République Algérienne Démocratique Et Populaire
Université Mohamed Boudiaf De M'sila
Faculté Des Mathématiques Et De L'informatique
Département De Mathématiques

MEMOIRE DE FIN D'ETUDE

Présenté pour l'obtention du Diplôme de **MASTER**

Domaine : Mathématiques et Informatique

Filière : Mathématiques

Option : Algèbre et Mathématiques Discrètes

Par

ELBAGOR Rachida

Sujet

Constructions géométriques à la règle et le compas

Date de soutenance : 18/06/2018.

Devant le jury :

Mr. AMROUNE Abdelaziz	Prof. Univ de M'sila	Président
Mr. LADJELAT Lahcene	MAA. Univ de M'sila	Rapporteur
Mr. SAADI Abderachid	MCB. Univ de M'sila	Examinateur

Promotion : 2017 / 2018

Remerciements

Je tiens à remercier tout premièrement **ALLAH** le tout puissant pour la volonté, la santé et la patience, qu'il nous a donné Durant toutes années.

Ainsi, Je tiens également à exprimer ma vifs remerciements à Mr. **LADJELAT Lahcene** pour l'intéressant sujet qu'il m'a proposé.

Je suis également reconnaissant pour la confiance qu'il m'a accordée.

Il m'est impossible de lui exprimer toute ma gratitude en seulement quelques lignes.

Je ne saurais oublier de remercier mon jury Mr. **LADJELAT Lahcene**, Mr. **AMROUNE Abdelaziz** et Mr. **SAADI Abde rachid** et toutes les personnes sayant contribué de près ou de loin à l'aboutissement de ce travail.

Pour finir mes derniers mots de remerciements vont tout naturellement à ma famille et mes amis, en particulier mes parents et mon marie pour leur soutient tout au long de mes études.

Dédicace

Je dédie ce travail à mes chers parents et mon marie, qu'ils trouvent
ici le témoignage de ma profonde gratitude pour leur amour,
leur encourage et leur soutien tout au long de mes études, que **ALLAH** les bénisse.

A mes chers soeurs
et mes chers frères.

A tous mes chères amies.

A tous mes collègues de promotion
A tous ceux que j'aime.

A tous ceux qui m'aiment.
Je dédie le fruit de mes efforts.

Table des matières

Introduction

Euclide a fondé sa géométrie sur un système d'axiomes, qui assure en particulier qu'il est toujours possible de tracer une droite passant par deux point donnés, et qu'il est toujours possible de tracer un cercle de centre donné, et passant par un point donné. La géométrie Euclidienne est donc la géométrie des droites et des cercles, donc de la régle et du compas. L'intuition d'Euclide était que tout nombre pouvait être construit, ou « obtenu », à l'aide des deux instruments.

Cette conjecture va d'une part remettre en question la définition d'un nombre : les nombres rationnel ne suffisent pas à exprimé toutes les longueures puisque la diagonale d'un carré de côté 1 est constructible, mais correspont au nombre $\sqrt{2}$ dont on démontre facilement qu'il ne saurait être le rapport de deux entiers et, d'autre part, engager la commuanté mathématique dans la recherche de résoluction impossible, comme la duplication du cube, la quadrature du cercle et la trisection de l'angle sont trois problèmes grecs classique qui été résolu grâce aux progrès de la théorie des corps au XVIIIè et XIXè s.

Ainsi, ce mémoire comport trois chapitres :

Dans le premier chapitre, on présente de notions fondamentales sur les anneaux, corps, sous-corps, idéaux d'un anneau, anneau quotient, anneau principal, et élèment irréductible.

Dans le deuxième chapitre, on définit les extensions d'un corps et le type de ces extensions : extensions simples, extensions algébriques et extensions finies.

Dans le troisième chapitre, on va donner des constructions géométriques et les trois problèmes grecs : la duplication du cube, la quadrature du cercle, et la trisection des angles, les nombres constructibles à la règle et au compas, nombre constructible et extensions quadratiques, applications aux problèmes grecs.

Chapitre 1

Notions fondamentales

1.1 Anneaux

Définition 1.1

Un anneau $(A, +, \cdot)$ est la donnée d'un ensemble non vide A, muni de deux lois de composition internes notées " $+$ " et " $\cdot$ " (appelées respectivement addition et multiplication) telles que :

- $(A, +)$ est un groupe abélien (on notera 0 son élément neutre)
- La loi " $\cdot$ " est associative i.e. $\forall x, y, z \in A,\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- La loi " $\cdot$ " est distributive par rapport à la loi " $+$ "

$$\forall x, y, z \in A,\ x \cdot (y + z) = x \cdot y + x \cdot z \ \text{ et } \ (x + y) \cdot z = x \cdot z + y \cdot z$$

Remarques 1.1

1. Si la loi " $\cdot$ " est commutative i.e $\forall x, y \in A,\ x \cdot y = y \cdot x$, on dit que l'anneau A est commutatif.
2. Si la loi " $\cdot$ " posséde un élément neutre 1, on dit que A est un anneau unitaire.

Exemples 1.1

$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs unitaires.

1.1.1 Diviseurs de zéro

Définition 1.2

Soit A un anneau non réduit à $\{0\}$, on dit qu'un élèment $a \in A$ est un diviseur de zéro à gauche (résp. a droite) si $a \neq 0$ et s' il existe un élément non nul b de A tel que $a \cdot b = 0$(resp. $b \cdot a = 0$)

Exemple 1.2

pour $\mathbb{Z}/6\mathbb{Z}$, $\overline{2}$ et $\overline{3}$ sont des diviseurs de zéro car $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$.

Définition 1.3

Un anneau commutatif A est dit intègre s'il est non nul, et si ne pssède pas de diviseur de zéro. Autrement dit l'anneau A est intégre si la relation $a \cdot b = 0$ implique $a = 0$ ou $b = 0$.

Exemples 1.3

1. Pour $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.
2. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des anneaux intégres.

1.1.2 Division dans un anneau

Définition 1.4

Soient A un anneau commutatif unitaire intègre, a et b deux éléments de A. On dit que a divise b et on ecrit $a \mid b$ si il existe q de A tel que $b = a \cdot q$.

Exemples 1.4

1) $A = \mathbb{Z}$, $3 \mid 9$ et $(-3) \mid 9$

2) $A = \mathbb{Z}/6\mathbb{Z}$, $\overline{5} \mid \overline{4}$ car $\overline{2} \cdot \overline{5} = \overline{10} = \overline{4}$

1.1.3 Eléments invèrsibles (unités)

Définition 1.5

Soit A un anneau unitaire, et soit $a \in A$. On dit que a est un élément inversible ou élément unité de A si a possède un symétrique pour la multiplicalion. Nous noterons $U(A)$ l'ensemble des éléments inversibles

de A.

Exemples 1.5

1. Pour $\mathbb{Z}$, les éléments inversibles sont 1 et -1. De façon général, dans tout anneau unitaire 1 et -1 sont des éléments unités.
2. Pour $\mathbb{R}$, tout réal non nul est inversible.
3. Pour $\mathbb{Z}/6\mathbb{Z}$, $\overline{1}$ et $\overline{5}$ sont des élément unités.

Proposition 1.1

Soit A un anneau unitaire.

L'ensemble $U(A)$ des éléments inversibles de A est un groupe pour la multiplication de A.

Exemples 1.6

1. Dans l'anneau $\mathbb{Z}$, on a $U(\mathbb{Z}) = \{-1, 1\}$
2. Pour $n \geqslant 1$, $U(\mathbb{Z}/n\mathbb{Z}) = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z},\ (x, n) = 1\}$.
   si $n = 6$, $U(\mathbb{Z}/6\mathbb{Z}) = \{\overline{1}, \overline{5}\}$.

1.2 Corps

Définition 1.6

Un corps est un anneau commutatif, non nul, dans lequel tout élément non nul admet un inverse.

Exemple 1.7

$(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des corps.

Définition 1.7

Un polynôme d'indéterminée X et à cofficients dans A est une somme formelle

$P(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \ldots . + a_nX^n$

avec $\forall\ i \geq 0$, $a_i \in A$ et $a_i = 0$ pour $i \geqslant n+1$.

Définition 1.8

Si $a_n \neq 0$, on dit que $P(X)$ est de degré n , et on écrit deg $(P) = d^{\circ}P = n$;

si $a_0 = a_1 = \ldots = a_n = 0$, $P(X)$ est le polynôme nul ($P(X) = 0$)

Sur $A[X]$ on définit

• Addition

$f(X) = a_0 + a_1X + a_2X^2 + \ldots . + a_nX^n$

$g(X) = b_0 + b_1X + b_2X^2 + \ldots . + b_sX^s$

$(f+g)(X) = (a_0+b_0) + (a_1+b_1)X + (a_2+b_2)X^2 + \ldots$

• Multiplication

$(f \cdot g)(X) = c_0 + c_1X + c_2X^2 + \ldots . + a_kX^k$, tels que

$c_0 = a_0b_0$, $c_1 = a_0b_1 + a_1b_0$,

$c_2 = a_0b_2 + a_1b_1 + a_2b_0 \ldots c_k = a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \ldots + a_kb_0$

1.3 Sous-anneaux

Définition 1.9

Soient A un anneau, et B une partie non vide de A. On dit que B est un sous-anneau de A si $(B\ ,+,\cdot)$ est un anneau.

Exemples 1.8

1. $(2\mathbb{Z}, +, \cdot)$ est sous-anneau de $(\mathbb{Z}, +, \cdot)$.
2. $(\mathbb{Z}, +, \cdot)$ est sous-anneau de $(\mathbb{Q}, +, \cdot)$.

Proposition 1.2

Soient A un anneau, et B une partie non vide de A. Les conditions souivantes sont équivalentes :

1. *B est un sous-anneau de A.*

2. *$1 \in B$ et quels que soient $x, y \in B$, on a $x - y \in B$ et $x \cdot y \in B$.*

Preuve.

($\Rightarrow$)

B est un sous-anneau de$A$, il est clair que la condition 2) est vérifiée.

($\Leftarrow$)

$B \neq \emptyset$ car $1 \in B$ et B est sous-groupe du groupe additif A (puisque les relations $x \in B$ et $y \in B$ entraînent $x - y \in B$). D'autre part, comme les relations $x \in B$ et $y \in B$ impliquent $x \cdot y \in B$, on voit que B est bien un sous -anneau de A. ■

1.4 Idéaux d'un anneau

Définition 1.10

Soit $(A, +, \cdot)$ un anneau.

Un idéal bilatère de A est une partie non vide de A tel que :

1. $\forall x, y \in I$ on a $x - y \in I$

2. $\forall a \in A, \forall x \in I$ on a $x \cdot a \in I$ et $a \cdot x \in I$.

Exemples 1.9

1. $\{0\}$ et A sont des idéaux de A. Ce sont les seuls si A est un corps.

2. Les ideaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

Proposition 1.3

Soient A un anneau commutatif unitaire, et I un idéal de A.

1. *$1 \in I \iff I = A$*

2. *Soit $x \in U(A)$* $\qquad\qquad$ *$x \in I \iff I = A$*

Preuve.

1) L'implication ($\Leftarrow$) est evidente

($\Rightarrow$)

Supponsons que $1 \in I$. Comme $I \subset A$, il suffit de montrer que $A \subset I$.

Soit $x \in A$ et $1 \in I$ et comme I est un idéal de A alors $x \cdot 1 = 1 \cdot x = x \in I$

Donc $A \subset I$.

2) Soit $x \in U(A)$

L'implication ($\Leftarrow$) est evidente

($\Rightarrow$)

Si $x \in I$ avec $x \in U(A)$, alors il existe $y \in A$ tel que $x \cdot y = y \cdot x = 1$

Il resulte que $1 \in I$, donc $I = A$. ■

1.5 Anneau quotient

Définition 1.11

Soit A un anneau commutatif et unitaire, et soit I un idéal de A, et $a \in A$. On définit $a + I = \{a + x\,;\, x \in I\}$, appelée la classe de a modulo l'idéal I.

Définition 1.12

On définit sur A la relation binaire suivante

$$a \; R \; b \Leftrightarrow a - b \in I$$

R est une relation d'équivalence sur A

la réflexivité :

$a \; R \; a$, car $a - a = 0 \in I$

la symétrie :

$a \; R \; b \Leftrightarrow a - b \in I \Leftrightarrow -(a - b) \in I \Leftrightarrow b - a \in I \Leftrightarrow b \; R \; a$

la transitivité :

$(a \; R \; b \text{ et } b \; R \; c\,) \Leftrightarrow (a - b \in I \text{ et } b - c \in I) \Rightarrow (a - b) + (b - c) \in I \Rightarrow a - c \in I \Rightarrow a \; R \; c$

Soit $a \in A$

$$\begin{aligned} \bar{a} = \{b \in A\,;\, b \; R \; a\,\} = \{b \in A\,;\, b - a \in I\,\} \\ = \{b \in A\,;\, b - a = x\ ,\ x \in I\,\} \\ = \{b \in A\,;\, b = a + x, x \in I\,\} \\ = a + I. \end{aligned}$$

Proposition 1.4

1. $A/I = A/R = \{\overline{a}\ ; a \in A\} = \{a + I,\ a \in A\}$
2. $(a + I) + (b + I) = a + b + I.$
3. $(a + I) \cdot (b + I) = a \cdot b + I.$

C'est -a-dire $\overline{a} + \overline{b} = \overline{b} + \overline{a}$ *et* $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

Théorème 1.1

L'ensemble A/I pour les lois intèrnes définies ci-dessus, est un anneau appelée l'anneau quotient de A sur I.

Exemple 1.10

$A = \mathbb{Z}$, $I = n\mathbb{Z}$, $n \in \mathbb{N}$.

1.6 Anneau principal

Définition 1.13

Soit A un anneau, et I un idéal de A. On dit que I est un idéal principal de A s' il existe $a \in A$ tel que $I = (a) = \{a \cdot x \mid x \in A\}$

Définition 1.14

Un anneau est dit principal si il est intègre, et si tout ses idéaux sont principaux.

Exemples 1.11

1) $\mathbb{Z}$ est un anneau principal .

2) Soit $\Bbbk$ un corps commitatif, l'anneau $\Bbbk[X]$ est principal.

1.6.1 Idéal premier

Définition 1.15

Soit $(A, +, \cdot)$ un anneau. Un idéal I est dit premier, s'il est porpre ($I \neq A$), et s'il vérifie :

$$\forall\ x, y \in A\ ,\quad x \cdot y \in I\ \Rightarrow x \in I \text{ ou } y \in I\ .$$

Exemples 1.12

1. Les idéaux premiers de $\mathbb{Z}$ sont les $p\mathbb{Z}$, où p est premier.

Pour $A = \mathbb{Z}$, soit $I = (5) = 5\mathbb{Z}$. I est idéal premier de $\mathbb{Z}$ car si $x, y \in \mathbb{Z}$, tels que $x \cdot y \in 5\mathbb{Z}$, on a $5 \mid x \cdot y$, et comme 5 est premier, alors $5 \mid x$ ou $5 \mid y$ c ést à dire $x \in 5\mathbb{Z}$ ou $y \in 5\mathbb{Z}$.

Théorème 1.2

Soit A un anneau et I un idéal de A.

I est un idéal premier si et seulement si A/I est intégre.

Preuve.

($\Leftarrow$) Soient $x, y \in A$ tel que $x \cdot y \in I$, on a :

$x \cdot y + I = I$

$\Rightarrow (x + I) \cdot (y + I) = I$

$\Rightarrow x + I = I$ ou $y + I = I$

$\Rightarrow x \in I$ ou $y \in I$, donc I premier.

($\Rightarrow$)I premier tel que :

$x \cdot y \in I \Rightarrow x \in I$ ou $y \in I$

$\Rightarrow x + I = I$ ou $y + I = I$ donc A/I est intégre. ■

1.6.2 Idéal maximal

Définition 1.16

Un idéal I est un idéal maximal dans A si :

1. $I \neq A$,
2. Si J est idéal de A tel que : $I \subset J$ alors $J = I$ ou $J = A$.

Exemples 1.13

1. Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$, où p est premier.

$A = \mathbb{Z}$, $I = 3\mathbb{Z}$, I est idéal maximal car on a $3\mathbb{Z} \neq \mathbb{Z}$, et si $J = n\mathbb{Z}$ un idéal de $\mathbb{Z}$ vérifiant $3\mathbb{Z} \subset n\mathbb{Z}$, alors $n \mid 3$ d'ou $n = 1$ ou $n = 3$

Si $n = 1$ alors $J = \mathbb{Z} = A$.

Si $n = 3$ alors $J = 3\mathbb{Z} = I$.

Théorème 1.3

1. *I idéal maximal $\Longleftrightarrow$ A/I corps*
2. *I idéal maximal $\Rightarrow$ I idéal premier.*

Preuve.

De 2) I idéal maximal $\Leftrightarrow$ A/I corps $\Rightarrow$ A/I intégre $\Leftrightarrow$ I idéal premier, donc I idéal maximal $\Rightarrow$ I idéal premier. ■

1.6.3 Homomorphisme d'anneaux

Définition 1.17

Si A et B sont deux anneaux, un homomorphisme d'anneaux est une application $f : A \to B$ vérifiant les propriétés suivantes :

a) Pour tous a et $b \in A$, $f(a+b) = f(a) + f(b)$;

b) Pour tous a et $b \in A$, $f(a \cdot b) = f(a) \cdot f(b)$;

Proposition 1.5

Si f est homomorphisme d'anneaux, on a

1. $f(0_A) = 0_B$.
2. $f(1_A) = 1_B$.
3. $f(-a) = -f(a)$, $a \in A$.
4. $f(a^n) = [f(a)]^n$, $n \in \mathbb{N}$ *et* $a \in A$.

Définition 1.18

Un isomorphisme est un homomorphisme bijectif ; un automorphisme est un isomorphisme d'un anneau sur lui-même.

L'image d'un homomorphisme d'anneaux $A \to B$ est sous-anneau de B .

Exemple 1.14

Si I est idéal bilatère d'un anneau A. L'application canonique $\Pi : A \to A/I$, $x \to x + I$ est un morphisme d'anneaux. On l'appelle l'homomorphisme canonique.

1.7 Elèments irréductibles

Définition 1.19

Un élèment $p \in A$ est dit irréductible si :

1. $p \neq 0$, et $p \notin U(A)$
2. $p = a.b$ avec $a, b \in A$, alors $a \in U(A)$ ou $b \in U(A)$.

Exemples 1.15

$A = \mathbb{Z}$, les élèment irréductibles de $\mathbb{Z}$, sont les élèment $\pm p$ avec p premiers.

Chapitre 2

Extension d'un corps

Nous citions des propositions qui lient deux corps, lorsque l'un est inclus dans l'autre.

2.1 Extension d'un corps

Définition 2.1

Une extension d'un corps commutatif K est un corps L qui contient K comme sous-corps.

On note parfois L/K pour indiquer que L est une extenion de K.

Exemples 2.1

1. $\mathbb{C}$ est une extension de $\mathbb{R}$.
2. $\mathbb{R}$ est une extension de $\mathbb{Q}$.

2.2 Extensions simples

Définition 2.2

Une extension L d'un corps K est dite simple, s'il existe un élément a de L, tel que L est égale à $K(a)$,

où $K(a) = \{\frac{f(a)}{g(a)},\ f, g \in K[x],\ g(a) \neq 0\}$.

2.2.1 Homomorphisme de corps

Définition 2.3

Un homomorphisme de corps commutatifs est par définition un homomorphisme d'anneaux entre deux corps commutatifs.

Les monomorphisme sont les homomorphisme injectifs. Un homomorphisme surjectif est un épimorphisme.

Définition 2.4

Soinent L_1 et L_2 deux extension du même corps K, si $f : L_1 \to L_2$ est un homomorphisme de corps, et pour tout $x \in K$, $f(x) = x$. On dit que f est $K-$ homomorphisme.

Proposition 2.1

Si $f : E_1 \to E_2$ est un homomorphisme de corps, alors $f \cong 0$ ($\forall x \in E_1 : f(x) = 0$) ou f est injectif.

Preuve.

$Ker\ f = \{x \in E_1 : f(x) = 0\}$ est un idéal de E_1. Les seuls idéaux de E_1 sont $\{0\}$ et E_1. Si $Ker\ f = E_1$ alors $f = 0$. Si $Ker\ f = \{0\}$ alors f injectif (dans ce cas E_1 peut être considére comme sous corps de E_2). ■

Exemple 2.2

$f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$

$a + b\sqrt{2} \to a - b\sqrt{2}$

On a : si $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$ dans $\mathbb{Q}(\sqrt{2})$,

$$\begin{aligned} f(x+y) &= f((a+c) + (b+d)\sqrt{2}) \\ &= (a+c) - (b+d)\sqrt{2} \\ &= (a - b\sqrt{2}) + (c - d\sqrt{2}) \\ &= f(x) + f(y), \end{aligned}$$

et de même $f(x \cdot y) = f(x) \cdot f(y)$.

Donc f est un $\mathbb{Q}-$ homomorphisme de corps.

2.2.2 Eléments algébriques et éléments transcendants

Définition 2.5

Soit L/K une extension.

Un élément α de L est dit algébrique sur K, s'il existe un polynôme non nul à coefficients dans K, tel que $f(\alpha) = 0$.

Un élément qui n'est pas algérique sur K est dit transcendant sur K.

Exemples 2.3

1. $\alpha \in K$, est algébrique sur K, car α est une racine de $f(x) = x - \alpha$, $f(x) \in K[x]$,
2. $K = \mathbb{Q}$, $L = \mathbb{R}$, $\alpha = \sqrt{2}$ est algébrique sur $\mathbb{Q}$, car α est une racine de $f(x) = x^2 - 2$,
3. $K = \mathbb{Q}$, $L = \mathbb{R}$, $\alpha = \sqrt[3]{5}$ est algébrique sur $\mathbb{Q}$, car α est une racine de $f(x) = x^3 - 5$,
4. $K = \mathbb{R}$, $L = \mathbb{C}$, $\alpha = i$ est algébrique sur $\mathbb{R}$, car α est une racine de $f(x) = x^2+1$, $f(x) \in \mathbb{R}[x]$.
5. le nombre e ou le nombre π sont des réels transcendants sur $\mathbb{Q}$.

Théorème 2.1 *[Gelfond-Shneider]*

Si $\alpha \neq 0$ et 1 est algébrique sur $\mathbb{Q}$, β est algébrique sur $\mathbb{Q}$ et $\beta \notin \mathbb{Q}$ alors α^β est transcendant sur $\mathbb{Q}$.

Exemples 2.4

a) $\alpha = 2$, $\beta = \sqrt{2}$, implique $2^{\sqrt{2}}$ est transcendant sur $\mathbb{Q}$.

b) $\alpha = \sqrt{2}$, $\beta = \sqrt{3}$, implique $\sqrt{2}^{\sqrt{3}}$ est transcendant sur $\mathbb{Q}$.

Théorème 2.2

Si $\alpha \in L$ est algébrique sur K alors :

1. *il existe un polynôme $P(x) \in K[x]$, irréductible normalisé unique qui vérifie $P(\alpha) = 0$.*
2. *si $f(x) \in K[x]$ tel que $f(\alpha) = 0$ alors $P(x)|f(x)$.*

Définition 2.6

Soit L/K une extension.

Le polynôme $P(x)$ défini par le théorème précédent est noté ;

$Irr(\alpha, K, x) = Irr_K(\alpha, x)$ est appelé le polynôme minimal de α sur K.

Exemples 2.5

1. K=$\mathbb{Q}$, L=$\mathbb{R}$, $\alpha = \sqrt{2}$, on a $Irr(\sqrt{2}, \mathbb{Q}, x) = x^2 - 2$.
2. K=$\mathbb{R}$, L=$\mathbb{C}$, $\alpha = i$, on a $Irr(i, \mathbb{R}, x) = x^2 + 1$.

Théorème 2.3

Soit $\alpha \in L$ algébrique sur K, et $P(x) = Irr(\alpha, K, x)$ alors :

1. $[K(x) : K] = n$, *avec* $n = \deg(P(x))$
2. $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ *est une base de $K(\alpha)$ sur K.*

Exemples 2.6

a) $K = \mathbb{Q}$, $L = \mathbb{R}$, $\alpha = \sqrt{2}$, on a $Irr(\sqrt{2}, \mathbb{Q}, x) = x^2 - 2$ et

1. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$
2. $\{1, \sqrt{2}\}$est une base de $\mathbb{Q}(\sqrt{2})$ sur $\mathbb{Q}$.

   Donc $\mathbb{Q}(\sqrt{2}) = \{a \cdot 1 + b \cdot \sqrt{2} : a, b \in \mathbb{Q}\}$.

b) $K = \mathbb{R}$, $L = \mathbb{C}$, $\alpha = i$, on a $Irr(i, \mathbb{R}, x) = x^2 + 1$ et

1. $[\mathbb{R}(i) : \mathbb{R}] = 2$
2. $\{1, i\}$est une base de $\mathbb{R}(i)$ sur $\mathbb{R}$.

   Donc $\mathbb{R}(i) = \{a \cdot 1 + b \cdot i : a, b \in \mathbb{R}\}$.

c) $K = \mathbb{Q}$, $L = \mathbb{R}$, $\alpha = \sqrt[3]{5}$, on a $Irr(\sqrt[3]{5}, \mathbb{Q}, x) = x^3 - 5$ et

1. $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$
2. $\{1, \sqrt[3]{5}, \sqrt[3]{25}\}$est une base de $\mathbb{Q}(\sqrt[3]{5})$ sur $\mathbb{Q}$.

   Donc $\mathbb{Q}(\sqrt[3]{5}) = \{a \cdot 1 + b \cdot \sqrt[3]{5} + c \cdot \sqrt[3]{25} : a, b, c \in \mathbb{Q}\}$.

2.3 Extensions finies

Définition 2.7

Si la dimension de extension L d'un corps K, considéré comme$K$-espace vectoriel est finie, on dit que L est une extension finie de K, de degré $[L : K] = dim_K L$.

Si ce degré vaut 2, nous parlerons d'une *extension quadratique.*

Exemple 2.7

$[\mathbb{C} : \mathbb{R}] = 2$, $\mathbb{C}$ est une extension finie de $\mathbb{R}$.

Théorème 2.4

Soit L/K une extension, $\alpha \in L$.

$K(\alpha)$ est une extension finie de K si et sulement si α algébrique sur K.

Théorème 2.5

Si K, L, H sont trois corps avec $K \subset L \subset H$ et si les extensions ont un degré fini alors : $[H : K] = [H : L][L : K]$.

Preuve.

Soit $\{l_1, l_2, ..., l_n\}$ une base de H sur L et soit $\{e_1, e_2, ..., e_m\}$ une base de L sur K. $\{l_1e_1, l_1e_2, ..., l_1e_m, l_2e_1, l_2e_2, ..., l_2e_m, ..., l_ne_1, l_ne_2, ..., l_ne_m\} = \{l_ie_j,\ 1 \leqslant i \leqslant n,$

$1 \leqslant j \leqslant m\}$ est une base de H sur K.Donc H est une extension finie de K et on a $[H : K] = m \cdot n = [H : L][L : K]$. ■

Remarque 2.1

Soit L/K une extension.

$$[L : K] = 1 \Leftrightarrow L = K.$$

Proposition 2.2

1. *Soit L une extension finie du corps K. Si $x \in L$, alors x est un nombre algébrique.*
2. *Si x un nombre algébrique, alors $K(x)$ est une extension finie de K.*
3. *Si x est un nombre algébrique, alors le degré de l'extension $[K(x) : K]$ et le degré algébrique de x coïncident.*

Preuve.

1) Soit L une extension finie de K, et soit $n = [L : K]$. Fixons $x \in L$. Les $n+1$ éléments$(1, x, x^2, ..., x^n)$ forment une famille de n + 1 vecteurs dans un espace vectoriel de dimension n. Donc cette famille est liée. Il existe donc une combinaison linéaire nulle non triviale, c'est-à-dire il existe $a_i \in K$ non tous nuls tels que $\sum_{i=0}^{n} a_i x^i = 0$. Si l'on définit $P(X) = \sum_{i=0}^{n} a_i X_i$, alors $P(X) \in K[X]$, $P(X)$ n'est pas le polynôme nul et $P(x) = 0$. C'est exactement dire que x est un nombre algébrique.

2) Soit $P(X) = \sum_{i=0}^{n} a_i X^i$ non nul qui vérifie $P(x) = 0$. En écartant le le cas trivial $x = 0$, on peut donc supposer que $a_0 \neq 0$ et $a_n \neq 0$.

Alors $x^n = -\frac{1}{a_n} \sum_{i=0}^{n-1} a_i x^i$ et $\frac{1}{x} = \frac{1}{a_0} \sum_{i=1}^{n} a_i x^{i-1}$. Ce qui prouve que $x^n \in Vect(1, x, ..., x^{n-1})$ et $\frac{1}{x} \in Vect(1, x, ..., x^{n-1})$. De même pour tout $k \in \mathbb{Z}$, $x^k \in Vect(1, x, ..., x^{n-1})$, donc $K(x) \subset Vect(1, x, ..., x^{n-1})$. Ce qui prouve que $K(x)$ est un espace vectoriel de dimension finie sur K.

3) Ce sont à peu près les mêmes arguments. Si $m = [K(x) : K]$ alors il existe $a_i \in K$ non tous nuls tels que $\sum_{i=0}^{m} a_i x^i = 0$.Donc il existe un polynôme non nul de degré m annulant x. Donc le degré algébrique de x est inférieur ou égal à m.

Mais s'il existait un polynôme $P(X) = \sum_{i=0}^{m-1} b_i X^i$ non nul de degré strictement inférieur à m qui annulait x, alors nous aurions une combinaison linéaire nulle non triviale $\sum_{i=0}^{m-1} b_i x^i = 0$. Cela impliquerait que $x^{m-1} \in Vect(1, x, ..., x^{m-2})$ et plus généralement que $K(x) \subset Vect(1, x, ..., x^{m-2})$, ce qui contredirait le fait que $K(x)$ soit un espace vectoriel de dimension m sur K.

Donc le degré algébrique de x est exactement $[K(x) : K]$. ■

Corollaire 2.1

Si x et y sont des nombres réels algébriques sur K, alors $x + y$ et xy sont aussi.

Preuve.

Comme x est un nombre algébrique alors $L = K(x)$ est une extension finie de K. Posons $M = K(x, y) = (K(x))(y)$. Comme y est un nombre algébrique alors M est une extension finie de $K(x)$. Par le théorème *2.4* $M = K(x, y)$ est une extension finie de K.

Comme $x + y \in K(x + y) \subset K(x, y)$ et que $K(x, y)$ est une extension finie de K alors par la proposition *2.1* , $x + y$ est un nombre algébrique.

C'est la même preuve pour $xy \in K(xy) \subset K(x, y)$. ■

Corollaire 2.2

Si L est une extension finie d'un corps K, de degré n, alors tout élément de L est algébrique sur K et son degré est diviseur n.

Preuve.

Quel que soit $\alpha \in L$, les $n+1$ éléments $\alpha^0 = 1, \alpha, \alpha^2, ..., \alpha^n$ de L sont linéairement dépendants sur K. On a danc une relation de la forme :

$a_n\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_0 = 0$ ($a_i \in K$, i de 0 à n)

où les a_i ne sont pas tout nuls. Donc α est zéro d'un polynôme non nul de $K[x]$, c'est -à-dire α est algébrique sur K. L'élément α engendre une extension simple $K(\alpha) \subset L$.

On a donc d'après le théorème 2.4 :

$$[L : K(\alpha)][K(\alpha) : K] = n. \quad ■$$

2.4 Extensions algébriques

Définition 2.8

On dira qu'une extension L d'un corps K que c'est une extension algébrique de K, si tout élément $\alpha \in L$ est algébrique sur K.

Exemple 2.8

Toute extension finie du corps K est une extension algébrique de K.

Théorème 2.6

Soit H une extension algébrique d'un corps K et L une extension algébrique de H, alors L est une extension algébrique de K.

Preuve.

Un élément α de L est par hypothèse un élément algébrique sur H. Soit $g(X) = \sum_{i=0}^{n} h_i X^i$ le polynôme de $H[X]$ annulé par α et $F = K(h_0,h_1,...,h_n)$ le corps obtenu par adjonction d'un nombre fini d'éléments algébriques sur K, coefficients de g. Ce corps F est une extension finie de K et on a $K \subset F \subset F(\alpha)$. Puisque $F(\alpha)$ est une extension finie de K, donc α est un élément algébrique sur K. ■

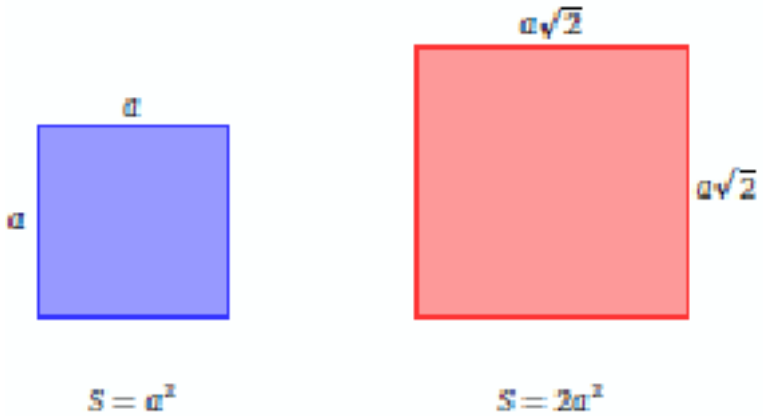
Chapitre 3

Constructions géométriques

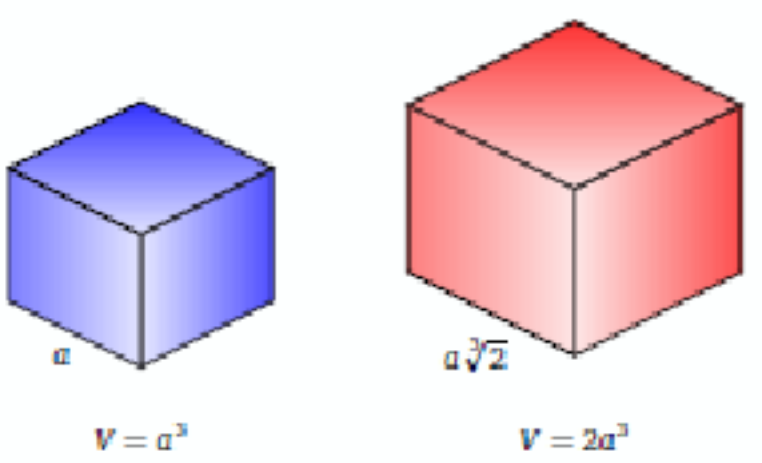
3.1 Constructions et les trois problèmes grecs

3.1.1 La duplication du cube

Commençons par un problème assez simple : étant donné un carré, construire (à la règle et au compas) un carré dont l'aire est le double. C'est facile, car cela revient à savoir tracer un côté de longueur $a\sqrt{2}$ à partir d'un côté de longueur a. En fait diagonale de notre carré original a la longeur volume $a\sqrt{2}$. Partant de cette longeur, on construit un carré dont l'aire est $(a\sqrt{2})^2 = 2a^2$: son aire est bien le double de cette carré de départ.



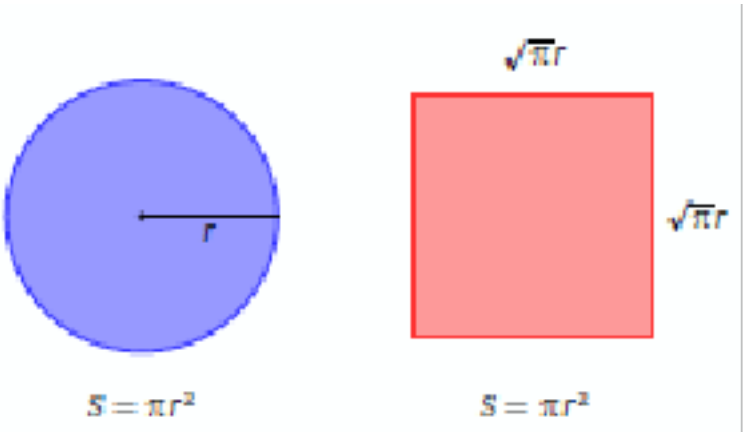
Posons nous la question dans l'espace : étant donné un cube, peut-on construire un second cube dont le volume est le double de celui du premier ? Si le premier cube a ses côtés de longueur a, alors le second doit avoir ses côtés de longueur $a\sqrt[3]{2}$. La question se formule alors de la manière suivante :



Problème de la duplication du cube. Étant donné un segment de longueur 1, peut-on construire à la règle et au compas un segment de longueur $\sqrt[3]{2}$?

3.1.2 La quadrature du cercle

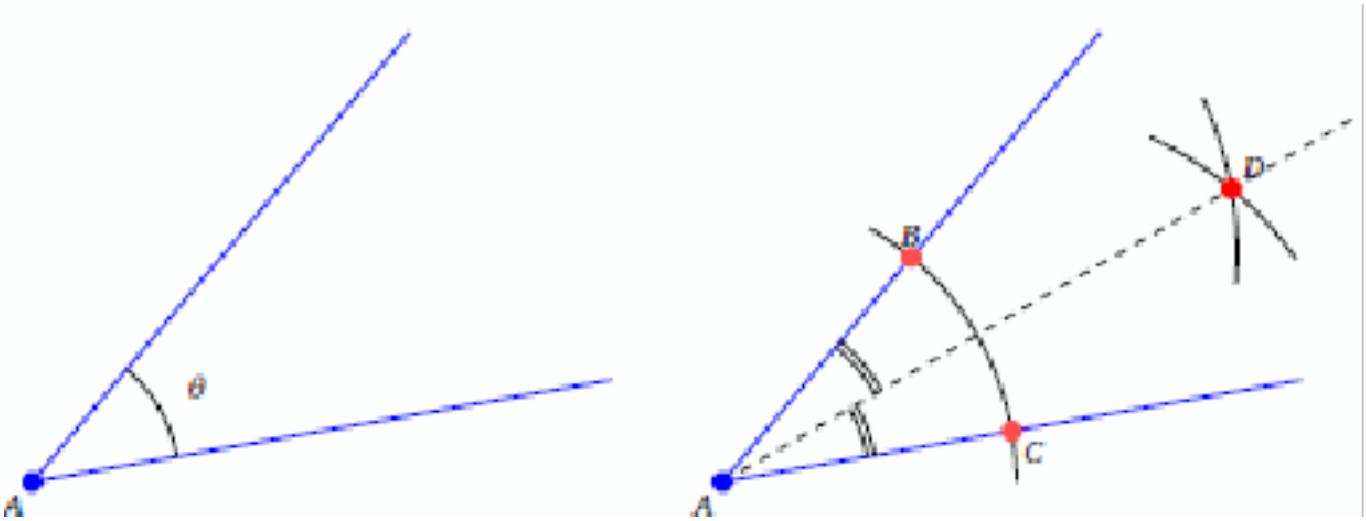
Problème de la quadrature du cercle. Étant donné un cercle, peut-on construire à la règle et au compas un carré de même aire ?



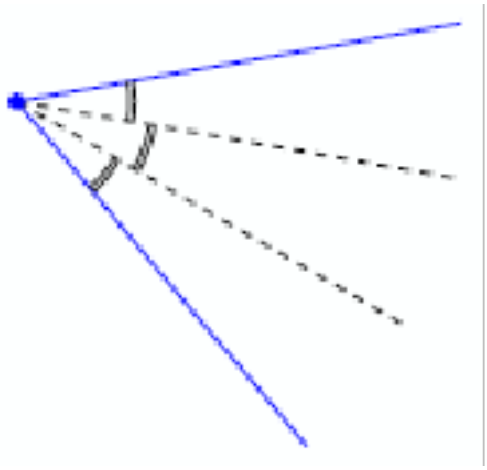
Cela revient à construire un segment de longueur $\sqrt{\pi}$ à la règle et au compas, à partir d'un segment de longueur 1.

3.1.3 La trisection des angles

Considérons un angle θ, c'est-à-dire la donnée d'un point A et de deux demi-droites issues de ce point. Nous savons diviser cet angle en deux à l'aide d'une règle et d'un compas : il suffit de tracer la bissectrice. Pour cela on fixe un écartement de compas et on trace un cercle centré en A : il recoupe les demi-droites en des points B et C. On trace maintenant deux cercles centrés en B puis C (avec le même rayon pour les deux cercles). Si D est un point de l'intersection de ces deux cercles alors la droite (AD) est la bissectrice de l'angle.

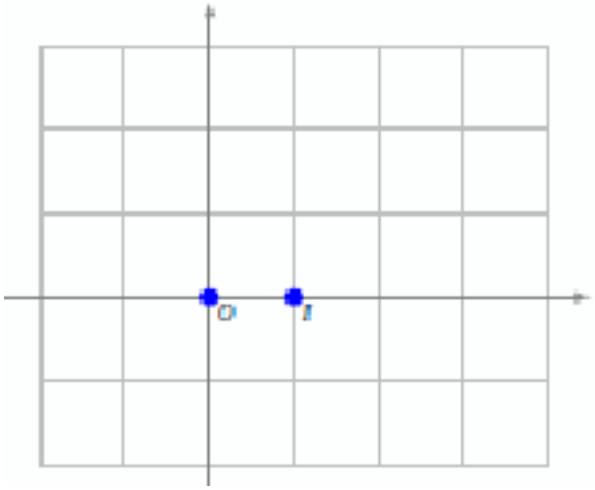


Problème de la trisection. Peut-on diviser un angle donné en trois angles égaux à l'aide de la règle et du compas ?



3.2 Les nombres constructibles à la règle et au compas

On considère le plan euclidien ξ muni d'un repère orthonormé, que l'on identifiera à $\mathbb{R}^2$ (ou $\mathbb{C}$). On définit des ensembles de points $X_i \subset \xi$ par récurrence.



• On se donne au départ seulement deux points : $X_0 = \{O; I\}$ où $O = (0, 0)$ et $I = (1, 0)$.

• Fixons $i \geqslant 0$, et supposons qu'un certain ensemble de points X_i soit déjà construit. Alors on définit X_{i+1} par récurrence, comme l'ensemble des points élémentairement constructibles à partir de X_i.

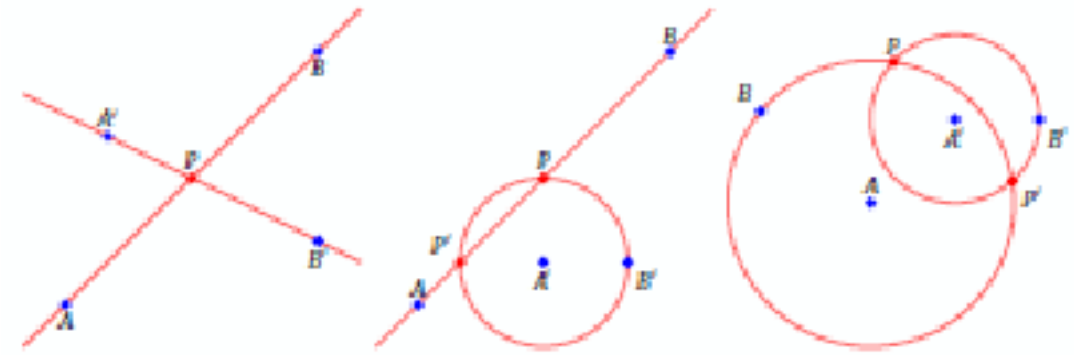
C'est-à-dire : $P \in X_{i+1}$ si et seulement si

1. $P \in X_i$
2. ou $P \in (AB) \cap (A'B')$ avec $A, B, A', B' \in X_i$,
3. ou $P \in (AB) \cap X(A', A'B')$ avec $A, B, A', B' \in X_i$,
4. ou$P \in X(A, AB) \cap X(A', A'B')$ avec$A, B, A', B' \in X_i$.

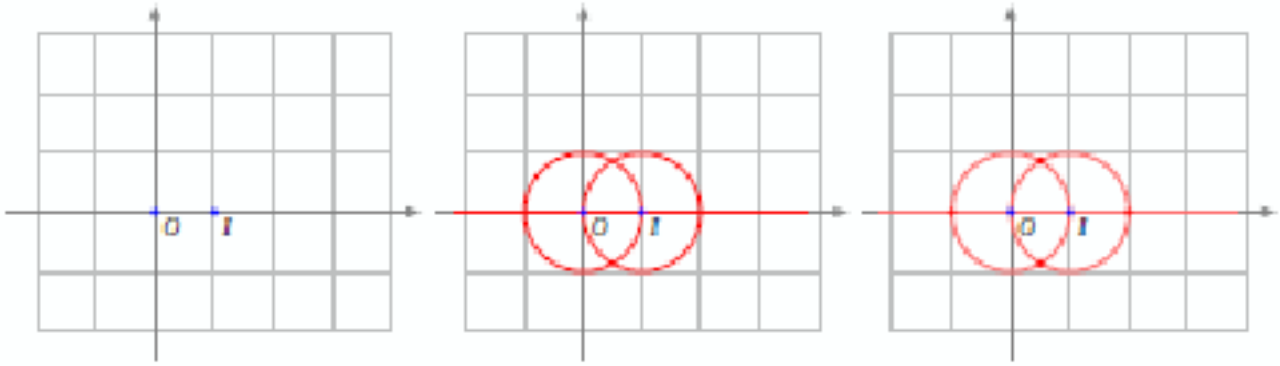
On a noté $X(A, r)$ le cercle de centre A et de rayon r.

Il faut comprendre cette construction ainsi : si A, B, A', B' ont été construits et sont dans X_i alors, à partir de ces points, on peut tracer plusieurs objets à la règle et au compas : par exemple la droite (AB) – à l'aide de la règle – ou le cercle de centre A'et de rayon de longueur $A'B'$ en plaçant la pointe du compas en A' avec un écartement faisant passer le cercle par B'. Si cette droite (AB) et ce cercle $X(A, A'B')$ s'intersectent alors les points d'intersection sont par définition dansX_{i+1}.

Voici les trois situations possibles. Les points A, B, A', B' en bleu sont dans X_i , et les points P rouge sont dans X_{i+1}.



Voici la première étape. Partant de X_0 (en bleu à gauche), on peut tracer une droite et deux cercles (au milieu), ce qui donne pour X_1 quatre points supplémentaires (en rouge à droite).



Pour X_2 on repartirait de tous les points (rouges ou bleus) de X_1, et on tracerait tous les cercles ou droites possibles (il y en a beaucoup !), et les points d'intersection formeraient l'ensemble X_2.

Définition 3.1

- $X = \cup_{i \geqslant 0} X_i$ est l'ensemble des *points constructibles*. Autrement dit

  $X = X_0 \cup X_1 \cup X_2 ...$

  De plus $P \in X$ si et seulement s'il existe i $\geqslant 0$ tel que $P \in X_i$.

- $X_{\mathbb{R}} \subset \mathbb{R}$ est l'ensemble des abscisses des points constructibles : ce sont les *nombres (réels) constructibles.*
- $X_{\mathbb{C}} \subset \mathbb{C}$ est l'ensemble des affixes des points constructibles : ce sont les *nombres complexes constructibles.*

Attention ! Même si deux points A, B sont constructibles et que l'on peut tracer la droite (AB), pour autant les points de (AB) ne sont pas tous constructibles. Seuls les points d'intersection de(AB) avec d'autres objets construits sont constructibles.

Déterminer les points constructibles X ou déterminer les nombres constructibles $X_{\mathbb{R}}$ sont deux problèmes équivalents.

En effet, si (x, y) est un point constructible alors par projection sur l'axe des abscisses nous obtenons le réel constructible x, et de même pour y projection sur l'axe des ordonnées, puis report sur l'axe des abscisses. Réciproquement on peut passer de deux nombres constructibles x, $y \in \mathbb{R}$ à un point constructible (x, y) dans le plan. Voici comment : partant du point$(y, 0)$ on construit $(0, y)$ sur l'axe des ordonnées par un coup de compas en reportant y. Une fois que $(x, 0)$ et $(0, y)$ sont construits, il est facile de construire (x, y).

3.3 Nombre constructible et extensions quadratiques

Théorème 3.1 *[Wantzel, 1837]*

Un nombre réel x est constructible si et seulement s'il existe des extensions quadratiques

$$\mathbb{Q} = K_0 \subset K_1 \subset ... \subset K_r, \text{ telles que } x \in K_r.$$

Preuve.

intersection d'une droite et d'un cercle (ou de deux cercles) dont les équations sont à coefficients dans K. On est ramené à résoudre une équation du deuxième degré dont les racines sont dans une extension quadratique de K.

Tout revient à dire qu'il existe une suite infinie de corps :

$\mathbb{Q} = K_0 \subset K_1 \subset ... \subset K_r$, telles que $x \in K_r$.

tel que $[K_i : K_{i-1}] = 2$. Un nombre réel est constructible si son degré sur $\mathbb{Q}$ est une puissance de 2. ■

Corollaire 3.1

Tout nombre réel constructible est un nombre algébrique dont le degré algébrique est de la forme 2^n, $n \geqslant 0$.

Preuve.

Si x nombre est constructible. Par le théorème de Wantzel, il existe des extensions quadratiques $\mathbb{Q} = K_0 \subset K_1 \subset ... \subset K_r$ telles que $x \in K_r$. Donc x appartient à une extension de $\mathbb{Q}$ de degré fini. Ainsi, par la proposition , x est un nombre algébrique.

On sait de plus que $[K_{i+1} : K_i] = 2$, donc par la proposition, nous avons

$[K_r : \mathbb{Q}] = 2^r$. Il nous reste à en déduire le degré algébrique $[\mathbb{Q}(x) : \mathbb{Q}]$. Comme $\mathbb{Q}(x) \subset K_r$, alors nous avons toujours par la proposition que :

$[K_r : \mathbb{Q}(x)][\mathbb{Q}(x) : \mathbb{Q}] = [K_r : \mathbb{Q}] = 2^r$. Donc $[\mathbb{Q}(x) : \mathbb{Q}]$ divise 2^r et est donc de la forme 2^n. ■

Corollaire 3.2

$X_{\mathbb{R}}$ est le plus petit sous-corps de $\mathbb{R}$ stable par racine carrée, c'est-à-dire tel que :

- *$(x \in X_{\mathbb{R}}$ et $x \geqslant 0) \Rightarrow \sqrt{x} \in X_{\mathbb{R}}$,*
- *si K est un autre sous-corps de $\mathbb{R}$ stable par racine carrée alors $X_{\mathbb{R}} \subset K$.*

3.4 Applications aux problèmes grecs

Corollaire 3.3

1. *Si un nombre réel x est constructible, alors x est un nombre algébrique. C'est-à-dire qu'il existe un polynôme $P \in \mathbb{Q}[X]$ tel que $P(x) = 0$.*
2. *De plus le degré algébrique de x est de la forme 2^n, $n \geqslant 0$. C'est-à-dire que le plus petit degré, parmi tous les degrés des polynômes $P \in \mathbb{Q}[X]$ vérifiant $P(x) = 0$, est une puissance de 2.*

3.4.1 L'impossibilité de la duplication du cube

Théorème 3.2

$\sqrt[3]{2}$ n'est pas un nombre constructible.

Preuve.

$\sqrt[3]{2}$ est une racine du polynôme $P(X) = X^3 - 2$. Ce polynôme est unitaire et irréductible dans $\mathbb{Q}[X]$, $\sqrt[3]{2}$ donc est un nombre algébrique de degré 3. Ainsi son degré algébrique n'est pas de la forme 2^n. Donc $\sqrt[3]{2}$ n'est pas constructible. ■

3.4.2 L'impossibilité de la quadrature du cercle

Théorème 3.3

π n'est pas un nombre algébrique (donc n'est pas constructible).

Preuve. Comme π n'est pas constructible, alors $\sqrt{\pi}$ n'est pas constructible non plus (c'est la contraposée de $x \in X_{\mathbb{R}} \Rightarrow x^2 \in X_{\mathbb{R}}$).

Le fait que π est transcendant (c'est á dire non algébrique) est démontré par Lindemann en 1982. ■

3.4.3 L'impossibilité de la trisection des angles

Théorème 3.4

L'angle $\frac{\pi}{3}$ est constructible, mais ne peut pas être coupé en trois car $cos\frac{\pi}{9}$ n'est pas un nombre constructible.

Preuve.

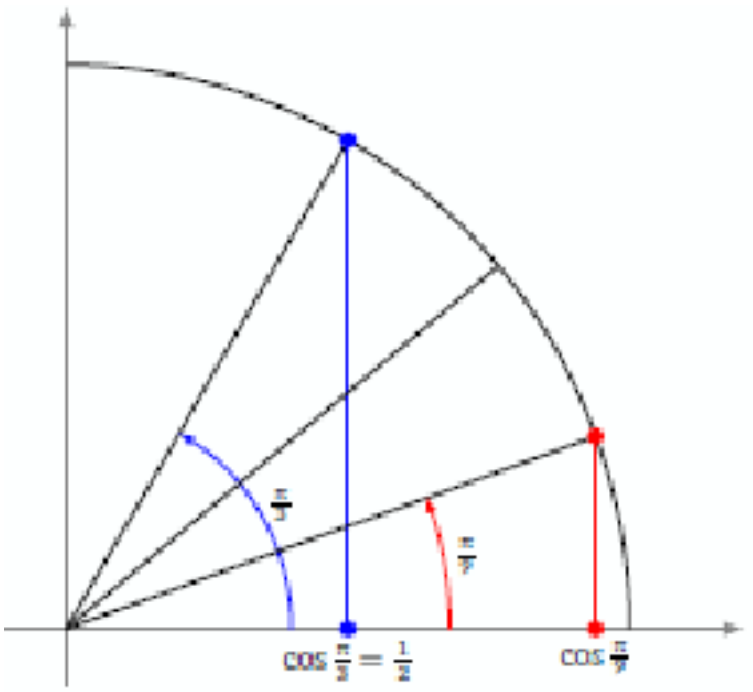
L'angle $3\theta = \frac{\pi}{3}$ est constructible car $\cos 3\theta = \cos \frac{\pi}{3} = \frac{1}{2}$, impossible dans le cas général car $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$, on posant $\cos\theta = \cos\frac{\pi}{9} = x$, il faut résoudre l'équation $4x^3 - 3x - \cos\frac{\pi}{3} = 0$ qui irréductible, x est algébrique sur $\mathbb{Q}$ de degré algébrique 3, donc il n'est pas constructible. ■

Remarque 3.1

α est constructible si seulement si $\cos\alpha$ est constructible.

Exemple 3.1

pour l'angle $3\theta = \frac{\pi}{3}$



La trisection n'est donc pas possible en général, mais attention, pour certains angles particuliers c'est possible : par exemple les angles π ou $\frac{\pi}{2}$!

Conclusion

Nous avons présenté dans ce travail des constructions, et les trois problèmes grecs : la duplication du cube, la quadrature du cercle et la trisection des angles, les nombres constructibles à la règle et au compas et nombre constructible et extensions quadratiques qui nous a donné des applications aux problèmes grecs comme l'impossibilité de la duplication du cube, l'impossibilité de la quadrature du cercle et l'impossibilité de la trisection des angles.

Bibliographie

[1] **F.ARNAULT et all**, *Mathématiques L3 Algèbre, Cours complet avec 400 tests et exercices corrigés,* Pearson Éducation France, 2009.

[2] **J.BICHION,** *Algèbre Approfondie,* Département de Mathématiques Université Blaise Pascal, 2013-2014.

[3] **T.CONNOR et J.VERCRUYSSE**, *Algèbre I Cours pour $2^{ème}$ année de Bachelier en sciences mathématiques,* année académique 2012-2013, Version du 12 septembre 2012.

[4] **O.DEBARRE,** *Algèbre 2,* École Normale supérieure, 2012-2013.

[5] **J-R.Durbin**, *Modern Algebra,* An Introduction, Sixth Edition, The University of Texas at Austin.

[6] **J-P.ESCOFIER.**, *Tout l'algèbre de la licence Cours et exercices corrigés,* premier décembre 2005.

[7] **D.FREDON et M.MAUMY-BERTRAND et F.BERTRAND**, *Mathématiques Algèbre et géométrie en 30 fiches,* paris 2009.

[8] **D.HARARI**, *Cours d'algèbre* 1, fait à l'E.N.S. (première année du M.M.F.A.I.) en 2003-2004 et 2004-2005.

[9] **L.LADJELAT**, *Cours Master1, Algèbre Arithmétique,* Université M.Boudiaf de Msila. Année univ 2016-2017.

[10] **P.LISSY,** *Anneaux Principaux. Applications,* Université Paris Dauphine, 6 May 2010.

[11] **J-C.MADO**, *Cours d'Algèbre,* 2002-2003.

[12] **J-P.MARCO, et L.LAZZARINI,** *Mathématiques L1 Algèbre, Cours complet avec 1000 tests et exercices corrigés,* Pearson Education France, 2007.

[13] **J-P.MARCO, et PH.THIEULLEN et J.ARTHUR WEIL,** *Mathématiques L2 Algèbre, Cours complet avec 700 tests et exercices corrigés,* Pearson Education France, 2007.

[14] **J.QUERRE**, *Cours D'algébre,* Université Bretagne Occidentale, Masson paris , New york , Barcelene, Milan, 1976.

[15] **E.VIEILLArRD-BARON et all**, *Anneau et corps,* Janvier 2001.

ملخص:

في هذه المذكرة, قمنا بدراسة مسائل الانشاءات الهندسية باستعمال المسطرة و المدور فقط. هذه الدراسة مبنية على نظرية توسيعات للحقول. قمنا بتطبيق هذه الدراسة على حالات خاصة في مسائل الانشاءات الهندسية المطروحة في اليونان القديمة : تضعيف المكعب, تربيع الدائرة و تثليث الزاوية.

الكلمات المفتاحية

الانشاءات الهندسية - تضعيف المكعب- تربيع الدائرة - تثليث الزاوية- المدور- المسطرة

Résumé:

Dans ce mémoire, nous avons étudié le problème de les constrictions géométriques, en n' utilisant que la règle et le compas. Cette étude est basée sur la théorie des extensions de corps. En particulier, nous avons appliqué cette étude aux problèmes grecs connus : la duplication du cube, la quadrature du cercle et trisection de angles.

Mots clés :

constrictions géométriques - la duplication du cube- la quadrature du cercle- trisection de angles- régle- compas.

Abstract:

In this work, we have studied the problem of geometric construction, using only the rule and the compass. This study is based on the theory of field extension. In particular we applied this study to the in ancient greece problems : the duplication the cube, quadrature of the circle and trisection of angles.

Keywords:

geometric construction - the duplication the cube- quadrature of the circle-trisection of angles- rule- compass.