veut dire que* $< b > \subseteq < a >$.

Définition 1.4.2. *Soit $P \in K[X]$ un polynôme de $\deg P > 1$. On dit que P est **irréductible** si pour tout $Q \in K[X]$ divisant P, alors, soit $Q \in K^*$, soit il existe $\lambda \in K^*$ tel que $Q = \lambda P$.*

Remarque 1.4.1.
• *Un polynôme irréductible P est donc un polynôme non constant dont les seuls diviseurs de P sont les constantes ou P lui-même (à une constante multiplicative près).*
• *Dans le cas contraire, on dit que P est **réductible**; il existe alors des polynômes A, B de $K[X]$ tels que $P = AB$, avec $\deg A > 1$ et $\deg B > 1$.*

Définition 1.4.3. *Soient A un anneau et $p \in A$. On dit que p est irréductible si :*
- $p \notin U(A)$.
- Si $p = ab$, avec $a, b \in A$, alors $a \in U(A)$ ou $b \in U(A)$.

1.5 Corps et sous-corps :

Définition 1.5.1. *Un **corps** est un anneau unitaire dans lequel tout élément non nul est inversible, c'est à dire que $A - \{0\}$ est un groupe pour la multiplication. Si la multiplication d'un corps est commutative, on dit que le corps est commutatif.*

Définition 1.5.2. *Soit K un corps et L une partie de K. On dit que L est un **sous-corps** de K si :*
- $L \neq \emptyset$
- $\forall\ x, y \in L : x - y \in L$
- $\forall (x, y) \in (L^*)^2 : xy^{-1} \in L^*$.
L'intersection d'une famille quelconque de $sous - corps$ de K est un sous-corps de K.

Exemple 1.5.1. *$(\mathbb{R}, +, .)$ est un corps et il admet $(\mathbb{Q}, +, .)$ comme un sous-corps.*

1.6 Extension

Définition 1.6.1. *On dit qu'un corps E est une **extension** du corps K si, et seulement si, K est un sous-corps de E, autrement dit $K \subseteq E$.*

Exemple 1.6.1.
1. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}/a, b \in \mathbb{Q}\}$ est une extension de $\mathbb{Q}$.

2. $\mathbb{C}$ est une extension de $\mathbb{R}$.
3. Tout corps K est un sous-corps du corps $K(X)$ des fractions rationnelle à coefficient dans K : $K(X)$ est une extension de K.

Définition 1.6.2. *Soit L une extension d'un corps K. Alors L est K-espace vectoriel tel que l'addition vectoriel est l'addition dans L est la multiplication par un scalaire est la restriction de la multiplication de L dans $K \times L$.*
On appelle le degré de l'extension L de K est la dimension de L comme un K-espace vectoriel, et on le note par $[L : K]$.

Remarque 1.6.1. *Si $[L : K] = 2$ on dit que l'extension est quadratique.*

Exemple 1.6.2. *L'inclusion de corps $\mathbb{R} \subset \mathbb{C}$ est une extension finie avec $[\mathbb{C} : \mathbb{R}] = 2$; $\mathbb{C}$ est un espace vectoriel sur $\mathbb{R}$ de dimension 2.*

Extension simple

Une extension E de K est simple si, et seulement si, $\exists a \in E$ tel que : $E = K(a)$.

Exemple 1.6.3. *$\mathbb{C}$ est une extension simple de $\mathbb{R}$ car $\mathbb{C} = \mathbb{R}(i)$.*

Élément algébrique

Soit $K \hookrightarrow E$ une extension de corps, x un élément de E. On dit que x est algébrique sur K s'il existe un polynôme non nul $P \in K[X]$ tel que $P(x) = 0$. x est transcendante dans le cas contraire.

Exemple 1.6.4.
$\sqrt{3} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$, en effet :
$\sqrt{3}$ est un racine de $P(X) = X^2 - 3 \in \mathbb{Q}[X]$.

Extension algébrique

Une extension E de K est dite algébrique si, et seulement si, tout élément a de E est algébrique sur K.

Théorème 1.6.1. *Une extension simple $E = K(a)$ est algébrique si, et seulement si, a est algébrique sur K.*
(En général : l'extension $E = K(a_1, a_2, ..., a_n)$ de K est algébrique si, et seulement si, les éléments $a_1, a_2, ..., a_n$ sont tous algébriques sur K).

Démonstration
Si a est algébrique sur K, alors E est une extension finie de K ce qui prouve que cette extension est algébrique.
Réciproquement, si l'extension E est algébrique, alors a élément de E, est algébrique sur K.

Théorème 1.6.2. *Si $K \subseteq L \subseteq E$,alors si $a \in E$ est algébrique sur K, alors il est algébrique sur L.*

Démonstration
Si a est algébrique sur K, alors a est une racine d'un polynôme $f \in K[X]$, mais $f \in L[X]$ car $K \subseteq L$. Il en résulte que a est algébrique sur L.

1.7 Le groupe symétrique

Soit E un ensemble quelconque. On munit l'ensemble S(E) des bijections de E sur E de la composition des applications. On sait que la composition est associative et que l'application identique est l'élément neutre, comme toute bijection admet une bijection réciproque alors tout élément de S(E) est inversible. Donc S(E) est un groupe pour la composition des applications qu'on appelle groupe symétrique de E.
Dans la suite, on prend $E := \{1, 2, ..., n\}$ et on note S(E) par S_n : un élément de S_n sera dit une permutation.

Représentation d'une permutation
Soit σ une permutation de S_n. On représente σ par une matrice :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & \cdots & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \cdots & \cdots & \sigma(n) \end{pmatrix}$$

où la première ligne représente l'ensemble de départ, et la second ligne l'ensemble d'arrivée, les éléments de la seconde ligne étant les images des éléments de la première ligne par σ.
L'élément neutre I_d est représenté par :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & \cdots & \cdots & n \\ 1 & 2 & \cdots & \cdots & \cdots & n \end{pmatrix}$$

et l'inverse σ^{-1} de σ est la permutation :

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \cdots & \cdots & \sigma(n) \\ 1 & 2 & \cdots & \cdots & \cdots & n \end{pmatrix}$$

Pour alléger les écritures, on notera, pour tout couple (σ, ψ) d'élément de S_n, $\sigma\psi$ à la place de $\sigma \circ \psi$. On parlera de produit de deux permutations plutôt que de composition de deux permutations.

2

Expression des racines d'une équation

Notre problème maintenant est de trouver une « formule » donnant ces racines en fonction des coefficients du polynôme.

2.1 Équation algébrique

Définition 2.1.1. *Une équation algébrique ou polynômiale est une équation de la forme :*

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0$$

où l'inconnue est x et $a_0, a_1, ..., a_{n-1}$ sont des nombres connus qu'on appelle coefficients de l'équation avec $n \in \mathbb{N}$. On dit que l'équation est de degré n.

Expressions rationnelles :
Soit $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0$ une équation algébrique. Si on arrive à exprimer les racines en fonction des coefficients du polynôme, faisant intervenir des « opérations » du corps $\mathbb{C}$ (addition, multiplication, soustraction, division). On dira que les racines s'expriment rationnellement en fonction des a_i $\forall i = \{0, 1, ..., n-1\}$.

Exemple 2.1.1.
1. L'équation $2x - 5 = 0$ admet la solution $\frac{5}{2}$.
2. L'équation $x^2 - 2 = 0$ a pour solution $\pm\sqrt{2}$ qui sont hors du corps $\mathbb{Q}$.

Remarque 2.1.1. *Il est hors de question d'exprimer les racines d'un polynôme arbitraire à l'aide des coefficients si l'on ne s'autorise que ces opérations rationnelles. En d'autres termes, les racines d'un polynôme n'ont aucune raison d'appartenir au corps engendré par les coefficients du polynôme.*

Expression algébrique

En partant de la famille d'éléments $(a_i)_{i\in I}$ de $\mathbb{C}$, il est logique de considérer non seulement les expressions rationnelles des a_i (c'est-à-dire les éléments du corps engendré), mais tous les complexes que l'on peut écrire à partir des a_i à l'aide d'opérations rationnelles et d'extraction de racines. On dira qu'un élément ainsi obtenu s'exprime **algébriquement** à l'aide des a_i .

Exemple 2.1.2. $\sqrt{2}+i$, $\sqrt[3]{1+\sqrt{2}}$, $\sqrt[3]{\frac{2-\sqrt[4]{2}}{\sqrt{3}}}-\frac{1+\sqrt[5]{3+\sqrt{2}}}{\sqrt[4]{-5}}$ *s'expriment algébriquement à partir de* $\mathbb{Q}$.

2.2 Résolution par radicaux

Définition 2.2.1. *Toute équation algébrique de la forme* $x^n - d = 0$ *avec* $d \in \mathbb{C}, n \in \mathbb{N}^*$, *s'appelle* ***équation binomiale****.*

L'étude d'une équation de Binôme montre que si l'on veut avoir une chance d'exprimer les racines de tout polynôme à partir des coefficients il faut au moins, outre les opérations rationnelles, admettre les extractions de racines n-ièmes, pour tout n, c'est-à-dire « adjoindre » au corps engendré par les coefficients, les éléments qui ont une puissance dans ce corps.

Définition 2.2.2. *Un élément ayant une puissance dans un corps donné s'appelle un* ***radicale*** *relatif à ce corps.*

Remarque 2.2.1.
• *Les radicaux relatifs à un corps sont donc toutes les racines des équations binômes à coefficients dans ce corps.*
• *Étant donné un nombre complexe d et un entier naturel non nul n. On appelle racine n-ième de d tout nombre complexe z tel que* $x^n = d$.
•*Si n un entier naturel non nul, on appelle racine n-ième de l'unité toute racine n-ième de 1 c'est à dire* $x^n = 1$.
• *Pour* $n \in \mathbb{N}^*$, *il y a exactement n racines n-ième de l'unité qui sont données par :*

$$w_k = \exp(i\frac{2k\pi}{n}) = \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n})$$

avec $(0 \preceq k \preceq n-1)$

Proposition 2.2.1.
• *L'équation* $x^n = 0$ *tel que* $d \in \mathbb{C}, n \in \mathbb{N}^*$ *admet 0 comme l'unique racine n-ième.*
• *Si d est un réel et si n est impair, il y a une seule racine n-ième réelle de d, que l'on désigne en général par* $\sqrt[n]{d}$.

Démonstration
On a $x^n = \mid d \mid \iff \frac{x^n}{|d|} = 1$ *or n est impair :+* $n = 2p + 1$
donc :

$$\frac{x^{2p+1}}{\mid d \mid} = 1$$

$$\iff (\frac{x}{\sqrt[2p+1]{\mid d \mid}})^{2p+1} = 1$$

Pour $r = \sqrt[2p+1]{\mid d \mid}$ *l'équation devient :* $(\frac{x}{r})^{2p+1} = 1$
On sait que les racines sont de la forme :

$$w_k = \exp(\frac{2i\pi k}{n})$$

tel que $k = \{0, 1, ..., n-1\}$, $w_0 = \sqrt[n]{\mid d \mid} \in \mathbb{R}$ *est un racine réel. En effet, soit* w_k *un autre racine réelle avec* $k \in \{1, ..., n-1\}$ *, on a*

$$w_k = \exp(\frac{2i\pi k}{n}) = cos(\frac{2\pi k}{n}) + isin(\frac{2\pi k}{n})$$

et comme $w_k \in \mathbb{R}$ *alors* $sin(\frac{2\pi k}{n}) = 0$ *, donc :*

$$\frac{2\pi k}{n} = q\pi \text{ tel que } q \in \mathbb{Z}$$

$$\implies \frac{2k}{n} = q \text{ (plus précieusement } q \in \mathbb{N})$$

donc n divise 2k, comme n est impaire le plus petit entier paire divisible par n est 2n
alors $2n \leqslant 2k \implies n \leqslant k$ *contradiction*
D'où l'équation admet une seul racine réel.

• *Si d est un réel positif et si n est pair, il y a deux racines n-ièmes réelles de d opposées l'une de l'autre et c'est à la racine positive que l'on associe le symbole* $\sqrt[n]{d}$.

Démonstration

On a la solution est $w_k = \sqrt[n]{d}\exp(\frac{2i\pi k}{n})$ *avec n est pair alors n=2p.*
Pour k=0 : $w_0 = \sqrt[n]{d} \in \mathbb{R}$ *et* $k = \frac{n}{2}$ *tel que* $k \in \{0, ..., n-1\}$

$$w_{\frac{n}{2}} = \sqrt[n]{d}\exp(\frac{2\pi}{n} \times \frac{n}{2}i) = \sqrt[n]{d}\exp(i\pi) = -\sqrt[n]{d} \in \mathbb{R}.$$

Exemple 2.2.1. *L'équation* $x^4 - 1 = 0$ *admet les 4 racines n-ièmes de 1 :* $x_k = \exp(i\frac{2k\pi}{n})$ *avec* $n = 4$ *et* $(0 \preceq k \preceq 3)$*, d'où les solutions de l'équation sont les suivantes* $\{x_0 = 1, x_1 = i, x_2 = -1, x_3 = -i\}$.

Définition 2.2.3. *Les éléments d'un corps K sont bien sûr des radicaux relatifs à K et ce sont les seuls dans le cas d'un corps comme* $\mathbb{C}$ *puisque ce dernier contient toutes les racines de ses polynômes.*

Remarque 2.2.2. *Par contre,* $\sqrt{2}$ *ou i ou* $i+1$ *sont des radicaux relatifs à* $\mathbb{Q}$ *sans être dans* $\mathbb{Q}$ *:*
$(\sqrt{2})^2 = 2 \in \mathbb{Q}$, $i^2 = -1 \in \mathbb{Q}$ *et* $(i+1)^2 = 2i \notin \mathbb{Q}$
$(i+1)^4 = -4 \in \mathbb{Q}$
L'élément $\sqrt{2} + i$*, n'est pas un radical relatif à* $\mathbb{Q}$*, mais il s'exprime rationnellement à l'aide des radicaux relatifs à* $\mathbb{Q}$.

Définition 2.2.4. *Soit K un corps engendré par les coefficients d'une équation algébrique, on adjoint à K tous ses radicaux, puis toutes les expressions algébriques, cette adjonction donne une extension* K_r*, on l'appelle* ***la saturation par radicaux*** *de K.*

Définition 2.2.5. *On dit que les racines d'une équation algébrique s'expriment algébriquement à l'aide des coefficients, c'est équivalent à dire que ses racines appartiennent à la saturation par radicaux du corps K engendré par les coefficients : on dit que l'équation* $P = 0$ *est* ***résoluble par radicaux****.*

Exemple 2.2.2. *Soit* $\alpha = \sqrt{(2 + \sqrt[3]{3})}$ *est dans la saturation par radicaux de* $\mathbb{Q}$*. Pour l'obtenir, on peut passer d'abord de* $\mathbb{Q}$ *au corps* $\mathbb{Q}_1$ *engendré par* $\mathbb{Q}$ *et* $\sqrt[3]{3}$*, puis de* $\mathbb{Q}_1$ *au corps* $\mathbb{Q}_2$ *engendré par* $\mathbb{Q}_1$ *et une racine carrée de* $2 + \sqrt[3]{3} \in \mathbb{Q}$.

2.3 Indépendance algébrique

Définition 2.3.1. *Soient* $x_1, x_2, ..., x_n$ *des éléments d'une extension L d'un corps K, on dira qu'ils sont* ***algébriquement indépendants*** *sur K si le seul polynôme à n indéterminées sur K nul en* $(x_1, x_2, ..., x_n)$ *est le polynôme*

nul.
Par contre, si $(x_1, x_2, ..., x_n)$ *sont algébriquement dépendants sur* K*, alors il existe un polynôme non nul* $P \in K[X_1, X_2, ..., X_n]$ *vérifiant* $P(x_1, x_2, ..., x_n)$ *une telle égalité s'appelle une relation de dépendance algébrique sur* K *entre les* x_i *; on dit une relation de* ***dépendance rationnelle****.*

Exemple 2.3.1. *les relations de dépendance algébrique entre* $u = \sqrt{2}$ *et* $v = \sqrt{3}$ *sur* $\mathbb{Q}$ *seront :*

$$u^2 - 2 = 0, \text{ ou } v^2 - 3 = 0, \text{ ou } u^2 + v^2 = 5.$$

2.4 L'équation générale de n degré

Définition 2.4.1. *On dira que les éléments* $a_1, a_2, ..., a_n$ *sont algébriquement indépendants sur* $\mathbb{Q}$ *si, et seulement si, ces éléments ne satisfont aucune relation de la forme :*

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0$$

à coefficients non nuls ; on appellera ***équation générale*** *de degré n sur* $\mathbb{Q}$*.*

Il est bien connu depuis le 16 ème siècle que l'on peut résoudre par radicaux des équations de degré $n \preceq 4$. Par contre, selon un résultat célèbre d'Abel, l'équation générale de degré $n \succeq 5$ n'est pas résoluble par radicaux. Le problème de sa résolution consiste à exprimer ses racines à l'aide d'opération rationnelles et de radicaux à partir du corps $\mathbb{Q}(a_0, a_1, ..., a_{n-1})$ des fractions rationnelles à n indéterminées sur $\mathbb{Q}$, qui est le plus petit corps contenant les coefficients. On doit donc introduire la saturation par radicaux de ce corps, mais la difficulté provient de ce que le corps $\mathbb{Q}(a_0, a_1, ..., a_{n-1})$ n'est plus sous-corps de $\mathbb{C}$. On ne peut pas donc partir de ce grand « fourre -tout » qu'est $\mathbb{C}$ pour ensuite le diminuer, il faut partir de ce que l'on a et l'augmenter. C'est pour quoi, au lieu de faire la théorie sur les sous-corps de $\mathbb{C}$, on la fera sur un corps K arbitraire.

a-Équation de degré 2 :

Cette équation est de la forme : $x^2 + bx + c = 0$
Nous avons $u_0 - u_1 = \delta$ et $u_0 + u_1 = b$. En résolvant le système linéaire suivant :

$$\begin{cases} u_0 - u_1 = \delta \\ u_0 + u_1 = b \end{cases}$$

nous obtenons :

$$u_0 = \frac{-b+\delta}{2} \; et \; u_1 = \frac{-b-\delta}{2}$$

Alors

$$x^2 + bx + c = 0 \Leftrightarrow (x-u_0)(x-u_1) = 0$$
$$\Leftrightarrow T_1 T_2 = 0$$

Avec T_1 et T_2 des résolvantes partielles de l'équation $x^2+bx+c=0$ tel que $T_i = x - u_i \; et \; i = 0, ..., n$.

b-Équation de degré 3 :

On résout l'équation par la méthode de Cardan. Soit l'équation $x^3+px+q = 0$; la méthode de Cardan consiste à chercher x sous la forme $x = u+v$ afin d'obtenir une équation plus simple à résoudre. En remplaçant dans l'équation, on obtient :
$(u+v)^3 + p(u+v) + q = 0 \Leftrightarrow u^3+v^3+(u+v)(3uv+p)+q = 0$
On va imposer la condition $3uv+p=0$
donc $3uv+p=0 \Leftrightarrow uv = \frac{-p}{3}$.
Alors on obtient le système suivant :

$$\begin{cases} u^3 - v^3 = -q \\ (uv)^3 = -(\frac{p}{3})^3 \end{cases}$$
$$\Leftrightarrow \begin{cases} u^3 - v^3 = -q \\ u^3 v^3 = -(\frac{p}{3})^3 \end{cases}$$

Or, si on connait la somme et le produit de deux nombres ici(u^3, v^3) on peut trouver ces nombres comme solutions d'équation du second degré.
En effet :

$$(X-u^3)(X-v^3) = 0 \Leftrightarrow X^2 - X(u^3+v^3) - (\frac{p}{3})^3 = 0$$
$$\Leftrightarrow X^2 + Xq - (\tfrac{p}{3})^3 = 0$$

D'où,

$$x = u+v = \sqrt[3]{\frac{-q+\sqrt{q^2+4(\frac{p}{3})^3}}{2}} + \sqrt[3]{\frac{-q-\sqrt{q^2+4(\frac{p}{3})^3}}{2}}$$

alors toute équation de degré 3 est résoluble par radicaux.

c-Équation de degré 4 :

On résout l'équation par la méthode de Ferrari : Soit l'équation

$$x^4 + cx^2 + dx + e = 0$$

Deux cas sont alors possibles :
• si $d = 0$, l'équation $x^4 + cx^2 + e = 0$ est bicarrée, en posant $x' = x^2$ on retrouve une équation de degré 2.
• si $d \neq 0$ en posant $x' = x^2 + t$, où t paramètre à choisir judicieusement. Élevons au carré, et injectons l'équation $x^4 + cx^2 + dx + e = 0$:

$$\begin{aligned} x'^2 &= (x^2 + t)^2 \\ &= x^4 + 2tx^2 + t^2 \\ &= -cx^2 - dx - e + 2tx^2 + t^2 \\ &= (2t - c)x^2 - dx + (t^2 - e) \end{aligned}$$

Donc on a $(x^2+t)^2 = (2t-c)x^2-dx+(t^2-e)$, il reste à poser une condition sur t. L'idée de Ferrari est d'écrire le membre de droit de cette dernière équation sous la forme d'un carré, et ainsi d'obtenir $x'^2 = y^2 \Leftrightarrow (x' + y)(x' - y) = 0$, où $(x' + y)$ et $(x' - y)$ sont des équations de degré 2. Pour cela, choisissons t de manière à ce que le discriminant de $(2t - c)x^2 - dx + (t^2 - e)$ soit nul, c'est-à-dire $d^2 - 4(2t - c)(t^2 - e) = 0$
Nous savons résoudre une telle équation d'ordre 3 (Méthode de cardan). Une fois t déterminé, la résolution est simple, car :
x solution de $x^4 + cx^2 + dx + e = 0$
$d \neq 0 \Leftrightarrow x$ et solution de $(x' + y)(x' - y) = 0$
d'où $d^2 - 4(2t - c)(t^2 - e) = 0$. Nous savons résoudre ce dernier système, composé d'une équation de degré 4 factorisable en deux équations de degré 2, et d'une équation de degré 3.

3 Racines et corps de rupture

Le corps $\mathbb{C}$ des complexes joue le rôle d'un grand corps dans lequel « tout se passe ». On montre en fait que pour tout corps il existe un « grand corps » jouant ce rôle.

3.1 Corps de rupture d'un polynôme

Définition 3.1.1. *Un corps K est dit* ***corps algébriquement clos*** *si tout $P \in K[X]$ non constant a au moins une racine dans K.*

Définition 3.1.2. ***La clôture algébrique*** *d'un corps K est une extension algébrique de corps $K \hookrightarrow L$ telle que L est un corps algébriquement clos.*

Si K est algébriquement clos, tout polynôme irréductible de $K[X]$ est de degré 1.

Proposition 3.1.1. *Si K est algébriquement clos, tout $P \in K[X]$ de degré d non constant est scindé.*

Démonstration
Soit $P \in K[X]$ de degré d et comme K est algébriquement clos, P possède dans K au moins une racine α_1 donc $P(X) = (X - \alpha_1)Q$ avec $Q \in K[X]$ de $\deg Q = d - 1$; Et de même $Q \in K[X]$, Q possède dans K au moins une racine α_2, donc $P(X) = (X-\alpha_1)(X-\alpha_2)H$ avec $H \in K[X]$ et $\deg H = d-2$. De la même manière on trouve que $P(X) = a(X - \alpha_1)(X - \alpha_2)...(X - \alpha_d)$ avec a est le coefficient dominant et les α_i sont dans K (pas nécessairement distincts), d'où le polynôme P est scindé.

Définition 3.1.3. *Une extension E de K est un corps de décomposition pour P sur K si P peut être scindé dans $E[X]$, c'est à dire qu'il peut être*

décomposé en produit des polynômes linéaires dans $E[X]$ (de degré 1) et qui soit minimale pour cette propriété.

Exemple 3.1.1. *Le corps $\mathbb{Q}(\sqrt{2})$ est un corps de décomposition sur $\mathbb{Q}$ pour le polynôme $X^2 - 2$.*

Définition 3.1.4. *Soit K un corps et $P \in K[X]$ irréductible. On appelle* ***corps de rupture*** *de P sur K toute extension E tel que :*

- Dans E, P admet une racine a.

- E est engendrée par K et a (extension simple K (a)). (On dit parfois plutôt, que corps de décomposition ou corps des racines.)

Exemple 3.1.2. *le polynôme $P(X) = X^2 + 1 \in \mathbb{R}$ est irréductible. Un corps de rupture de ce polynôme est $\mathbb{C}$, et $\mathbb{C} = \mathbb{R}(i)$.*

Remarque 3.1.1. *Tout polynôme $P \in K[X]$ possède un corps de rupture sur K.*

Exemple 3.1.3. *Le corps de rupture de $X^2 + aX + b$ sur $\mathbb{Q}$ est engendré par une racine carrée de $a^2 - 4b$: $\mathbb{Q}(\sqrt{a^2 - 4b}) = \{A + B\sqrt{a^2 - 4b} \ / \ A, B \in \mathbb{Q}\}$.*

Remarque 3.1.2. *Le corps de rupture d'une équation binôme $x^n - d = 0$ sur un corps K est le corps engendré par K, une racine n-ième de d et toutes les racines n-ième de l'unité c'est-à-dire le corps engendré par une racine n-ième de d et le corps de rupture de $x^n - 1 = 0$ sur $K[X]$.*

3.2 Factorisation d'un polynôme

Soit L et K deux corps $(K \subset L)$ et soit $P \in K[X]$ non nul qui possède une racine α dans une extension L de K. Il existe $Q \in L[X]$ tel que $P = (x - \alpha)Q$. En recommençant, au cas où Q admet α pour racine, on arrive à l'existence de $T \in L[X]$ vérifiant $P = (x - \alpha)^m T$ et $T(\alpha) \neq 0$.

Définition 3.2.1. *On appelle m l'ordre de multiplicité de la racine α.*

Remarque 3.2.1.

• *La racine α est dite simple pour $m = 1$, et multiple pour $m \succeq 2$.*

• *Si $\deg P = n$ alors $\deg T = m - n$, donc la somme des ordres de multiplicité des racines de P ne peut dépasser n.*

Théorème 3.2.1. *Soit L et K deux corps avec $(K \subset L)$ et soit $P \in K[X]$ non nul qui possède des racines α_i avec $1 \preceq i \preceq r$ dans une extension L de K. Alors la somme des ordres de multiplicité des racines de P égale à n si,*

et seulement si, l'extension L de K contient le corps de rupture de P sur K. On dit que P est totalement factorisable dans L.
Dans $L[X]$ on écrit alors la factorisation totale

$$P = a(X - \alpha_1)^{m_1}.....(X - \alpha_r)^{m_r}.$$

Démonstration
les racines α_i du polynôme P s'expriment algébriquement en fonction des coefficients si, et seulement si, elles sont contenues dans une extension par radicaux successifs du corps engendré par les coefficients de P.
Équivaut de dire que le corps de rupture du polynôme P est contenu dans la saturation par radicaux du corps engendré par les coefficients de P, c'est équivalent de dire qu'il existe une extension par radicaux successifs du corps engendré par les coefficients, dans laquelle le polynôme est totalement factorisable.

Exemple 3.2.1. *Soit le polynôme $(X^2 + 1)^2(X - 2)^3 \in \mathbb{Q}[X]$ ayant pour racines i,$-i$,2, mais la famille de ses racines s'écrira : $(i, i, -i, -i, 2, 2, 2)$.*

3.3 Racines multiples

Soit $P = a_0 + a_1X + ... + a_nX^n \in K[X]$ un polynôme. On définit le polynôme dérivé de P par :

$$P' = \sum_{k=1}^{n} ka_kX^{k-1}.$$

On dit que le polynôme P est **séparable** s'il possède n racines distinctes dans une extension de K.

Définition 3.3.1. *Soit $P = a_0 + a_1X + ... + a_nx^n \in K[X]$ un polynôme non constant. Alors P est irréductible si, et seulement si, les seuls diviseurs sont les polynômes constants et les polynômes proportionnels au polynôme P.*

Théorème 3.3.1. *Soit $P = a_0 + a_1X + ... + a_nx^n \in K[X]$.*
Le polynôme P n'a que des racines simples si, et seulement si, P et P' sont premiers entre eux.

Démonstration
Les racines multiples de P sont exactement les racines communes de P et de P', ce sont donc les racines du P.G.C.D de polynôme P et P'. Or ce P.G.C.D n'aura pas de racine si, et seulement si, il est constant. D'où l'équivalence :
Le polynôme P n'a que des racines simples $\Leftrightarrow$ P et P' sont premiers entre eux.

Exemple 3.3.1. *On a l'équation de binôme* $X^n - 1 = 0$ *sur un corps* K *arbitraire, le dérivé de* $X^n - 1 = 0$ *est* nX^{n-1}.
Si n *est non nul dans le corps* K *(le cas si* K *contient le corps* $\mathbb{Q}$ *), alors* 0 *est seul racine de* nX^{n-1} *et n'est pas racine de* $X^n - 1$.
Le polynôme $X^n - 1$ *n'aura alors que des racines simples, et il y aura bien* n *racines* n*-ièmes de l'unité dans* K.
Si K *contient* $\mathbb{Q}$*, il y aura* n *racines* n*-ièmes à tout élément non nul* x *de* K*, ce qui signifie que le symbole* $\sqrt[n]{x}$ *représente exactement* n *élément.*

Remarque 3.3.1. *Un cas particulier est donné par un polynôme* P ***irréductible*** *sur* K*. Son dérivé* P'*, s'il n'est pas nul, est de degré strictement inférieur à celui de* P*, de même que tous ses diviseurs, donc aucun de ceux-ci ne peut diviser* P *: il en résulte que* P *et* P' *sont premier entre eux, et* P *n'a que des racines simples. Reste le cas où* P' *est nul. Si le corps* K *contient* $\mathbb{Q}$*, la nullité de* P' *exige que* P *soit constant, et, comme il est non nul, il n'a pas de racine multiple.*

Critère d'Eisenstein

Soit $P = a_0 + a_1X + ... + a_nX^n \in \mathbb{Z}[X]$ et p un nombre premier. On suppose que :

i) p ne divise pas a_n.
ii) p divise $a_0, a_1, ..., a_{n-1}$.
iii) p^2 ne divise pas a_0.

Alors, le polynôme $P(x)$ est irréductible dans $\mathbb{Z}[X]$, donc dans $\mathbb{Q}[X]$.

Démonstration

Supposons par l'absurde qu'il existe deux éléments non constants
$Q = b_0 + b_1X + ... + b_qX^q$ et $R = c_0 + c_1X + ... + c_rX^r$ de $\mathbb{Z}[X]$ tel que $P = QR$, puisqu'on a $a_0 = b_0c_0$ et que p est premier, donc p divise l'un des deux éléments b_0 et c_0.
Supposons par exemple que p divise b_0. Puisque p^2 ne divise pas a_0, p ne divise pas c_0.
Ainsi, p est premier avec c_0, or, pour tout entier $s \in [1, q]$
$a_s = b_0c_s + b_1c_{s-1} + ... + b_sc_0$, puisque p divise b_0 et que p est premier avec c_0, par récurrence sur s on montre que p divise b_s.
Finalement, p divise b_q, donc p divise $a_n = b_qc_r$ ce qui contredit l'hypothèse i.

Exemple 3.3.2. *Soit Le polynôme* $X^3 + 7X^2 + 14X + 21$ *est irréductible sur* $\mathbb{Q}[X]$*, il suffit d'appliquer le critère d'Eisenstein avec le nombre premier* $p = 7$.

Théorème 3.3.2. *Soit un corps K contenant $\mathbb{Q}$ et soit $P \in K[X]$.*
Si P est un polynôme irréductible, alors P n'a que des racines simples.

Démonstration
Soit P un polynôme irréductible non nul et P' le polynôme dérivé de P.
Si $P' \neq 0$ avec $\deg P' < \deg P$:
Les degrés de tous les diviseurs de P' sont strictement inférieurs à celui de P, donc aucun de ceux-ci ne peut diviser P.
D'où, P et P' sont premiers entre eux, alors P n'a que des racines simples.
Si $P' = 0$:
Comme le corps K contient $\mathbb{Q}$, la nullité de P' exige que P soit constant, et comme P est non nul, d'où il n'a pas de racines multiples.

4

Les fonctions symétriques

4.1 Polynômes symétriques élémentaires

Définition 4.1.1. *Soit K un corps, un polynôme en $X_1, ..., X_n$ avec coefficients dans K est une somme $P(X) = \sum_{(i_1,..,i_n)\in\mathbb{N}^*} a_{i_1,...,i_n} X_{1,...,n}^{i_1,...,i_n}$, on dit que $P(X)$ est un polynôme à n indéterminées ou (à plusieurs variables), avec les $a_{i_1,...,i_n} \in K$ et tous sauf un nombre fini des $a_{i_1,...,i_n}$ égaux à 0.*
Les $X_{1,...,n}^{i_1,...,i_n}$ sont des monômes et les $a_{i_1,...,i_n} X_{1,...,n}^{i_1,...,i_n}$ sont des termes.

Remarque 4.1.1. *Un polynôme à plusieurs variables est une somme d'un nombre fini de termes et une combinaison linéaire d'un nombre fini de monômes.*

Définition 4.1.2. *Un polynôme $P(X)$ en n indéterminées est symétrique si pour toute permutation $\rho \in S_n$ on a :*

$$P(X_1, ..., X_n) = P(X_{\rho(1)}, ..., X_{\rho(n)})$$

Exemple 4.1.1. *Les polynômes :*
$P(X, Y, Z) = X + Y + Z$ et $R(X, Y, Z) = X^3Y + Y^3Z + Z^3X + Y^3X + Z^3Y + X^3Z$ sont symétriques.

Définition 4.1.3. *Étant donné n indéterminées sur un corps K on appelle **polynômes symétriques élémentaires** les n polynômes suivants :*

- *Somme des indéterminées, soit $\sum_{i=1}^{n} X_i$.*
- *Somme des produits deux à deux des indéterminées, soit $\sum_{i<j} X_i X_j$.*
- *Somme des produits p à q des indéterminées, soit $\sum_{1\leqslant i_1<i_2<...<i_p\leqslant n} X_{i_1} X_{i_2} ... X_{i_p}$.*
- *produit des indéterminées, qui n'autre que la somme des produits n à n (car il y a seul tel produit).*

On appellera $\sigma_1, \sigma_2, ..., \sigma_n$ ces n polynômes.

Définition 4.1.4. *Les valeurs de n polynômes symétriques élémentaires sur une famille de n éléments s'appellent les fonctions symétriques élémentaires de ces éléments.*

Exemple 4.1.2. *Les fonctions symétriques élémentaires en 1,2,3 sont :* $\sigma_1 = 1+2+3$, $\sigma_2 = 1\times 2+1\times 3+2\times 3$ *et* $\sigma_3 = 1\times 2\times 3$.

Théorème 4.1.1. *Les fonctions symétriques élémentaires des racines d'un polynôme appartiennent au corps engendré par les coefficients.*

Démonstration
Soit le polynôme $P(X) = a_0 + a_1X + ... + a_nX^n$, les coefficients $a_i \in K$.
On suppose a_n non nul, et on note $(x_1, x_2, ..., x_n)$ la famille des racines (on répète les racines suivant leur ordre de multiplicité) .
Le corps de rupture est alors engendré par K et les x_i , dans ce corps, on écrit

$$a_0 + a_1X + ... + a_nX^n = a_n(X - x_1)(X - x2)...(X - x_n)$$

En développant le second membre, on trouve les n égalités suivantes, dites « Relations entre coefficients et racines » :

$$x_1 + x_2 + ... + x_n = -\frac{a_{n-1}}{an}$$
$$\sum_{i<j} x_ix_j = \frac{a_{n-2}}{a_n}$$
$$\sum_{i<j<k} x_ix_jx_k = -\frac{a_{n-3}}{a_n}$$
$$.....$$
$$x_1x_2...x_n = (-1)^n\frac{a_0}{a_n}$$

Donc les fonctions symétriques élémentaires des racines d'un polynôme appartiennent au corps engendré par les coefficients car les éléments :
$\frac{-a_{n-1}}{a_n}, \frac{-a_{n-2}}{a_n}, ..., (-1)^n\frac{a_0}{a_n}$ appartiennent au corps engendré par les coefficients de $P(X)$.

Remarque 4.1.2. *La résolution d'une équation algébrique se ramène à celle d'un système d'équations (n équations) à n inconnues.*

Exemple 4.1.3.
• *Les racines* x_1 *et* x_2 *de* $X^2 + aX + b$ *sont caractérisées par :*

$$\begin{cases} x_1 + x_2 = -a \\ x_1x_2 = b \end{cases}$$

• *Les racines* x_1 , x_2 *et* x_3 *de* $X^3 + pX + q$ *sont caractérisées par :*

$$\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1x_2 + x_1x_3 + x_2x_3 = p \\ x_1x_2x_3 = -q \end{cases}$$

Théorème 4.1.2. *Tout polynôme symétrique s'écrit d'une façon unique comme une expression polynomiale en les polynômes symétriques élémentaires.*

Démonstration

Un polynôme est une combinaison linéaire d'un nombre fini de monômes, donc un tel polynôme s'obtient en partant d'un monôme $X_1^{i_1}X_2^{i_2}.....X_n^{i_n}$ et en lui ajoutant les monômes différents obtenus en remplaçant la suite des indices des indéterminées par toutes les autres suites.
On l'écrira symboliquement $\sum X_1^{i_1}X_2^{i_2}.....X_n^{i_n}$.
Ainsi les polynômes symétriques élémentaires sont :

$$\sigma_1 = \sum_{i=1}^{n} X_i \ , ..., \ \sigma_p = \sum_{1 \preceq i_1 < ... \prec i_p \preceq n}^{n} X_{i_1}...X_{i_p}$$

D'autres « simples » sont ceux obtenus en partant d'un monôme ne comptant qu'une indéterminée. On posera $S_1 = \sum_{i=1}^{n} X_1^i$ la somme des puissances i-ième des indéterminées.
On va montrer que tous les S_i sont des polynômes en les polynômes symétriques élémentaires.
Soit le polynôme $P(Y) = Y^n - \sigma_1 Y^{n-1} + \sigma_2 Y^{n-2} + ... + (-1)^n \sigma_n$ et $X_1, X_2, ..., X_n$ les racines de ce polynôme.
Donc $P(Y) = (Y - X_1)(Y - X_2).....(Y - X_n)$.
Dérivons par rapport à Y, on trouve $P'(Y) = \frac{P(Y)}{Y - X_1} + ... + \frac{P(Y)}{Y - X_n}$
D'où

$$\frac{P'(Y)}{P(Y)} = \frac{1}{Y - X_1} + ... + \frac{1}{Y - X_n}$$

La division Euclidienne suivant les puissances croissantes donne, pour tout entier q :

$$\frac{1}{Y - X_1} = \frac{1}{Y} + \frac{X_1}{Y^2} + ... + \frac{X_1^{q-1}}{Y^q} + \frac{X_1^q}{Y^q}\frac{1}{Y - X_1}$$

On multiplie par Y et on fait la somme pour tous les $\frac{1}{Y - X_i}$ il reste

$$\frac{YP'(Y)}{P(Y)} = n + \frac{S_1}{Y} + \frac{S_2}{Y^2} + ... + \frac{S_{q-1}}{Y^{q-1}} + \frac{1}{Y^{q-1}}[\sum_i \frac{X_i^q}{Y - X_i}]$$

Posons enfin $X = \frac{1}{Y}$, pour arriver à :

$$\frac{P'(\frac{1}{X})}{XP(\frac{1}{X})} = n + S_1X + S_2X^2 + ... + S_{q-1}X^{q-1} + X^q[\sum \frac{X_i^q}{Y - X_i}]$$

On obtient donc les S_i en effectuant la division suivant les puissances croissantes de deux polynômes dont les coefficients sont en fonction des σ_i. Plus précisément, on peut calculer :

$$\frac{YP'(Y)}{P(Y)} = \frac{nY^n - (n-1)\sigma_1Y^{n-1} + (n-2)\sigma_2Y^{n-2} + ... + (-1)^{n-1}\sigma_{n-1}Y}{Y^n - \sigma_1Y^{n-1} + \sigma_2Y^{n-2} + ... + (-1)^n\sigma_n}$$

La transformation $X = \frac{1}{Y}$ conduit au quotient :

$$\frac{P'(\frac{1}{X})}{XP(\frac{1}{X})} = \frac{n - (n-1)\sigma_1X + (n-2)\sigma_2X^2 + ... + (-1)^{n-1}\sigma_{n-1}X^{n-1}}{1 - \sigma_1X + \sigma_2X^2 + ... + (-1)^n\sigma_nX^n}$$

Par division Euclidienne suivant les puissances croissantes, on trouve que :

$$\frac{P'(\frac{1}{X})}{XP(\frac{1}{X})} = n + \sigma_1X + (\sigma_1^2 - 2\sigma_2)X^2 + (\sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3)X^3 + ...$$

D'où l'on tire :

$$S_1 = \sigma_1$$
$$S_2 = \sigma_1^2 - 2\sigma_2$$
$$S_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$$

Alors pour tout entier i, la somme des puissances i-ième des indéterminées est un polynôme en les polynômes symétriques élémentaires.
De plus les $\sigma_1, \sigma_2, ..., \sigma_n$ algébriquement indépendants sur le corps K, d'où l'unicité d'une telle représentation.
Donc tout polynôme symétrique est un polynôme en les polynômes symétriques élémentaires.

4.2 Résultant de deux polynômes

Soit P et Q des polynômes sur un corps K ; appelons $(\alpha_1, ..., \alpha_n)$ et $(\beta_1, ..., \beta_n)$ les familles respectives de racines (dans le corps de rupture de

PQ par exemple). La condition nécessaire et suffisante pour que P et Q aient une racine commune s'écrit :

$$\prod_{\substack{1\preceq i\preceq n\\ 1\preceq j\preceq m}} (\alpha_i - \beta_j) = 0.$$

On pose : $P(X) = u\prod_{i=1}^{n}(X-\alpha_i)$ et $Q(X) = v\prod_{i=1}^{m}(X-\beta_j)$, $u, v \in K$.

Définition 4.2.1. *On appelle résultant des deux polynômes non nuls P et Q le produit :*

$$\begin{aligned} Res(P,Q) &= \frac{1}{v^n}\prod_{i}^{n} Q(\alpha_i) \\ &= \frac{(-1)^{nm}}{u^m}\prod_{j=1}^{m} P(\beta_j) \end{aligned}$$

Remarque 4.2.1.

- *Si $P = 0$ ou $Q = 0$ on pose $Res(P,Q) = 0$.*
- *On peut ajouter à l'un des polynômes un multiple scalaire de l'autre sans changer le résultant.*

Proposition 4.2.1.

- *Si P et Q ont une racine commune, il en est de même de Q et R où R est le reste de la division euclidienne de P par Q, et réciproquement ; or le couple (Q,R) est plus facile que le couple (P,Q), pour raisons de degré.*
- *Pour éliminer X entre X^2+aX+b et $X^2+\alpha X+\beta$ on écrit leur différence*

$$(a-\alpha)X + b - \beta.$$

Si l'on suppose $a \neq \alpha$, le résultant s'obtient en prenant la valeur de l'un des polynômes en $-\frac{b-\beta}{a-\alpha}$. On trouve

$$R = [(b-\beta)^2 + (a-\alpha)(a\beta - b\alpha)]$$

C'est encore valable dans le cas $a = \alpha$: l'existence d'une racine commune équivaut à $b = \beta$, donc à $R = 0$.

Corollaire 4.2.1. *Soient $\alpha \in K$ et $P, Q, R \in K[X]$ des polynômes non constants. Alors :*
$Res(X-\alpha, Q) = Q(\alpha)$, $Res(P, QR) = Res(P,Q)Res(P,R)$.

Remarque 4.2.2. *Un cas particulier : le résultant d'un polynôme et de sa dérivé, résultant dont la nullité correspond à l'existence d'une racine multiple du polynôme donné. Ce résultant joue un rôle spécial, on l'appelle le* ***discriminant****.*

4.3 Déterminant de Sylvester

Soit $P(X) = a_0 + a_1X + ... + a_nX^n = 0$ et $Q(X) = b_0 + b_1X + ... + b_pX^p = 0$ deux équations algébriques.
Un moyen « systématique » de calculer le résultant utilise la méthode dite « déterminant de Sylvester ».
La remarque de départ est la suivante : l'existence d'une racine commune de P et Q équivaut au fait que le P.G.C.D. de P et Q est de degré supérieur à 1 ; en appelant U et V les quotients de P et Q par ce P.G.C.D., on trouve l'égalité

$$VA - UB = 0$$

avec les relations

$$d^\circ U < d^\circ P \text{ et } d^\circ V < d^\circ Q$$

Définition 4.3.1. *La matrice de Sylvester de P et Q est une matrice carrée de taille $n + p$*

$$\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & \cdots & \cdots & a_n & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & \cdots & \cdots & a_{n-1} & a_n & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ b_0 & b_1 & b_2 & \cdots & \cdots & \cdots & b_p & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & \cdots & \cdots & b_{p-1} & b_p & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \end{pmatrix}$$

Remarque 4.3.1. *Le résultant de P et Q est le déterminant de la matrice de Sylvester de P et Q.*

Définition 4.3.2. *L'existence d'une racine commune à A et B équivaut donc à la nullité du déterminant d'ordre $n + p$ de la matrice de Sylvester.*

Exemple 4.3.1. *Soit les équations :*

$$X^2 + aX + b \quad et \quad X^2 + \alpha X + \beta$$

le déterminant s'appelle de Sylvester est d'ordre 4 et égale à :

$$\begin{vmatrix} b & a & 1 & 0 \\ 0 & b & a & 1 \\ \beta & \alpha & 1 & 0 \\ 1 & \beta & \alpha & 1 \end{vmatrix}$$

On peut remplacer le couple de polynôme par l'un d'eux et leur différence $(a - \alpha)X + b - \beta$, d'où le déterminant d'ordre 3 :

$$\begin{vmatrix} b & a & 1 \\ b - \beta & a - \alpha & 0 \\ 0 & b - \beta & a - \alpha \end{vmatrix} = (b - \beta)^2 + (\alpha - \alpha)(a\beta - b\alpha)$$

que l'on déduit d'ailleurs facilement du précédent.

4.4 Discriminant

Définition 4.4.1. *Soit P un polynôme non nul de $K[X]$ de degré n et de coefficient dominant a. Le discriminant $\Delta(P)$ est défini comme suit :*

$$\Delta(P) = \frac{(-1)^{\frac{n(n-1)}{2}} Res(P, P')}{a}.$$

Proposition 4.4.1. *Le discriminant de polynôme $P(X) = aX^2 + bX + c$ est $\Delta(aX^2 + bX + c) = b^2 - 4ac$.*

Démonstration

• méthode 1 :

$$\begin{aligned}\Delta(aX^2 + bX + c) &= \frac{(-1)^{\frac{2}{2}}}{a} Res(aX^2 + bX + c, 2aX + b) \\ &= -4a^2(x_1x_2 - 2ab(x_1 + x_2) - b^2\end{aligned}$$

Avec $x_1 et x_2$ deux racines de $P(X)$ et avec $x_1x_2 = \frac{c}{a}$ et $x_1 + x_2 = \frac{-b}{c}$
Alors

$$\Delta(aX^2 + bX + c) = b^2 - 4ac$$

• méthode 2 :

$$\Delta(aX^2 + bX + c) = \frac{(-1)^{\frac{2}{2}}}{a} Res(aX^2 + bX + c, 2aX + b)$$

Avec

$$Res(aX^2 + bX + c, 2aX + b) = \begin{vmatrix} c & b & a \\ b & 2a & 0 \\ 0 & b & 2a \end{vmatrix} = 4a^2c - b^2a$$

Donc

$$\begin{aligned}\Delta(aX^2 + bX + c) &= \frac{(-1)^{\frac{2}{2}}}{a} 4a^2c - b^2a \\ &= b^2 - 4ac.\end{aligned}$$

Proposition 4.4.1. *Le discriminant de $P(X) = X^3 + pX + q$ est $\Delta(X^3 + pX + q) = -4p^3 - 27q^2$.*

Démonstration

$$\Delta(X^3 + pX + q) = \frac{(-1)^3 Res(X^3 + pX + q, 3X^2 + p)}{1}$$

Avec

$$Res(X^3+pX+q, 3X^2+p) = \begin{vmatrix} q & p & 0 & 1 & 0 \\ 0 & q & p & 0 & 1 \\ p & 0 & 3 & 0 & 0 \\ 0 & p & 0 & 3 & 0 \\ 0 & 0 & p & 0 & 3 \end{vmatrix} = 4p^3 + 27q^2$$

Donc

$$\Delta(X^3+pX+q) = -4p^3 - 27q^2.$$

Conclusion

D'un point de vue mathématique, ce travail m'aura permis de développer mes connaissances en structure algébrique et plus précisément la résolution et la factorisation des polynôme dans un corps de rupture.

Bibliographie

[1] Claude Mutafian : «*equations algébriques et théorie de galois*»

[2] I.El Hage : «*Théorie de Galois*» (2001).

[3] Josette Calais «*Extension de corps, Théorie de Galois, Niveau M1-M2*».

[4] Najib Mahdou : «*Structure Algébrique S5*» FST-FES, (2017-2018).