UNIVERSITE D'ETAT D'HAÏTI

Ecole Normale Supérieure

Mémoire de master 2

Spécialité :

MATHEMATIQUES

Construction à la règle et le compas :

James Kelson LOUIS

Proposé et encadré par : M. Cyrille OSPEL

Soutenue le ... Février 2019 devant le jury composé de :

M. ...	Université ...	Examinateur
M. ...	Université ...	Examinateur
M. ...	Université ...	Examinateur

Après avis des rapporteurs :

M.	Université ...
M.	Université ...

Remerciements.

Je commence par remercier Dieu de m'avoir accompagné durant toute ma vie, tu as mis en moi cette passion pour les mathématiques, Grâce à toi j'ai pu surmonter tous les obstacles pour arriver jusqu'ici.
J'exprime mes profonds remerciements à mon encadreur : Mr Cyrille OSPEL, de m'avoir aiguillé durant les quatre mois à Poitiers. Grâce à lui, j'ai acquis pleins de connaissances, sa façon de faire a développé en moi beaucoup d'aptitudes, merci pour ces conseils : (Si vous voulez faire les maths, il faut être rigoureux partout,... tu verras ce n'est pas compliqué,... juste un petit détail qui manque), merci pour votre gentillesse, votre disponibilité, merci infiniment.

J'adresse maintenant mes remerciements aux différents professeurs qui ont choisi de laisser leur pays, leurs familles pour venir enseigner en Haïti durant les deux années de Master, plus précisément Cyrille OSPEL, Pol VANHAECKE, Souleymane KADRI, Antoine DELCROIX, Christian SILVY, Patrice NAUDIN, Alain MIRANVILLE, Alain PIETRUS, Julien DAMBRINE et Torasso PIERRE.
Les professeurs de l'Ecole Normale Supérieure : Achis CHERY, Yvesner MARCELIN, Aril MILCE.

Mr Pol VANHEACKE, que je remercie de m'avoir guidé durant mon séjour en France, il a pris le soin de m'expliquer en utilisant des notions de géométrie, l'endroit où il devait m'attendre à la gare de Poitiers et m'a accompagné jusqu'à la résidence universitaire, c'était trop gentil.
Un remerciement spécial à ma mère, Jacqueline LOUIS, pour son courage, son amour inconditionnel. Je te dédie tous mes succès.

Ma femme, ma première conseillère Angeline Pierre LOUIS.
Ma famille : Stanley LOUIS, Jimmy LOUIS, Chancy DESAUGUSTE, Ebel ABELLARD, Edeline ABELLARD, Edwige ABELLARD, Paulimus MONFILSTON, Marjorie MONFILSTON, Marc Dalin CAZY, Stéphanie JEAN NOEL,...

Isilda C. J'ai eu toujours l'impression d'être auprès de ma mère, elle m'a toujours conseillé au moment opportun, elle était toujours là pour me supporter.
Marlène Sam, je suis content d'avoir travaillé en votre compagnie. Vos conseils, je ne cesserai de les appliquer durant toute ma vie.

Mes amis Haïtiens à Poitiers, Woodlens CHERY, Thomas KENEL, Wanglaise FATEON, Rubenson MAREUS, je n'oublierai jamais les agréables moments passés ensemble.
Mes voisins (es) de la cité Rabelais : Amal TASHBAEV, Sarah KOLO, Agath KOUA, Hocine OUSSAMA, Yihang LI, Anastasia ROBIN.

Les étudiants de la promotion : Watson SAINVIL, Kenley CHERY, Enel DERUISSEAU, Emmanuel JOSEPH, Solide DAVICKSON, Rony KERVERSAINT.
Mes amies Larissa KOUMTOUDJI, Grace GUIYELIGOU, vous êtes trop gentilles.

Je n'oublie bien évidemment pas la ville de Poitiers, pour sa beauté, son histoire.
ERASMUS PLUS qui m'a donné tous les moyens nécessaires pour effectuer ce stage mémorable en France.
Enfin, je tiens à remercier tous ceux qui ont contribué à la réalisation de ce travail.

TABLE DES MATIÈRES

Sujet

Construction à la règle et au compas.

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 points donnés et qu'il est toujours possible de tracer un cercle de centre donné et passant par un point donné. La géométrie d'Euclide est donc la géométrie des droite et des cercles, tracés à la règle et au compas. L'intuition (conjecturale) d'Euclide était que tout point géométrique pouvait être construit, ou obtenu, à l'aide de ces deux instruments. En particulier, tout nombre devait pouvoir être accessible comme grandeur géométrique constructible. On étudiera cette conjecture notamment au travers des problèmes suivants :

- Problème 1 : La quadrature du cercle
  Peut-on construire à la règle et au compas un carré ayant un même aire qu'un cercle donné ?
- Problème 2 : La duplication du cube
  Peut-on construire à la règle et au compas l'arête d'un cube ayant un volume égal au double du volume d'un cube donné ?
- Problème 3 : La trisection de l'angle
  Peut-on construire à la règle et au compas les demi-droites partageant un angle quelconque en trois angles égaux ?
- Problème 4 : Les polygones réguliers
  Pour chaque n entier supérieur ou égal à 3 peut-on construire à la règle et au compas un polygone régulier à n côtés ?

Pour chaque n entier supérieur ou égal à 3, peut-on construire à la rêgle et au compas un polygone régulier à n côtés ?

On pourra par exemple répondre aux questions suivantes :

i) Qu'appelle t-on des nombres constructibles à la règle et au compas ? Peut-on les caractériser ?

ii) Peut-on obtenir le même type de résultats pour des constructions au compas seulement ? à la règle seulement ?

0.1 Introduction.

En nous léguant ses précieux travaux intellectuels, la Grèce antique a grandement contribué au savoir moderne. Que ce soit dans le domaine de la philosophie ou des mathématiques, ils se sont fait pionniers de bien des disciplines qui furent ensuite développées à travers le temps.

La géométrie a été l'un des principaux centres d'intérêt du monde antique. Considérée à l'époque comme l'ensemble même des sciences mathématiques, elle n'a pas manqué d'éveiller les esprits lorsqu'une interdiction a été informellement prononcée de négliger les mathématiques sous peine de malédictions de la part des dieux, comme le rapporte si bien la mythologie grecque.

Cependant, ces problèmes insolubles tirent leur origine dans les expériences des contemporains de l'époque, animés du souci de mettre les mathématiques au service des progrès de leur temps.
De l'imagination des esprits de l'époque ont vus le jour certains exercices qui, jusqu'à aujourd'hui ne cessent de faire brûler les neurones des passionnés des sciences mathématiques.
Quand il a été formellement décidé de les résoudre à la règle et au compas, instruments devant être capables d'aider à construire tout nombre donné, ces exercices devenaient totalement impossibles.
À noter qu'à cette époque il manquait les nouvelles théories qui ont vu le jour bien des siècles plus tard et qui ont permis de les rendre possibles à l'aide de nouvelles méthodes.

Ce travail va considérer dans sa première partie, les notions de théorie des anneaux nécessaires pour comprendre certaines propositions sur la théorie d'extension de corps, la deuxième partie traite la construction par la règle et le compas, on donnera la formulation géométrique et la formulation algébrique du problème, quelques exemples de constructions réalisées par la règle et le compas à partir d'un ensemble de points constructibles, une caractérisation des constructions possibles à la règle et au compas, puis les trois problèmes qui existent depuis l'Antiquité et dont l'impossibilité de résolution perdure en raison de l'héritage d'Euclide.

Le premier problème : Quadrature du cercle.
Quadrer un cercle reviendrait à tracer un carré ayant la même aire que le cercle en question. Cela peut sembler être assez simple mais quand le principe reviendrait à ce que le carré soit tracé à la règle et au compas le procédé se révèle vain car π se révèle être transcendant et non algébrique.
D'où une impossibilité de résoudre cet exercice à la règle et au compas, l'absence de méthodes appropriées en donne la confirmation.

Le deuxième problème : Duplication du cube.
Dupliquer un cube consisterait à construire $\sqrt[3]{2}$ avec le compas et la règle. Cependant la construction de ce nombre ne peut être réalisé en raison de sa non constructibilité.

Le troisième problème : Trisection de l'angle.
Tracer à partir d'un angle trois autres angles plus petits que l'initial mais égaux est le troisième problème qui sera abordé. Cet exercice se révèle impossible à la règle et au compas, $\cos\frac{\pi}{3}$ n'étant pas constructible en lui-même et l'équation qui y est appropriée n'étant pas réductible au second degré dans $\mathbb{Q}$, ce que Wantzel a démontré postérieurement aux premières tentatives d'explications.

L'apport des nouvelles théories a été fort utile pour mieux appréhender ces trois dilemmes. Les travaux de Wantzel qui sont venus déterminer les nombres constructibles, apportent ainsi les raisons de l'impossibilité des trois problèmes ci-dessus mentionnés.

L'objectif de ce travail sera donc de confirmer par démonstration algébrique l'impossibilité de résoudre ces différents exercices, de caractériser les nombres réels constructibles et de répondre à certaines questions concernant la construction de polygones réguliers.

CHAPITRE 1

THÉORIE DES CORPS.

1.1 Anneau et Sous anneau.

1.1.1 Anneau.

Définition 1. *On appelle anneau tout ensemble non vide A muni de deux lois de composition internes, généralement notées l'une additivement, l'autre multiplicativement, vérifiant les propriétés suivantes :*

i) $(A, +)$ *est un groupe abélien, (on note* 0 *son élément neutre).*

ii) La multiplication est associative, quels que soient $x, y, z \in A$,
$x(yz) = (xy)z$.

iii) La multiplication est distributive sur l'addition à gauche et à droite :
$\forall x, y, z \in A,\ x(y+z) = xy + xz$ *et* $(x+y)z = xz + yz$.

— *Si de plus la multiplication est commutative, c'est-à-dire :*
$\forall x, y \in A,\ xy = yx$, *alors* A *est dit commutatif.*

— *Si la multiplication admet un neutre* 1, *c'est-à-dire :*
$\forall x \in A,\ x \cdot 1 = 1 \cdot x = x$, *alors* A *est dit unitaire.*

Exemples :

i) Muni de l'addition et de la multiplication, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, *et* $\mathbb{C}$ *sont des anneaux commutatifs unitaires.*

ii) $(\mathbb{Z}/n\mathbb{Z}, +, .)$ *est un anneau commutatif unitaire.*

iii) L'ensemble $\mathbb{Z}[i] = \{a + bi\,;\, a, b \in \mathbb{Z}\}$ *muni de l'addition et de la multiplication est un anneau commutatif unitaire.*

iv) $A = \{0\}$ *est un anneau, c'est le seul anneau dans lequel* $1 = 0$.

v) A *étant un anneau commutatif unitaire,* $A[X] = \left\{ \sum_{k\geq 0} a_k X^k, a_k \in A \right\}$, *où tous les* a_k *sont nuls sauf pour un nombre fini, on le munit d'une addition et d'une multiplication :* $\sum_{k\geq 0} a_k X^k + \sum_{k\geq 0} b_k X^k = \sum_{k\geq 0} (a_k + b_k) X^k$ *et* $\sum_{k\geq 0} a_k X^k \times \sum_{k\geq 0} b_k X^k = \sum_{k\geq 0} c_k X^k$ *avec* $c_k = \sum_{n+m=k} a_n b_m$, *c'est un anneau commutatif unitaire, appelé anneau des polynômes en une indéterminée à coefficients dans* A.

Remarque. *Pour tout élément* P *non-nul de* $A[X]$, *il existe un unique entier naturel* n *et un unique* $(n+1)$*-uplet* $(a_0, a_1, \ldots, a_n)$ *d'éléments de* A *tels que :*
$P = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$ *et* $a_n \neq 0$.
L'entier n *est appelé le degré de* P, *noté* $\deg P$, *l'élément non-nul* a_n *est appelé le coefficient dominant de* P, *noté* $cd(P)$, *par convention, on pose* $\deg 0 = -\infty$ *et* $cd0 = 0$.

1.1.2 Sous-Anneau.

Définition 2. *A étant un anneau, B une partie non vide de A, on dit que B est un sous-anneau de A si :*

i) B est un sous groupe du groupe additif.

ii) B est stable pour la multiplication de A, c'est-à-dire :
$\forall x, y \in B$, $xy \in B$.

Définition 3. *Soit A un anneau unitaire, on appelle sous-anneau unitaire de A tout sous-anneau de A qui contient 1_A.*

Exemple :

i) $\mathbb{Z}$ est un sous-anneau unitaire de $\mathbb{R}$.

ii) Tout anneau unitaire A est un sous-anneau unitaire de $A[X]$.

Remarques.

i) Pour démontrer qu'une partie non vide B de A est un sous-anneau de A, il suffit de vérifier que pour x et y dans A on a :
$(x, y) \in B \times B \Rightarrow (x - y) \in B$ et $xy \in B$.

ii) Si l'anneau A est commutatif, alors tout sous-anneau de A est commutatif.

1.1.3 Élément inversible.

Définition 4. *Soit A un anneau commutatif unitaire et soit x un élément de A, on dit que x est un élément inversible dans A, s'il existe $y \in A$ tel que $xy = 1$.*

Remarques.

i) Si $x \in A$ est inversible dans A alors il existe un unique élément $y \in A$ tel que $xy = 1$.

Preuve. *Supossons qu'il existe y, $y' \in A$ tel que $xy = 1$ et $xy' = 1$,*
$xy = 1 \Rightarrow y' \cdot (xy) = y' \cdot 1$,
$\Rightarrow (y'x) \cdot y = y'$,
$\Rightarrow 1 \cdot y = y'$,
$\Rightarrow y = y'$.

ii) L'élément 0 n'est jamais inversible dans A dès lors que $A \neq \{0\}$.

Preuve. *Tout revient à prouver que : $0 \cdot x = 0$, pour tout $x \in A$.*
$0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$,
Puisque tout élément de A est régulier pour l'addition, c'est-à-dire :
$\forall a, b \in A, a + b = a \Rightarrow b = 0$,
donc, $0 \cdot x = 0$.

Proposition 1. *Soit A un anneau commutatif unitaire, l'ensemble des éléments de A inversibles dans A est un groupe pour la multiplication, appelé groupe des unités de A, et noté $U(A)$.*

Démonstration. $U(A) \neq \emptyset$, *car il contient* 1,
soit $a, b \in U(A)$,
$a, b \in U(A) \Rightarrow \exists a', b' \in A, aa' = 1$ *et* $bb' = 1$,
donc, $(ab)(b'a') = a(bb')a' = aa' = 1$, *ce qui prouve que* $ab \in U(A)$
la multiplication dans $U(A)$ est une loi de composition interne, elle est associative car elle l'est dans A, elle admet un neutre dans $U(A)$ et tout élément de $U(A)$ admet un inverse dans $U(A)$, car si $a \in U(A)$ on a : $aa' = a'a = 1$, ce qui prouve que $a' \in U(A)$.

Exemples :

i) $U(\mathbb{Z}) = \{-1, 1\}$.

ii) $U(\mathbb{Z}[i]) = \{-1, 1, i, -i\}$.

Preuve. *Soient $x, y \in \mathbb{Z}[i]$, il existe alors $a, b, c, d \in \mathbb{Z}$ tels que : $x = a + ib$ et $y = c + id$, supposons $xy = 1$, on a alors $N(x)N(y) = 1$, avec $N(x) = \sqrt{a^2 + b^2} \in \mathbb{N}^*$, d'où $N(x) = N(y) = 1$ ce qui équivaut à $a^2 + b^2 = 1$, cette égalité se produit dans $\mathbb{Z}$ si et seulement si $((a = 0$ et $b = \pm 1)$ ou $(b = 0$ et $a = \pm 1))$ autrement dit : si et seulement si $x = \pm 1$ ou $x = \pm i$.*

iii) $U(\mathbb{Z}/n\mathbb{Z}) = \{\bar{x}\,;\, 0 \leq x \leq n-1,\ x \wedge n = 1\}$.

Preuve. *Voir Théorème 1, Page12.*

1.1.4 Diviseur de zéro.

Définition 5. *A étant un anneau commutatif non réduit à $\{0\}$, soit $a \in A$, on dit que a est un diviseur de zéro dans A, si $a \neq 0$ et s'il existe $b \neq 0$ dans A tel que $ab = ba = 0$.*

1.1.5 Intégrité.

Définition 6. *Soit A un anneau commutatif, on dit que A est intègre ou encore un domaine d'intégrité s'il est non-nul et n'admet pas de diviseur de zéro, c'est-à-dire :*
$\forall a,\ b \in A,\ (ab = 0) \Leftrightarrow (a = 0\ ou\ b = 0)$.

1.1.6 Morphisme d'anneaux.

Définition 7. *Soit A et B deux anneaux unitaires, une application f de A dans B est un morphisme d'anneaux unitaires ou un homomorphisme d'anneaux unitaires si :*

i) $f(a+b) = f(a) + f(b)$

ii) $f(ab) = f(a)f(b)$

iii) $f(1_A) = 1_B$ *quels que soient* $a,\ b \in A$.

Propriétés.

i) Si $f : A \longrightarrow B$ est un morphisme d'anneaux unitaires, alors l'image directe par f de tout sous-anneau unitaire de A est un sous-anneau unitaire de B.

Preuve. *Soit I un sous anneau-unitaire de A et f un morphisme d'anneaux unitaires de A vers B. Comme $1_A \in I$ et $f(1_A) = 1_B \in f(I)$ donc $f(I)$ est non vide. Soit a', $b' \in f(I)$, alors il existe $a,\ b \in I$, $f(a) = a'$ et $f(b) = b'$, $a'b' = f(a)f(b) = f(ab) \in f(I)$, $a' - b' = f(a) - f(b) = f(a-b) \in f(I)$, donc $f(I)$ est un sous-anneau unitaire de B.*

ii) Si $f : A \longrightarrow B$ est un morphisme d'anneaux unitaires, alors l'image réciproque par f de tout sous-anneau unitaire de B est un sous-anneau unitaire de A.

Preuve. *Soit J un sous anneau-unitaire de B, $f(1_A) = 1_B$, et $1_B \in J$, $1_A \in f^{-1}(J)$ donc $f^{-1}(J)$ est non vide, soit $a,\ b \in f^{-1}(J)$, il existe $a',\ b' \in J$, $f(a) = a'$ et $f(b) = b'$, $a'b' = f(a)f(b) = f(ab)$ c'est-à-dire $ab \in f^{-1}(J)$, $a'-b' = f(a)-f(b) = f(a-b)$ c'est-à-dire $a - b \in f^{-1}(J)$, donc $f^{-1}(J)$ est un sous-anneau unitaire de A.*

iii) Si $f : A \longrightarrow B$ et $g : B \longrightarrow C$ sont des morphisme d'anneaux unitaires, alors $g \circ f : A \longrightarrow C$ est un morphisme d'anneaux unitaires.

Preuve. $g \circ f(1_A) = g[f(1_A)] = g(1_B) = 1_C$,
$\forall a, b \in A$ *on a* : $g \circ f(a+b) = g[f(a+b)] = g[f(a)+f(b)] = g[f(a)] + g[f(b)] = g \circ f(a) + g \circ f(b)$,
$g \circ f(ab) = g[f(ab)] = g[f(a)f(b)] = g[f(a)]g[f(b)] = g \circ f(a) g \circ f(b)$.

1.1.7 Caractéristique d'un anneau.

Soit A un anneau, le morphisme d'anneau :

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & A \\ & n & \longmapsto & n \times 1_A \end{array}$$

a un noyau de la forme $k\mathbb{Z}$, l'entier positif k est appelé caractéristique de A, noté $Car(A)$.
$Car(A) = 0 \Longleftrightarrow \forall n \in \mathbb{N}^*,\ n \times 1_A \neq 0$,
Sinon $Car(A) = inf\{n \in \mathbb{N}^*\,;\, n \times 1_A = 0\}$.

1.2 Corps.

Définition 8. *On appelle corps, tout anneau commutatif, unitaire et intègre dans lequel tout élément non-nul est inversible.*
Exemples :
Muni de l'addition et de la multiplication, $\mathbb{Q}$, $\mathbb{R}$ *et* $\mathbb{C}$ *sont des corps.*

Théorème 1. *Soient* $n \geq 2$, $n \in \mathbb{N}$, $x \in \mathbb{N}$. $\overline{x}$ *est inversible dans* $\mathbb{Z}/n\mathbb{Z}$ *si et seulement si* $x \wedge n = 1$.

Démonstration. *Supposons* $\overline{x}$ *est inversible dans* $\mathbb{Z}/n\mathbb{Z}$, *il existe* $\overline{y}$ *dans* $\mathbb{Z}/n\mathbb{Z}$ *tel que* $\overline{x} \cdot \overline{y} = 1$, *il existe alors* $h \in \mathbb{Z}$, $xy - 1 = nh$, *on en déduit que* $xy + n(-h) = 1$. *D'après le théorème de Bézout, il en résulte que* $x \wedge n = 1$.
Supposons maintenant $x \wedge n = 1$, *d'après le théorème de Bésout, il existe* $(u, v) \in \mathbb{Z}^2$ *tel que :*
$xu + nv = 1$,
$xu + nv = 1 \Longrightarrow \overline{xu + nv} = \overline{1}$,
$\Longrightarrow \overline{xu} + \overline{nv} = \overline{1}$,
$\Longrightarrow \overline{x} \cdot \overline{u} + \overline{n} \cdot \overline{v} = \overline{1}$,
$\Longrightarrow \overline{x} \cdot \overline{u} = \overline{1}$, *car* $\overline{n} = \overline{0}$,
donc $\overline{x}$ *est inversible dans* $\mathbb{Z}/n\mathbb{Z}$.

Lemme 1. *Tout corps est un anneau intègre.*

Démonstration. *Soit* K *un corps, soient* x, $y \in K$ *tels que* $xy = 0$. *Par définition, si* $x \neq 0$, x *est inversible dans* K, *donc en multipliant les deux membres de l'égalité par* x^{-1} *on a* $x^{-1}xy = 0 \Rightarrow y = 0$, *de même* $y \neq 0 \Rightarrow x = 0$.

Proposition 2. *Pour tout entier $n \geq 2$, ($\mathbb{Z}/n\mathbb{Z}$ est un corps) $\Leftrightarrow$ (n est un nombre premier) $\Leftrightarrow$ ($\mathbb{Z}/n\mathbb{Z}$ est intègre).*

Démonstration. *Montrons d'abord ($\mathbb{Z}/n\mathbb{Z}$ est un corps) $\Leftrightarrow$ (n est un nombre premier). Soit $n \in \mathbb{N}^*$, $n \geq 2$,*
($\forall k \in \mathbb{N}^*$, $1 \leq k \leq n-1$, $k \wedge n = 1$) $\Leftrightarrow$(n est un nombre premier).
si $\mathbb{Z}/n\mathbb{Z}$ est un corps, alors tout entier non-nul de $\mathbb{Z}/n\mathbb{Z}$ est inversible, donc pour tout $k \in \mathbb{N}$ vérifiant : $1 \leq k \leq n-1$, $k \wedge n = 1$ et n est donc premier.
Si n est premier, alors pour tout $k \in \mathbb{N}$ vérifiant $1 \leq k \leq n-1$, $k \wedge n = 1$, alors $\overline{k}$ est inversible.
Montrons que ($\mathbb{Z}/n\mathbb{Z}$ est un corps) $\Leftrightarrow$ ($\mathbb{Z}/n\mathbb{Z}$ est intègre).
D'après le lemme 1, ($\mathbb{Z}/n\mathbb{Z}$ est un corps) $\Longrightarrow$ ($\mathbb{Z}/n\mathbb{Z}$ est intègre).
Réciproquement, supposons $\mathbb{Z}/n\mathbb{Z}$ intègre.
Supposons n n'est pas premier ; il existe donc p, $q \in \mathbb{Z}$, tels que $n = pq$, avec $1 < p < n$ et $1 < q < n$, on a alors $\overline{pq} = \overline{n} = \overline{0}$, bien que $\overline{p} \neq 0$ et $\overline{q} \neq 0$.
Cela prouve $\mathbb{Z}/n\mathbb{Z}$ intègre $\Longrightarrow$ n premier, or n premier $\Longleftrightarrow$ $\mathbb{Z}/n\mathbb{Z}$ corps, du coup $\mathbb{Z}/n\mathbb{Z}$ intègre $\Longrightarrow$ $\mathbb{Z}/n\mathbb{Z}$ corps.

Proposition 3. *Soit A un anneau commutatif unitaire.*

i) Si A est intègre, alors pour tous polynômes P, $Q \in A[X]$ on a :
$\deg(PQ) = \deg P + \deg Q$ *et* $cd(PQ) = cd(P) \cdot cd(Q)$

ii) $A[X]$ est intègre si et seulement si A est intègre.

Démonstration. *i) Supposons P ou Q est nul, dans ce cas nous avons* $\deg(PQ) = \deg P + \deg Q$ *et $cd(PQ) = cd(P) \cdot cd(Q)$, supposons maintenant $P \neq 0$ et $Q \neq 0$, $P = a_nX^n + \ldots + a_1X + a_0$ et $Q = b_nX^n + \ldots + b_1X + b_0$ avec $a_n \neq 0$ et $b_n \neq 0$ on a :*
$PQ = a_nb_mX^{n+m} + (a_nb_{m-1} + a_{n-1}b_m)X^{n+m-1} + \ldots + (a_1b_0 + a_0b_1)X + a_0b_0$.
A étant intègre, $a_nb_m \neq 0$, donc $deg(PQ) = n + m = \deg P + \deg Q$ et $cd(PQ) = a_nb_m = cd(P) \cdot cd(Q)$.

ii) D'après i) le produit de deux éléments non-nuls de $A[X]$ est non-nul, ce qui prouve que $A[X]$ est intègre. Réciproquement si $A[X]$ est intègre, alors A est intègre car A est un sous-anneau de $A[X]$.

Corollaire 1. *Soit A un anneau commutatif unitaire, si A est intègre alors $U(A[X]) = U(A)$.*

Démonstration. *A étant un sous-anneau de $A[X]$, $A \subseteq A[X]$.*
Soit $P(X) \in A[X]$, supposons qu'il existe $Q(X) \in A[X]$, $P(X)Q(X) = 1$, nécessairement ces deux polynômes sont non-nuls, d'après la proposition précédente $\deg P + \deg Q = 0$, *ce qui implique* $\deg P = \deg Q = 0$, *alors il existe $c \in A^*$, $P(X) = c$, il s'en suit $A[X] \subseteq A$, donc $U(A[X]) = U(A)$.*

1.2.1 Corps des fractions d'un anneau intègre.

Pour tout anneau intègre A, on peut construire un corps K tel que $A \subset K$.

Construction

i) On définit une relation d'équivalence dans $A \times A^*$ par :
$(a,b) \sim (c,d) \Longleftrightarrow ad = bc$.
Pout tout couple (a,b) on note $\frac{a}{b}$ la classe d'équivalence appelée fraction,
$\frac{a}{b} = \{(c,d) \in A \times A^* \,;\, (c,d) \sim (a,b)\}$.
L'ensemble des fractions est notée : $K = (A \times A^*)/\sim$: l'ensemble quotient de $A \times A^*$ par la relation $\sim$.

ii) On définit deux lois de composition internes :
$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ et $\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$

Ainsi l'ensemble $K = (A \times A^*)/\sim$ des fractions sur A, muni des lois construites ci-dessus, est un corps commutatif qui contient A comme sous-anneau unitaire.

1.3 Idéal.

Définition 9. *Soit A un anneau commutatif unitaire, I une partie de A, on dit que I est un idéal de A si*

i) I est un sous-groupe du groupe additif.

ii) $\forall x \in I$, $\forall a \in A$, $xa \in I$.

Exemple :

Dans tout anneau A les sous-groupes triviaux $\{0\}$ et A sont des idéaux de A.

Lemme 2. *Soit A un anneau commutatif unitaire.*

i) Si I est un idéal de A qui contient 1_A alors $I = A$.

ii) Si I est un idéal de A qui contient un élément de $U(A)$, alors $I = A$.

Démonstration. *i) Supposons $1_A \in I$, $\forall x \in A$, $x = 1 \cdot x \in I$, ce qui implique $A \subseteq I$, or par définition nous avons $I \subseteq A$, donc $I = A$.*

ii) Supposons qu'il existe $a \in I$, $a \in U(A)$, alors I contient $1 = a \cdot a^{-1}$, d'après i) on a $I = A$.

Proposition 4. *Soit A un anneau commutatif unitaire, pour tout $x \in A$:*

i) l'ensemble $xA = \{xy \,;\, y \in A\}$ est un idéal de A.

ii) $(xA = A) \Leftrightarrow (x \in U(A))$.

Démonstration. *i) $xA \neq \emptyset$ car $x = x \cdot 1 \in xA$, soit $y, z \in xA$, il existe $a, b \in A$, $y = xa$ et $z = xb$, nous avons $y - z = xa - xb = x(a - b) \in xA$, xA est donc un sous-groupe additif. Soit $m \in xA$, $n \in A$, il existe $c \in A$, $m = xc$, donc $mn = (xc)n = x(cn) \in xA$ car $cn \in A$ on conclut que xA est un idéal de A.*

ii) Supposons $xA = A$, alors $1_A \in xA$, il existe donc $y \in A$, $xy = 1$, donc $x \in U(A)$. Réciproquement si $x \in U(A)$, d'après le lemme 2, xA est un idéal de A qui contient un élément de $U(A)$, alors $xA = A$.

Corollaire 2. *Soit A un anneau commutatif unitaire, A est un corps si et seulement s'il a exactement deux idéaux A et $\{0_A\}$.*

Démonstration. *Supposons que A est un corps, soit I un idéal de A distinct de $\{0_A\}$, alors I contient un élément non-nul, notons i cet élément, A étant un corps, i est inversible dans A, d'après le lemme 2, $I = A$.*
Réciproquement, supposons que A contient exactement deux idéaux A et $\{0_A\}$, soit x un élément non-nul de A, l'idéal xA étant alors distinct de $\{0_A\}$, nécessairement $xA = A$ d'où $x \in U(A)$, ainsi tout élément non-nul de A est inversible dans A, on conclut que A est un corps.

1.3.1 Idéal principal.

Définition 10. *Soit A un anneau commutatif unitaire, on dit qu'un idéal I de A est un idéal principal, s'il existe $x \in A$, $I = xA$.*

1.3.2 Idéal premier.

Définition 11. *Soit A un anneau commutatif unitaire, on dit qu'un idéal P de A est un idéal premier, si $P \neq A$ et vérifie : pour tout x, $y \in A$, si $xy \in P$, alors $x \in P$ ou $y \in P$.*

1.3.3 Idéal maximal.

Définition 12. *Soit A un anneau commutatif unitaire, on dit qu'un idéal I de A est un idéal maximal, si $I \neq A$, et si pour tout idéal J différent de I, $I \subset J \Rightarrow J = A$.*

Proposition 5. *Soit $f : A \longrightarrow B$ un morphisme d'anneaux unitaires, on a :*

i) Pour tout idéal J de B l'image réciproque $f^{-1}(J)$ est un idéal de A.

ii) Pour tout idéal I de A l'image directe $f(I)$ est un idéal de $f(A)$.

Démonstration. *i) Soit J un idéal de B, montrons d'abord $f^{-1}(J)$ est un sous-groupe du groupe additif.*
$f^{-1}(J) \neq \emptyset$ car $f(0_A) = 0_B$ et que $0_B \in J$, donc $0_A \in f^{-1}(J)$, soit x, $y \in f^{-1}(J)$, il existe x', $y' \in J$, $f(x) = x'$ et $f(y) = y'$, nous avons $x' - y' = f(x) - f(y) = f(x - y) \in J$ car J est un idéal de B, donc $x - y \in f^{-1}(J)$, ce qui prouve $f^{-1}(J)$ est un sous-groupe du groupe additif.

Soit $z \in f^{-1}(J)$ et $a \in A$, $z \in f^{-1}(J) \Rightarrow \exists z' \in J$, $f(z) = z'$, donc $f(az) = f(a)f(z) = f(a)z' \in J$ car J est un idéal de B, on en déduit que $az \in f^{-1}(J)$, ce qui prouve le résultat voulu.

ii) Soit I un idéal de A, montrons d'abord $f(I)$ est un sous-groupe du groupe additif.
$f(I) \neq \emptyset$, car $f(0_A) = 0_B$ et que $0_A \in I$, donc $0_B \in f(I)$, soit x', $y' \in f(I)$, il existe x, $y \in I$ tel que $f(x) = x'$ et $f(y) = y'$, nous avons $x' - y' = f(x) - f(y) = f(x - y) \in f(I)$ ce qui prouve $f(I)$ est un sous-groupe du groupe additif.
Soit $x' \in f(I)$, il existe $x \in I$, $f(x) = x'$, pour tout élément $a' \in f(A)$, il existe $a \in A$, $f(a) = a'$ on a alors $x'a' = f(x)f(a) = f(xa) \in f(I)$, car $xa \in I$, ce qui prouve $f(I)$ est un idéal de $f(A)$.

Proposition 6. *Soit $f : A \longrightarrow B$ un morphisme d'anneaux unitaires, le noyau de f est un idéal de A différent de A.*

Démonstration. *Il suffit de prendre $J = \{0_B\}$, d'après la proposition 5, $Kerf = f^{-1}(\{0_B\})$ est un idéal de A, de plus $f(1_A) = 1_B \Rightarrow 1_A \notin Kerf$ donc $Kerf \neq A$.*

Proposition 7. *Soient K et L deux corps, alors tout morphisme de corps $f : K \longrightarrow L$ est injectif.*

Démonstration. *D'après la proposition 6, $Kerf$ est un idéal de K, K étant un corps, d'après le corollaire 2, à la page 15, les idéaux de K sont K et $\{0\}$, f est un morphisme de corps, $f(1_K) = 1_L$, donc $Kerf \neq K$, nécessairement $Kerf = \{0\}$, f est donc injectif.*

1.4 Anneaux Quotients.

1.4.1 Quotient d'un anneau par un idéal.

Théorème 2. *Soit A un anneau commutatif unitaire. Pour tout idéal I de A, la relation binaire définie par : $x \sim y \Longleftrightarrow x - y \in I$ est une relation d'équivalence. L'ensemble quotient noté A/I est un anneau commutatif, et la surjection canonique $p : A \longrightarrow A/I$ est un morphisme d'anneaux unitaires.*

Démonstration. ***Réfléxivité :*** *Pour tout $x \in A$, $x \sim x$, car $x - x = 0 \in I$.*
Symétrie : *Soit x, $y \in I$, supposons $x \sim y$,*
$x \sim y \Longrightarrow x - y \in I \Longrightarrow -(x - y) \in I$ car I est un sous groupe du groupe additif, d'où $y - x \in I \Longrightarrow y \sim x$.
Transitivité : *Soit x, y, $z \in A$, supposons $x \sim y$ et $y \sim z$, ($x \sim y$ et $y \sim z$) $\Longrightarrow$ ($x - y \in I$ et $y - z \in I$), en additionnant membre à membre on obtient $x - z \in I \Longrightarrow x \sim z$.*
Par définition on note $\overline{a}$, la classe d'un élément a de A,
$\overline{a} = \{b \in A\ ;\ a - b \in I\} = a + I$, l'addition dans A/I est définie par :
$\overline{a} + \overline{b} = \overline{a + b}$ pour tous a, $b \in A$,
ainsi A/I est un groupe abélien de neutre $\overline{0} = I$ et la surjection canonique $p : A \longrightarrow A/I$ qui à

tout élément de A fait correspondre sa classe $\overline{a}$ est un morphisme de groupes pour l'addition.
La multiplication dans A/I est définie par :
$\overline{a} \cdot \overline{b} = \overline{ab}$ *pour tous* $a, b \in A$,

- *montrons d'abord qu'elle est bien définie,*
  soit $x' \in \overline{x}$ *et* $y' \in \overline{y}$, *alors* $x' - x \in I$ *et* $y' - y \in I$, *on a :*
  $x'y' - xy = (x' - x + x)(y' - y + y) - xy = (x' - x)(y' - y) + (x' - x)y + x(y' - y)$.
  Comme $x' - x \in I$ *et que* I *est un idéal, on a* $(x' - x)(y' - y) \in I$ *et* $(x' - x)y \in I$ *; de même* $x(y' - y) \in I$ *puisque* $y' - y \in I$. *On conclut que* $x'y' - xy \in I$, *comme somme de trois éléments de* I *et donc* $\overline{x'y'} = \overline{xy}$.

- *Montrons qu'elle est associative, commutative, distributive sur l'addition dans* A/I *et admet* $\overline{1}$ *comme neutre.*
  Quelques soient $x, y, z \in A$,*on a :*
  $(\overline{x} \cdot \overline{y})\overline{z} = \overline{(xy)}\overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x} \cdot \overline{(yz)} = \overline{x}(\overline{y} \cdot \overline{z})$.
  $\overline{x}(\overline{y} + \overline{z}) = \overline{x}\overline{(y+z)} = \overline{x(y+z)} = \overline{xy + xz} = \overline{xy} + \overline{xz} = \overline{x} \cdot \overline{y} + \overline{x} \cdot \overline{z}$.
  Pour tout $x \in A$, $\overline{x} \cdot \overline{1} = \overline{x \cdot 1} = \overline{x}$.
- *La surjection canonique* p *vérifie* $p(1) = \overline{1}$ *et pour tous* $x, y \in A$, $p(xy) = \overline{xy} = \overline{x} \cdot \overline{y} = p(x)p(y)$.

Théorème 3. *(**Premier théorème d'isomorphisme**) Soient* A *et* A' *deux anneaux commutatifs unitaires, et* $f : A \longrightarrow A'$ *un morphisme d'anneaux unitaires. Alors* Imf *est isomorphe à l'anneau quotient de* A *par l'idéal* $Kerf$. *On note* $A/Kerf \simeq Imf$.

Démonstration. *Considérons l'application*

$$\begin{array}{rccc} \varphi : & A/Kerf & \longrightarrow & Imf \\ & \overline{x} & \longmapsto & f(x). \end{array}$$

Cette application est bien définie, en effet, si l'on choisit un autre représentant $y \in \overline{x}$, *on a par définition* $x - y \in Kerf$, *donc* $f(x - y) = 0 \Longrightarrow f(x) - f(y) = 0 \Longrightarrow f(x) = f(y) \Longrightarrow \varphi(\overline{x}) = \varphi(\overline{y})$.
φ *est surjective par construction, montrons qu'elle est injective. Soit* $\overline{x} \in Ker\varphi$, *on a alors* $\varphi(\overline{x}) = 0$, *d'où* $f(x) = 0 \Longrightarrow x \in Kerf \Longrightarrow \overline{x} = \overline{0}$, *ceci montre que* $Ker\varphi = \{\overline{0}\}$, *donc* φ *est injective.*
Soit $\overline{x}, \overline{y} \in A/Kerf$,
$\varphi(\overline{1_A}) = f(1_A) = 1_{A'}$.
$\varphi(\overline{x} + \overline{y}) = \varphi(\overline{x + y}) = f(x + y) = f(x) + f(y) = \varphi(\overline{x}) + \varphi(\overline{y})$.
$\varphi(\overline{x} \cdot \overline{y}) = \varphi(\overline{x \cdot y}) = f(x \cdot y) = f(x) \cdot f(y) = \varphi(\overline{x}) \cdot \varphi(\overline{y})$.
On conclut que φ *est un isomorphisme d'anneaux.*

Proposition 8. *Soit* A *un anneau commutatif et* I *un idéal de* A. *Tout idéal de* A/I *est de la forme* J/I, *pour* J *un unique idéal de* A *contenant* I, *avec la notation naturelle* $J/I = p(J)$.

Démonstration. ***Existence :*** *Soit K un idéal de A/I, posons $J = p^{-1}(K) = \{x \in A\,;\ p(x) \in K\}$, J est un idéal de A. Si $x \in I$, on a $p(x) = \overline{0}$, donc $p(x) \in K$, de sorte que $x \in p^{-1}(K)$, c'est-à-dire $x \in J$, ceci montre que $I \subseteq J$. Par définition de J, on a $p(J) \subseteq K$. Réciproquement soit $\overline{x} \in K$, avec $x \in A$, comme $p(x) = \overline{x} \in K$, on a $x \in p^{-1}(K) = J$, et donc $\overline{x} = p(x) \in p(J)$. En résumé, $K = p(J)$, ce que l'on note $K = J/I$.*
Unicité : *Soit J' un idéal de A contenant I tel que $p(J) = p(J')$. Soit $x \in J$, on a $\overline{x} = p(x) \in p(J)$, donc $\overline{x} \in p(J')$, il existe donc $y \in J'$ tel que $\overline{x} = \overline{y}$, c'est-à-dire $x - y \in I$. Mais $I \subseteq J'$, donc $x - y \in J'$ ce qui, comme $y \in J'$, implique que $x \in J'$, Ceci montre que J est inclus dans J'. L'inclusion réciproque s'obtient de même.*

Proposition 9. *Soit A un anneau commutatif et I un idéal de A, nous avons :*
I maximal $\Longleftrightarrow$ A/I corps $\Longrightarrow$ A/I intègre $\Longleftrightarrow$ I premier et I maximal $\Longrightarrow$ I premier.

Démonstration. *Soit M un idéal de A, supposons que M est un idéal maximal de A, $A/M \neq 0$, car $M \neq A$, soit K un idéal de A/M, d'après la proposition 8, il existe un idéal J de A contenant M tel que $K = J/M$, par maximalité de M, $M \subseteq J$ implique $J = M$ ou $J = A$, c'est-à-dire $J/M = \{\overline{0}\}$ ou $J/M = A/M$, ce qui prouve que les seuls idéaux de A/M sont $\{\overline{0}\}$ et A/M, on conclut que A/M est un corps, les mêmes raisonnements prouvent la réciproque, donc :*
I maximal $\Longleftrightarrow$ A/I corps.
Soit P un idéal de A, supposons P est un idéal premier de A, $A/P \neq 0$, car $P \neq A$, considérons $\overline{x}, \overline{y} \in A/P$ tels que $\overline{x} \cdot \overline{y} = \overline{0}$, c'est-à-dire $xy \in P$, comme P est premier, on a $x \in P$ ou $y \in P$ c'est-à-dire $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$, les mêmes calculs prouvent la réciproque, on conclut :
A/I intègre $\Longleftrightarrow$ I premier.
Tout corps est un anneau intègre, donc A/I corps $\Longrightarrow$ A/I intègre.
du coup on montre aussi I maximal $\Longrightarrow$ I premier.

1.5 Anneaux Euclidiens.

Définition 13. *Soit A un anneau commutatif unitaire, x et y deux éléments de A, on dit que x divise y dans A, lorqu'il existe $a \in A$ tel que $y = xa$, on note alors $x \mid y$.*
Dire que x divise y dans A équivaut à dire x est un diviseur de y dans A ou encore que y est un multiple de x dans A.

Définition 14. *On appelle anneau euclidien, un anneau commutatif unitaire qui est intègre et pour lequel il existe une application $\delta : A^* \longrightarrow \mathbb{N}$ vérifiant les deux conditions suivantes :*

i) pour tous $a, b \in A^*$, $(a \mid b) \Longrightarrow (\delta(a) \leq \delta(b))$,

ii) pour tout $a \in A$ et $b \in A^*$, il existe q et $r \in A$ tels que :
$(a = bq + r)$ et $(r = 0$ ou $\delta(r) < \delta(b))$.
Une telle application s'appelle un stathme euclidien.

Proposition 10. *Soit K un corps commutatif, quels que soient des polynômes F et G dans $K[X]$, avec $G \neq 0$, il existe $Q \in K[X]$ et $R \in K[X]$ uniques tels que $F = GQ + R$ et $\deg R < \deg G$.*

Démonstration. ***Existence :*** *Notons $n = \deg F \in \mathbb{N}$ et $m = \deg G \in \mathbb{N}$. Si $n < m$ alors on peut écrire $F = 0 \times G + F$, avec $\deg F < \deg G$, donc $Q = 0$ et $R = F$ conviennent.*
Si $n \geq m \geq 0$, notons $F = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ et $G = b_m X^n + b_{m-1}X^{n-1} + \ldots + b_1 X + b_0$ avec les a_i et les b_j dans K tels que $a_n \neq 0$ et $b_m \neq 0$.
Si $n = m = 0$, alors $F = a_0 \neq 0$ et $G = b_0 \neq 0$, donc $F = (a_0 b_0^{-1})G$, ce qui prouve le résultat voulu avec $Q = a_0 b_0^{-1}$ et $R = 0$.
Par récurrence sur n, supposons la propriété vraie pour G et tout polynôme F_1 de degré n_1 tel que $n > n_1 \geq m \geq 0$. Or on peut écrire $F = a_n {b_m}^{-1} X^{n-m} G + F_1$, avec $\deg F_1 \leq n - 1 < n$. Par hypothèse de récurrence, il existe Q_1, $R_1 \in K[X]$ tels que $F_1 = Q_1 G + R_1$ et $\deg R_1 < \deg G$. On déduit que $F = (a_n b_m^{-1} X^{n-m} + Q_1)G + R_1$, ce qui prouve le résultat voulu avec $Q = a_n b_m^{-1} X^{n-m} + Q_1$ et $R = R_1$.
Unicité : *Supposons qu'il existe deux couples (Q, R), (Q', R') dans $K[X]$ tels que $F = GQ + R = GQ' + R'$ avec $\deg R < \deg G$ et $\deg R' < \deg G$. On a alors $G(Q - Q') = R - R'$. Comme K est un corps on a l'égalité $\deg Q + \deg(Q - Q') = \deg(R' - R)$ or $\deg R < \deg G$ et $\deg R' < \deg G$ impliquent que $\deg(R' - R) < \deg G$. Donc $\deg G + \deg(Q - Q') < \deg G$, ce qui n'est possible que si $\deg(Q - Q') = -\infty$, c'est-à-dire $Q = Q'$, on a alors $R = R'$.*

1.5.1 Éléments associés.

Définition 15. *Soit A un anneau commutatif unitaire, x et y deux éléments de A, on dit que x et y sont associés dans A, si $x = y = 0$ ou $((x, y) \in A^* \times A^*$, $x \mid y$ et $y \mid x)$, on note alors $x \sim y$.*

1.5.2 Élément irréductible.

Définition 16. *Soit A un anneau commutatif unitaire, un élément $x \in A$ est dit irréductible dans A si :*

i) $x \notin U(A)$,

ii) $x = ab$ *dans* $A \Rightarrow a \in U(A)$ *ou* $b \in U(A)$.

1.5.3 Élément premier.

Définition 17. *Soit A un anneau commutatif unitaire, un élément $x \in A$ est dit premier dans A si :*

i) $x \neq 0, x \notin U(A)$,

ii) $x \mid ab$ *dans* $A \Rightarrow x \mid a$ *ou* $x \mid b$ *dans* A.

1.5.4 Éléments premiers entre eux.

Définition 18. *Soit A un anneau commutatif unitaire, Soient x et y deux éléments de A, on dit que x et y sont premiers entre eux, lorsque les seuls éléments de A qui divisent à la fois x et y sont les éléments de $U(A)$.*

1.5.5 Notion de p.g.c.d.

Définition 19. *Etant donné n éléments non-nuls $a_1, a_2, \ldots, a_n$ dans A on appelle p.g.c.d dans A des a_i, $(1 \leq i \leq n)$, tout élément $d \in A^*$ tel que :*

i) $\forall i, (1 \leq i \leq n)$, $d \mid a_i$;

ii) Pour $c \in A^*$, $(\forall i (1 \leq i \leq n)$, $c \mid a_i) \Longrightarrow c \mid d$.

N.B. Le p.g.c.d de deux nombres a et b est noté $a \wedge b$.

1.5.6 Notion de p.p.c.m.

Définition 20. *On appelle p.p.c.m de n éléments non-nuls $a_1, a_2, \ldots, a_n$ dans A, $n \geq 2$ tout $m \in A^*$ tel que :*

i) $\forall i, (1 \leq i \leq n)$, $a_i \mid m$;

ii) Pour $l \in A^*$, $(\forall i (1 \leq i \leq n)$, $a_i \mid l) \Longrightarrow m \mid l$.

Proposition 11. *Soit A un anneau commutatif unitaire, pour tous x, $y \in A$, on a :*

$$(x \mid y) \Leftrightarrow (y \in xA) \Leftrightarrow (yA \subseteq xA).$$

Démonstration. *Supposons $x \mid y$ dans A.*
$(x \mid y) \Leftrightarrow \exists a \in A,\ y = xa \Leftrightarrow y \in xA$
Supposons $y \in xA$, il existe $b \in a$, $y = xb$. Soit $z \in yA$, il existe $a \in A$, tel que $z = ya$, alors $z = xba = x(ba) \in xA$ car $ab \in A$, on conclut $(yA \subseteq xA)$.
Réciproquement supposons $(yA \subseteq xA)$, en particulier $y = y \cdot 1_A \in yA$, donc il existe $a \in A$, $y = xa$, on conclut $y \in xA$.

Corollaire 3. *Soit A un anneau commutatif unitaire.*

i) Pour tout $u \in A$, $(u \in U(A)) \Leftrightarrow (uA = A) \Leftrightarrow (\forall y \in A,\ u \mid y)$.

ii) Pour tous x, $u \in A$, $(u \in U(A)$ et $x \mid u) \Rightarrow (x \in U(A))$.

Démonstration. *i) D'après la proposition 4 à la page 14, $(u \in U(A)) \Leftrightarrow (uA = A)$.*
Supposons $u \in U(A)$, pour tout $y \in A$, $y = 1 \cdot y = uu^{-1}y$, donc $u \mid y$. Réciproquement supposons pour tout $y \in A$, $u \mid y$, en particulier pour $y = 1$, $\exists a \in A$, $1 = ua$, on conclut $u \in U(A)$.

ii) Soit $u \in U(A)$ et $x \in A$, tel que $x \mid u$, alors $u = bx$, $b \in A^*$, d'où $1 = uu^{-1} = bxu^{-1} \Rightarrow x \in U(A)$.

Proposition 12. *Soit A un anneau commutatif unitaire intègre, x et y deux éléments de A on a :*

$$(x \sim y) \Leftrightarrow (xA = yA) \Leftrightarrow (\exists u \in U(A), x = uy)$$

Démonstration. *Suppososns $x \sim y$, par définition nous avons $x \mid y$ et $y \mid x$, d'après la proposition 11, $yA \subseteq xA$ et $xA \subseteq yA$ donc $xA = yA$.*
Supposons $x \sim y$, ça implique $x \mid y$ et $y \mid x$, donc il existe u, $v \in A$, $x = uy$ et $y = vx$, si $x = 0$ alors $y = 0$ et $x = uy$ pour tout $u \in U(A)$ sinon $x = uvx$, donc $x(1 - uv) = 0$, par hypothèse A est intègre et $x \neq 0$, $1 - uv = 0 \Rightarrow uv = 1$, d'où u, $v \in U(A)$.
Réciproquement, si $x = uy$, $u \in U(A)$, on a $y \mid x$ et, puisque $y = u^{-1}x$ avec $u^{-1}x \in A$ on a aussi $x \mid y$, on conclut $x \sim y$.

Proposition 13. *Soit A un anneau commutatif unitaire et intègre, pour tout $x \in A$ on a :*

i) (x est irréductible dans A) $\Leftrightarrow$ (xA est maximal parmi les idéaux principaux distincts de A).

ii) (x est premier dans A) $\Leftrightarrow$ (xA idéal premier non-nul de A).

Démonstration. *i) Supposons x irréductible, l'idéal principal $M = xA$ est distinct de A, car $x \notin U(A)$, soit $J = aA$ un idéal principal de A distinct de A, c'est-à-dire $a \notin U(A)$, et supposons $M \subseteq J$, alors en particulier $x \in J$, donc il existe $b \in A$, tel que $x = ab$, puisque $a \notin U(A)$, l'irréductibilité de x implique que $b \in U(A)$. Donc $x \sim a$, d'où $M = J$, ceci prouve que M est maximal parmi les idéaux principaux distincts de A.*
Réciproquement soit $x \in A$, tel que xA soit maximal parmi les idéaux principaux distincts de A, soient a, $b \in A$, tels que $x = ab$, alors $x \in aA$ et donc $xA \subseteq aA$. Si $a \in U(A)$, alors $aA = A$, sinon $aA \neq A$ et la maximalité de xA implique alors que $xA = aA$, donc $x \sim a$, d'où l'existence de $u \in U(A)$ tel que $x = ua$, mais $x = ua = ba$ implique par intégrité de A que $b = u$ et donc $b \in U(A)$.

ii) Soit x un élément premier dans A ; $x \neq 0 \Longrightarrow xA \neq \{0\}$.
Supposons qu'il existe a, $b \in A$ tel que $ab \in xA$, donc $x \mid ab$ dans A, alors x premier implique $x \mid a$ ou $x \mid b$ c'est-à-dire $a \in xA$ ou $b \in xA$ ce qui prouve xA est premier, non-nul dans A.
Réciproquement, supposons xA est un idéal premier non-nul de A, alors pour a et b dans A^* :
$ab \in xA \Longrightarrow a \in xA$ ou $b \in xA$, autrement dit $x \mid ab \Longrightarrow x \mid a$ ou $x \mid b$, donc x est un élément premier dans A.

Proposition 14. *Soit A un anneau commutatif unitaire et intègre, tout élément premier dans A est irréductible dans A.*

Démonstration. *Soit p un élément de A, supposons p premier et $p = ab$, $a, b \in A^*$;*
$p = ab \Longrightarrow p \mid ab \Longrightarrow p \mid a$ ou $p \mid b$.
Si $p \nmid a$, $p \mid b$; donc il existe $q \in A^*$, tel que $b = pq$.
Or $p = ab$, ça implique $p = apq \Longrightarrow p(1 - aq) = 0$, A est intègre et de plus $p \neq 0$, donc $a \in U(A)$, de même on montre $p \mid a \Longrightarrow b \in U(A)$, on conclut que p est irréductible.

Définition 21. *Un anneau est principal, s'il est intègre et tous ses idéaux sont principaux.*

Proposition 15. *Dans un anneau principal, tout élément irréductible est premier.*

Démonstration. *Soit A un anneau principal, et $x \in A$ un élément irréductible de A, d'après la proposition 13 i), xA est maximal parmi les idéaux principaux distincts de A, par contre tout idéal de A est principal, xA est tout simplement un idéal maximal de A, donc xA est premier (Proposition 9, Page18), ce qui implique x premier (Proposition 13 ii)).*

Théorème 4 (**Théorème de Bézout**). *A étant un anneau principal, pour a et b non-nuls dans A on a :*

$$a \wedge b = 1 \Longleftrightarrow \exists (u, v) \in A \times A, au + bv = 1$$

.

Démonstration. *Si $1 = ua + bv$, alors tout diviseur commun de a et b divise 1, donc est inversible (cette implication est vraie dans tout anneau commutatif). En sens inverse, si a et b sont premiers entre eux, alors l'idéal engendré par a et b s'écrit dA avec $d \in A$ car A est principal. En particulier d divise a et b, donc est inversible donc $dA = A$.*

Théorème 5 (**Lemme de Gauss**). *A étant un anneau commutatif unitaire et intègre dans lequel les p.g.c.d existent, $\forall a$, b, $c \in A^*$ on a :*
$(a \mid bc$ et $a \wedge b = 1) \Rightarrow a \mid c$

Démonstration. *a et b étant premiers entre eux, il existe d'après le théorème de Bésout, $u, v \in A$ tels que $au + bv = 1$, en multipliant les deux membres par c on a : $auc + bvc = c$, par hypothèse nous avons $a \mid bc$, donc $bvc \in aA$ de plus $acu \in aA$, on conclut que $c = auc + bvc \in aA$, donc $a \mid c$.*

Proposition 16. *Dans un anneau principal, tout idéal premier non-nul est maximal.*

Démonstration. *Soit A un anneau principal, et I un idéal premier non-nul de A, il existe donc $a \in A$, $I = aA$, d'après la proposition 13 i), a est premier, donc irréductible (Proposition 14, page 14) d'après la Proposisition 13 ii)), aA est maximal parmi les idéaux principaux distincts de A, par hypothèse A est principal, c'est-à-dire tout idéal de A est principal,ce qui implique aA est maximal dans A.*

Proposition 17. *Tout anneau euclidien est principal.*

Démonstration. *Soit I un idéal de A dont on veut montrer qu'il est principal. Comme l'idéal nul est principal, on peut supposer que $I \neq \{0\}$. Soit alors $a \in I$ un élément non-nul tel que $\delta(a)$ soit minimal. Bien entendu, $aA \subseteq I$ et il s'agit de montrer que $I = aA$. Soit x un élément quelconque de I et choisissons q et r tels que $x = aq + r$. Si $r \neq 0$, on a $\delta(r) < \delta(a)$, ce qui est absurde puisque $r = x - aq$ appartient à I. Donc $r = 0$ et $x = aq \in aA$: Par suite, $I = aA$ et tout idéal de A est principal.*
δ : le stathme euclidien de A.

1.6 Anneaux Factoriels.

Définition 22. *On dit qu'un anneau A est factoriel si :*

i) A est un domaine d'intégrité.

ii) A vérifie les deux conditions suivantes :

a) $(F1)$ tout élément $a \in A$, $a \neq 0, a \notin U(A)$, s'écrit $a = r_1 r_2 \dots r_n$, avec $r_1, r_2, \dots, r_n$ irréductibles dans A ;

b) $(F2)$ si $r_1 r_2 \dots r_n = s_1 s_2 \dots s_m$, avec $r_1, r_2, \dots, r_n, s_1, s_2, \dots s_m$ irréductibles dans A, alors $m = n$ et il existe une permutation $\sigma \in S_n$ telle que $s_i \sim r_{\sigma(i)}$ pour tout $i, (1 \leq i \leq n)$.

On a une définition équivalente :

Définition 23. *On dit qu'un anneau A est factoriel si :*

i) A est un domaine d'intégrité.

ii) A vérifie les deux conditions suivantes :

a) $(F1)$ tout élément $a \in A$, $a \neq 0, a \notin U(A)$, s'écrit $a = r_1 r_2 \dots r_n$, avec $r_1, r_2, \dots, r_n$ irréductibles dans A ;

b) $(F2')$ tout élément irréductible dans A est premier dans A.

Proposition 18. *Tout anneau principal est factoriel.*

Démonstration. *Soit A un anneau principal, les idéaux d'un anneau principal vérifient la condition de chaîne ascendante, à savoir : "Toute suite croissante d'idéaux est stationnaire". En effet, si :*

$$I_1 \subset I_2 \subset \dots \subset I_k \subset \dots$$

est une suite croissante d'idéaux, la réunion $\bigcup_{k\in\mathbb{N}} I_k$ *est encore un idéal. Comme* A *est un anneau principal,* $I = aA$, $a \in A$ *et il existe* $k \in \mathbb{N}$ *tel que* $a \in I_k$, *on en déduit* $aA \subset I_k$, *comme l'inclusion inverse est évidente, on trouve* $I_k = I$ *et* $(I_n)_n$ *sera stationnaire à partir du rang* k. *À partir de là on débute un raisonnement par l'absurde en supposant l'existence d'un élément non nul* a *de* A *sans décomposition en produit de facteurs irréductibles. Alors* a *n'est pas irréductible donc il existe* a_1, $b_1 \notin A^*$ *tels que* $a = a_1b_1$. *L'un au moins des deux facteurs, disons* a_1 *ne se décompose pas en produit de facteurs irréductibles. Il existe alors* a_2, $b_2 \notin A^*$ *tels que* $a_1 = a_2b_2$. *Par exemple* a_2 *ne se décompose pas en produit de facteurs irréductibles, et, l'on continue de la même manière. On obtient une suite infinie strictement croissante d'idéaux :*

$$aA \subsetneq a_1A \subsetneq a_2A \subsetneq \ldots \subsetneq a_nA \subsetneq \ldots$$

en contradiction avec la condition de chaîne ascendante. On notera que la suite d'idéaux est bien strictement croissante puisque $a_iA = a_{i+1}A$ *entraîne l'existence de* $u \in A^*$ *etl que* $a_{i+1} = ua_i$ *et puisqu'en remplaçant dans* $a_i = a_{i+1}b_{i+1}$ *on trouve* $1 = ub_{i+1}$, *en contradiction avec l'hypothèse* $b_{i+1} \notin A^*$.

Proposition 19. *Soit* A *un anneau commutatif unitaire, les trois conditions suivantes sont équivalentes.*

i) A *est un corps.*

ii) $A[X]$ *est euclidien.*

iii) $A[X]$ *est principal.*

Démonstration. *D'après la proposition 10, i)* $\Longrightarrow$ *ii), d'après la proposition 17, ii)* $\Longrightarrow$ *iii), montrons que iii)* $\Longrightarrow$ *i).*
Si $A[X]$ *est principal, il est en particulier intègre, par suite l'anneau* A *est intègre (Proposition 3, Page 13). Considérons l'application*

$$\begin{array}{rccc} \gamma : & A[X] & \longrightarrow & A \\ & \sum_{i=0}^{n} a_iX^i & \longmapsto & a_0. \end{array}$$

Vérifions que γ *est un morphisme surjectif d'anneaux unitaires.*
L'application γ *est surjective par construction.*
Nous avons $\gamma(1) = 1$.
Soit $P(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ *et* $Q(X) = b_mX^m + b_{m-1}X^{m-1} + \ldots + b_1X + b_0$ *dans* $A[X]$,

$$\gamma(P+Q) = \gamma\left(\sum_{k=0}^{max(n,m)} (a_k + b_k)X^k\right) = a_0 + b_0 = \gamma(P) + \gamma(Q),$$

$$\gamma(PQ) = \gamma\left(\sum_{k=0}^{n+m}(\sum_{j=0}^{k} a_jb_{k-j})X^k\right) = a_0b_0 = \gamma(P)\gamma(Q).$$

γ est donc un morphisme d'anneaux unitaires.
D'après le premier théorème d'isomorphisme $A \simeq \dfrac{A[X]}{Ker\gamma}$.
A intègre implique $\dfrac{A[X]}{Ker\gamma}$ *intègre, par suite* $Ker\gamma$ *est un idéal premier non-nul de* $A[X]$*, mais par hypothèse* $A[X]$ *est principal, donc* $Ker\gamma$ *est un idéal maximal de* $A[X]$*, on en conclut que* $\dfrac{A[X]}{Ker\gamma}$ *est un corps, donc* A *est un corps.*

1.6.1 Recherche de racines rationnelles d'un polynôme à coefficients entiers.

Proposition 20. *Soit* $P(X) = \sum_{k=0}^{n} a_k X^k$ *dans* $\mathbb{Z}[X]$*, si* $\dfrac{p}{q}$ *est une racine de* $P(X)$*,* $(p,q) \in \mathbb{Z} \times \mathbb{Z}^*$ *et* $p \wedge q = 1$*, alors* $p \mid a_0$ *et* $q \mid a_n$

Démonstration. *supposons* $\dfrac{p}{q}$ *est une racine de* $P(X)$*,* $(p,q) \in \mathbb{Z} \times \mathbb{Z}^*$ *et* $p \wedge q = 1$*,*
cela implique

$$P\left(\frac{p}{q}\right) = 0$$

$a_0 + a_1\left(\dfrac{p}{q}\right) + a_2\left(\dfrac{p}{q}\right)^2 + \cdots + a_n\left(\dfrac{p}{q}\right)^n = 0,$
ce qui équivaut à :
$\dfrac{q^n a_0 + a_1 p q^{n-1} + a_2 p^2 q^{n-2} + \cdots + a_n p^n}{q^n} = 0,$
multiplions les deux membres de cette expression par q^n*,*
$q^n a_0 + a_1 p q^{n-1} + a_2 p^2 q^{n-2} + \cdots + a_n p^n = 0,$
d'une part :
$q^n a_0 = -p\,(a_1 q^{n-1} + a_2 p q^{n-2} + \cdots + a_n p^{n-1}),$
donc $p \mid q^n a_0$*,*
or par hypothèse on a $p \wedge q = 1$*,*
alors $p \mid a_0$*,*
d'autre part :
$a_n p^n = -\,(q^n a_0 + a_1 p q^{n-1} + \cdots + a_{n-1} p^{n-1} q),$
$a_n p^n = -q\,(q^{n-1} a_0 + a_1 p q^{n-2} + \cdots + a_{n-1} p^{n-1}),$
donc $q \mid a_n p^n$*,*
or par hypothèse on a $p \wedge q = 1$*,*
alors $q \mid a_n$*.*

Proposition 21. *Soit* $\mathbb{K}$ *un corps,* $a \in \mathbb{K}$*,*
$f(X) \in \mathbb{K}[X]$ *irréductible sur* $\mathbb{K} \iff f(X+a)$ *est irréductible sur* $\mathbb{K}$*.*

Démonstration. *Supposons* $f(X)$ *irréductible sur* $\mathbb{K}$ *et* $f(X+a)$ *réductible sur* $\mathbb{K}$*.*
$f(X+a)$ *réductible sur* $\mathbb{K} \iff (f(X+a) \in U(\mathbb{K}[X]))$ *ou* $(Si\ f(X+a) = P(X) \cdot Q(X)\ ;\ P(X),$ $Q(X) \in \mathbb{K}[X]$ *alors* $P(X) \notin U(\mathbb{K}[X])$ *et* $Q(X) \notin U(\mathbb{K}[X])$*,*

i) 1^{er} *cas*

Si $f(X+a) \in U(\mathbb{K}[X])$,

$f(X+a) \in U(\mathbb{K}[X]) \iff \exists\ c \in \mathbb{K}^*,\ f(X+a) = c$,

$\iff \exists\ c \in \mathbb{K}^*,\ f(X) = c$,

$\iff f(X) \in U(\mathbb{K}[X])$,

$\iff f(X)$ *est réductible,*

Contradiction.

ii) 2^{me} *cas*

Si $f(X+a) = P(X) \cdot Q(X)$ *;* $P(X)$, $Q(X) \in \mathbb{K}[X]$,

en remplaçant X *par* $X - a$ *on a :*

$f(X) = P(X-a) \cdot Q(X-a)$.

D'après le 1^{er} *cas,*

$P(X-a)$, $Q(X-a) \notin U(\mathbb{K}[X])$,

donc $f(X)$ *est réductible.*

Contradiction.

Ce qui prouve $f(X) \in \mathbb{K}[X]$ *irréductible sur* $\mathbb{K} \Longrightarrow f(X+a)$ *est irréductible sur* $\mathbb{K}$.

La réciproque découle du même raisonnement.

Remarque. *On utilisera le résultat suivant sans le démontrer.*

1.6.2 Critère d'Eisenstein.

Proposition 22. *Soit* A *un anneau factoriel et* K *son corps des fractions, soit*

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$

un polynôme de degré $n \geq 1$ *à coefficients dans* A*, supposons qu'il existe un élément irréductible* $p \in A$ *tel que :*

- p *ne divise pas* a_n,
- p *divise les* a_k *sauf pour* $k = n$,
- p^2 *ne divise pas* a_0,

alors P *est irréductible dans* $K[X]$.

Remarque. *On admet le résultat suivant.*

1.6.3 Transcendance de π.

Proposition 23. π *est transcendant sur* $\mathbb{Q}$.

1.7 Extension de Corps.

Définition 24. *Etant donné un corps K on appelle extension de K tout-corps L contenant un sous-corps isomorphe à K, dans ce cas on note $L : K$, ce qui traduit L est une extension de K.*

Remarque. *si L est une extension de K, L est un espace vectoriel sur K, où l'addition vectorielle est l'addition dans L et la multiplication par un scalaire $K \times L \longrightarrow L$ est la restriction à $K \times L$ de la multiplication dans L.*

1.7.1 Extension de corps obtenu par adjonction.

Définition 25. *soit $L : K$ une extensioin de corps, pour toute partie non vide T de L, on appelle extension de K obtenu par adjonction de T à K, noté $K(T)$, le sous-corps de L engendré par $K \cup T$, c'est le plus petit sous-corps de L contenant K et T.*

Cas particuliers

i) Pour $T = \{\alpha\}$, $\alpha \in L$, $K(T)$ s'écrit $K(\alpha)$ et est dit : extension simple de K obtenu par adjonction de α à K.
Remarque : Si $\alpha \in K$, alors $K(\alpha) = K$.

ii) Plus généralement pour $T = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}, n \in \mathbb{N}^*$ et les α_i pour $(1 \leq i \leq n)$ sont des éléments de L, $K(T)$ s'écrit $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ et appelé extension de K obtenu par l'adjonction de $\alpha_1, \alpha_2, \ldots, \alpha_n$ à K.

Proposition 24. *Soit L une extension d'un corps K ; alors, pour tout $\alpha \in L$ on a :*

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)}; \frac{f(X)}{g(X)} \in K(X), g(\alpha) \neq 0 \right\}$$

où $K(X)$ désigne le corps des fractions rationnelles à coefficients dans K.
Plus généralement, $K(X_1, X_2, \ldots, X_n)$ étant le corps des fractions rationnelles à n indéterminées sur K pour $\alpha_1, \alpha_2, \ldots, \alpha_n$, dans L, $n \geq 1$, dans $\mathbb{N}$ on a :

$$K(\alpha_1, \alpha_2, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \alpha_2, \ldots, \alpha_n)}{g(\alpha_1, \alpha_2, \ldots, \alpha_n)} \right\}$$

où $\dfrac{f(X_1, X_2, \ldots, X_n)}{g(X_1, X_2, \ldots, X_n)} \in K(X_1, X_2, \ldots, X_n)$ *et* $g(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$.

Démonstration. *Soit* $A = \left\{ \dfrac{f(\alpha)}{g(\alpha)}; \dfrac{f(X)}{g(X)} \in K(X), g(\alpha) \neq 0 \right\}$.
Montrons que A est un sous-corps de L contenant K et α.
Soit $x_1 = \dfrac{f_1(\alpha)}{g_1(\alpha)} \in A$, $x_2 = \dfrac{f_2(\alpha)}{g_2(\alpha)} \in A$

$$x_1 - x_2 = \frac{f_1(\alpha)g_2(\alpha) - f_2(\alpha)g_1(\alpha)}{g_1(\alpha)g_2(\alpha)} \in A$$

$$x_1 x_2 = \frac{f_1(\alpha)f_2(\alpha)}{g_1(\alpha)g_2(\alpha)} \in A$$

Soit $\beta \in K$, *en choisissant* $f(X) = \beta$ *et* $g(X) = 1$ *on a* $\dfrac{f(\alpha)}{g(\alpha)} = \dfrac{\beta}{1} = \beta \in A$

en posant $f(X) = X$ *et* $g(X) = 1$ *on a* $\dfrac{f(\alpha)}{g(\alpha)} = \dfrac{\alpha}{1} = \alpha \in A.$

A *est donc un sous-corps de* L *contenant* K *et* α, *de plus* $K(\alpha)$ *est le plus petit sous-corps contenant* K *et* α

$K(\alpha) \subset A$ *(*).*

Soit $\beta \in A$, $\beta = \dfrac{\sum_{k=0}^{n} a_k \alpha^k}{\sum_{j=0}^{m} b_j \alpha^j} \in K(\alpha)$ *car* $\sum_{k=0}^{n} a_k \alpha^k \in K(\alpha)$ *et* $\sum_{j=0}^{m} b_j \alpha^j \in K(\alpha).$

donc $A \subset K(\alpha)$ *(**)*

(*) et (**) $\Rightarrow K(\alpha) = A.$

De la même manière on montre $K(\alpha_1, \alpha_2, \ldots, \alpha_n) = \left\{ \dfrac{f(\alpha_1, \alpha_2, \ldots, \alpha_n)}{g(\alpha_1, \alpha_2, \ldots, \alpha_n)} \right\}.$

1.7.2 Degré d'une extension de corps.

Définition 26. *Si* $L : K$ *est une extension de corps, alors* L *est un espace vectoriel sur* K, *on appelle degré de* $L : K$, *noté* $[L : K]$, *la dimension de* L *comme* K*-espace vectoriel.*

Proposition 25. *Quelques soient les extensions de corps* $L : K$ *et* $M : L$ *on a :*

$$[M : K] = [M : L][L : K]$$

.

Démonstration. *Soient* $(x_1, \ldots, x_m)$ *une base de* M *comme* L*-espace vectoriel,* $(y_1, \ldots, y_n)$ *une base de* L *comme* K*-espace vectoriel, alors* $(x_i y_j)_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ *est une base de* M *comme* K*-espace vectoriel.*

Soit $x \in M$, *alors il existe* $\lambda_1, \ldots, \lambda_m \in L$ *tels que* $x = \sum_{i=1}^{m} \lambda_i x_i.$

Pour chaque λ_i *il existe* $\mu_{ij} \in K$ *tels que* $\lambda_i = \sum_{j=1}^{n} \mu_{ij} y_j$, *alors* $x = \sum_{i=1}^{m} \sum_{j=1}^{n} \mu_{ij} y_j x_i.$

La famille $(x_i y_j)_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ *est génératrice.*

Supposons $\sum_{i=1}^{m} \sum_{j=1}^{n} \mu_{ij} y_j x_i = 0$

nous avons $\sum_{j=1}^{n} \mu_{ij} y_j = 0$ *car* $(x_1, \ldots, x_m)$ *est une base,*

$\forall i, j, \mu_{ij} = 0$ *car* $(y_1, \ldots, y_n)$ *est une base, donc La famille* $(x_i y_j)_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ *est libre, c'est donc une base de* M *comme* K*-espace vectoriel.*

donc $[M : L] = dim_K L$

$[M : L] = mn$

$[M : L] = dim_L M \cdot dim_K L$

$[M : L] = [M : K][K : L].$

1.7.3 Élément algébrique.

Définition 27. *Soit $L : K$ une extension de corps, un élément $a \in L$ est dit algébrique sur K, s'il existe un polynôme $f(X) \in K[X] \setminus K$, $f(a) = 0$.*
Dans ce cas on dit que $K(a)$ est une extension simple, algébrique sur K.

1.7.4 Élément transcendant.

Définition 28. *Soit $L : K$ une extension de corps, un élément $a \in L$ est dit transcendant sur K, s'il n'est pas algébrique sur K, c'est-à-dire, si $\forall f(X) \in K[X] \setminus K, f(a) \neq 0$.*
Dans ce cas on dit que $K(a)$ est une extension simple, transcendante de K.

Proposition 26. *Soit $L : K$ une extension de corps, à tout $\alpha \in L$, on associe l'application :*

$$\begin{array}{rccc} \theta_\alpha : & K[X] & \longrightarrow & L \\ & f(X) & \longmapsto & f(\alpha) \end{array}$$

θ_α est un morphisme d'anneaux unitaires, on pose $K[\alpha] = Im\theta_\alpha$, $K[\alpha]$ est donc un domaine d'intégrité.
θ_α non injectif $\Longleftrightarrow$ α est algébrique sur K.
θ_α injectif $\Longleftrightarrow$ α est transcendant sur K.

Démonstration. *Vérifions d'abord que θ_α est un morphisme d'anneaux unitaires.*
Pour $f(X) = 1_{K[X]}$, $\theta_\alpha(f(X)) = f(\alpha) = 1_L$.
Soient $f(X)$, $g(X) \in K[X]$, $\theta_\alpha(f(X) \cdot g(X)) = f(\alpha) \cdot g(\alpha) = \theta_\alpha(f(X)) \cdot \theta_\alpha(g(X))$,
et $\theta_\alpha(f(X) + g(X)) = f(\alpha) + g(\alpha) = \theta_\alpha(f(X)) + \theta_\alpha(g(X))$.
On conclut que θ_α est un morphisme d'anneaux unitaires.
$K[\alpha] = Im\theta_\alpha$ est un sous-anneau unitaire du corps L, c'est donc un domaine d'intégrité.
θ_α non injectif $\Longleftrightarrow$ $Ker\theta_\alpha \neq \{0\}$,
θ_α non injectif $\Longleftrightarrow$ $\exists f(X) \in K[X] \setminus \{0\}, f(\alpha) = 0$,
θ_α non injectif $\Longleftrightarrow$ α est algébrique sur K.
En prenant la contraposée de cette équivalence on obtient :
θ_α injectif $\Longleftrightarrow$ α est transcendant sur K.

1.7.5 Extension simple transcendante.

Théorème 6. *Toute extension simple transcendante $K(\alpha) : K$ est K-isomorphe à l'extension $K(X) : K$, où $K(X)$ est le corps des fractions rationnelles à une indéterminée sur K.*
Plus précisément il existe un isomorphisme μ de $K(X)$ sur $K(\alpha)$ tel que :

$$\mu_{/K} = Id_K \text{ et } \mu(X) = \alpha.$$

Démonstration. *Par hypothèse, quelque soit $f(X) \in K[X] \setminus K$, $f(\alpha) \neq 0$, or d'après la proposition 24,*

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)}; \frac{f(X)}{g(X)} \in K(X), g(\alpha) \neq 0 \right\}$$

Par suite l'hypothèse implique

$$K(\alpha) = \{q(\alpha); q(X) \in K(X)\}.$$

Vérifions que l'application

$$\begin{array}{rccc} \mu: & K(X) & \longrightarrow & K(\alpha) \\ & q(X) & \longmapsto & q(\alpha) \end{array}$$

définit un isomorphisme du corps $K(X)$ sur le corps $K(\alpha)$ vérifiant $\mu_{/K} = Id_K$ et $\mu(X) = \alpha$.
Pour $q(X) = 1_{K(X)}$, $\mu(q(X)) = q(\alpha) = 1_{K(\alpha)}$
Soit $q(X), r(X) \in K(X)$, $\mu(q(X) \cdot r(X)) = q(\alpha) \cdot r(\alpha) = \mu(q(\alpha)) \cdot \mu(r(\alpha)$.
L'application μ est bien un morphisme de corps.
D'après la proposition 7 à la page 16, l'application μ est injective, de plus elle est surjective par construction, on conclut que μ définit un isomorphisme du corps $K(X)$ sur le corps $K(\alpha)$ vérifiant $\mu_{/K} = Id_K$ et $\mu(X) = \alpha$.

Corollaire 4. *Deux extensions simples, transcendantes d'un corps K sont K-isomorphes.*

Démonstration. *C'est une conséquence du théorème 6.*

Proposition 27. *Si $K(\alpha)$ est une extension simple, transcendante d'un corps K, alors $K(\alpha)$ est le corps des fractions rationnelles du domaine d'intégrité $K[\alpha]$.*

Démonstration. *L'élément α étant transcendant sur K on a :*

$$K[\alpha] = \{f(\alpha); f(X) \in K[X]\} \simeq K[X]$$
$$K(\alpha) = \{q(\alpha); q(X) \in K(X)\} \simeq K(X)$$

Or $K(X)$ est le corps des fractions rationnelles du domaine d'intégrité $K[X]$, on conclut que $K(\alpha)$ est le corps des fractions rationnelles du domaine d'intégrité $K[\alpha]$.

1.7.6 Caractérisation des extensions simples algébriques.

Théorème 7. *Etant donné une extension de corps $L : K$, si α est un élément de L algébrique sur K, alors :*

i) Il existe un unique polynôme $p(X)$ unitaire et irréductible dans $K[X]$ tel que
$(f(X) \in K[X] \setminus \{0\}$ et $f(\alpha) = 0) \Longleftrightarrow (p(X) \mid f(X)$ dans $K[X])$.

ii) L'extension $K(\alpha)$ vérifie l'égalité

$$K(\alpha) = \{f(\alpha); f(X) \in K[X]\}.$$

iii) $[K(\alpha) : K] = \deg p$.

Démonstration. *i) L'élément α étant fixé, considérons le morphisme θ_α défini dans la proposition 26, on a :*

$$Ker\theta_\alpha = \{f(X) \in K[X]; f(\alpha) = 0\}$$
$$K[\alpha] = Im\theta_\alpha = \{f(\alpha); f(X) \in K[X]\}$$

$Ker\theta_\alpha$ est un idéal propre de $K[X]$, $K[X]$ est euclidien, donc principal (Proposition 19), il existe un unique polynôme unitaire $p(X)$ non constant dans $K[X]$ qui engendre $Ker\theta_\alpha$, on peut écrire $Ker\theta_\alpha = (p(X))$, d'après le premier théorème d'isomorphisme(Théorème 3, Page 17), nous avons :

$$Im\theta_\alpha \simeq \frac{K[X]}{(p(X))}$$

$K[\alpha]$ est un sous-anneau d'un corps, donc intègre, par suite $p(X)$ est un élément premier, donc irréductible dans $K[X]$ (Proposition 14), alors :
$(f(X) \in Ker\theta_\alpha = (p(X))$ et $f(X) \neq 0) \Longleftrightarrow p(X) \mid f(X)$ dans $K[X]$.

ii) $K[X]$ étant principal, l'idéal premier non-nul $Ker\theta_\alpha = (p(X))$ est maximal (Proposition 16), donc $\frac{K[X]}{(p(X))} \simeq K[\alpha]$ est un corps (Proposition 9, page 18), c'est un sous-corps de L contenant K et α.
Or par définition $K(\alpha)$ est le plus petit sous-corps de L contenant K et α, d'où $K(\alpha) \subseteq K[\alpha]$.
d'autre part pour tout $f(X)$ dans $K[X]$ on a $f(\alpha)$ dans $K(\alpha)$, on déduit l'égalité $K[\alpha] = K(\alpha)$.

iii) Montrons d'abord que la famille $\{\alpha^k,\ 0 \leq k \leq d-1\}$ est libre sur K.
Posons $d = \deg p$ dans $K[X] \setminus K$, $p(X)$ est le polynôme unitaire de plus petit degré tel que $p(\alpha) = 0$, il en résulte que dans le K-espace vectoriel L, les éléments $\alpha^k, 0 \leq k \leq d-1$ sont linéairements indépendants, car aucun polynôme de degré stictement inférieur à d, n'est annulé par α, nous avons :
$\left(\sum_{k=0}^{d-1} \lambda_k \alpha^k = 0, \lambda_k \in K, \forall k, (0 \leq k \leq d-1)\right) \Longrightarrow \lambda_k = 0, \forall k, (0 \leq k \leq d-1)$. *Montrons que la famille $\{\alpha^k,\ 0 \leq k \leq d-1\}$ engendre $K[a]$.*
Si s est un polynôme de $K[X]$ et si $s = pq + r$, avec $\deg r < \deg p$, par division euclidienne, on a $s(\alpha) = r(\alpha)$, comme $\deg r \leq d-1$, $s(\alpha) = \sum_{k=0}^{d-1} \lambda_k \alpha^k$ où $\lambda_k \in K$, $\forall k$, $(0 \leq k \leq d-1)$.
La famille $\{\alpha^k,\ 0 \leq k \leq d-1\}$ étant à la fois libre et génératrice donc elle forme une base dans le K-espace vectoriel $K(\alpha) = K[\alpha]$, donc $\deg p = [K(\alpha) : K] = d$.

1.7.7 Polynôme irréductible de α sur K.

Définition 29. *Etant donné une extension de corps $L : K$ et α un élément de L algébrique sur K, l'unique polynôme irréductible et unitaire de $K[X]$, associé à α, est appelé le polynôme irréductible de α sur K, ou polynôme minimal de α sur K, on écrira*

$$p(X) = Irr_K(\alpha, X) \text{ ou } p(X) = Irr_K(\alpha).$$

Théorème 8. *K étant un corps, soit $P(X)$ un polynôme irréductible et unitaire de $K[X]$; il existe alors une extension $K(\alpha) : K$ telle que α est algébrique sur K et $Irr_K(\alpha) = p(X)$.*

Démonstration. *$K[X]$ étant un anneau factoriel, le polynôme irréductible $p(X)$ est un élément premier, non-nul de $K[X]$, mais $K[X]$ étant aussi un anneau principal, l'idéal premier non-nul ($p(X)$ est maximal dans $K[X]$, par suite $F = \dfrac{K[X]}{(p(X))}$ est un corps.*
Soit u l'injection canonique de K dans $K[X]$ et π la surjection canonique de $K[X]$ sur F.
$\pi \circ u$ est un morphisme d'anneaux unitaires de K dans F, on en déduit que F est une extension de K telle que tout $a \in K$ peut être identifié à son image par $\pi \circ u$ dans F.
Posons : $\alpha = \pi(X)$,
alors $F = \{\pi(f(X)) \, ; \, f(X) \in K[X]\} = \{f(\alpha) \, ; \, f(X) \in K[X]\}$,
de plus $\pi(p(X)) = 0 \Longrightarrow p(\alpha) = 0$, donc l'élément α de F est algébrique sur K, ainsi $F = K(\alpha)$ est une extension simple, algébrique de K et le polynôme $p(X)$ étant par hypothèse unitaire et irréductible dans $K[X]$,

$$p(\alpha) = 0 \Longrightarrow p(X) = Irr_K(\alpha).$$

Corollaire 5. *Toute extension simple, algébrique d'un corps K est isomorphe à un corps de la forme : $\dfrac{K[X]}{(p(X))}$, où $p(X)$ est un polynôme unitaire et irréductible de $K[X]$.*

Démonstration. *C'est une conséquence du théorème précédent.*

1.7.8 Corps de rupture.

Définition 30. *K étant un corps, soit $P(X)$ un polynôme irréductible et unitaire de $K[X]$, on appellera corps de rupture de $p(X)$ sur K, toute extension simple $K(\alpha)$ de K telle que $Irr_K(\alpha) = p(X)$.*

1.7.9 Extensions algébriques, extensions transcendantes.

Définition 31. *Une extension L d'un corps K est dite algébrique sur K, si tout élément de L est algébrique sur K.*

Exemple :

$\mathbb{C}$ est une extension algébrique de $\mathbb{R}$, car un élément $a+bi$, $a, b \in \mathbb{R}$ de $\mathbb{C}$, est racine de l'équation à coefficients réels $X^2 - 2aX + a^2 + b^2 = 0$.

Théorème 9. *Toute extension L de degré fini n sur un corps K est algébrique sur K et tout élément de L est algébrique de degré $\leq n$.*

Démonstration. *Soit α dans L, la famille $\{\alpha^k,\ 0 \leq k \leq n\}$ ayant plus de n éléments n'est pas libre sur K, ce qui signifie qu'il existe une famille $\{\beta_k,\ 0 \leq k \leq n\}$ d'éléments de K non tous nuls tels que $\sum_{k=0}^{n} \beta_k X^k = 0$; le polynôme $f(X) = \sum_{k=0}^{n} \beta_k X^k$ de $K[X]$ s'annule en α, comme $f \neq 0$, α est algébrique de degré $\leq n$ sur K.*

Corollaire 6. *Toute extension simple, algébrique d'un corps K est une extension algébrique de K*

Démonstration. *Toute extension simple, algébrique est une extension de degré fini, d'après le théorème précédent, elle est une extension algébrique.*

Remarque. *Soit $L : K$ une extension de corps, $B = \{x_i\}_{1 \leq i \leq n}$, $n \in \mathbb{N}$ une base de L sur K, alors L peut toujours être considéré comme obtenu par l'adjonction de B à K.*
En effet, $B \subseteq L$, $K \subseteq L$, donc l'extension $K(B)$ est un sous-corps de L.
D'autre part, tout $x \in L$ s'écrit de façon unique : $x = \sum_{i=0}^{n} \alpha_i x^i$, par suite, tout élément de L est dans $K(B)$, on en conclut que $L = K(B)$.
En particulier, si $[L : K] = n \in \mathbb{N}^*$ et si $\{x_i\}_{1 \leq i \leq n}$ est une base de L sur K, alors $L = K(x_1, x_2, \ldots, x_n)$.

Théorème 10. *Une extension $L : K$ est algébrique et de degré fini si et seulement si L est obtenu par l'adjonction à K d'un nombre fini d'éléments algébriques sur K.*

Démonstration. *Supposons $L : K$ est algébrique et $[L : K] = n$, $n \in \mathbb{N}^*$, soit $\{x_1, x_2, \ldots, x_n\}$ une base de L sur K, d'après la remarque précédente $L = K(x_1, x_2, \ldots, x_n)$ et l'extension $L : K$ étant algébrique, chaque x_i, $1 \leq i \leq n$ est algébrique sur K.*
Réciproquement, considérons $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ où $n \in \mathbb{N}^*$ et chaque α_i, $1 \leq i \leq n$ est algébrique sur K.
Faisons une démonstration par récurrence sur n,
α_1 algébrique sur $K \Longrightarrow [K(\alpha_1) : K] < \infty$.
α_2 algébrique sur $K \Longrightarrow \alpha_2$ algébrique sur $K(\alpha_1) \Longrightarrow [K(\alpha_1, \alpha_2) : K(\alpha_1)] < \infty$.
Supposons que pour tout i, $1 \leq i \leq n-1$, $[K(\alpha_1, \alpha_2, \ldots, \alpha_i) : K(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})] < \infty$,
alors α_n est algébrique sur $K \Longrightarrow \alpha_n$ est algébrique sur $K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$, d'où $[K(\alpha_1, \alpha_2, \ldots, \alpha_n) : K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})] < \infty$,
on conclut $[L : K] = [K(\alpha_1, \alpha_2, \ldots, \alpha_n) : K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})] \times \ldots \times [K(\alpha_1) : K] < \infty$

Théorème 11. *Soit $L : K$ et $M : L$ des extensions de corps alors :*
$(L : K$ et $M : L$ algébriques $) \Longrightarrow M : K$ algébrique .

Démonstration. *Tout revient à montrer que tout élément λ de M est algébrique sur K.*
$M : L$ algébrique $\Longrightarrow \lambda$ est algébrique sur L, il existe donc un nombre fini d'éléments non tous

nuls dans L, $b_0, b_1, \ldots, b_m$ *tels que :*

$$\sum_{i=0}^{m} b_i \lambda^i = 0.$$

Or pour tout i, $(1 \leq i \leq m)$, b_i *est algébrique sur* K, *Soit* G *l'extension obtenue par l'adjonction à* K, *des éléments* $b_0, b_1, \ldots, b_m$, $G = K(b_0, b_1, \ldots, b_m)$ *est une extension algébrique et de degré fini, on en déduit que* λ *est algébrique sur* G, *donc* $[G(\lambda) : G] < \infty$ *et*

$$[G(\lambda) : G][G : K] = [G(\lambda) : K] < \infty$$

Donc λ *est algébrique sur* K.

Définition 32. *Une extension* L *d'un corps* K *est dite transcendante sur* K, *si elle n'est pas algébrique sur* K *; autrement dit s'il existe au moins un élément* $\alpha \in L$ *transcendant sur* K.
Exemple :
$\mathbb{R} : \mathbb{Q}$ *et* $\mathbb{C} : \mathbb{Q}$ *sont des extensions transcendantes, car ils contiennent des éléments transcendants sur* $\mathbb{Q}$.

1.7.10 Quelques résultats de transcendance.

i) Le nombre de Liouville $l = \sum_{k=0}^{\infty} 10^{-k!}$ (construit en 1844) est transcendant.

ii) Hermite a démontré la transcendance de e en 1873.

iii) Lindemann a démontré la transcendance de π en 1882.

Proposition 28. *Soit* $L : K$ *une extension de corps.*

i) $(\alpha \in L$ *et* α *transcendant sur* $K) \Longleftrightarrow [K(\alpha) : K]$ *infini.*

ii) L *transcendant sur* $K \Longrightarrow [L : K]$ *infini.*

Démonstration. *i) D'après les théorèmes 7 et 9,*
$[K(\alpha) : K] < \infty \Longleftrightarrow \alpha$ *algébrique.*
La contraposée de cette relation donne le premier résultat.

ii) Si L *est transcendant sur* K, *alors il existe un élément* $\alpha \in L$ *transcendant sur* K, *Or* $[L : K] = [L : K(\alpha)][K(\alpha) : K]$.
D'après le i), $[K(\alpha) : K]$ *infini, ça implique* $[L : K]$ *infini.*

CHAPITRE 2

CONSTRUCTION PAR LA RÈGLE ET LE COMPAS.

2.1 Formulation Géométrique du problème.

Dans le plan $\mathbb{R}^2$ rapporté au repère orthonormé $(O, \vec{i}, \vec{j})$, on désigne par $\mathcal{P}_0$ un ensemble renfermant au moins deux points.

Opérations élémentaires.

On se limite à deux types de réalisation possible :

i) Tracer la droite passant par deux points de $\mathcal{P}_0$.

ii) Tracer le cercle de centre : un point de $\mathcal{P}_0$ et de rayon : la distance de deux points de $\mathcal{P}_0$.

Point constructible en une étape à partir d'un ensemble de points déjà constructibles.

Définition 33. *Un point est dit constructible en une étape à partir d'un ensemble de points déjà constructibles, s'il est obtenu par les opérations élémentaires, c'est-à-dire s'il est soit :*

i) l'intersection de deux droites.

ii) l'intersection de deux cercles.

iii) l'intersection d'une droite et d'un cercle.

Point constructible à la règle et au compas à partir de $\mathcal{P}_0$.

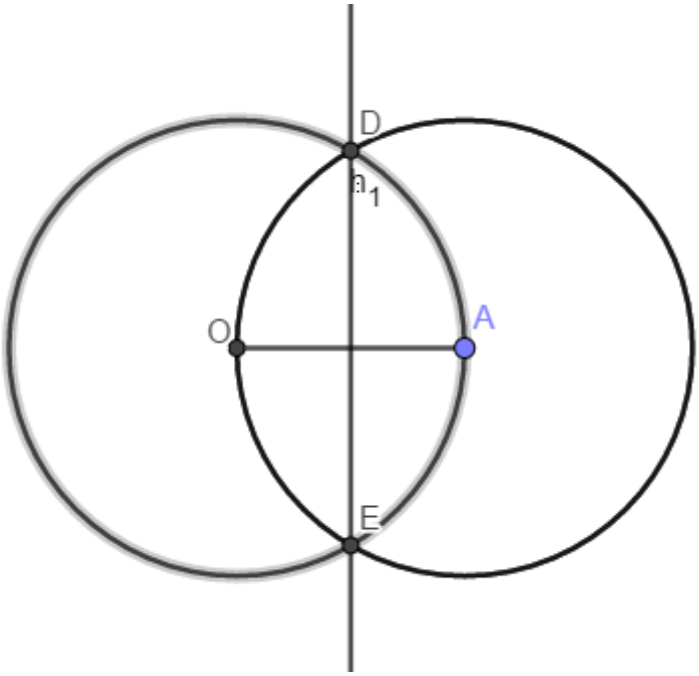
Un point M du plan $\mathbb{R}^2$ sera dit constructible à partir de $\mathcal{P}_0$, s'il existe une suite finie de points $M_1, M_2, \ldots, M_n = M$ tels que, pour tout i, $(1 \leq i \leq n)$) le point M_i est construit en une étape à partir de l'ensemble des points de $\mathcal{P}_0 \cup \{M_1, M_2, \ldots, M_{i-1}\}$.

Nombre constructible.

Définition 34. *Un nombre est dit constructible, si une unité de mesure étant choisie, on peut tracer à la règle et au compas un segment de longueur ce nombre.*

2.1.1 Quelques constructions réalisées à la règle et au compas.

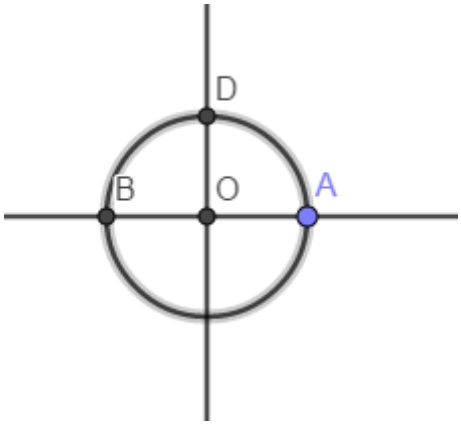
Construction de la médiatrice d'un segment.



Tracez les cercles de centre O et A et de rayon r avec r : distance entre deux points constructibles O et A, la droite qui passe par les points d'intersection des deux cercles est la médiatrice du segment $[OA]$.

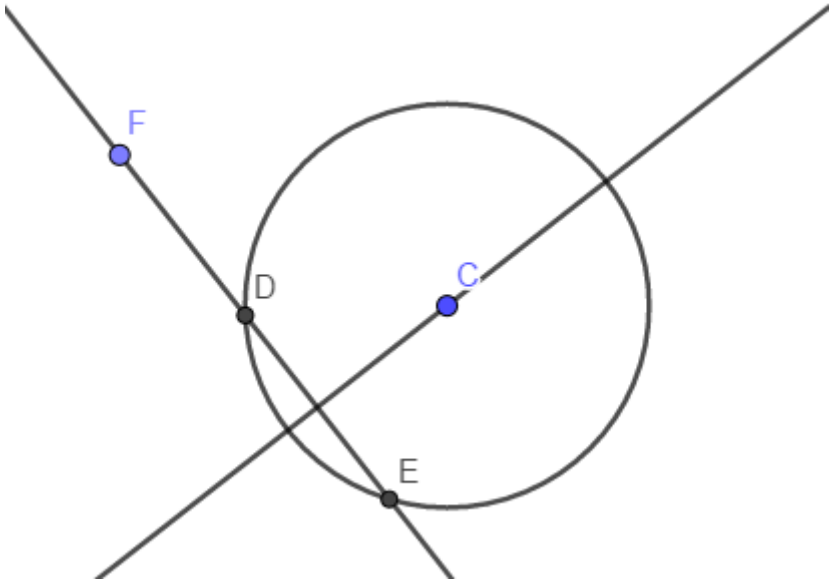
Construction d'un repère orthonormé.

Soit $\mathcal{P}_0 = \{O, A\}$, $O(0,0)$, $A(1,0)$



Tracez la droite (OA), tracez le cercle C de centre O passant par A, ce cercle recoupe la droite (OA) en B, le point de rencontre entre la médiatrice du segment $[BA]$ et le cercle C donne le point D tel que $\|\overrightarrow{OA}\| = \|\overrightarrow{OD}\|$ d'où la construction du repère $(O, \vec{i}, \vec{j})$ avec $\vec{i} = \overrightarrow{OA}$ et $\vec{j} = \overrightarrow{OD}$.

Construction de la perpendiculaire à une droite passant par un point extérieur.



Soit C le point donné, la droite étant constructible, elle contient au moins deux points constructibles F et D.

- Si le cercle de centre C et de rayon $r = d(C, D)$ rencontre la droite en un seul point, c'est-à-dire $(D = E)$, alors la droite (CD) est la perpendiculaire à la droite issue de C.
- Si le cercle rencontre la droite en deux points distincts D et E, alors la médiatrice du segment $[DE]$ est la perpendiculaire à la droite passant par C.

2.2 Formulation Algébrique du Problème.

Soit $\mathcal{P}_0 = \{P_1, P_2\}$, désignons par $\mathbb{K}_0$ le sous-corps de $\mathbb{R}$ engendré par les coordonnées des points de $\mathcal{P}_0$, nécéssairement $Car(\mathbb{K}_0) = 0$, donc $\mathbb{K}_0$ contient $\mathbb{Q}$, par suite, $\mathbb{K}_0$ est l'extension de $\mathbb{Q}$ obtenu par les adjonctions des coordonnées des points de $\mathcal{P}_0$.
Etant donné une construction successive de points $M_1, M_2, \ldots, M_n$, pour tout $i, 1 \leq i \leq n$, on note (x_i, y_i) les coordonnées de M_i et on définit le corps $\mathbb{K}_i$, tel que :

$$\mathbb{K}_i = \mathbb{K}_{i-1}(x_i, y_i)$$

On obtient la chaine d'extension de corps :

$$\mathbb{Q} \subseteq \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \ldots \subseteq \mathbb{K}_n \subset \mathbb{R}$$

Lemme 3. *Avec les notations précédentes, pour tout $i, 1 \leq i \leq n$, les nombres réels x_i et y_i sont racines de polynômes de $\mathbb{K}_{i-1}[X]$ de degré 1 ou 2.*

Démonstration. *D'après la définition 33, trois cas sont à considérer,*

1) Supposons M_i est l'intersection de deux droites.

Étant donné $A(m, m')$ et $B(n, n')$ deux points distincts dans le plan affine $\mathbb{R}^2$ dont les coordonnées m, m', n, n' sont dans $\mathbb{K}_{i-1}$, l'équation de la droite (AB) est donnée par :

$$(x - m)(n' - m') = (y - m')(n - m)$$

Alors les coordonnées de M_i sont solutions d'un système de la forme :

$$\begin{cases} ax + by + c = 0 \\ a'x + b'y + c' = 0 \end{cases}$$

Avec a, b, c, a', b', $c' \in \mathbb{K}_{i-1}$.
Utilisons la méthode de Cramer
Posons $\Delta = \begin{vmatrix} a & b \\ a' & b' \end{vmatrix}$, $\Delta x = \begin{vmatrix} c & b \\ c' & b' \end{vmatrix}$, $\Delta y = \begin{vmatrix} a & c \\ a' & c' \end{vmatrix}$
puisque M_i est le point de rencontre des deux droites, alors $\Delta \neq 0$.
$x = \dfrac{\Delta x}{\Delta}$ *et* $y = \dfrac{\Delta y}{\Delta}$, *c'est-à-dire :*
$x = \dfrac{cb' - c'b}{ab' - ba'}$ *et* $y = \dfrac{ac' - ca'}{ab' - ba'}$
ainsi $x \in \mathbb{K}_{i-1}$ et $y \in \mathbb{K}_{i-1}$, ce qui implique $\mathbb{K}_i = \mathbb{K}_{i-1}$ et $[K_i : K_{i-1}] = 1$.

2) Supposons M_i est l'intersection d'une droite et d'un cercle.

Étant donné un point $\Omega(c, c')$ dont les coordonnés sont dans $\mathbb{K}_{i-1}$, si r est la distance deux points de $\mathcal{P}_0 \cup \{M_1, M_2, \ldots, M_{i-1}\}$, $r^2 \in \mathbb{K}_{i-1}$, l'équation du cercle C de centre Ω et de rayon r est donnée par :

$$(x - c)^2 + (y - c')^2 = r^2$$

Alors les coordonnées de M_i sont solutions d'un système de la forme :

$$\begin{cases} ax + by + c = 0 \\ (x - d)^2 + (y - d')^2 - r^2 = 0 \end{cases}$$

Avec a, b, c, d, d', $r^2 \in \mathbb{K}_{i-1}$,
$ax + by + c = 0$ étant l'équation d'une droite, $a \neq 0$ ou $b \neq 0$.

1) Supposons $a \neq 0$ et $b = 0$,
nous avons $x = -\dfrac{c}{a} \in \mathbb{K}_{i-1}$, et $\mathbb{K}_{i-1}(x) = \mathbb{K}_{i-1}$.
En remplaçant x dans la deuxième équation, on trouve :
$(-\dfrac{c}{a} - d)^2 + (y - d')^2 - r^2 = 0$, y est donc une racine d'un polynôme du second degré à

coefficients dans $\mathbb{K}_{i-1}$, $[\mathbb{K}_{i-1}(y) : \mathbb{K}_{i-1}] = 1$ *ou* 2. *De même on montre que si* $b \neq 0$ *et* $a = 0$, $\mathbb{K}_{i-1}(y) = \mathbb{K}_{i-1}$ *et* $[\mathbb{K}_{i-1}(x) : \mathbb{K}_{i-1}] = 1$ *ou* 2.

2) *Supposons* $a \neq 0$ *et* $b \neq 0$,
nous avons $x = \dfrac{-by - c}{a}$, *en remplaçant* x *dans la deuxième équation, on obtient :*
$(\dfrac{-by - c}{a} - d)^2 + (y - d')^2 - r^2 = 0$, y *est donc une racine d'un polynôme du second degré à coefficients dans* $\mathbb{K}_{i-1}$, $[\mathbb{K}_{i-1}(y) : \mathbb{K}_{i-1}] = 1$ *ou* 2, *puisque* $x = \dfrac{-by - c}{a}$, $x \in \mathbb{K}_{i-1}(y)$ *et* $[\mathbb{K}_{i-1}(x) : \mathbb{K}_{i-1}] = 1$ *ou* 2.

Dans les deux cas, on conclut : $[\mathbb{K}_i : \mathbb{K}_{i-1}] = 1$ *ou* 2.

3) *Supposons* M_i *est l'intersection de deux cercles.*
Alors les coordonnées de M_i *sont solutions d'un système de la forme :*

$$\begin{cases} (x-c)^2 + (y-c')^2 - r^2 = 0 \\ (x-d)^2 + (y-d')^2 - r'^2 = 0 \end{cases}$$

Avec c, c', r^2, d, d', $r'^2 \in \mathbb{K}_{i-1}$

$$\begin{cases} x^2 - 2cx + c^2 + y^2 - 2c'y + c'^2 - r^2 = 0 \\ x^2 - 2dx + d^2 + y^2 - 2d'y + d'^2 - r'^2 = 0 \end{cases}$$

En soustrayant membre à membre, on obtient :
$-2cx + 2dx + c^2 - d^2 - 2c'y + 2d'y + c'^2 - d'^2 - r^2 + r'^2 = 0$
$(-2c + 2d)x + (-2c' + 2d')y + c^2 - d^2 + c'^2 - d'^2 - r^2 + r'^2 = 0$
En posant $\theta = -2c + 2d$, $\gamma = -2c' + 2d'$ *et* $\phi = c^2 - d^2 + c'^2 - d'^2 - r^2 + r'^2$,
le système devient :

$$\begin{cases} (x-c)^2 + (y-c')^2 - r^2 = 0 \\ \theta x + \gamma y + \phi = 0 \end{cases}$$

Avec c, c', r^2, θ, γ, $\phi \in \mathbb{K}_{i-1}$ *ce qui nous ramène au cas précédent, donc* $\mathbb{K}_i = \mathbb{K}_{i-1}(x_i, y_i) = \mathbb{K}_{i-1}(x_i) = \mathbb{K}_{i-1}(y_i)$ *et* $[\mathbb{K}_i : \mathbb{K}_{i-1}] = 1$ *ou* 2.

Théorème 12. *Si un point* $M(x, y)$ *est constructible à partir d'un ensemble* $\mathcal{P}_0$ *de points de l'espace affine euclidien* $\mathbb{R}^2$ *et si* $\mathbb{K}_0$ *est le sous-corps de* $\mathbb{R}$ *engendré par les coordonnées des points de* $\mathcal{P}_0$ *alors* $[\mathbb{K}_0(x) : \mathbb{K}_0]$ *et* $[\mathbb{K}_0(y) : \mathbb{K}_0]$ *sont des puissances de deux.*

Démonstration. *Supposons que* M *résulte des constructions successives des points* $M_1, M_2, \ldots, M_n = M$ *pour tout* $i, 1 \leq i \leq n$, *d'après le lemme 3 nous avons* $\mathbb{K}_i = \mathbb{K}_{i-1}(x_i,\ y_i) = \mathbb{K}_{i-1}(x_i) = \mathbb{K}_{i-1}(y_i)$ *et* $[\mathbb{K}_i : \mathbb{K}_{i-1}] = 1$ *ou* 2.
On en déduit que $[\mathbb{K}_n : \mathbb{K}_0] = [\mathbb{K}_n : \mathbb{K}_{n-1}][\mathbb{K}_{n-1} : \mathbb{K}_{n-2}] \ldots [\mathbb{K}_1 : \mathbb{K}_0]$ *est une puissance de deux, alors* $[\mathbb{K}_n : \mathbb{K}_0] = [\mathbb{K}_n : \mathbb{K}_0(x)][\mathbb{K}_0(x) : \mathbb{K}_0]$ *est aussi une puissance de deux, ce qui implique*

$[\mathbb{K}_0(x) : \mathbb{K}_0]$ est une puissance de deux, le même raisonnement montre $[\mathbb{K}_0(y) : \mathbb{K}_0]$ est une puissance de deux.

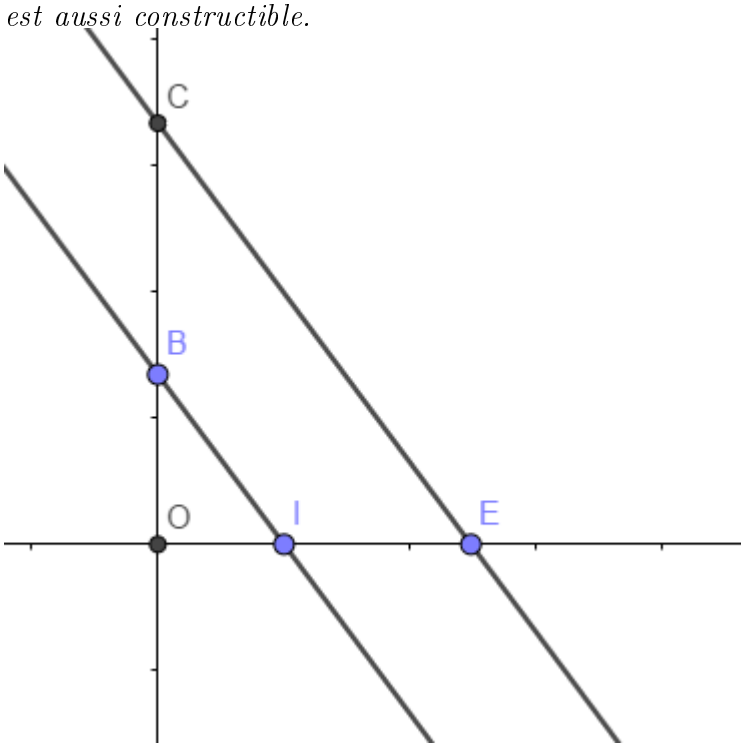
2.3 Caractérisation des constructions possibles.

Lemme 4. *Un point $(a, b) \in \mathbb{R}^2$ est constructible à partir de $\mathcal{P}_0 = \{O, I\}$, $O(0, 0)$ et $I(1, 0)$, si a, b appartiennent au sous-corps $\mathbb{K}_0$ de $\mathbb{R}$.*

Démonstration. *On remarque qu'étant donné un point $M(a, b)$ du plan $\mathbb{R}^2$, il est possible de construire les points $A(0, a)$ et $B(0, b)$.*
Etapes. *En utilisant le même raisonnement de la construction de la perpendiculaire à une droite issue d'un point extérieur, on trace la droite passant par le point M et qui est perpendiculaire à l'axe (Oy), cette droite rencontre (Oy) en $B(0, b)$, puis, la perpendiculaire à l'axe (Ox) passant par M rencontre (Ox) en $E(a, 0)$, le cercle de centre O et de rayon $r = d(O, E)$, coupe (Oy) en $A(0, a)$.*
Réciproquement, si les deux points $A(0, a)$ et $B(0, b)$ sont constructibles, alors le point $M(a, b)$ est aussi constructible. En effet, il suffit de construire le point $E(a, 0)$ par report de compas puis le parallélogramme $EOBM$.
Pour démontrer le lemme 4, il suffit de prouver qu'étant donné des points $A(0, a)$ et $B(0, b)$ de $\mathcal{P}_0$, alors les points $(0, a + b)$, $(0, a - b)$, $(0, ab)$ et $\left(0, \frac{a}{b}\right)$, si $b \neq 0$, sont constructibles.

i) Etant donné les points $A(0, a)$ et $B(0, b)$, les points de coordonnées $(0, a+b)$, $(0, a-b)$ sont obtenus par report de compas.

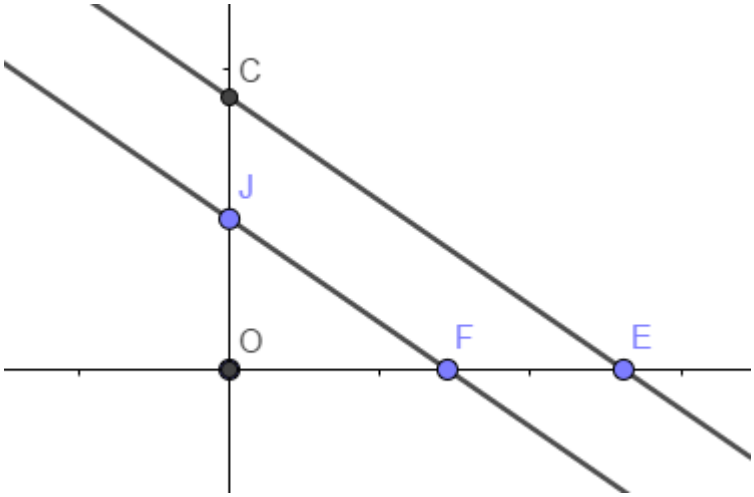
ii) On peut toujours supposer a et b positifs, car si $(0, a)$ est constructible avec $a > 0$, $(0, -a)$ est aussi constructible.



On construit le point $E(a, 0)$ par report de compas, on trace la paralléle à la droite (BI)

passant par E, elle coupe l'axe (Oy) en C, d'après le théorème de THALES, $\frac{\overline{OC}}{\overline{OB}} = \frac{\overline{OE}}{\overline{OI}}$, *ce qui donne* $\overline{OC} = ab$.

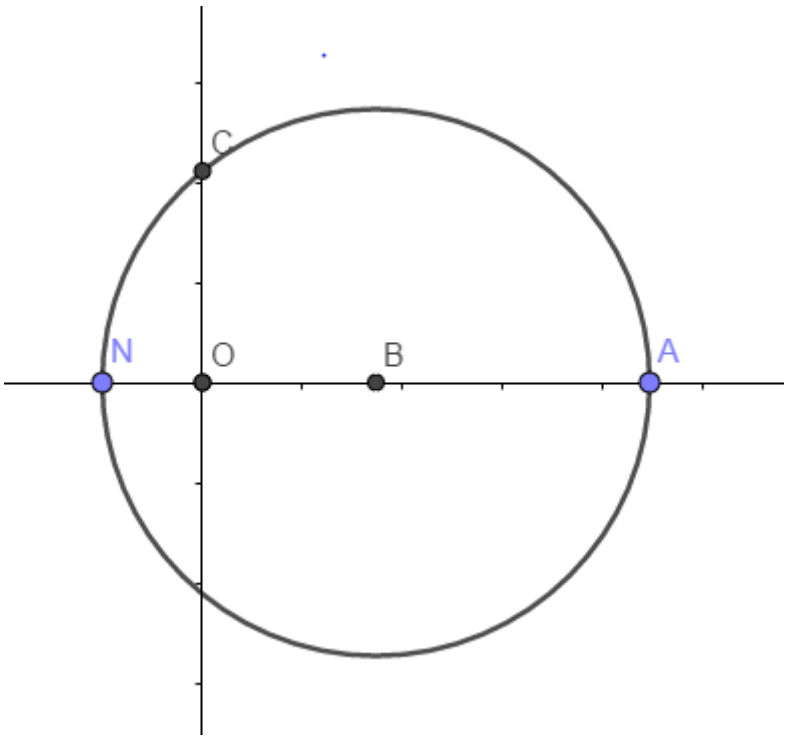
iii) On suppose à nouveau $a > 0$ et $b > 0$,



on construit les points $J(0,1)$, et $F(b,0)$ par report de compas, On trace la parallèle à la droite (JF) passant par E, elle coupe l'axe (Oy) en C, d'après le théorème de THALES, $\frac{\overline{OE}}{\overline{OF}} = \frac{\overline{OC}}{\overline{OJ}}$, *ce qui donne* $\overline{OC} = \frac{a}{b}$.

Lemme 5. *On considère une extension $K_0(\alpha) : K_0$ telle que :*
$K_0(\alpha) \subset \mathbb{R}$ et $[K_0(\alpha) : K_0] = 2$;
alors tout point (x, y) du plan $\mathbb{R}^2$, tel que $(x, y) \in K_0(\alpha) \times K_0(\alpha)$ est constructible à partir d'un ensemble fini de points dont les coordonnées sont dans K_0.

Démonstration. $[K_0(\alpha) : K_0] = 2 \Longrightarrow \alpha$ *est algébrique sur K_0 et $p_\alpha(X) = Irr_K(\alpha)$ est de degré 2. Posons $p_\alpha(X) = X^2 + bX + c$, dans $K_0[X] \subset \mathbb{R}[X]$.*
$\alpha \in \mathbb{R} \Longrightarrow b^2 - 4c \geq 0$ *et* $\alpha = \dfrac{-b \pm \sqrt{b^2 - 4c}}{2}$
Compte tenu du Lemme 4, pour prouver le Lemme 5, il suffit de prouver que le point $(0, \sqrt{b^2 - 4c})$ est constructible à partir d'un nombre fini de points dont les coordonnées sont dans K_0. Cela revient à montrer que, quelque soit $a > 0$ dans K_0, le point $(0, \sqrt{a})$ est constructible à partir d'un nombre fini de points dont les coordonnées sont dans K_0.
Construction



Soit $A(a,0)$, on construit le point $N(-1,0)$ à partir de $\mathcal{P}_0$, on construit le point B milieu du segment $[NA]$, le cercle de centre B et de rayon $r = d(B,A)$ rencontre l'axe (Oy) en $C(0,\sqrt{a})$.
En effet,
Soient $A(a,0)$, $B(\frac{a-1}{2},0)$, $N(-1,0)$ et $C(0,x)$
Le point B étant le centre du cercle, alors $d(B,C) = d(B,N)$, c'est-à-dire :

$$\sqrt{\left(\frac{a-1}{2}-0\right)^2+(x-0)^2} = \sqrt{\left(\frac{a-1}{2}+1\right)^2+(0-0)^2}$$

$$\iff \sqrt{\frac{a^2-2a+1+4x^2}{4}} = \sqrt{\frac{a^2+2a+1}{4}}$$

$$\iff \sqrt{a^2-2a+1+4x^2} = \sqrt{a^2+2a+1}$$

$$\iff 4x^2 = 4a$$

$$\iff x = \pm\sqrt{a}.$$

Théorème 13 (Théorème de Laurent Wantzel). *Soit $L : K_0$ une extension de corps, tel que $L \subseteq \mathbb{R}$ et x, y des éléments de L, alors le point de coordonnées (x,y) du plan $\mathbb{R}^2$, est constructible, si et seulement s'il existe un nombre fini de corps intermédiaires entre K_0 et K_r, avec $K_r \subset \mathbb{R}$, $x, y \in K_r$ tels que :*
$\mathbb{Q} \subseteq K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r$, $r \geq 1$ et $[K_i : K_{i-1}] = 2$, $\forall i, (1 \leq i \leq r)$.

Démonstration. *Si M est constructible à partir des points de $\mathcal{P}_0$, alors il existe une chaîne croissante finie de corps $\{K_i\}_{0\leq i\leq n}$, $n \in \mathbb{N}$, telle que :*

$$\mathbb{Q} \subseteq K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r$$

et $\forall i (1 \leq i \leq n)$, $[K_i : K_{i-1}] = 1$ ou 2.
En éliminant les cas où deux corps consécutifs sont égaux, on peut extraire de la chaine précédente une chaine finie strictement croissante $\{K_j\}_{0\leq j\leq r}$, $0 \leq r \leq n$, que l'on écrira :

$\mathbb{Q} \subset K_0 \subset K_1 \subset \ldots \subset K_r$ *et* $[K_j : K_{j-1}] = 2$, $1 \leq j \leq r$.
Réciproquement, supposons qu'il existe une chaîne finie strictement croissante de corps intermédiaires entre K_0 *et* $K_r \subset \mathbb{R}$ *vérifiant les conditions du théorême, montrons qu'alors, le point* $M(x, y)$ *est constructible.*
Pour $r = 0$, *le résultat est donné par le lemme 4,*
Pour $r > 1$, *faisons un raisonnement par récurrence sur* r.
Pour tout j, $1 \leq j \leq r$, *soit* $\alpha_j \in K_j \setminus K_{j-1}$, *on a* $[K_j : K_{j-1}] = 2$, *donc* α_j *est algébrique sur* K_{j-1} *et le degré du polynôme* $Irr_K(\alpha)$ *est* 2 *; on en déduit que* $K_{j-1}(\alpha_j) = K_j$.
D'après le lemme 5 tout point (x, y) *dont les coordonnées sont dans* K_j *est constructible à partir d'un nombre fini de points dont les coordonnées sont dans* K_{j-1}, *l'hypothèse de récurrence et le raisonnement précédent, appliqué au cas* $j = r$, *donnent le résultat énoncé.*

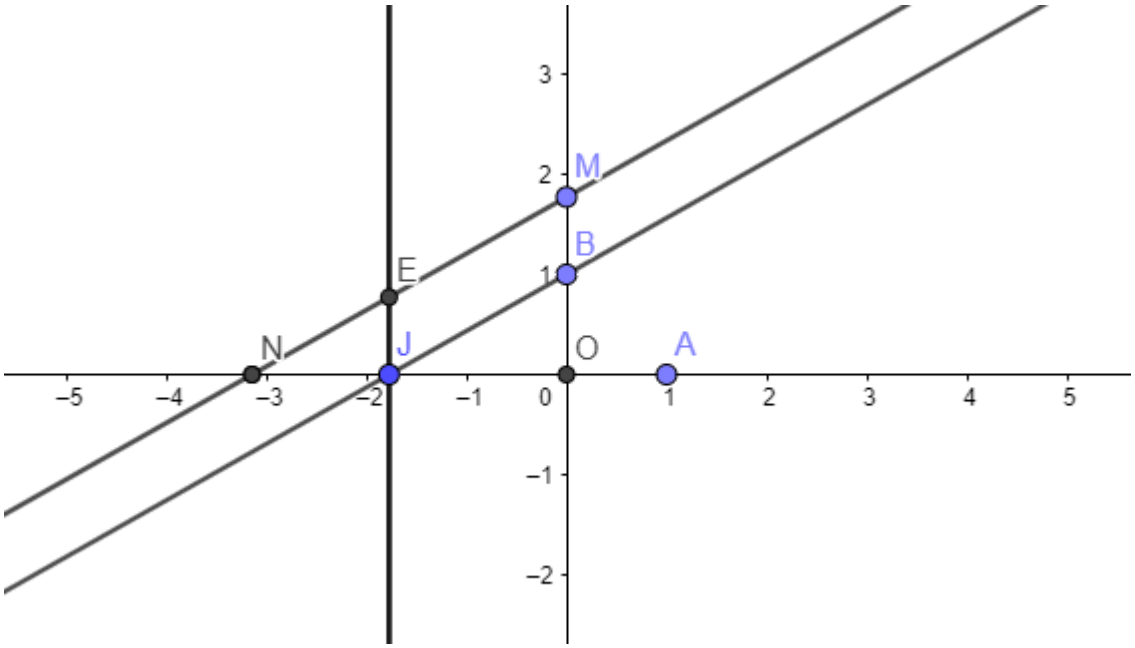
2.4 Constructions Impossibles.

2.4.1 Quadrature du cercle.

Le problème consiste à construire un carré de même aire qu'un disque donné à l'aide d'une règle et d'un compas.

Proposition 29. *La quadrature du cercle est impossible par la règle et le compas.*

Démonstration. *Considérons dans le plan* $\mathbb{R}^2$ *rapporté au repère orthonormé* $(O, \vec{i}, \vec{j})$, *le cercle de centre* O *et de rayon* 1, *son aire est égale à* π.
Résoudre la quadrature du cercle, revient à construire le point $M = (0, \sqrt{\pi})$ *à partir de* $\mathcal{P}_0 = \{O, A\}$, $O(0, 0)$, $A(1, 0)$ *on a* $\mathbb{K}_0 = \mathbb{Q}$.
Si le point M *était constructible à partir de* $\mathcal{P}_0$, *alors on pourrait construire le point* $N(-\pi, 0)$.



Étapes de la construction

1 ˚) Le point d'intersection entre le cercle $C(O,r)$, $r = d(O,A)$, et l'axe (Oy) donne le point $B(0,1)$.

2 ˚) Le point d'intersection entre le cercle $C'(O,r')$, $r' = d(O,M)$ et l'axe (Ox) donne le point $J(-\sqrt{\pi},0)$.

3 ˚) Avec les points M, B, J, on trace le parallélogramme $MBJE$.

Construction

On place la pointe sèche du compas en M, avec une ouverture égale à la distance de B par rapport à J, on fait un arc de cercle.

On place la pointe sèche du compas en J, avec une ouverture égale à la distance de B par rapport à M, on fait un arc de cercle.

Le point de rencontre des deux arcs de cercles donne le point E.

4 ˚) Le point d'intersection entre (ME) et l'axe (Ox) donne le point N.

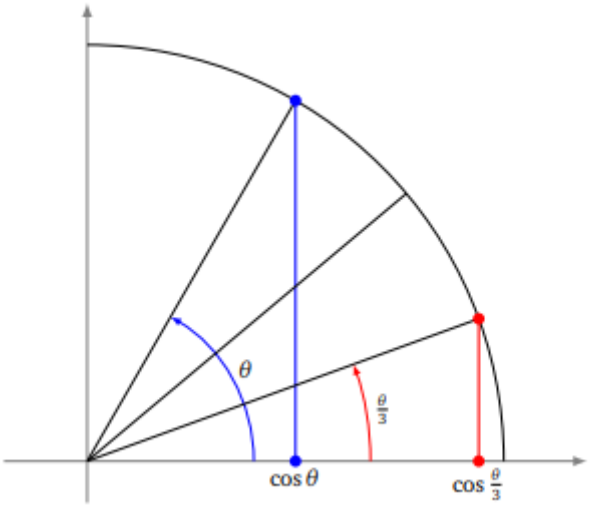
En effet,
en posant $y = d(O,N)$, $x = d(O,J) = d(O,M)$.
Les droites (ME) et (BJ) étant parallèles, les triangles OBJ et OMN sont semblables,
D'après THALES on a :
$\frac{\overline{ON}}{\overline{OJ}} = \frac{\overline{OM}}{\overline{OB}}$
$\frac{y}{x} = \frac{x}{1} \Longrightarrow y = x^2$
pour $x = \sqrt{\pi}$ on a bien $y = \pi$.
Le point N étant constructible, on aurait $[\mathbb{Q}(\pi) : \mathbb{Q}]$ égal à une puissance de 2, ce qui est en contradiction avec la transcendance de π sur $\mathbb{Q}$, car $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$,
donc, la quadrature du cercle est impossible par la règle et le compas.

2.4.2 Trisection d'un angle.

Ce problème consiste à diviser un angle donné en trois angles de même mesure à l'aide d'une règle et d'un compas.

Proposition 30. *L'angle de mesure $\frac{\pi}{3}$ ne peut être divisé en trois angles égaux, par la règle et le compas.*

Démonstration. *On suppose choisie une unité de longueur dans le plan affine euclidien $\mathbb{R}^2$, rapporté à un repère orthonormé $(O,\vec{i},\vec{j})$, alors l'ensemble $\mathcal{P}_0$ est formé des points de coordonnées $(0,0)$ et $(1,0)$, d'où $\mathbb{K}_0 = \mathbb{Q}$.*



Si le point $A(a,0)$, $a=\cos\dfrac{\pi}{9}$ *était constructible alors le point* $B(b,0)$, $b=2a$ *le serait aussi,*
en posant $\alpha=\dfrac{\pi}{9}$, *alors* $3\alpha=\dfrac{\pi}{3}$,
or $\cos 3\alpha=4\cos^3\alpha-3\cos\alpha$,
en remplaçant α *par sa valeur, on a :*
$\cos\dfrac{\pi}{3}=4\cos^3\dfrac{\pi}{9}-3\cos\dfrac{\pi}{9}$
c'est-à-dire :
$\dfrac{1}{2}=4\cos^3\dfrac{\pi}{9}-3\cos\dfrac{\pi}{9}$
$\iff \dfrac{1}{2}=4a^3-3a$, *car* $a=\cos\dfrac{\pi}{9}$
$\iff \dfrac{1}{2}=4\left(\dfrac{b}{2}\right)^3-3\left(\dfrac{b}{2}\right)$
$\iff \dfrac{1}{2}=\dfrac{b^3}{2}-\dfrac{3b}{2}$
$\iff b^3-3b-1=0$
b *est racine du polynôme* $f(X)=X^3-3X-1$,
$f(X+1)=X^3+3X^2-3$
$\boldsymbol{p}=3$ *est un nombre premier, tel que* $\boldsymbol{p}\mid a_i$, *pour* $0\leq i\leq 2$, $\boldsymbol{p}\nmid a_3$ *et* $\boldsymbol{p}^2\nmid a_0$,
en appliquant le critère d'Eisenstein sur $f(X+1)$, $f(X+1)$ *est irréductible sur* $\mathbb{Q}$, *d'après la proposition 21 à la page 25,* $f(X)$ *est aussi irréductible sur* $\mathbb{Q}$,
cela entraîne $[\mathbb{Q}(b):\mathbb{Q}]=3$,
si B *était contructible à la règle et le compas, le degré de l'extension serait une puissance de* 2, *alors* B *n'est pas constructible à la règle et au compas, il s'en suit que* A *n'est pas constructible à la règle et au compas.*
donc, l'angle de mesure $\dfrac{\pi}{3}$ *n'est pas trisectable par la règle et le compas.*

Remarque. *L'angle de mesure* π *est trisectable par la règle et le compas.*

Preuve. $\cos\dfrac{\pi}{3}=\dfrac{1}{2}$
Tout revient à construire le point $B\left(\dfrac{1}{2},0\right)$ *à partir de* $\mathcal{P}_0$.
B *est le milieu de* $[OA]$, *le point d'intersection entre la médiatrice de* $[OA]$ *et la droite* (OA)

donne le point B.
Donc l'angle de mesure π est bien trisectable.

La proposition 30 permet d'affirmer qu'étant donné un angle de mesure θ, $0 \leq \theta \leq 2\pi$, la trisection de cet angle est impossible d'une manière générale, par contre les angles π, $\frac{\pi}{2}$ et $\frac{\pi}{3}$ qui ont pour Cosinus -1, 0, $\frac{1}{2}$ sont constructibles.

2.4.3 Duplication du cube.

Ce problème consiste à construire un cube dont le volume vaut le double d'un cube donné à l'aide de la règle et du compas.

Proposition 31. *Il est impossible de construire, par la règle et le compas, un cube ayant un volume double de celui d'un cube donné.*

Démonstration. *Soit $\mathbb{C}_1$ un cube donné dans l'espace affine $\mathbb{R}^3$, rapporté à un repère orthonormé $\left(O, \vec{i}, \vec{j}, \vec{k}\right)$, supposons que l'origine du repère soit l'un des sommets du cube et que l'une de ses arêtes est sur l'axe (Ox), tel que $a = 1$,*
donc $V_1 = 1^3 = 1$.
L'ensemble $\mathcal{P}_0$ est formé des points $(0,0)$ et $(1,0)$ d'où $\mathbb{K}_0 = \mathbb{Q}$.
Résoudre le problème de la duplication du cube revient à construire le point $A(a,0)$ tel que : $V_2 = a^3 = 2$.
a est racine du polynôme $f(X) = X^3 - 2$, irréductible sur $\mathbb{Q}$,
alors, $[\mathbb{Q}(a) : \mathbb{Q}] = 3$,
cela entraîne que a n'est pas constructible.
donc, la duplication du cube est impossible par la règle et le compas.

2.4.4 Quelques problèmes.

1) Peut-on construire géométriquement un polygone régulier de 5 côtés en utilisant la règle et le compas ?
2) Montrer qu'il est impossible de construire un polygone régulier de 7 côtés à la règle et au compas.
3) Peut-on construire un polygone régulier de 9 côtés en utilisant la règle et le compas ?

2.4.5 Résolution des problèmes.

Solution 1

Considérons l'équation $Z^5 - 1 = 0$ dans $\mathbb{C}$, ses solutions sont les racines cinquièmes de l'unité, géométriquement elles représentent les affixes des sommets du pentagone régulier dans le plan complexe.
Les racines n-ièmes de l'unité peuvent s'écrire :

$S = \left\{1, e^{\frac{2i\pi}{n}}, e^{\frac{4i\pi}{n}}, \ldots, e^{\frac{2(n-1)i\pi}{n}}\right\}$
$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$
$Z^5 - 1 = (Z-1)(Z^4 + Z^3 + Z^2 + Z + 1)$
$Z^5 - 1 = 0 \Rightarrow Z - 1 = 0$ ou $Z^4 + Z^3 + Z^2 + Z + 1 = 0$
$Z^5 - 1 = 0 \Rightarrow Z = 1$ ou $\sum_{k=0}^{4} e^{\frac{2ik\pi}{5}} = 0$
$\cos\frac{8\pi}{5} + \cos\frac{6\pi}{5} + \cos\frac{4\pi}{5} + \cos\frac{2\pi}{5} + 1 = 0$
$2\cos\frac{4\pi}{5} + 2\cos\frac{2\pi}{5} + 1 = 0$, car $\cos\frac{8\pi}{5} = \cos\frac{2\pi}{5}$ et $\cos\frac{6\pi}{5} = \cos\frac{4\pi}{5}$
pour tout réel x on a :

$$\cos 2x = 2\cos^2 x - 1$$

l'équation devient :

$$2\left(2\cos^2\frac{2\pi}{5} - 1\right) + 2\cos\frac{2\pi}{5} + 1 = 0$$

d'où

$$4\cos^2\frac{2\pi}{5} + 2\cos\frac{2\pi}{5} - 1 = 0$$

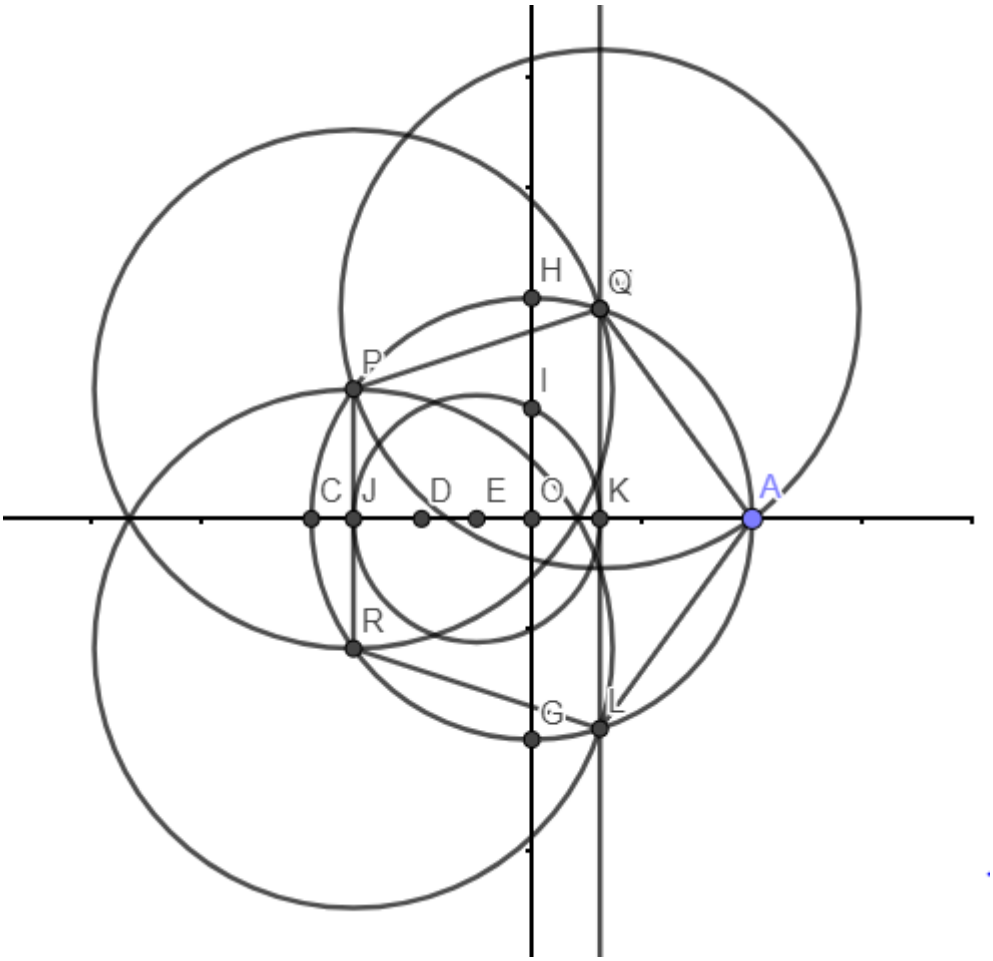
en posant $X = \cos\frac{2\pi}{5}$ on a :

$$4X^2 + 2X - 1 = 0$$

$$\Delta = 20$$

les solutions de l'équation sont :
$X' = \frac{-1-\sqrt{5}}{4}$ et $X'' = \frac{-1+\sqrt{5}}{4}$,
puisque $0 < \frac{2\pi}{5} < \frac{\pi}{2}$,
$\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$.

2.4.6 Construction du polygone régulier de 5 côtés.



Étapes

1 °) Construction de $\frac{1}{4}$.

2 °) Construction de $\frac{\sqrt{5}}{4}$.

3 °) Construction du point de coordonnées $\left(\cos\frac{2\pi}{5}, \sin\frac{2\pi}{5}\right)$

4 °) Reporter la distance des deux premiers sommets pour obtenir les sommets du pentagone régulier.

Description.

Considérons dans le plan, l'ensemble $\mathcal{P}_0 = \{O, A\}$
On trace le cercle (ε) de centre O et de rayon $r = \overline{OA}$, ce cercle recoupe (OA) en C, la médiatrice du segment $[CA]$ rencontre (ε) en H et G (H d'ordonnée positive).
Ainsi (OA) représente l'axe des abscisses (Ox) et (OH) l'axe des ordonnées (Oy).
Soit D le milieu de $[OC]$ et E celui de $[DO]$, nous avons $\overline{EO} = \frac{1}{4}$.
En effet :

$\overline{OA} = \overline{OC}$ et $\overline{OD} = \frac{1}{2}\left(\overline{OC}\right) = \frac{1}{2}\left(\overline{OA}\right)$
or $\overline{EO} = \frac{1}{2}\left(\overline{OD}\right)$, ça implique $\overline{EO} = \frac{1}{2}\left(\frac{1}{2}\left(\overline{OA}\right)\right) = \frac{1}{4}\left(\overline{OA}\right) = \frac{1}{4} \times 1 = \frac{1}{4}$.
Soit I le milieu de $[OH]$, le cercle de centre E et de rayon $\overline{EI}$ rencontre (Ox) en J et K (K le point d'abscisse positive).
Nous avons :
$\overline{EI} = \frac{\sqrt{5}}{4}$, En effet :
le triangle EOI étant rectangle en O, $\overline{EO} = \frac{1}{4}$ et $\overline{OI} = \frac{1}{2}$,
d'aprés Pythagore,
$\left(\overline{EI}\right)^2 = \left(\overline{EO}\right)^2 + \left(\overline{OI}\right)^2$
$\overline{EI} = \sqrt{\left(\frac{1}{4}\right)^2 + \left(\frac{1}{2}\right)^2} = \frac{\sqrt{5}}{4}$.
La droite qui passe par K et parrallèle à (Oy) rencontre (ε) en Q et L tel que $\widehat{AOQ} = \frac{2\pi}{5}$ et l'abscisse du point K vaut $\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$, car $\overline{OK} = \overline{EK} - \overline{EO} = \overline{EI} - \overline{EO} = \frac{\sqrt{5}}{4} - \frac{1}{4} = \frac{\sqrt{5}-1}{4}$.
Enfin, le cercle de centre Q et de rayon $r = \overline{AQ}$ rencontre (ε) en P, le cercle de centre P et de rayon $r = \overline{QP}$ rencontre (ε) en R, ainsi nous avons le pentagone régulier $AQPRL$.

Solution 2

Montrons qu'il est impossible de construire un polygone régulier de 7 côtés en utilisant la règle et le compas.
Considérons dans $\mathbb{C}$ l'équation $Z^7 - 1 = 0$,
en utilisant les mêmes raisonnements de l'exercice précédent, nous avons :
$\cos\frac{2\pi}{7} + \cos\frac{4\pi}{7} + \cos\frac{6\pi}{7} + \cos\frac{8\pi}{7} + \cos\frac{10\pi}{7} + \cos\frac{12\pi}{7} + 1 = 0$
puisque $\cos\frac{2\pi}{7} = \cos\frac{12\pi}{7}$, $\cos\frac{4\pi}{7} = \cos\frac{10\pi}{7}$ et $\cos\frac{6\pi}{7} = \cos\frac{8\pi}{7}$,
l'équation devient :
$2\cos\frac{2\pi}{7} + 2\cos\frac{4\pi}{7} + 2\cos\frac{6\pi}{7} + 1 = 0$
$2\cos\frac{2\pi}{7} + 2\left(2\cos^2\frac{2\pi}{7} - 1\right) + 2\left(4\cos^3\frac{2\pi}{7} - 3\cos\frac{2\pi}{7}\right) + 1 = 0$
$8\cos^3\frac{2\pi}{7} + 4\cos^2\frac{2\pi}{7} - 4\cos\frac{2\pi}{7} - 1 = 0$
en posant $X = \cos\frac{2\pi}{7}$ on a :
$8X^3 + 4X^2 - 4X - 1 = 0$
d'après la proposition 20 à la page 25, les racines éventuelles de cette équation appartiennent à l'ensemble $A = \{\pm 1\,;\, \pm\frac{1}{2}\,;\, \pm\frac{1}{4}\,;\, \pm\frac{1}{8}\}$, or il n'y a aucun élément de A qui annule l'équation,
donc le polynôme $P(X) = 8X^3 + 4X^2 - 4X - 1$ est irréductible sur $\mathbb{Q}$
on en déduit $X = \cos\frac{2\pi}{7}$ n'est pas constructible à la règle et au compas.
Il est impossible de construire à la règle et le compas un polygone régulier de 7 côtés.

Solution 3

Vérifions s'il est possible de construire un polygone régulier de 9 côtés en utilisant la règle et le compas.

Construire un polygone régulier de 9 côtés en utilisant la règle et le compas, revient à construire le point $A(a,0)$, $a = \cos\dfrac{2\pi}{9}$, ce qui revient au même à trisecter l'angle $\dfrac{2\pi}{3}$.

1 °) $\cos\dfrac{2\pi}{3}$ est constructible.

En effet, $\cos\dfrac{2\pi}{3} = -\dfrac{1}{2}$

Le cercle de centre O et de rayon $r = d(O,A)$ recoupe la droite (OA) en $B(-1,0)$, la médiatrice du segment $[BO]$ rencontre la droite (OA) en $C(-\dfrac{1}{2},0)$. Donc $\cos\dfrac{2\pi}{3}$ est constructible.

2 °) Vérifions si l'angle $\dfrac{2\pi}{3}$ est trisectable.

Posons $\alpha = \dfrac{2\pi}{9}$,

$3\alpha = \dfrac{2\pi}{3} \Rightarrow \cos 3\alpha = -\dfrac{1}{2}$,

utilisons la formule trigonométrique :

$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$,

en remplaçant α par sa valeur, on a :

$-\dfrac{1}{2} = 4\cos^3\dfrac{2\pi}{9} - 3\cos\dfrac{2\pi}{9}$,

en posant $Y = \cos\dfrac{2\pi}{9}$ on a :

$8Y^3 - 6Y + 1 = 0$,

soit $P(Y) = 8Y^3 - 6Y + 1$, $P(Y+1) = 8Y^3 + 24Y^2 + 18Y + 3$.

En appliquant le critère d'Eisenstein sur $P(Y+1)$,

$p = 3$ est premier, $p \mid a_i$ pour $(0 \leq i \leq 2)$, $p \nmid a_3$ et $p^2 \nmid a_0$,

$P(Y+1)$ est irréductible sur $\mathbb{Q}$, ce qui implique $P(Y)$ irréductible sur $\mathbb{Q}$, on en déduit que l'angle $\dfrac{2\pi}{3}$ n'est pas trisectable.

Il est impossible de construire à la règle et le compas un polygone régulier de 9 côtés.

CONCLUSION.

L'objectif de ce mémoire a été d'étudier la conjecture : « Tout nombre réel devait pouvoir être accessible comme grandeur géométrique constructible » en utilisant les trois problèmes : duplication du cube, trisection de l'angle et quadrature du cercle ; de caractériser, si possible, les nombres réels constructibles et de résoudre certains problèmes de construction de polygones réguliers.

A première vue le sujet peut laisser croire qu'il s'agissait purement de géométrie, ce qui est totalement erroné, car sans l'algèbre, on pourrait jusqu'aujourd'hui être en quête d'une solution aux problèmes.

La première partie du mémoire consiste en un rappel d'une série de théories obligatoires qui permettront de comprendre la construction à la règle et au compas. La théorie des groupes étant considérée comme acquis, une grande partie de la théorie des anneaux a été développée, puis les notions d'extensions de corps qui vont aider à faire le transport de la formulation géométrique vers la formulation algébrique du problème.

La deuxième partie traite directement de la construction à la règle et au compas. On arrive à caractériser un point constructible à l'aide du résultat de Laurent Wantzel, ce qui permet d'aboutir à une conclusion aux trois problèmes surnommés les « problèmes impossibles ». Le même résultat permet aussi de faire des déductions sur la construction à la règle et au compas de polygones réguliers de 5, 7 et 9 côtés.

BIBLIOGRAPHIE.

[1] **Josette CALAIS**, *Extension de corps- Théorie de Galois*. Ellipses, 2006.

[2] **Jean Pierre ESCOFIER**, *Théorie de Galois*. Dunod, 2000.

[3] **Josette CALAIS**, *Éléments de théorie des anneaux-Anneaux commutatifs*. Ellipses, 2006.

[4] **Francois DUMAS**, *Algèbre : groupes et anneaux 1*, 2007.

http ://math.univ-bpclermont.fr/ fdumas/enseignement.html