Année Universitaire : 2014-2015

Licence Sciences et Techniques en Mathématiques et Applications

MEMOIRE DE FIN D'ETUDES

Pour l'Obtention du Diplôme de Licence Sciences et Techniques

Vers la Théorie de Galois :

Extension des Corps et Equations Algébriques

Préparé par:

- ***KHOUNA ABDELKARIM***

Soutenu le 15 Juin 2015 devant le jury composé de:

- ***Pr. S.GMIRA*** (***encadrant***)
- ***Pr. A.RAHMOUNI HASSANI*** (***examinatrice***)
- ***Pr. A.OUADGHIRI*** (***examinateur***)
- ***Pr. A.HILALI*** (***examinateur***)

Dédicace

Aucun travail n'est possible dans l'isolement. Les rencontres, les conseils et les encouragements constituent des aides précieuses souvent décisives. C'est pourquoi je tiens à dédier ce rapport à tous ceux qui ont contribué à ce travail parfois sans le savoir

Je dédie ce travail à:

Mes parents

Pour les sacrifices déployés à mon égard ; pour leur patience

Leur amour et leur confiance en moi

Ils ont tout fait pour mon bonheur et ma réussite.

Nulle dédicace ne peut exprimer ce que je leur dois

Que dieu leur réserve la bonne santé et une longue vie.

Ma famille et Mes chers amis

Pour leur présence et leur aide et encouragements.

Et enfin à tous les enseignants et les étudiants de la filière

Mathématique et applications

J'espère que ce rapport donnera une satisfaction à toutes ces personnes et à tous ceux qui auront l'occasion de le lire.

Remerciements

Au terme de ce travail, je tiens à exprimer ma profonde gratitude et mes sincères remerciements à mon encadrant de la Faculté des Sciences et des Techniques de Fès le professeur SEDDIK GMIRA pour tout le temps qu'il m'a consacré, et pour ses précieuses directives.

Mes remerciements vont enfin à toute personne qui a contribué de près ou de loin à l'élaboration de ce travail.

Table des matières

Introduction *1*

1 Construction à la règle et au compas

1.1 Construction géométrique à la règle et au compas. 3

1.1.1 Problèmes historiques de la construction à la règle et au compas 4

1.1.2 Premières constructions géométriques 5

1. 2 Constructibilité des nombres 7

1. 3 Extension de corps 13

1. 4 Problèmes historiques 15

2 Expression des racines d'une équation algébrique

2.1 Equation algébrique 16

2.2 Résolution par radicaux 17

2. 3 Indépendance algébrique 20

3 ***Racines et corps de rupture***

3.1 *Clôture algébrique 22*

3.2 Corps de rupture. 23

3.3 Factorisation d'un polynôme. 24

3.4 Existence de racines multiples 25

3.4.1 Racines simples 25

3.4.2 Critère d'Eisenstein 25

4 Les fonctions symétriques

4.1 polynômes symétriques élémentaires 27

4.2 Résultant de deux polynômes 31

4.3 Déterminant de Sylvester. 33

4.4 Discriminant d'un polynôme. 33

Conclusion *36*

Introduction

Dans ce travail nous allons nous intéresser à l'une des plus importantes constructions historiques des nombres. Il s'agit de la construction à la règle et au compas : Etant donné un nombre fini de points sur le plan, et en disposant uniquement d'une règle non graduée et d'un compas uniquement en problème *est de savoir quels sont les points du plan qu'on peut atteindre avec cette construction purement géométrique, elle permet d'obtenir tous les point*s *qui sont intersection de droites, de cercles, et de droites et de cercles.*

Dans un premier temps, et à l'aide de la règle et au compas nous allons construire le corps des rationnels et dans un deuxième temps, un corps plus grand, c'est le saturé par radicaux qui contient d'une manière naturelle le corps $\mathbb{Q}$.

Ensuite nous allons utiliser des équations algébriques et la théorie des extensions des corps pour chercher des conditions raisonnables qui permettent de construire des nombres à la règle et au compas. Ces conditions caractérisent totalement les points constructibles par cette méthode géométrique. Ceci permet de répondre aux vielles questions, posées par des problèmes historiques : la quadrature du cercle, la trisection d'un angle et la duplication d'un cube.

Le contenu de ce travail est réparti sur quatre chapitres :

Chapitre 1 : Construction à la règle et au compas

- *Construction géométrique*
- *Constructibilité des nombres*
- *Extension de corps*
- *Problèmes historiques*

Chapitre 2 : Expression des racines d'une équation algébrique

- *Equation algébrique*
- *Résolution par radicaux*
- *Indépendance algébrique*

Chapitre 3 : Racines et corps de rupture

- *Clôture algébrique*
- *Corps de rupture*
- *Factorisation*
- *Existence de racines multiples*

Chapitre 4 : Fonctions symétriques

- *Polynômes symétriques*
- *Résultant de deux polynômes*
- *Déterminant de Sylvester*
- *Discriminant*

Chapitre 1

Construction à la règle et au compas

Pour les Grecs de l'antiquité, nombres et mesures de longueurs étaient deux concepts intimement liés .C'est ainsi qu'ils se sont posés les problèmes de constructions géométriques de nombres remarquables.

Ne dispose que d'une règle non graduée, d'un compas et de certains points du plan, à partir de ceux-ci quels sont les points que l'on peut « atteindre » c'est-à-dire obtenir comme intersection de deux cercles, deux droites ou d'un cercle et d'une droite au bout d'un nombre fini (mais arbitraire) de constructions.

1.1 Construction géométrique à la règle et au compas :

Les seuls outils de géométrie autorisés étant la règle non graduée et le compas et les seuls opérations permises à partir d'éléments de départ indiqués (sous ensemble $\mathcal{P}$) sont :

- *Tracer une droite(ou une demi-droite ou un segment) passant par deux points connus.*
- *Tracer un cercle (ou un arc de cercle) dont le centre est un point connu et passant par un point connu.*
- *Prendre un écartement au compas égal à la distance entre deux points connus.*
- *Tracer le point d'intersection de deux droites connues.*
- *Tracer un point d'intersection d'une droite et d'un cercle connus.*
- *Tracer un point d'intersection de deux cercles connus.*

Soyons plus précis le plan est identifié au Corps $\mathbb{C}$ des complexes dont on se donne certains éléments, c'est-à-dire un sous ensemble de points $\mathcal{P}$.

A ce sous ensemble on adjoint tous les points qui sont :

- *Soit intersection de droites définies par les points de $\mathcal{P}$.*
- *Soit intersection de cercles centrés en des points de $\mathcal{P}$ et de rayon égal à la distance de deux points de $\mathcal{P}$.*
- *Soit intersection d'une droite de la première famille et d'un cercle de la seconde.*

On obtient ainsi une partie $\mathcal{P}_1$ contenant $\mathcal{P}$ à partir de $\mathcal{P}_1$,et on obtient une partie $\mathcal{P}_2$ plus grande et ainsi de suite……..On obtient de cette manière une suite $\{\mathcal{P}_1, \mathcal{P}_2, \dots \dots \mathcal{P}_i \dots \dots \mathcal{P}_n\}_{1 \le i \le n}$croissante de parties de $\mathbb{C}$.

1.1.1 Les problèmes de la construction à la règle et au compas :

Définition 1.1.1 $\mathcal{A} = \{\mathcal{P}i\}_{1\leq i\leq n}$ *s'appelle l'ensemble des points constructibles à partir de l'ensemble* $\mathcal{P}$ *à l'aide de la règle et du compas.*

Tout le problème est de trouver des conditions nécessaires ou suffisantes pour qu'un point soit constructible à partir de $\mathcal{P}$.

L'ensemble des points constructibles à partir de 0 et 1 sera appelé ensemble des points constructibles du plan, et sa détermination donne la réponse à ces fameux problèmes

- ***La quadrature du Cercle :*** *Etant donné un cercle, construire à la règle et au compas un carré de même aire ?*
  Cela revient à chercher si π *est un nombre constructible.*
- ***La duplication du Cube :*** *Posons nous la question dans l'espace qu'étant donné un cube, Peut –on construire un second cube dont le volume est le double du premier ? Si le premier cube a ses cotés de longueur* $\boldsymbol{a}$ *alors le second doit avoir ses cotés de la longueur* $\times \sqrt[3]{2}$. *La question se formule alors de la manière suivante : étant donné un segment de longueur 1, construire à la règle et au compas un segment de longueur* $\sqrt[3]{2}$.
- ***La trisection des angles :*** *Considérons un angle* α, *c'est-à-dire la donnée d'un point et de deux demi- droites issues de ce points, nous savons diviser cet angle en deux angles égaux à l'aide d'une règle et d'un compas il suffit de tracer la bissectrice.*

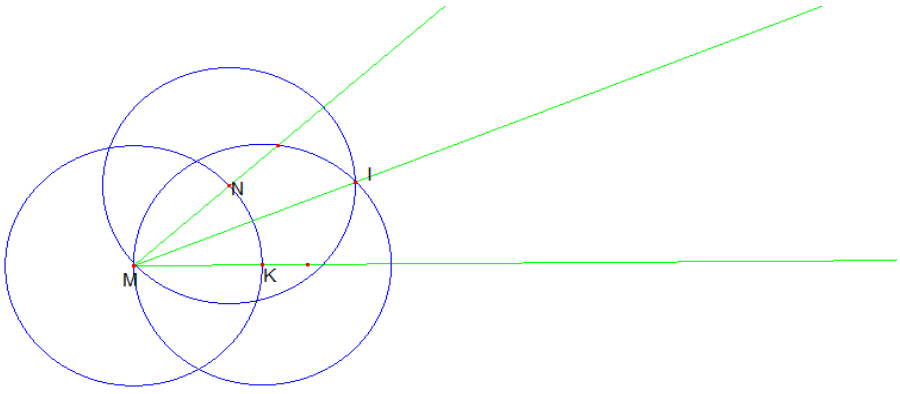

Figure 1 : La bissection d'angle

Problème de la trisection : *Peut-on diviser un angle en trois angles égaux à l'aide de la règle et du compas.*

1.1.2 Premières constructions géométriques:

On supposera toujours que la partie $\mathcal{P}$ contient 0 et 1, ce qui permet de construire à la règle et au compas l'axe réel et l'axe imaginaire.

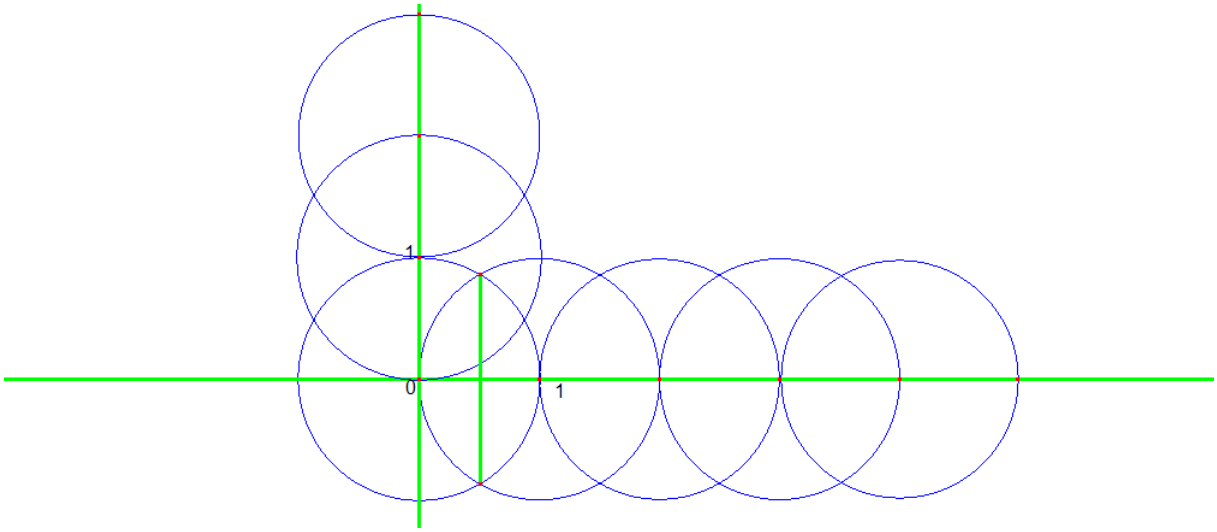

Figure 2 : Construction de l'axe réel et l'axe imaginaire

1. La médiatrice :

*Soit **A** et **B** deux points On peut tracer la médiatrice du segment [**A B**] en traçant les deux points d'intersection de deux cercles de centres respectifs **A** et **B** et de même rayon.la droite MM' coupe le segment [**A B**] en milieu.*

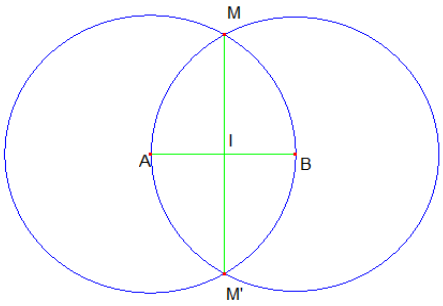

Figure 3 : La médiatrice d'un segment

2. La perpendiculaire et le parallèle à une droite à partir d'un point donné :

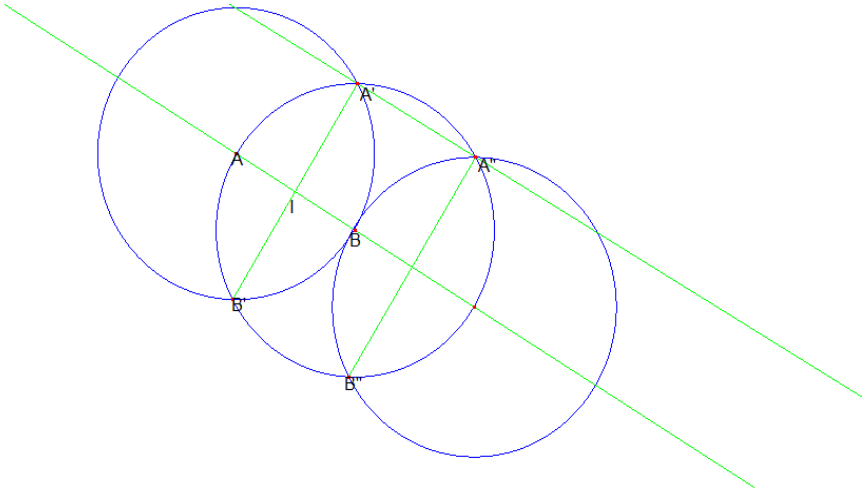

Figure 4 : La perpendiculaire et le parallèle à une droite

3. Constructibilité des nombres irrationnels :

Les nombres irrationnels sont des nombres constructibles car :

Si a est un réel positif constructible, il est possible de construire la racine carrée en exploitant la relation : $\sqrt{a} = \sqrt{(\frac{a+1}{2})^2 - (\frac{a-1}{2})^2}$ *cette relation permet de percevoir* $\sqrt{a}$ *comme étant la longueur d'un côté d'un triangle rectangle dont l'hypoténuse est de longueur* $(\frac{a+1}{2})$ *et l'autre côté de longueur* $(\frac{a-1}{2})$ *.*

Exemple : *Construction de* $\sqrt{2}$ *à l'aide de la règle et au compas :*

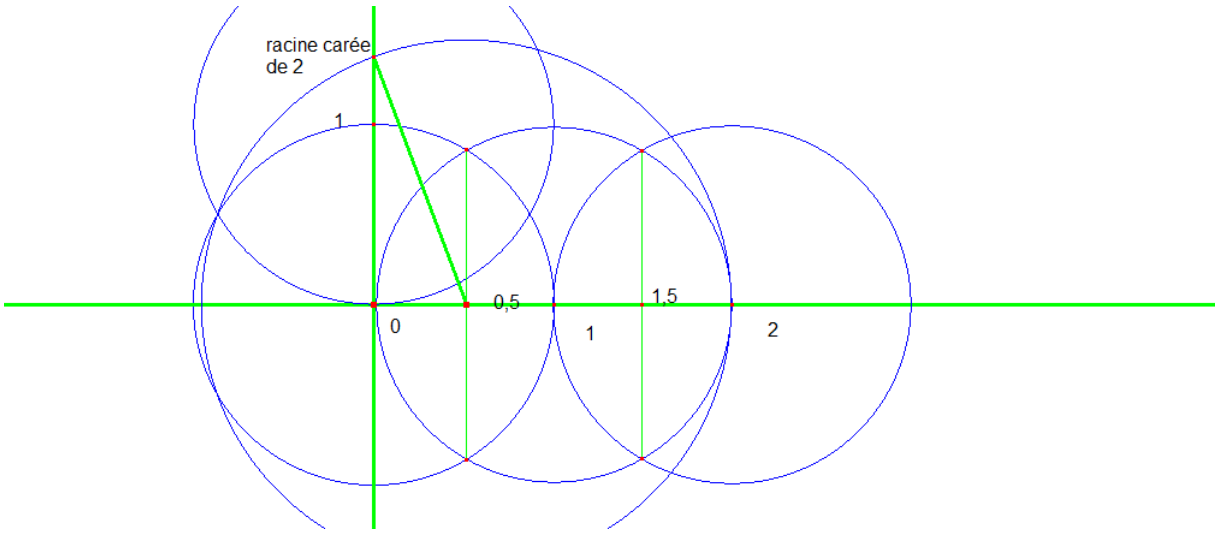

Figure 5 : Construction de $\sqrt{2}$ *à la règle et au compas*

4. Construction d'un carré de coté donné à l'aide de la règle et au compas :

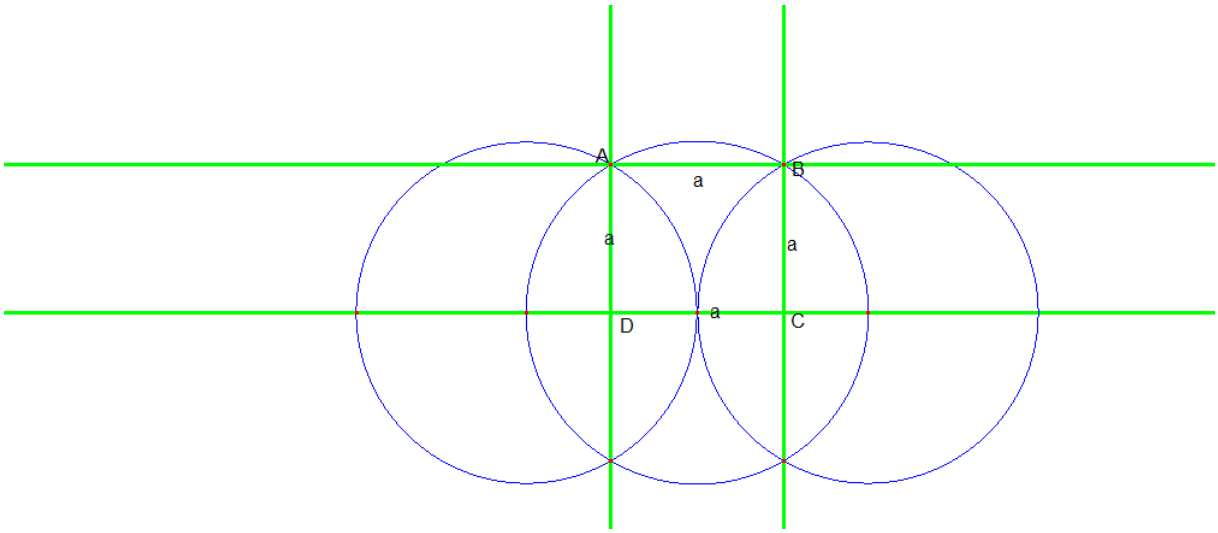

Figure 6 : Construction d'un carré

5. Construction d'un losange de cotés donnés :

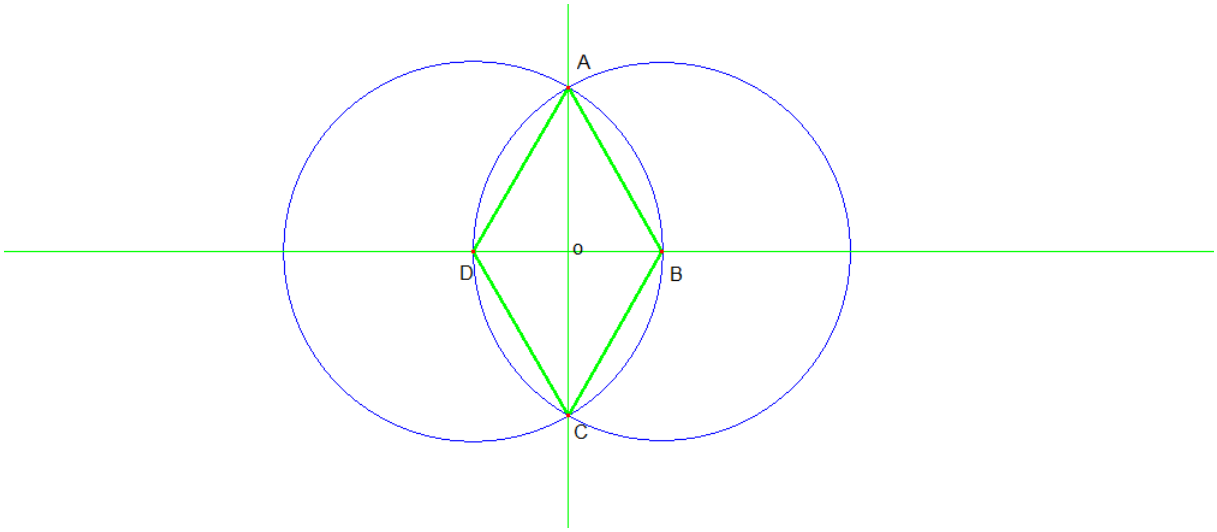

Figure 7 : Construction d'un losange

1.2 Constructibilité des nombres :

Proposition 1.2.1 *l'ensemble des nombres constructibles à partir de $\mathcal{P}$ une partie de plan contenant 1 est :*

Un corps stable par conjugaison et fermé par extraction de racines carrées.

Démonstration : *Pour montrer que* $(\mathcal{A} = \{\mathcal{P}i\}_{1\leq i\leq n}, +, \times)$ *est un corps avec* $\mathcal{P}_i$ *des parties de* $\mathbb{C}$ *il suffit de montrer :*

- $(\mathcal{A}, +)$ *est un groupe commutatif d'élément neutre 0.*
- $(\mathcal{A} / \{0\}, \times)$ *est un groupe commutatif d'élément neutre 1.*
- *La loi* $\times$ *est distributive par rapport a la loi* $+$.
  - $\forall\, \mathcal{Z}_1, \mathcal{Z}_2 \in \mathcal{A}$ *avec* $\mathcal{Z}_1, \mathcal{Z}_2$ *sont deux nombres constructibles. Alors* $\mathcal{Z}_1 + \mathcal{Z}_2$ *est un nombre constructible alors* $\mathcal{Z}_1 + \mathcal{Z}_2 \in \mathcal{A}$.
    En effet, soit $\mathcal{Z}_1, \mathcal{Z}_2$ *deux nombres constructibles. Alors* $\mathcal{Z}_1 + \mathcal{Z}_2$ *est constructible à l'aide de la règle et au compas.*

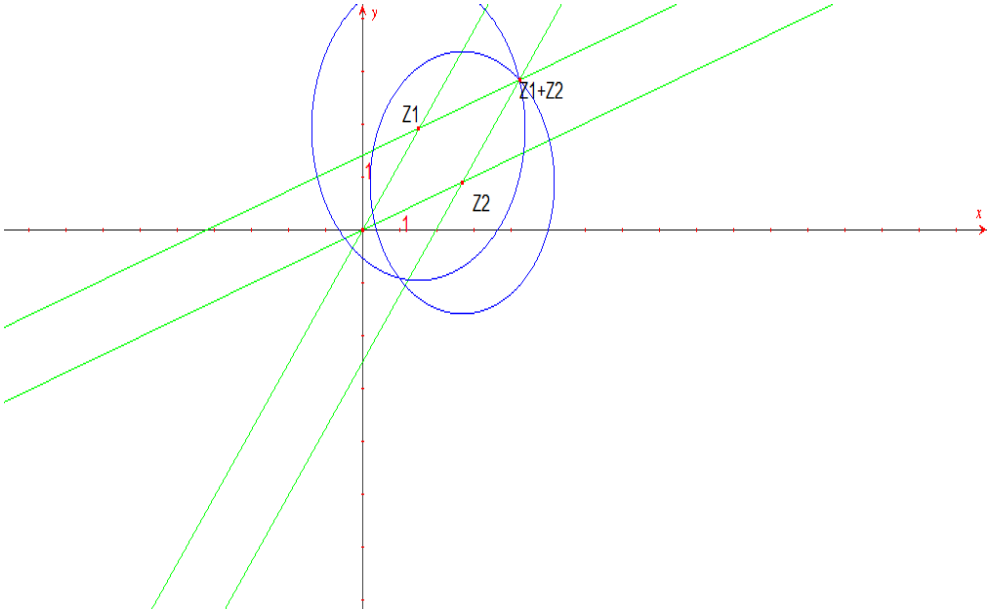

Figure 8 : Construction de $\mathcal{Z}_1 + \mathcal{Z}_2$

- $\forall\, \mathcal{Z} \in \mathcal{A}$ $(\mathcal{Z} + 0) = (0 + \mathcal{Z}) = \mathcal{Z}$ *donc* 0 *est un élément neutre de* $\mathcal{A}$.

- *Soit* $\mathcal{Z} \in \mathcal{A}$ *un nombre constructible. Alors* $-\mathcal{Z}$ *est constructible donc* $-\mathcal{Z} \in \mathcal{A}$ *d'où* $\mathcal{Z}$ *admet un inverse.*

  En effet, soit $\mathcal{Z}$ *un nombre complexe. Alors* $(-\mathcal{Z})$ *est constructible en traçant le droit passant par O et* $\mathcal{Z}$ *et en reportant de l'autre coté la longueur* $|\mathcal{Z}|$ *à l'aide du compas.*

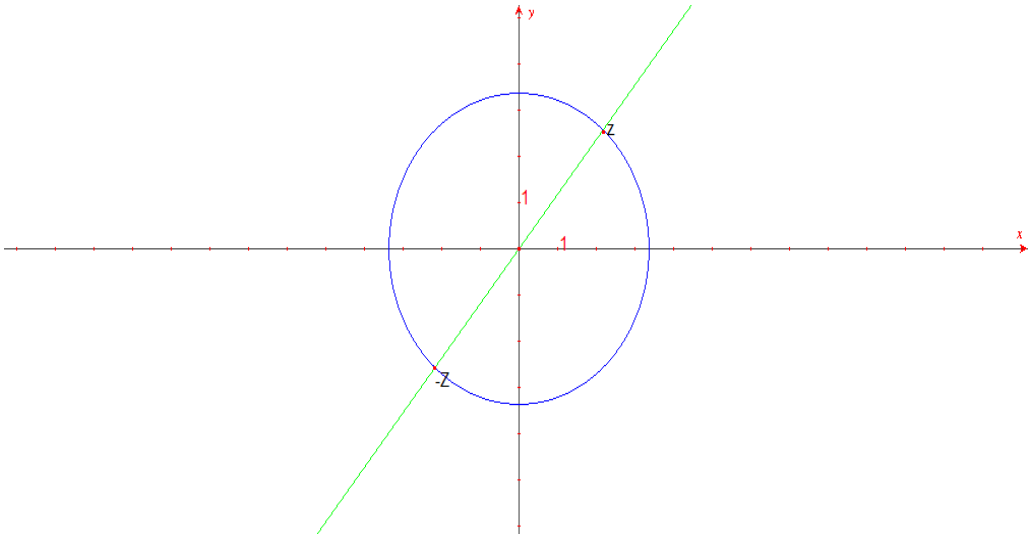

Figure 9 : Construction de $-\mathcal{Z}$

- $\forall\, \mathcal{Z}_1, \mathcal{Z}_2 \in \mathcal{A}$ *alors on a :* $\mathcal{Z}_1 + \mathcal{Z}_2 = \mathcal{Z}_2 + \mathcal{Z}_1$

Donc on a bien montré que $(\mathcal{A}, +)$ *est un groupe commutatif.*

De même on montre que $(\mathcal{A}/\{0\}, \times)$ *est un groupe commutatif.*

- $\forall\, \mathcal{Z}_1, \mathcal{Z}_2 \in \mathcal{A} \,/\, \{0\}$ *avec* $\mathcal{Z}_1, \mathcal{Z}_2$ *deux nombres constructibles, alors* $\mathcal{Z}_1 \times \mathcal{Z}_2$ *est constructible donc* $\mathcal{Z}_1 \times \mathcal{Z}_2 \in \mathcal{A} \,/\, \{0\}$.
  En effet, soit A et B deux nombres complexes constructibles. Alors $A \times B$ *est un nombre constructible à l'aide de la règle et au compas.*

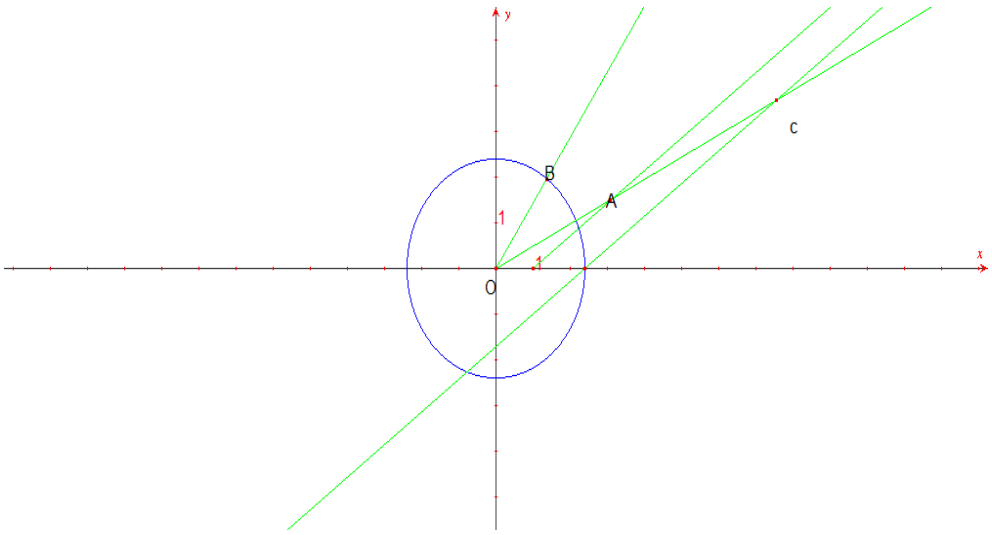

Figure 10 : Construction de $\mathcal{Z}_1 \times \mathcal{Z}_2$

- $\forall\, \mathcal{Z} \in \mathcal{A} \,/\, \{0\}$ $\mathcal{Z} \times 1 = 1 \times \mathcal{Z} = \mathcal{Z}$ *donc 1 est un élément neutre de* $\mathcal{A}/\{0\}$.
- *Soit* $\mathcal{Z} \in \mathcal{A} \,/\, \{0\}$ *(nombre constructible). Alors* $1/\mathcal{Z}$ *est constructible donc* $1/\mathcal{Z} \in \mathcal{A} \,/\, \{0\}$ *d'où* $\mathcal{Z}$ *admet un inverse dans* $\mathcal{A} \,/\, \{0\}$.

En effet, pour construire l'inverse de $\mathcal{Z}$, On part de la conjugué de $\mathcal{Z}$ et tout revient à construire sur la droite joignant O à la conjugué de $\mathcal{Z}$ la longueur inverse de $|\mathcal{Z}|$ ce qui se fait facilement à l'aide de parallèles.

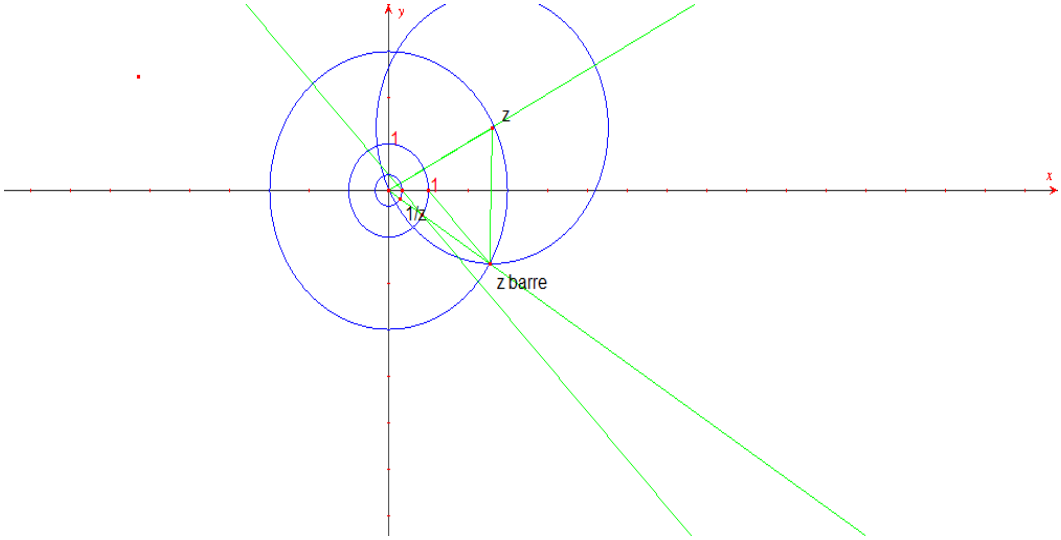

Figure 11 : Construction de $^{1}/_{\mathcal{Z}}$

- *De plus la loi $\times$ est commutative.*

Donc on a bien montré que $(\mathcal{A}/\{0\},\times)$ est un groupe commutatif de plus la loi $\times$ est distributive par rapport $+$.

Donc l'ensemble des nombres constructibles à partir de l'ensemble de départ $\mathcal{P}$ est un corps.

- *$\forall\, \mathcal{Z} \in \mathcal{A}$ un nombre constructible alors $\bar{\mathcal{Z}}$ est constructible, donc $\bar{\mathcal{Z}} \in \mathcal{A}$ donc ce corps est stable par conjugaison.*

  En effet, soit $\mathcal{Z}$ un nombre complexe constructible. Alors $\bar{\mathcal{Z}}$ est constructible.

  Le conjugué de $\mathcal{Z}$ est le symétrique de $\mathcal{Z}$ par rapport à l'axe réel.

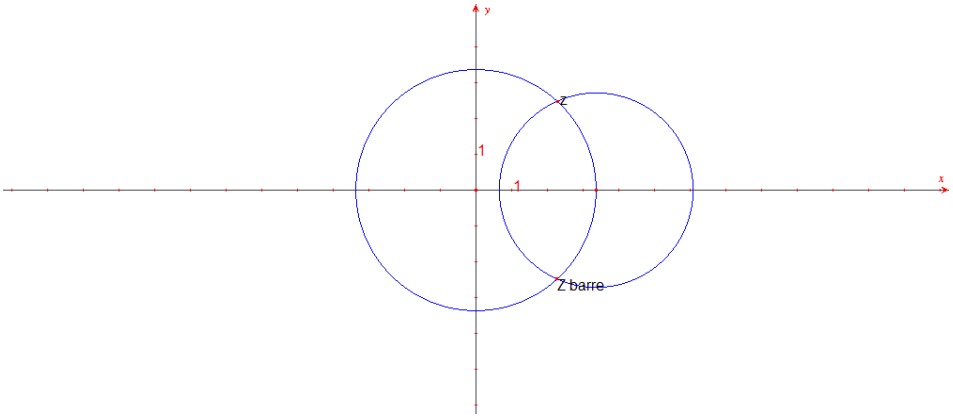

Figure 12 : Construction de $\bar{\mathcal{Z}}$

- *De plus* $\forall\, \mathcal{Z} \in \mathcal{A}$ *on trouve que les deux racines carrées de* $\mathcal{Z}$ *appartient à l'ensemble* $\mathcal{A}$ *, donc ce corps est fermé par extraction de racines carrées. En effet, soit* $\mathcal{Z} \in \mathbb{C}$ *. Alors* $\mathcal{Z} = \rho e^{i\theta}$

  $\mathcal{Z}^{\frac{1}{2}} = \mathcal{W} \Longrightarrow \mathcal{Z} = \mathcal{W}^2$ *Avec* $\mathcal{W} = re^{i\varphi}$

  Donc on trouve que $r = \sqrt{\rho}$ *et* $\begin{cases} \varphi = \frac{\theta}{2} \\ \varphi = \frac{\theta}{2} + \pi \end{cases}$ *alors les deux racines carrées de* $\mathcal{Z}$ *sont :* $\mathcal{Z}_1 = \sqrt{\rho} e^{i\frac{\theta}{2}}$ *et* $\mathcal{Z}_2 = \sqrt{\rho} e^{i(\frac{\theta}{2}+\pi)}$ *et sont constructibles à l'aide de la règle et du compas.*

  On remarque que $\mathcal{Z}_1 = -\mathcal{Z}_2$ *,*

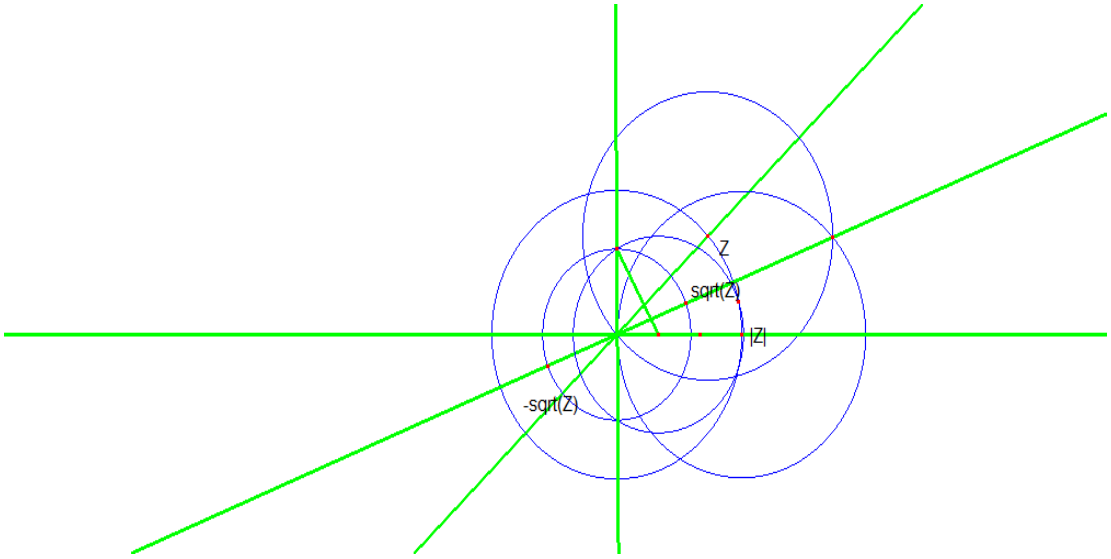

Figure 13 : *Construction des racines carrés de* $\mathcal{Z}$

Théorème 1.2.1 *Soit* $\mathcal{P}$ *une partie du plan (la partie est supposée symétrique par rapport à l'axe réel) et* $\mathcal{S}$ *est un sous corps de* $\mathbb{C}$ *contenant* $\mathcal{P}$*et saturé par racines carrées. Alors les nombres constructibles à partir de* $\mathcal{P}$ *forment le plus petit corps contenant* $\mathcal{P}$ *et saturé par racines carrées* $\mathcal{A} = \mathbb{K}(\mathcal{P}) = \cap\, \mathcal{S}$ *.*

Démonstration :

Soit $\mathcal{P}$ *l'ensemble de départ (une partie de* $\mathbb{C}$*). D'après la proposition 1 .1 on a*

$(\mathcal{A} = \{\mathcal{P}i\}_{1\leq i\leq n}, +, \times)$ *est un sous corps de* $\mathbb{C}$ *stable par conjugaison et saturée par racines carrées et comme* $\mathbb{K}(\mathcal{P})$ *est un sous corps engendré par* $\mathcal{P}$ *et saturé par racines carrées, d'où* $\mathbb{K}(\mathcal{P}) \subseteq \mathcal{A}$*.*

Il reste de montrer l'inclusion suivant $\mathcal{A} \subseteq \mathbb{K}(\mathcal{P})$*, c'est-à-dire* $\forall \mathcal{Z} \in \mathcal{A} \Rightarrow \mathcal{Z} \in \mathbb{K}(\mathcal{P})$

Lemme 1.2.1 *Toute droite constructible est donnée sous forme algébrique par :* $ux+vy+w=0$*, et tout cercle constructible par la forme :* $x^2 + y^2 + ux + vy + w = 0$ *.*

Démonstration :

L'équation de la droite passant par les points $\mathcal{Z}_1 = a + ib$ *et* $\mathcal{Z}_2 = c + id$ *est :*

$$(c-a)(y-b) - (d-b)(x-a) = 0 \Leftrightarrow (cy - cb - ay + ab) - (dx - da - bx + ba)$$

$$\Leftrightarrow (c-a)y + (b-d)x + da - cb = 0$$

Elle s'écrit donc sous la forme $ux + vy + w = 0$ *; les réels u, v, w étant des sommes de produits de* a, b, c, d *donc aussi de* $\mathcal{Z}_1$, $\mathcal{Z}_2$, $\overline{\mathcal{Z}_1}$, $\overline{\mathcal{Z}_2}$.

Passons à un cercle centré en $\mathcal{Z} = a + ib$ *et de rayon R. Son équation est :*

$(x-a)^2 + (y-b)^2 - R^2 = 0$ *et on l'écrit* $x^2 + y^2 + ux + vy + w = 0$ *; les réels u, v, w étant ici des sommes de produits de* $\mathcal{Z}, \bar{\mathcal{Z}}, R$.

Remarque :

Dans ces conditions, partons d'une partie $\mathcal{P}$ *symétrique par rapport à l'axe réel. Cette partie engendre un sous corps* $\mathbb{K}(\mathcal{P})$ *de* $\mathbb{C}$ *et saturé par racines carrées qui contient le conjugué, la partie réelle et la partie imaginaire de tous ses éléments.*

Lemme 1.2.2 *Tout point constructible a ses coordonnées dans* $\mathbb{K}(\mathcal{P})$ *(le corps engendré par* $\mathcal{P}$ *et saturé par racines carrées).*

Démonstration :

Deux droites définies par des points de $\mathcal{P}$ *auront des équations de la forme* $(u_1x + v_1y + w_1 = 0)$ *et (* $u_2x + v_2y + w_2 = 0$ *) tous les coefficients appartenant au corps* $\mathbb{K}(\mathcal{P})$ *d'après ce qui précède. Leur intersection est donnée par la solution du système linéaire :*

$$\begin{cases} u_1x + v_1y + w_1 = 0 \\ u_2x + v_2y + w_2 = 0 \end{cases}$$

Laquelle solution s'exprime à partir des coefficients à l'aide de sommes, produits, quotients, donc reste dans le corps $\mathbb{K}(\mathcal{P})$.

Remplaçons maintenant la seconde droite par un cercle centré en un point de $\mathcal{P}$ *et de rayon égal à la distance de deux points de l'ensemble* $\mathcal{P}$. *Les intersections de la première droite et de cercle seront données par le système suivant :*

$$\begin{cases} u_1x + v_1y + w_1 = 0 \\ x^2 + y^2 + u_3x + v_3y + w_3 = 0 \end{cases}$$

Où tous les coefficients sont dans le corps $\mathbb{K}(P)$. *Pour le résoudre on peut tirer* y *de la première équation, le reporter dans la seconde, ce qui nous amène à* $x^2 + sx + t = 0$, *les réels* s *et* t *étant encore dans* $\mathbb{K}(\mathcal{P})$. *La résolution de cette équation fait intervenir les racines carrées de l'élément* $(\alpha = s^2 - 4t)$, *lequel* α *est encore dans* $\mathbb{K}(\mathcal{P})$. *D'où la nécessité éventuelle « d'augmenter »* $\mathbb{K}(\mathcal{P})$ *en considérant le sous corps de* $\mathbb{C}$ *engendré non seulement par* $\mathcal{P}$, *mais par* $\mathcal{P}$ *et une racine carrée de* α *et on obtient alors les valeurs de* x *et donc celles de* y.

Enfin, si l'on remplace la droite elle aussi par un cercle, on cherche les intersections de deux cercles, chacun centré en un point de $\mathcal{P}$ et de rayon égal à la distance de deux points de $\mathcal{P}$. Le système s'écrit : $\begin{cases} x^2 + y^2 + a\,x + b\,y + c = 0 \\ x^2 + y^2 + e\,x + f\,y + g = 0 \end{cases}$ *les coefficients étant toujours dans le corps $\mathbb{K}(\mathcal{P})$ il suffit de remplacer l'une des équations par la différence des deux pour se ramener au cas précédent.*

D'où tout point constructible à ses coordonnées dans $\mathbb{K}(\mathcal{P})$.

D'après le lemme1.2 si $\mathcal{Z}$ est un nombre constructible à partir de $\mathcal{P}$, il s'obtient à partir de $\mathbb{K}(\mathcal{P})$ par un nombre fini d'opérations consistant à passer d'un corps à un corps plus grand engendré par le précédent et les racines carrées d'un de ses éléments . Il en résulte que $\mathcal{Z}$ appartient à tous les corps contenant $\mathcal{P}$ et saturés par racines carrées, donc à leur intersection.

Alors $\mathcal{A} \subseteq \mathbb{K}(\mathcal{P})$.

Ceci prouve l'égalité suivant $\mathcal{A} = \mathbb{K}(\mathcal{P})$.

Corollaire 1 .2.1 *Soit $\mathcal{Z} \in \mathbb{C}$ et $\mathcal{P}$ une partie du plan supposé symétrique par rapport à l'axe réel. Alors $\mathcal{Z}$ est constructible à partir de $\mathcal{P}$ c'est équivalent de dire que $\mathcal{Z}$ appartient au saturé du corps $\mathbb{K}(\mathcal{P})$.*

1.3 Extension de corps :

Définition 1.3.1 *Soit K, L deux corps avec $\mathrm{K} \subset \mathrm{L}$. On dit que L est une extension de K*

si K est un sous corps de L.

Remarque : *On peut considérer L comme un espace vectoriel sur K .*

Définition 1.3.2 *Soit K, L deux corps avec $\mathrm{K} \subset \mathrm{L}$. Si la dimension de L (l'espace vectoriel sur K) est finie, on l'appelle degré d'extension la dimension de L qui sera noté*

$[\mathrm{L}:\mathrm{K}] = dim_{\mathrm{K}}\mathrm{L}$.

Remarque : *Si* $[\mathrm{L}:\mathrm{K}] = 2$ *nous parlerons d'une extension quadratique.*

Exemple :

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

Théorème 1.3.1

Soit $\mathcal{P}$ une partie du plan supposé symétrique par rapport à l'axe réel et $\mathcal{Z} \in \mathbb{C}$. Alors $\mathcal{Z}$ est constructible à partir de $\mathcal{P}$ si et seulement s'il existe une suite finie croissante de corps

$\mathbb{K}(\mathcal{P}) \subset \mathrm{K}_1 \subset \mathrm{K}_2 \subset \cdots \subset \mathrm{K}_m$ *telles que* $\mathcal{Z} \in \mathrm{K}_m$*et* $\forall\, i = \{1, \ldots\ldots, m-1\}$ *chaque corps* K_{i+1} *est engendré par* K_i *et par un élément dont le carré est dans* K_i .

Remarque :

- K_{i+1} *est extension de* K_i *par racine carrée* $\forall\, i = \{1, \ldots\ldots, (m-1)\}$.
- K_m *est extension de* $\mathbb{K}(\mathcal{P})$ *par racines carrées successives.*
- K_{i+1} *contient strictement* K_i*, il est engendré par* K_i *et les racines carrées d'un élément* α *de* K_i $(\sqrt{\alpha},\ -\sqrt{\alpha}\ )$.

Exemples :

- *Partons du cas classique* $\mathcal{P} = \{0,1\}$ *le corps engendré par la partie* $\mathcal{P}$ *est le corps* $\mathbb{K}(\mathcal{P}) = \mathbb{Q}$.
- $\mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2}\,/\,x, y \in \mathbb{Q}\}$ *est un corps, l'élément* $\sqrt{2} \notin \mathbb{Q}$*, mais il est constructible car :* $\mathbb{Q}(\sqrt{2})$ *est un espace vectoriel sur* $\mathbb{Q}$ *avec* $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ *donc le sous corps de* $\mathbb{C}$ *engendré par* $\mathbb{Q}$ *et* $\sqrt{2}$ *est une extension par racine carrée.*
- $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \{A' + B'\sqrt{3}\ ;\ A', B' \in \mathbb{Q}(\sqrt{2})\}$

$$= \{a + b\sqrt{2} + (a' + b'\sqrt{2})\sqrt{3}\ ; a, b, a', b' \in \mathbb{Q}\}$$

$$= \{a + b\sqrt{2} + a'\sqrt{3} + b'\sqrt{6}\ ; a, b, a', b' \in \mathbb{Q}\}$$

Définition 1.3.3 *Soit* L *une extension d'un corps* K*,* α *un élément de* L *et* $\mathrm{K}(\alpha)$ *l'extension de* K *obtenue par l'adjonction de* α.

1) α *est dit algébrique sur le corps* K*, s'il existe un polynôme non constant* $P(X)$ *dans* $\mathrm{K}[X]$ *tel que* $P(\alpha) = 0$*, dans ce cas on dit que* $\mathrm{K}(\alpha)$ *est une extension simple, algébrique de* K.
2) α *est dit transcendant sur* K*, si* α *n'est pas algébrique sur* K.

Définition 1.3.4 *Une extension* L *d'un corps* K *est dit algébrique sur* K *si tout élément de* L *est algébrique sur* K.

Définition 1 .3.5 *Soit* α *un nombre algébrique, alors le plus petit degré parmi tous les degrés des polynômes* $P(X)$ *dans* $\mathrm{K}[X]$ *tel que* $P(\alpha) = 0$ *est le degré algébrique de* α.

Exemple : *Le nombre* $\sqrt[3]{2}$ *est algébrique de degré 3 car il est annulé par* $P(X) = X^3 - 2$ *mais pas par des polynômes de degré plus petit.*

Corollaire 1.3.1 *Tout nombre réel constructible est un nombre algébrique dont le degré algébrique est de la forme* 2^n $n \geq 0$.

1.4 Problèmes historiques :

- ***L'impossibilité de la duplication du cube :*** *la duplication du cube ne peut s'effectuer à la règle et au compas car* $\sqrt[3]{2}$ *n'est pas constructible,* $\sqrt[3]{2}$ *est une racine de* $P(X) = X^3 - 2$ *ce polynôme est unitaire et irréductible dans* $\mathbb{Q}[X]$*, donc* $\sqrt[3]{2}$ *est un nombre algébrique de degré 3, ainsi le degré algébrique n'est pas de la forme* 2^n*, d'où* $\sqrt[3]{2}$ *n'est pas constructible.*
- ***L'impossibilité de la quadrature du cercle :*** *la quadrature du cercle ne peut s'effectuer à la règle et au compas car* π *est un nombre transcendant* (*théorème de Ferdinand Van Lindemann*) *donc n'est pas constructible, et comme* π *n'est pas constructible alors* $\sqrt{\pi}$ *n'est pas constructible.*
- ***L'impossibilité de la trisection des angles :*** *la trisection d'angle ne peut s'effectuer à la règle et au compas, plus précisément nous allons exhiber un angle que l'on ne peut pas couper en trois angles égaux. l'angle* $\frac{\pi}{3}$ *ne peut pas être coupé en trois angles égaux car* $\cos(\frac{\pi}{9})$ *n'est pas un nombre constructible,* $\cos(\frac{\pi}{9})$ *est une racine de* $P(X) = 8X^3 - 6X - 1$ *ce polynôme est irréductible dans* $\mathbb{Q}[X]$*, donc* $\cos(\frac{\pi}{9})$ *est un nombre algébrique de degré 3, ainsi le degré algébrique n'est pas de la forme* 2^n*, d'où l'impossibilité de la trisection d'angle .*

Aujourd'hui plus que jamais nous pouvons dire que la construction à la règle et au compas permet d'avoir des meilleurs résultats concernant la résolution des problèmes historiques, cette construction donne lieu à plusieurs notions par exemple la constructibilité des nombres (*rationnels, irrationnels …*).

Donc l'obtention des résultats de l'impossibilité des problèmes déjà cités nécessite l'utilisation de quelques éléments de la théorie de corps (*extension de corps, degré d'extension, degré algébrique d'un nombre …*).

Chapitre 2

Expression des racines d'une équation algébrique

Un autre problème historique introduit naturellement l'étude des extensions de corps : c'est celui de la résolution des équations algébriques.

Le problème consistant à « résoudre » une équation algébrique peut prendre différentes formes selon les besoins. On peut par exemple chercher à trouver des solutions approchées par des méthodes numériques. Ou bien chercher à construire géométriquement les solutions comme intersections de certaines courbes dans le plan. Il se trouve que, historiquement, le problème de la résolution de telles équations a acquis, pour les algébristes, un sens très précis, celui de la résolution par radicaux.

Problème :

Le problème est alors de calculer ces racines, c'est-à-dire de trouver une « formule » donnant ces racines en fonction des coefficients de l'équation.

2.1 Equation algébrique :

Définition 2 .1.1 *Une équation algébrique* (*ou polynômiale*) *est une équation de la forme* $x^n + a_{n-1}\, x^{n-1} + \ldots\ldots\ldots + a_1 x + a_0 = 0$ *où l'inconnue est* x *et* $a_0, a_1, \ldots\ldots, a_{n-1}$ *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* $x^n + a_{n-1}\, x^{n-1} + \ldots\ldots\ldots + a_1 x + a_0 = 0$ *une équation algébrique, si on' arrive à exprimer les racines d'équation (polynôme) en fonction des coefficients du polynôme, on 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 $\forall i = \{0,1, \ldots\ldots, (n-1)\}$.

Exemple : *Soit l'équation* $3x + 2 = 0$, *alors la solution de cette équation est* $\frac{-2}{3}$, *pour la résoudre nous n'avons pas eu besoin d'autre chose que les quatre « opérations » dans le corps* $\mathbb{C}$.

Remarque :

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.

Expressions algébriques : *Soit* $x^n + a_{n-1}\, x^{n-1} + \ldots\ldots\ldots + a_1\, x + a_0 = 0$ *une équation algébrique, si on' arrive à exprimer les racines d'équation* (polynôme) *en fonction de ces coefficients, en faisant intervenir non seulement les expressions rationnelles des* $a_i \;\; \forall i\{0,1,\ldots\ldots,(n-1)\}$ *avec* (a_i) *une famille d'éléments du corps* $\mathbb{C}$*, mais tous les complexes que l'on peut écrire à partir des* a_i *à l'aide d'opérations rationnelles et d'extractions de racines. On dira que les racines s'expriment algébriquement à l'aide des* a_i.

Exemple : *Soit l'équation* $x^2 - 2 = 0$ *avec* 1 *et* -2 *deux éléments de* $\mathbb{Q}$ *et* $\mathbb{K}\{1,-2\} = \mathbb{Q}$ *La solution d'équation est* $x = \pm\sqrt{2}$ *s'exprime algébriquement à l'aide des coefficients* -2 *et* 1 *et de plus* $x \notin \mathbb{K}\{1,-2\}$.

2.2 Résolution par radicaux :

Définition 2 .2.1 *Tout équation algébrique sous la forme* $x^n - d = 0$ *avec* d *est un nombre complexe et* n *un entier naturel non nul, s'appelle « équation de Binôme ».*

Remarque : *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 *Etant donné un nombre complexe* d *et* n *un entier naturel non nul, on appelle racine* n*-ième de* d *tout nombre complexe* $\mathcal{Z}$ *tel que* $\mathcal{Z}^n = d$.

Définition 2.2.3 *Etant donné un entier naturel non nul* n*, on appelle racine* n*-ième de l'unité toute racine* n*-ième de* 1.

Rappel : *Soit* n *un entier naturel non nul, il y a exactement* n *racines* n*-ième de l'unité qui sont données par :* $\omega_k = e^{i\frac{2k\pi}{n}} = cos\left(\frac{2k\pi}{n}\right) + i\, sin\left(\frac{2k\pi}{n}\right) \;\; (0 \leq k \leq n-1)$

Remarque :

- *Si* $d = 0$ *, l'équation* $\mathcal{Z}^n = 0$ *équivaut à* $\mathcal{Z} = 0$ *c'est-à-dire que* 0 *est l'unique racine* n*-ième de* 0 .

Définition 2.2.4 *Un élément ayant une puissance dans un corps donné s'appelle un « Radical » relatif à ce corps.*

Remarque : *Les éléments* $\sqrt{2}$ *,* i *et* $i+1$ *sont des radicaux relatifs à* $\mathbb{Q}$ *sans être dans* $\mathbb{Q}$ *car :* $(\sqrt{2})^2 = 2 \in \mathbb{Q}$, $i^2 = -1 \in \mathbb{Q}$ *et* $(1+i)^4 = -4 \in \mathbb{Q}$.

L'élément $\sqrt{2} + i$ *n'est pas un radical relatif à* $\mathbb{Q}$*, car aucune de ses puissances n'est dans* $\mathbb{Q}$.

Exemple de la résolution d'une équation de Binôme : *Soit l'équation* $x^4 - 1 = 0$ *alors les solutions de cette équation de Binôme sont les 4 racines* n*-ièmes de* 1*, donc* $x_k = e^{i\frac{2k\pi}{n}}$ *avec* $n = 4$ *et* $(0 \leq k \leq 3$ *), d'où les solutions de l'équation sont les suivantes* $\{x_0 = 1,\ x_1 = i,\ x_2 = -1,\ x_3 = -i\}$.

Définition 2.2.5 *Soit* $\mathbb{K}$ *un corps engendré par les coefficients d'une équation algébrique, on adjoint à* $\mathbb{K}$ *tous ses radicaux, puis toutes les expressions algébriques, cette adjonction donne une extension* $\mathbb{K}_r$ *, on l'appelle* $\mathbb{K}_r$ *la saturation par radicaux de* $\mathbb{K}$.

Définition 2.2.6 *On dit que les racines d'une équation algébrique s'expriment algébriquement à l'aide des coefficients, c'est équivalent de dire que ses racines appartiennent à la saturation par radicaux du corps* $\mathbb{K}$.

Définition 2.2.7 *Une équation résoluble par radicaux est une équation qui « se ramène » à la résolution d'un certain nombre d'équations binômes.*

Résolution d'une équation algébrique par radicaux :

i. Equation de degré 2 quelconque :

Soit l'équation $x^2 + 2bx + c = 0$.

On a $x^2 + 2bx + c = 0 \Leftrightarrow x^2 + 2bx + b^2 - b^2 + c$

$\Leftrightarrow (x + b)^2 + c - b^2$

On pose $u = x + b$

$\Leftrightarrow u^2 + c - b^2 = 0$

$\Leftrightarrow u = \pm\sqrt{b^2 - c}$

$\Leftrightarrow x = -b \pm \sqrt{b^2 - c}$

$\Leftrightarrow x = \frac{-2b \pm \sqrt{(2b)^2 - 4C}}{2}$

Alors $x^2 + 2bx + c = 0 \Leftrightarrow \left(x - \frac{-2b - \sqrt{(2b)^2 - 4c}}{2}\right)\left(x - \frac{-2b + \sqrt{(2b)^2 - 4c}}{2}\right) = 0$

$\Leftrightarrow T_1 T_2 = 0$

$\Leftrightarrow T_1 = 0$ *ou* $T_2 = 0$.

Avec T_1, T_2 *des résolvantes partielles de l'équation* $x^2 + 2bx + c = 0$.

ii. Equation du troisième degré quelconque :

Méthode de Cardan : on cherche à résoudre $x^3 + px + q = 0$ *; l'idée de 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 :

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

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.*

On effet, $(X-u^3)(X-v^3)=0 \Leftrightarrow X^2-X(u^3+v^3)-(\frac{p}{3})^3=0$

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

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 et résoluble par radicaux.*

Remarque :

Expliquons pourquoi nous sommes contentées de résoudre des équations du troisième degré du type $x^3+px+q=0$.

Soit l'équation $(E): x^3+ax^2+bx+c=0$ *, on pose le changement du variable* $x=(y-\frac{a}{3})$ *et on remplace dans*(E)*, on trouve l'équation* $y^3+p'y+q'=0$.

iii. Equation du quatrième degré quelconque :

Méthode de Ferrari : on cherche de résoudre $x^4+cx^2+dx+e=0$ *;*

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 $d\neq 0$*, posons* $x'=x^2+t$ *, où* t *paramètre à choisir judicieusement. Elevons 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* $(x' + y)(x' - y) = 0$, $d^2 - 4(2t - c)(t^2 - e) = 0$. *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.*

Remarque :

Expliquons pourquoi nous sommes contentées de résoudre des équations du quatrième degré du type $x^4 + cx^2 + dx + e = 0$.

Soit l'équation (E): $x^4 + bx^3 + cx^2 + dx + e = 0$, *on pose le changement du variable*

$x = (y - \frac{b}{4})$ *et on remplace dans*(E), *on trouve l'équation* $y^4 + c'y^2 + d'y + e' = 0$.

D'après ce qui précède on obtient le résultat suivant :

Théorème 2.2.2 *Soit* $\mathbb{K}$ *un corps et* α *un élément d'une extension de* $\mathbb{K}$, *alors* α *s'exprime algébriquement à partir de* $\mathbb{K}$ *si et seulement si, il existe une suite finie croissante de corps* $\mathbb{K} \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_m$ *telle que :*

- *Le corps* $\mathbb{K}_m$ *contient* α *;*
- *Pour tout i, le corps* $\mathbb{K}_{i+1}$ *est engendré par* $\mathbb{K}_i$ *et un radical* t_i *d'un élément de* $\mathbb{K}_i$ *;*

On écrira alors $\mathbb{K}_{i+1} = \mathbb{K}_i(t_i)$.

On dit alors que $\mathbb{K}_{i+1}$ *est extension par radical de* $\mathbb{K}_i$, *et que* $\mathbb{K}_m$ *est extension de* $\mathbb{K}$ *par radicaux successifs.*

Exemple : *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* $\sqrt[3]{2}$, *puis de* $\mathbb{Q}_1$ *au corps* $\mathbb{Q}_2$ *engendré par* $\mathbb{Q}_1$ *et une racine carrée de* $2 - \sqrt[3]{2} \in \mathbb{Q}_1$.

2.3 Indépendance algébrique:

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

Par contre, si $(x_1, x_2, \ldots\ldots, x_n)$ *sont algébriquement dépendants sur* $\mathbb{K}$, *alors il existe un polynôme non nul* $P \in \mathbb{K}[X_1, \ldots\ldots X_n]$ *vérifiant* $P(x_1, x_2, \ldots\ldots, x_n) = 0$ *: une telle égalité s'appelle une relation de dépendance algébrique sur* $\mathbb{K}$ *entre les* x_i.

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

$u^2 - 2 = 0$, *ou* $v^2 - 3 = 0$, *ou* $u^2 + v^2 = 5$.

Définition 2.3.2 *On appellera équation générale de degré* n *sur* $\mathbb{Q}$ *l'équation*

$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$, *où les* a_i *sont algébriquement indépendants sur* $\mathbb{Q}$.

D'après tout ce qu'on a vu dans ce chapitre (*équation algébrique, expression des racines, résolution par radicaux,…*)*, on peut dire que ce n'est pas facile et parfois impossible de résoudre des équations algébriques par radicaux. Donc on peut au moins retenir que toutes les équations de degré inférieur ou égal à 4 sont résolubles par radicaux.*

Chapitre 3

Racines et corps de rupture

L'objet de ce chapitre est le suivant :

Soit P un polynôme de $\mathbb{K}[X]$. On veut obtenir des informations sur le corps engendré par $\mathbb{K}$ et les racines de P (corps de rupture), en introduisant ensuite quelques propriétés sur les polynômes (irréductibilité, factorisation,…).

3.1 Clôture algébrique :

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

Proposition 3.1.1 *Si $\mathbb{K}$ est algébriquement clos, tout $P \in \mathbb{K}[X]$ non constant est scindé*

Démonstration :

Pour $d = 1$ ($degP = d$), alors $P = aX + b$ c'est-à-dire $P = a(X + \frac{b}{a})$ donc évident.

Soit $P \in \mathbb{K}[X]$ de degré d et comme $\mathbb{K}$ est algébriquement clos, alors P possède dans $\mathbb{K}$ au moins une racine α_1, donc $P = (X - \alpha_1)Q$ avec $Q \in \mathbb{K}[X]$ de $degQ = d - 1$;

Et de même $Q \in \mathbb{K}[X]$, alors Q possède dans $\mathbb{K}$ au moins une racine α_2, donc

$P = (X - \alpha_1)(X - \alpha_2)H$ *avec* $H \in \mathbb{K}[X]$ *et* $degH = d - 2$;

De la même manière on trouve que $P = a(X - \alpha_1)(X - \alpha_2) \dots\dots\dots (X - \alpha_d)$ avec, a le coefficient dominant et les α_i $sont\ dans$ $\mathbb{K}$ (pas nécessairement distincts), d'où le polynôme P est scindé.

Corollaire 3.1.1 *Si $\mathbb{K}$ est algébriquement clos, tout polynôme irréductible de $\mathbb{K}[X]$ est de degré 1.*

Définition 3.1.2 *On appelle clôture algébrique d'un corps $\mathbb{K}$, toute extension $\mathbb{L}$ de $\mathbb{K}$ telle que :*

1) *$\mathbb{L}$ est algébrique sur $\mathbb{K}$.*
2) *$\mathbb{L}$ est un corps algébriquement clos.*

Exemple :

Le corps $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$ car $\mathbb{C}$ est une extension algébrique de $\mathbb{R}$ ($\mathbb{C} = \mathbb{R}(i)$), et $\mathbb{C}$ est un corps algébriquement clos.

Remarque : *Un corps fini ne peut être algébriquement clos.*

En effet, soit $\mathbb{K}$ *un corps fini* $\mathbb{K} = \{a_i; 1 \leq i \leq q\}$, *considérons dans* $\mathbb{K}[X]$ *le polynôme*

$P(X) = \prod_{i=1}^{q}(X - a_i) + 1$, *alors* $\forall\, 1 \leq i \leq q$ *on trouve que* $P(a_i) \neq 0$.

Donc le corps $\mathbb{K}$ *n'est pas algébriquement clos.*

3.2 Corps de rupture :

Définition 3.2.1 *Soit* $\mathbb{K}$ *un corps et* P *un polynôme sur* $\mathbb{K}$. *On prend dans la clôture algébrique de* $\mathbb{K}$ *le sous corps engendré par* $\mathbb{K}$ *et les racines de* P, *ce sous corps s'appelle corps de rupture de* P *sur* $\mathbb{K}$.

Exemple 1 :

Le corps de rupture de $1 + X^2$ *sur* $\mathbb{R}$ *est* $\mathbb{C}$ *tout entier.*

En effet, $1 + X^2 = 0 \Leftrightarrow X^2 = -1$, *alors* $X = \pm i$ *et le corps de rupture de* $1 + X^2$ *sur* $\mathbb{R}$ *est le corps* $\mathbb{R}(i) = \mathbb{C}$.

Alors que son corps de rupture sur $\mathbb{Q}$ *est* $\mathbb{Q}(i)$, *corps des nombres complexes à parties réelles et imaginaires rationnelles.*

Exemple 2 :

Le corps de rupture de $x^2 + ax + b$ *sur* $\mathbb{Q}$ *est le corps :*

$\mathbb{Q}\left(\sqrt{a^2 - 4b}\right) = \left\{A + B\sqrt{a^2 - 4b}\,;\ A, B \in \mathbb{Q}\right\}$.

Exemple 3:

Le corps de rupture d'une équation binôme $x^n - d = 0$ *sur un corps* $\mathbb{K}$ *est le corps engendré par* $\mathbb{K}$, *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* $x^n - 1$ *sur* $\mathbb{K}$.

Remarque :

On ne change pas le corps de rupture en divisant (*si c'est possible*) *ou en multipliant par des polynômes ayant toutes leurs racines dans le corps de départ.*

***Exemple* 1**:

Soit $P(X) = 1 + X^2 + X^4 \in \mathbb{Q}[X]$. *Le corps de rupture de* $P(X)$ *sur* $\mathbb{Q}$ *est le corps engendré par* $\mathbb{Q}$ *est les racines de* $P(X)$.

Soit $\mathrm{H}(X) = X^2 - 1$, *donc* $X^2 - 1 \Leftrightarrow X = \pm 1$

Multiplions $P(X)$ *par* $\mathrm{H}(X)$, *le corps de rupture de* $P(X)$ *est celui de* $P(X)\ \mathrm{H}(X) = X^6 - 1$.

***Exemple* 2**:

Soit $P(X) = 1 + X + X^2 + X^3 \in \mathbb{Q}[X]$. *Il s'annule pour* $X = -1$, *son corps de rupture est celui de* ${}^{P}/_{X+1} = X^2 + 1$ $(division\ Euclidienne)$, *c'est le corps* $\mathbb{Q}(i)$ *des complexes à coordonnés rationnelles.*

Définition 3.2.1 *On appelle un corps cyclotomique d'indice* n, *le corps de rupture de* $X^n - 1$ *sur* $\mathbb{Q}$ *avec* $X^n - 1 = 0$ (*une équation de la division du cercle*).

3.3 Factorisations d'un polynôme :

Soit L *et* K *deux corps avec* $(\mathrm{K} \subset \mathrm{L})$ *et soit* $P \in \mathrm{K}[X]$ *non nul qui possède une racine* α *dans une extension* L *de* K . *Il existe* $Q \in \mathrm{L}[X]$ *avec* $P = (X - \alpha)Q$.

En recommençant, au cas où Q *admet aussi* α *pour racine, on arrive à l'existence de* $\mathrm{T} \in \mathrm{L}[X]$ *vérifiant* $P = (X - \alpha)^m \mathrm{T}$ *et* $\mathrm{T}(\alpha) \neq 0$.

Définition 3.3.1 *On appelle* m *l'ordre de multiplicité de la racine* α.

Remarque :

La racine est dite simple pour $m = 1$, *multiple pour* $m \geq 2$.

Si $degP = n$ *alors* $deg\mathrm{T} = m - n$.

La somme des ordres de multiplicité des racines de P *ne peut dépasser* n.

Théorème 3.3.1 *Soit* L *et* K *deux corps avec* $(\mathrm{K} \subset \mathrm{L})$ *et soit* $P \in \mathrm{K}[X]$ *non nul qui possède des racines* α_i *avec* $1 \leq i \leq r$ *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* $P = a(X - \alpha_1)^{m_1} \dots \dots (X - \alpha_r)^{m_r}$.

Démonstration :

D'après le théorème 2.2.2 (chapitre 2) 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.

Equivaut 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 : *Soit* $P(X) = X^3 - 3X^2 + 3X - 1 \in \mathbb{Q}[X]$. 1 *est une racine de* P *mais la famille de ses racines s'écrive* $(1,1,1)$, *D'où* $P(X) = (X - 1)^3$.

3.4 Existence de racines multiples :

Définition 3.4.1 *Soit* $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{K}[X]$ *un polynôme. On définit le polynôme dérivé de P par :* $P' = \sum_{k=1}^{n} k a_k X^{k-1}$.

Définition 3.4.2 *Soit* $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{K}[X]$ *un polynôme avec* $degP = n$. *On dit que le polynôme est séparable s'il possède* n *racines distinctes dans une extension de* $\mathbb{K}$.

Définition 3.4.3 *Soit* $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{K}[X]$ *un polynôme avec* $degP = n$. *On dit que le polynôme est inséparable s'il possède des racines multiples dans une extension de* $\mathbb{K}$.

Définition 3.4.4 *Soit* $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{K}[X]$ *un polynôme non constant. Alors P et irréductible si et seulement si les seuls diviseurs sont les polynômes constants et les polynômes proportionnels au polynôme P.*

3.4.1 Racines simples :

Théorème 3.4.1.1 *Soit* $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{K}[X]$ *un polynôme.*

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 :

Soit $P(X) = X^n - 1$ *, alors le polynôme dérivé de P est* $P' = nX^{n-1}$ *Donc par division Euclidien* $X^n - 1 = (nX^{n-1})(\frac{X}{n}) - 1$ *; le reste* $R = -1$ *est constant, d'où le polynôme* $P(X) = X^n - 1$ *n'aura alors que des racines simples, et il y aura bien* n *racines* n*-ième de l'unité.*

3.4.2 Critère d'Eisenstein:

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

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

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

Démonstration :

Supposons par l'absurde qu'il existe deux éléments non constants

$Q = b_0 + b_1X + \ldots\ldots + b_qX^q$ *et* $R = c_0 + c_1X + \ldots\ldots + c_rX^r$ *de* $\mathbb{Z}[X]$ *tels 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* $s \in [1, q]$ $a_s = b_0c_s + b_1c_{s-1} + \ldots + b_sc_0$, *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 :

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

Théorème 3.4.2.1 *Soit un corps* $\mathbb{K}$ *contenant* $\mathbb{Q}$ *et soit* $P \in \mathbb{K}[X]$.

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* $degP' < degP$ *:*

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 $\mathbb{K}$ *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.*

Tous les résultats nécessaires pour notre discussion ont bien été établis, nous pouvons maintenant exposer des résultats importants sur les fonctions symétriques et les relations coefficients-racines.

Chapitre 4

Les fonctions symétriques

Dans ce chapitre, nous nous intéressons aux liens unissant les coefficients d'un polynôme à ses racines.

Pour arriver à ce but, nous présenterons les polynômes symétriques ainsi que les polynômes symétriques élémentaires.

Nous introduirons ensuite la notion de résultant entre deux polynômes qui nous permettra de définir le discriminant d'un polynôme. Pour finir, nous distinguerons le type de racines d'un polynôme en fonction de son discriminant.

4.1 Polynômes symétriques élémentaires :

Définition 4.1.1 *Soit* $\mathbb{K}$ *un corps. Un polynôme en* $X_1, X_2, \dots\dots, X_n$ *avec coefficients dans* $\mathbb{K}$ *est une somme* $P(X) = \sum_{(i_{1,\dots\dots}i_n)\in\mathbb{N}^n} a_{i_{1,\dots\dots}i_n} X_1^{i_1} X_2^{i_2} \dots\dots\dots X_n^{i_n}$ *, on dit que* $P(X)$ *est un polynôme à* n *indéterminées* (*ou à plusieurs variables*), *avec les* $a_{i_{1,\dots\dots}i_n} \in \mathbb{K}$ *et tous sauf un nombre fini des* $a_{i_{1,\dots\dots}i_n}$ *égaux à* 0.

Les $X_1^{i_1} X_2^{i_2} \dots\dots\dots X_n^{i_n}$ *sont des monômes et les* $a_{i_{1,\dots\dots}i_n} X_1^{i_1} X_2^{i_2} \dots\dots\dots X_n^{i_n}$ *sont des termes.*

Remarque :

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 *Soit* $\mathbb{K}$ *un corps et* $P(X)$ *un polynôme à* n *indéterminées et à coefficients dans* $\mathbb{K}$. *Le degré d'un monôme ou d'un terme* $a_{i_{1,\dots\dots}i_n} X_1^{i_1} X_2^{i_2} \dots\dots\dots X_n^{i_n}$ *est la somme* $i_1 + i_2 + \cdots + i_n$.

Définition 4.1.3 *Soit* $\mathbb{K}$ *un corps et* $P(X)$ *un polynôme à* n *indéterminées et à coefficients dans* $\mathbb{K}$. *Alors le degré d'un polynôme* $P(X)$ *non nul est le degré maximal de ses termes.*

Définition 4.1.4 *Soit* $\mathbb{K}$ *un corps et* $P(X)$ *un polynôme à plusieurs variables et à coefficients dans* $\mathbb{K}$. *On dit qu'un polynôme non nul* $P(X)$ *est homogène de degré* d *si tous ses termes sont de degré* d.

Exemple :

Le polynôme $P(X) = X_1 X_3^3 + X_1^2 X_2^2 + X_2^4$ *est homogène de degré 4.*

Définition 4.1.5 *Un polynôme $P(X)$ en n indéterminées est symétrique si pour toute permutation $\rho \in S_n$ on a :*

$$P(X_1, X_2, \dots\dots, X_n) = P(X_{\rho(1)}, X_{\rho(2)}, \dots\dots, X_{\rho(n)})$$

Exemple :

Les polynômes $P(X,Y,Z) = X + Y + Z$ et $T(X,Y,Z) = X^3Y + Y^3Z + Z^3X + Y^3X + Z^3Y + X^3Z$ sont symétriques.

Définition 4.1.6 *Soit $\mathbb{K}$ un corps. On appelle une fraction rationnelle à n indéterminées toute fraction rationnelle $P, Q \in \mathbb{K}[X_1, X_2, \dots\dots, X_n]$:*

$\frac{P}{Q}\left(X_{\rho(1)}, X_{\rho(2)}, \dots\dots, X_{\rho(n)}\right) = \frac{P(X_1, X_2, \dots\dots, X_n)}{Q(X_1, X_2, \dots\dots, X_n)}$ *Pour toute permutation $\rho \in S_n$, avec $Q \neq 0$.*

Définition 4.1.7 *Etant donné n indéterminées sur un corps $\mathbb{K}$, on appelle polynômes symétriques élémentaires les n polynômes suivants :*

- *Somme des indéterminées ; $\sum_{i=1}^{n} X_i$*
- *Somme des produits deux à deux des indéterminées ; $\sum_{1 \le i < j \le n} X_i X_j$*
- *Somme des produits ; $\sum_{1 \le i < j < \cdots < m \le n} X_i X_j \dots\dots X_m$*
- *Produit des indéterminées ;*

On notera $\sigma_1, \sigma_2, \dots\dots, \sigma_n$ ces n polynômes.

Exemple :

Les polynômes symétriques élémentaires en trois variables sont :

$\sigma_1 = X_1 + X_2 + X_3$, $\sigma_2 = X_1X_2 + X_1X_3 + X_2X_3$ *et* $\sigma_3 = X_1X_2X_3$.

Définition 4.1.8 *Les valeurs de n polynômes symétriques élémentaires sur une famille de n éléments s'appellent les fonctions symétriques élémentaires de ces éléments.*

Exemple :

Les fonctions symétriques élémentaires en $1,2,3$ *sont :*

$\sigma_1 = 1 + 2 + 3 = 6$, $\sigma_2 = 1 \times 2 + 1 \times 3 + 2 \times 3 = 11$ *et* $\sigma_3 = 1 \times 2 \times 3 = 6$.

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

Démonstration :

Partons d'un polynôme $P(X) = a_nX^n + \cdots + a_1X + a_0$, les coefficients $a_i \in \mathbb{K}$.

On suppose a_n *non nul, et on note* $(x_1, x_2, \dots\dots, x_n)$ *la famille des racines* (*on répète les racines suivant leur ordre de multiplicité*).

Le corps de rupture est alors engendré par $\mathbb{K}$ *et les* x_i*, dans ce corps, on écrit*

$$a_n X^n + \cdots + a_1 X + a_0 = a_n (X - x_1)(X - x_2) \dots\dots (X - x_n).$$

En développant le second membre, on trouve les n égalités suivantes, dites

« Relations entre coefficients et racines » :

$$x_1 + x_2 + \dots\dots + x_n = \frac{-a_{n-1}}{a_n}$$

$$\sum_{1 \le i < j \le n} x_i x_j = \frac{a_{n-2}}{a_n}$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\sum_{1 \le i < j < \cdots < k \le n} x_i x_j \dots\dots x_k = \frac{(-1)^k a_{n-k}}{a_n}$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$x_1 x_2 \dots\dots\dots x_n = (-1)^n \frac{a_0}{a_n}$$

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

Corollaire 4.1.1 *La résolution d'une équation algébrique se ramène à celle d'un système d'équations* (n *équations*)*à* n *inconnues.*

Exemple :

Les racines x_1 *et* x_2 *de* $X^2 + aX + b$ *sont caractérisées par :* $\begin{cases} x_1 + x_2 = -a \\ x_1 x_2 = b \end{cases}$

Les racines x_1, x_2 *et* x_3 *de* $X^3 + pX + q$ *sont caractérisées par :* $\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1 x_2 + x_1 x_3 + x_2 x_3 = p \\ x_1 x_2 x_3 = -q \end{cases}$

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 $X_1^{i_1}X_2^{i_2}\dots\dots\dots X_m^{i_m}$ *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 $\sum X_1^{i_1}X_2^{i_2}\dots\dots\dots X_m^{i_m}$.

Ainsi les polynômes symétriques élémentaires sont $\sigma_1 = \sum_{i=1}^{n} X_i, \dots\dots, \sigma_n = X_1X_2\dots\dots X_n$

D'autres « simples » sont ceux obtenus en partant d'un monôme ne comptant qu'une indéterminée. On posera $S_i = \sum_{j=1}^{n} X_j^i$ *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 $P(Y) = Y^n - \sigma_1 Y^{n-1} + \sigma_2 Y^{n-2} + \dots\dots + (-1)^n\sigma_n$ *et* $X_1, X_2, \dots\dots, X_n$ *les racines de ce polynôme. Donc* $P(Y) = (Y - X_1)(Y - X_2)\dots\dots(Y - X_n)$.

Dérivons par rapport à Y, on trouve $P'(Y) = \frac{P(Y)}{Y-X_1} + \dots + \frac{P(Y)}{Y-X_n}$

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

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

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

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

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

Posons le $X = \frac{1}{Y}$ *, pour arriver à*

$$\frac{P'\left(\frac{1}{X}\right)}{XP\left(\frac{1}{X}\right)} = n + S_1X + S_2X^2 + \dots + S_{q-1}X^{q-1} + X^q\left[\sum_{i=1}^{n}\frac{X_i^q}{1 - XX_i}\right].$$

On a aussi

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

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

$$\frac{P'\left(\frac{1}{X}\right)}{XP\left(\frac{1}{X}\right)} = \frac{n-(n-1)\sigma_1 X+(n-2)\sigma_2 X^2+\ \ldots\ +(-1)^{n-1}\sigma_{n-1}X^{n-1}}{1-\sigma_1 X+\sigma_2 X^2+\cdots+(-1)^n\sigma_n X^n}$$

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

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

D'où l'on tire :

$$S_1 = \sigma_1$$

$$S_2 = \sigma_1^2 - 2\sigma_2$$

$$S_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$$

$$S_i = \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$S_n = \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Alors pour tout entier i, la somme des puissances i-ième des indéterminées est un polynôme en les polynômes symétriques élémentaires.

De plus les $\sigma_1, \sigma_2, \ldots\ldots\ldots, \sigma_n$ *algébriquement indépendants sur le corps* $\mathbb{K}$*, 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 $\overline{\mathbb{K}}$ *un corps algébriquement clos et* $\mathbb{K}$ *un corps contenu dans* $\overline{\mathbb{K}}$.

Soit P *et* Q *deux polynômes de* $\mathbb{K}[X]$ *de degrés* m *et* n *respectivement.*

On pose $P(X) = a\prod_{1\le i\le m}(X-x_i)$ *et* $Q(X) = b\prod_{1\le i\le n}(X-y_i)$

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

$$Rés(P,Q) = a^n b^m \prod_{\substack{1\le i\le m\\ 1\le j\le n}} (x_i - y_j)$$

Remarque :

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

Proposition 4.2.1

Soit P et Q deux polynômes définis comme ci-dessus. Alors :

i. *Le résultant de P et Q est un élément de $\mathbb{K}$.*
ii. *Le résultant de P et Q est nul si et seulement si P et Q ont une racine commune dans le corps $\overline{\mathbb{K}}$.*
iii. *Le résultant de P et Q est nul si et seulement si P et Q ont un $PGCD$ non constant.*

Démonstration :

i. *D'une part $P(X) \in \mathbb{K}[X]$ et ses racines $x_1, x_2, \dots\dots\dots, x_n$ dans le corps $\overline{\mathbb{K}}$.*
D'autre part, considérons $a^n b^m \prod_{\substack{1\le i\le m\\ 1\le j\le n}}(x_i - y_j) = a^n \prod_{1\le i\le m} Q(x_i)$, polynôme symétrique dans $\mathbb{K}[X_1, \dots\dots X_n]$, on $a^n \prod_{1\le i\le m} Q(x_i) \in \mathbb{K}$, car on a pour tout polynôme symétrique $S \in \mathbb{K}[X_1, \dots\dots, X_n]$, le nombre $S(x_1, \dots\dots, x_n)$ appartient à $\mathbb{K}$.

D'où

$$Rés(P, Q) = a^n b^m \prod_{\substack{1\le i\le m\\ 1\le j\le n}} (x_i - y_j) \in \mathbb{K}.$$

ii. *Si P et Q sont non nuls et si $Rés(P, Q) = 0$, donc par définition il existe i et j tels que $x_i = y_j$ s'implique que P et Q ont une racine commune dans le corps $\overline{\mathbb{K}}$.*
Il est clair que la réciproque est vraie.

iii. *Comme P et Q sont à coefficients dans $\mathbb{K}$, nous pouvons calculer leur $PGCD$ dans $\mathbb{K}[X]$, le $PGCD$ s'obtient avec l'algorithme de division d'Euclide, en particulier, pour $P = Q\mathrm{H} + R$ et R sont unique, alors le $PGCD$ de P et Q sont dans le corps $\overline{\mathbb{K}}$.*
Si P et Q ont une racine commune dans $\overline{\mathbb{K}}$ que nous noterons x_i, alors $x - x_i$ divise P, Q et donc le $PGCD$ de P et Q, il ensuit que le $PGCD$ de P et Q n'est pas constant.
Réciproquement, si le $PGCD$ de P et Q n'est pas constant, toutes racine de $PGCD$ de P et Q dans $\overline{\mathbb{K}}$ est une racine commune de P et Q, ce qui permet de conclure que $Rés(P, Q) = 0$.

4.3 Déterminant de Sylvester :

Soit $P(X) = a_0 + a_1X + \dots\dots + a_nX^n$ *et* $Q(X) = b_0 + b_1X + \dots\dots + b_pX^p$ *deux équations algébriques,* $\overline{\mathbb{K}}$ *un corps algébriquement clos et* $\mathbb{K}$ *un corps contenu dans* $\overline{\mathbb{K}}$.

Un moyen « systématique » de calculer le résultant de P et Q utilise la méthode dite « déterminant de Sylvester ».

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

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

Remarque :

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

4.4 Discriminant d'un polynôme :

Soit $\overline{\mathbb{K}}$ *un corps algébriquement clos et* $\mathbb{K}$ *un corps contenu dans* $\overline{\mathbb{K}}$.

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

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

Proposition 4.4.1 *Le discriminant* $\Delta(P)$ *d'un polynôme non constant* P *est un élément de* $\mathbb{K}$, *nul si et seulement si* P *a une racine multiple dans* $\overline{\mathbb{K}}$.

Démonstration :

C'est une conséquence de la proposition 4.2.1

Après avoir introduit les notions de résultant et discriminant, nous pouvons maintenant expliquer la relation entre le discriminant et le type de racines d'un polynôme de degré deux ou trois.

Proposition 4.4.2 *Le discriminant de polynôme* $p(X) = aX^2 + bX + c$ *est :*

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

Démonstration :

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

$$=-4a^2(x_1x_2)-2ab(x_1+x_2)-b^2$$

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

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

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

Avec $Rés(aX^2+bX+c\ ,\ 2aX+b)=det\begin{pmatrix}c & b & a\\ b & 2a & 0\\ 0 & b & 2a\end{pmatrix}$

$$=4a^2c-b^2a$$

Donc $\Delta(aX^2+bX+c)=\frac{(-1)^{\frac{2}{2}}}{a}(4a^2c-b^2a)$

$$=b^2-4ac$$

Proposition 4.4.3 *Le discriminant de polynôme* $p(X)=X^3+pX+q$ *est :*

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

Démonstration :

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

Avec $Rés(X^3+pX+q,3X^2+p)=det\begin{pmatrix}q & p & 0 & 1 & 0\\ 0 & q & p & 0 & 1\\ p & 0 & 3 & 0 & 0\\ 0 & p & 0 & 3 & 0\\ 0 & 0 & p & 0 & 3\end{pmatrix}$

$$=4p^3+27q^2$$

Donc $\Delta(x^3+px+q\ )=-4p^3-27q^2$.

Remarque :

a) Polynômes du second degré

Supposons a, b, c réels. Notons x_1 et x_2 les racines de $aX^2 + bX + c$ dans le corps $\mathbb{C}$.
D'après la formule ci-dessus et en utilisant le lien entre les coefficients et les racines d'un polynôme, nous avons : $\Delta(aX^2 + bX + c) = b^2 - 4ac = a^2(x_1 - x_2)^2$.
Si les racines sont réelles distinctes, alors $b^2 - 4ac > 0$.
Si x_1 et x_2 ne sont pas réelles, elles sont conjuguées dans $\mathbb{C}$ et $x_1 - x_2$ est un imaginaire pur, donc $b^2 - 4ac < 0$.

b) Polynômes du troisième degré

Supposons p, q réels et notons x_1, x_2, x_3 les racines de $X^3 + pX + q$ dans le corps $\mathbb{C}$.
Nous avons : $\Delta(X^3 + pX + q) = -4p^3 - 27q^2 = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2$.
Si les trois racines sont réelles distinctes, alors $-4p^3 - 27q^2 > 0$.
Si deux racines, par exemple x_1 et x_2, ne sont pas réelles, elles sont conjuguées dans $\mathbb{C}$ et $(x_1 - x_2)$ est alors un imaginaire pur, donc $(x_1 - x_2)^2 < 0$; $(x_1 - x_3)^2$ et $(x_1 - x_3)^2$ sont conjugués et leur produit est strictement positif, donc $-4p^3 - 27q^2 < 0$.

Conclusion

Vers la théorie de Galois

D'après ce qu'on a vu dans ce rapport, tous les résultats nécessaires pour commencer l'étude de la théorie de Galois ont bien été établis, nous pouvons donc donner une vision possible des idées d'Evariste Galois :

On se donne un certain nombre de règles « les principes de construction à la règle et au compas » et on dit qu'un élément est constructible si on peut l'obtenir à partir d'un ensemble de points en suivant ces règles.

Le problème qui se pose est : comment savoir si un nombre est constructible à la règle et au compas ?

La première étape consiste à traduire la notion de constructibilité par 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, «* $X^n - d = 0$ *»), on ajoute à* K *toutes les combinaisons algébriques possibles d'une racine* $\alpha_1 \notin \mathrm{K}$ *de cette équation, on obtient un corps* K_1 *avec* $(\mathrm{K} \subset \mathrm{K}_1)$ *avec* $\mathrm{K}_1 = \mathrm{K}(\alpha_1)$.

En répétant l'opération un nombre fini (n *fois*)*, on obtient une suite croissante de corps* $\mathrm{K} \subset \mathrm{K}(\alpha_1) \subset \ldots\ldots \subset \mathrm{K}_{n-1}(\alpha_n) = \mathrm{K}_n$ *et* $n \in \mathbb{N}^*$.

Exemple de groupe de Galois :

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

Les deux racines de $P(X)$ *sont* i *et* $-i$ *et on a* $\mathbb{C}$ *est une extension de* $\mathbb{R}$ *(* $\mathbb{R} \subset \mathbb{C}$ *) de degré* 2 *avec* $\mathbb{C} = \mathbb{R}(i) = \{x + iy\ ;\ (x, y) \in \mathbb{R} \times \mathbb{R}\}$.

On peut associer à cette extension deux $\mathbb{R}$*-automorphisme de* $\mathbb{C}$ σ_1, σ_2 *tel que*

$\forall\, x \in \mathbb{R}\ \ \sigma_1(x) = x$ *et* $\sigma_2(x) = x$.

Tout σ ($\mathbb{R}$*-automorphisme de* $\mathbb{C}$) *est déterminé par la donnée de* $\sigma(i)$ *car si on applique* σ *à tout élément dans* $\mathbb{C}$*, on a* $\sigma(x + iy) = x + \sigma(i)y$ *par propriétés de l'homomorphisme, et le fait que* σ $\mathbb{R}$*-homomorphisme laisse invariant les éléments de* $\mathbb{R}$.

Or, $i^2 = -1 \Longrightarrow \left(\sigma(i)\right)^2 = \sigma(i^2) = \sigma(-1) = -1.$

Donc $\sigma(i) = i$ *ou* $\sigma(i) = -i.$

Alors $\sigma_1(x + iy) = x + iy$ *et* $\sigma_2(x + iy) = x - iy.$

Donc $\sigma_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *et* $\sigma_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$

$\{id_{\mathbb{C}}, \sigma_2\}$ *S'appelle le Groupe de Galois de l'extension* $\mathbb{C}$ *de* $\mathbb{R}$

Bibliographie

Claude Mutafian, Equations algébriques et théorie de Galois, Vuibert.

Josette Calais, Extension de corps, Théorie de Galois, Niveau M1-M2.

Carrega J-C, Théorie des corps- La règle et au compas, Herman, 1981.