M102 : Polynômes et Géométrie
Table des Matières

CHAPITRE I

Anneaux de polynômes

I.1. Expressions algébriques

On appelle *polynôme* une *expression algébrique* du type

$$f = 3x^5 - 4x^2 + x + \pi.$$

Il y a des *coefficients*, réels ou complexes, et la lettre x qui intervient avec divers exposants. On appelle *monôme* un polynôme avec un seul terme (par exemple $2x^3$).

On peut écrire un polynôme suivant les puissances décroissantes (comme ci-dessus) ou suivant les puissances croissantes, on écrirait ici

$$f = \pi + x - 4x^2 + 3x^5.$$

On pourrait aussi écrire

$$f = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5$$

avec $a_0 = \pi, a_1 = 1, a_2 =_4, a_3 = a_4 = 0, a_5 = 3$. Par commodité il est admis de ne pas écrire les termes dont le coefficient est nul (ainsi, pour un monôme, on se contente d'écrire un seul terme). On peut aussi imaginer qu'il y a des termes nuls à la suite de ceux que l'on a écrit (ici, $a_6 = 0$), et même une infinité de termes (ici, $a_7 = a_8 = \ldots = 0$).

Écriture normalisée. On peut "normaliser" l'écriture des polynômes et définir f comme une suite (a_n) de coefficients (réels ou complexes), nulle à partir d'un certain rang (il existe N tel que, $\forall n > N, a_n = 0$). On écrit alors $f = (a_n)$.

Un polynôme est entièrement déterminé par la suite de ses coefficients. Dire que deux polynômes $f = (a_n)$ et $g = (b_n)$ sont égaux, c'est donc dire que $a_n = b_n$ pour tout n.

Alternativement on pourrait aussi écrire

$$f = a_0x^0 + a_1x^1 + \ldots + a_nx^n + \ldots$$

mais, contrairement à l'usage, la lettre x et les signes $+$ sont superflus.

Somme et produit. On peut aisément définir la somme et le produit de deux polynômes en écriture normalisée :

- *La somme* de $f = (a_n)$ et $g = (b_n)$ est le polynôme $f + g$ de coefficients s_n définis par

$$s_n = a_n + b_n.$$

- *Le produit* de $f = (a_n)$ et $g = (b_n)$ est le polynôme fg de coefficients p_n définis par

$$p_n = a_0 b_n + a_1 b_{n-1} + \ldots + a_0 b_n = \sum_{i+j=n} a_i b_j.$$

On peut vérifier que somme et produit sont *commutatifs* :

$$f + g = g + f \quad \text{et} \quad fg = gf,$$

qu'ils sont *associatifs* :

$$(f + g) + h = f = (g + h) \quad \text{et} \quad (fg)h = f(gh),$$

et enfin que le produit est *distributif* par rapport à la somme :

$$f(g + h) = fg + fh.$$

Il y a un polynôme nul, noté 0, dont tous les coefficients sont nuls, tel que

$$0 + f = f + 0 = f, \quad \text{et} \quad 0f = f0 = 0.$$

Il y a un polynôme unité, noté 1, défini par la suite de coefficients $(1, 0, \ldots, 0, \ldots)$, tel que

$$1f = f1 = f.$$

Enfin on note $-f$ le polynôme obtenu en changeant les signes de tous les coefficients de f de sorte qu'on a

$$f + (-f) = 0.$$

On retrouve ainsi toutes les règles usuelles de calcul sur les nombres et en particulier les identités remarquables, comme la fameuse égalité

$$(f + g)^2 = f^2 + 2fg + g^2.$$

On dit que les polynômes forment un *anneau*. On note $\mathbb{R}[X]$ l'anneau des polynômes réels (à coefficients réels) et $\mathbb{C}[X]$ l'anneau des polynômes complexes (à coefficients complexes).

Remarque I.1.1. Il est facile de vérifier que la somme des monômes $a_0, a_1 x, \ldots, a_n x^n$ n'est autre que le polynôme $a_0 + a_1 x + \ldots + a_n x^n$, il suffit en effet de faire la somme terme à terme des suites correspondantes, soit :

$$\begin{array}{cccccc} & (a_0, & 0, & 0, & \ldots) \\ + & (0, & a_1, & 0, & \ldots) \\ + & (0, & 0, & a_2, & \ldots) \\ + & \ldots & \ldots & \ldots & \ldots \\ \hline = & (a_0, & a_1, & a_2, & \ldots) \end{array}$$

Ceci justifie l'emploi du signe + dans la notation usuelle des polynômes.

I.2. Degré

DÉFINITION I.2.1. Soit $f = (a_n)$ un polynôme non nul. On appelle *degré de* f, on note $\deg(f)$, le plus grand entier n tel que $a_n \neq 0$.

On note que le polynôme nul n'a pas de degré (il n'y a pas d'entier n pour lequel $a_n \neq 0$). On conviendra de poser $\deg(0) = -\infty$.

PROPOSITION I.2.2. *Soient f et g deux polynômes. On a*

- $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$,
- $\deg(fg) = \deg(f) + \deg(g)$.

On observe qu'on peut étendre ce résultat et admettre des polynômes nuls si on convient que, pour tout entier n, on a

$-\infty \leq n$, $\quad -\infty \leq -\infty$,
$-\infty + n = -\infty$, $\quad -\infty + (-\infty) = -\infty$.

Quelques précisions de vocabulaire :

DÉFINITIONS I.2.3.

- Le coefficient a_0 de f s'appelle le *terme constant* de f.
- Si f est non nul, son coefficient de plus haut degré s'appelle le *coefficient directeur* de f.
- Un polynôme non nul de coefficient directeur égal à 1 s'appelle un *polynôme unitaire*.
- Un polynôme dont tous les termes non constants sont nuls (donc tel que $a_n = 0$ pour $n \geq 1$) s'appelle un *polynôme constant*, on dit aussi que c'est *une constante*

Les constantes non nulles sont donc les polynômes de degré 0. Le polynôme nul (encore appelé *constante nulle*) est le seul polynôme de degré $-\infty$.

LEMME I.2.4. *Le produit de deux polynômes non nuls est non nul.*

Notamment le degré du produit [proposition I.2.2] est supérieur ou égal à celui de chacun des facteurs. On tire la *règle de simplification* :

PROPOSITION I.2.5. *Si on a l'égalité $fh = gh$ avec $h \neq 0$, alors $f = g$.*

Démonstration. Le produit $(f-g)h$ est nul, donc l'un des facteurs est nul. Ce n'est pas le facteur h, c'est donc le facteur $f - g$. □

I.3. Division euclidienne

THÉORÈME I.3.1. *Soient f et g deux polynômes réels (resp. complexes), avec $g \neq 0$. Alors il existe un unique polynôme réel (resp. complexe) q et un unique polynôme réel (resp. complexe) r tels que*

$$f = gq + r \quad \text{et} \quad \deg(r) < \deg(g).$$

Notons que q et r peuvent être nuls ; si $r = 0$, l'inégalité $\deg(r) < \deg(g)$ est alors satisfaite grâce à la convention $\deg(0) = -\infty$. Avant de montrer ce résultat, fixons le vocabulaire.

DÉFINITION I.3.2. Lorsqu'on écrit $f = gq + r$, on dit qu'on effectue la division *euclidienne* ou *suivant les puissances décroissantes* de f par g. On dit que f est le *dividende*, g le *diviseur*, q le *quotient* et r le *reste* de cette division.

Démonstration. Si $\deg(f) < \deg(g)$, il suffit de prendre $q = 0$ et $r = f$. On a bien alors $f = gq + r = 0 + f$ avec $\deg(r) = \deg(f) < \deg(g)$. Sinon on procède par un algorithme qui permet d'abaisser le degré de f :

Première étape. On suppose qu'on a $\deg(f) = n \geq \deg(g) = m$ (de "vrais" degré puisque g est non nul). Il existe alors un monôme q_1 tel que gq_1 et f sont de même degré et de même coefficient directeur. En effet, si

$$f = a_n x^n + a_{n-1}x^{n-1} + \dots \quad \text{et} \quad g = b_m x^m + b_{m-1}x^{m-1} + \dots$$

il suffit de prendre $q_1 = (a_n/b_m)x^{n-m}$ (en particulier, $q_1 = a_n/b_m$ si $n = m$). On peut donc écrire

$$f = gq_1 + r_1 \quad \text{avec} \quad \deg(r_1) < \deg(f).$$

Si $\deg(r_1) < \deg(g)$, on a terminé. Sinon, on recommence.

Étapes suivantes. On écrit tour à tour

$$\begin{aligned} f &= gq_1 + r_1 \quad \text{avec} \quad \deg(r_1) < \deg(f), \\ r_1 &= gq_2 + r_2 \quad \text{avec} \quad \deg(r_2) < \deg(r_1). \\ r_2 &= gq_3 + r_3 \quad \text{avec} \quad \deg(r_2) < \deg(r_3) \end{aligned}$$

Ainsi de suite. On s'arrête lorsqu'on obtient un reste r_n (éventuellement nul) tel que $\deg(r_n) < \deg(g)$. Comme la suite des degrés des restes est strictement décroissante, ceci ne manque pas d'arriver! Si, par exemple, on s'arrête à r_3, on a donc

$$f = gq_1 + r_1 = gq_1 + gq_2 + r_2 = gq_1 + gq_2 + gq_3 + r_3 = g(q_1 + q_2 + q_3) + r_3.$$

Le quotient q est alors la somme des quotient partiels, soit $q = q_1 + q_2 + q_3$ et le reste r le dernier reste, soit $r = r_3$. Noter que les quotients partiels sont des monômes et que q se trouve ainsi naturellement écrit suivant les puissances décroissantes!

Unicité. Supposons données deux solutions

$$f = gq + r \text{ avec } \deg(r) < \deg(g) \quad \text{et} \quad f = gq^\star + r^\star \text{ avec } \deg(r^\star) < \deg(g).$$

On a alors $f = gq + r = gq^\star + r^\star$ et donc

$$g(q - q^\star) = r^\star - r.$$

Le degré du premier terme est

$$\deg(g(q - q^\star)) = \deg(g) + \deg(q - q^\star)$$

et pour le second terme on a

$$\deg(r^\star - r) \leq \max\{\deg(r^\star), \deg(r)\} < \deg(g).$$

On aurait une contradiction, sauf si les deux termes sont nuls (donc de degré égal à $-\infty$), soit $q = q^\star \quad \text{et} \quad r = r^\star$. □

I.4. Divisibilité

DÉFINITION I.4.1. Si $f = qg$ on dit que g *divise* f ou que g est un *diviseur* de f ou encore que f est un *multiple* de g. On note (g) l'ensemble des polynômes multiples de g.

Pour $g \neq 0$, dire que f est multiple de g signifie donc que le reste de la division de f par g est nul (la division *tombe juste*).

Faisons quelques remarques sur les ensembles de multiples :

- Parmi les multiples de g il y a toujours g lui-même (on peut écrire $g = 1g$). Autrement dit $g \in (g)$.
- Pour tout $g, 0$ est multiple de g (on peut écrire $0 = 0g$). Autrement dit $0 \in (g)$.
- Le seul multiple de 0 est 0 lui-même (pour tout $q, q0 = 0$). Autrement dit $(0) = \{0\}$.
- Tout polynôme f est multiple de 1 ($f = f1$). Autrement dit (1) est l'ensemble de tous les polynômes ($\mathbb{R}[X]$ si on considère les polynômes réels, $\mathbb{C}[X]$ si on considère les polynômes complexes).
- Plus généralement, si a est une constante non nulle, alors tout f est multiple de a ($f = (a^{-1}f)a$).

Combinaisons. On étend la notion de multiple comme suit.

DÉFINITION I.4.2. Soit $\{g_1, g_2, \ldots, g_n\}$ une famille finie de polynômes. On dit qu'un polynôme f est une *combinaison* de cette famille si on peut écrire

$$f = q_1 g_1 + q_2 g_2 + \ldots + q_n g_n.$$

On note $(g_1, g_2, \ldots, g_n)$ l'ensemble de ces combinaisons.

L'ensemble (g) des multiples de g est donc l'ensemble des combinaisons de la famille formée du seul polynôme g (ceci justifie l'emploi de la même notation).

PROPOSITION I.4.3. *Soit $\{g_1, g_2, \ldots, g_n\}$ une famille de polynômes. Alors*

- *La somme de deux (ou plusieurs) combinaisons de cette famille est encore une combinaison.*
- *Tout multiple d'une combinaison est encore une combinaison.*

Démonstration. Considérons deux combinaisons

$$f = q_1 g_1 + q_2 g_2 + \ldots + q_n g_n \quad \text{et} \quad f^\star = q_1^\star g_1 + q_2^\star g_2 + \ldots + q_n^\star g_n.$$

— Faisant la somme, on obtient la combinaison

$$f + f^\star = (q_1 + q_1^\star) g_1 + (q_2 + q_2^\star) g_2 + \ldots + (q_n + q_n^\star) g_n.$$

— Le multiple qf de f est la combinaison

$$qf = (qq_1) g_1 + (qq_2) g_2 + \ldots + (qq_n) g_n.$$

□

COROLLAIRE I.4.4. *Soit $\{g_1, g_2, \ldots, g_n\}$ une famille de polynômes. Alors une combinaison de deux (ou plusieurs) combinaisons de cette famille est encore une combinaison (de cette famille).*

Polynômes associés. On discute ici de la possibilité pour f et g de se diviser l'un l'autre ou encore d'être multiple l'un de l'autre. Comme un multiple d'un multiple est encore un multiple, cela veut dire que f et g ont le même ensemble de multiples.

DÉFINITION I.4.5. On dit que deux polynômes f et g sont *associés* s'ils se divisent l'un l'autre, soit $(f) = (g)$.

Si g divise f, soit $f = qg$, alors $\deg(g) \leq \deg(f)$ (sauf si f est nul). Si f et g se divisent l'un l'autre, ils ont donc même degré et le facteur q est une constante (en fait, si l'un est nul, alors l'autre aussi, et n'importe quel facteur convient) :

PROPOSITION I.4.6. *Deux polynômes f et g sont associés si et seulement si il existe une constante $a \neq 0$ telle que $f = ag$ et $g = a^{-1}f$.*

I.5. Pgcd

Une constante non nulle divise tout polynôme. Deux polynômes f et g admettent donc toujours des diviseurs communs. Si f et g sont non nuls, les degrés de ces diviseurs sont majorés (par les degrés de f et de g).

DÉFINITION I.5.1. Soient f et g deux polynômes (non nuls). On dit que d est un *plus grand commun diviseur* (ou *Pgcd*) de f et de g, on note $d = \mathrm{Pgcd}(f, g)$, si d est de degré maximal parmi les diviseurs de f et de g.

Algorithme d'Euclide. Soient f et g deux polynômes (non nuls). On pose $r_0 = g$. On divise f par g (donc par r_0) écrivant
$f = q_1 r_0 + r_1$ avec $\deg(r_1) < \deg(r_0)$.
Si r_1 n'est pas nul, on divise ensuite r_0 par r_1,
$r_0 = q_2 r_1 + r_2$ avec $\deg(r_2) < \deg(r_1)$.
Si r_2 n'est pas nul, on divise ensuite r_1 par r_2,
$r_1 = q_3 r_2 + r_3$ avec $\deg(r_3) < \deg(r_2)$,
ainsi de suite, tant que le reste n'est pas nul (et que la division est possible). Mais comme les restes sont de degrés strictement décroissants, il advient nécessairement qu'un reste soit nul.

PROPOSITION I.5.2. *Appliquant l'algorithme d'Euclide, le dernier reste non nul est un diviseur de f et de g multiple de tous les autres diviseurs communs, donc un Pgcd de f et de g.*

Avant de faire la démonstration faisons quelques remarques.

- Parmi plusieurs polynômes, si l'un est de degré maximal, il n'est pas nécessairement multiple de tous les autres. Il est donc remarquable qu'un Pgcd soit multiple de tous les autres diviseurs communs.

- Si le premier reste est nul, alors g divise f et $g = r_0$ est un Pgcd de f et de g.
- On peut échanger les rôles de f et de g. On a cependant intérêt à diviser le "plus grand" (de plus grand degré) par le "plus petit".

Démonstration. Sans perte de généralité, supposons que r_3 soit le dernier reste non nul.
— On montre que f et g sont multiple de r_3 ("en remontant") : d'abord, le reste de la division de r_2 par r_3 est nul, donc r_2 est multiple de r_3. Puis
$r_1 = q_3 r_2 + r_3$,
donc r_1 (combinaison des multiples r_2 et r_3) est multiple de r_3,
$r_0 = q_2 r_1 + r_2$,
donc $g = r_0$ (combinaison des multiples r_1 et r_2) est multiple de r_3,
$f = q_1 r_0 + r_1$,
donc f (combinaison des multiples r_0 et r_1) est multiple de r_3.

— Si d est un autre diviseur commun, on montre ("en descendant") que r_3 est multiple de d : $r_1 = f - q_1 r_0$,
donc r_1 (combinaison des multiples f et r_0) est multiple de d,
$r_2 = r_0 - q_2 r_1$,
donc r_2 (combinaison des multiples r_0 et r_1) est multiple de d,
$r_3 = r_1 - q_3 r_2$,
donc r_3 (combinaison des multiples r_1 et r_2) est multiple de d. □

Corollaire I.5.3. *Tous les Pgcd de f et de g sont associés entre eux.*

Démonstration. Si d et $d^\star$ sont associés, ils ont même degré et même ensemble de multiples. Si d est de degré maximal parmi les diviseurs communs de f et de g, il en est alors de même pour $d^\star$. Réciproquement, si d est le Pgcd fourni par l'algorithme d'Euclide et $d^\star$ un autre Pgcd, alors d est un multiple de $d^\star$ et le facteur multiplicatif est une constante puisqu'ils ont même degré. Ainsi, tous les Pgcd sont associés à d donc aussi entre eux. □

Relation de Bézout.

Proposition I.5.4. *Un polynôme d est un Pgcd de f et de g si et seulement il divise f et g et est combinaison de f et de g : $d = pf + qg$.*

Démonstration. Le Pgcd de l'algorithme d'Euclide [proposition I.5.2] est une combinaison de f et de g. En effet
$r_1 = f - q_1 r_0$,
est combinaison de f et de $r_0 = g$,
$r_2 = r_0 - q_2 r_1$,
est combinaison de r_0 et de r_1. Or une combinaison de combinaisons est une combinaison [corollaire I.4.4], donc r_2 est combinaison de f et de g.
$r_3 = r_1 - q_3 r_2$,
est combinaison de r_1 et de r_2, donc, pour la même raison, combinaison de

f et de g. Un autre Pgcd est associé à ce dernier, donc multiple par une constante (non nulle) et donc encore combinaison de f et de g.

Réciproquement, si $d = pf + qg$ est un diviseur commun, alors c'est un Pgcd. En effet, si $d^\star$ est un autre diviseur commun, alors d (combinaison de f et g, multiples de $d^\star$) est un multiple de $d^\star$. □

Polynômes étrangers.

Définition I.5.5. On dit que deux polynômes (non nuls) f et g sont *étrangers* s'ils n'admettent que les constantes (non nulles) pour diviseurs communs.

Autrement dit, les polynôme de degré 0 sont de degré maximal parmi les diviseurs communs et, en particulier, 1 est un Pgcd de f et de g. On a alors une forme particulière de la relation de Bézout :

Corollaire I.5.6. *Les polynômes f et g sont étrangers si et seulement si il existe p et q tels que $pf + qg = 1$.*

Démonstration. Cela résulte de la proposition I.5.4. Pour vérifier que 1 est un Pgcd, il suffit en effet de vérifier que c'est une combinaison de f et de g puisque c'est toujours un diviseur commun. □

I.6. Ppcm

Deux polynômes f et g admettent toujours des multiples communs, par exemple 0 ou le produit fg. Si on s'intéresse aux multiples non nuls, leur degré est supérieur à celui de f et de g.

Définition I.6.1. Soient f et g deux polynômes (non nuls). On dit que m est un *plus petit commun multiple* (ou *Ppcm*) de f et de g, on note $m = \mathrm{Ppcm}(f, g)$, si m est de degré minimal parmi les multiples non nuls de f et de g.

Proposition I.6.2. *Un Ppcm divise tous les autres communs multiples de f et de g.*

Démonstration. Soit m un Ppcm et $m^\star$ un autre commun multiple. Effectuant la division euclidienne de $m^\star$ par m, soit $m^\star = mq + r$, on a $r = m^\star - mq$. Ainsi le reste r est une combinaison de multiples de f et de g donc lui aussi un commun multiple. Il faut qu'il soit nul, donc que m divise $m^\star$, pour respecter le caractère minimal de m. □

Corollaire I.6.3. *Tous les Ppcm de f et de g sont associés entre eux.*

Relation entre Pgcd et Ppcm. Si m est un Ppcm, il divise le produit fg qui est un autre commun multiple, on peut donc écrire $fg = dm$. Étudiant cette relation, on va montrer comment calculer un Ppcm à l'aide d'un Pgcd.

PROPOSITION I.6.4. *Soient f, g, m, d des polynômes (non nuls) tels que $fg = md$. Alors*

(1) *d divise f si et seulement si m est un multiple de g.*
(2) *d divise g si et seulement si m est un multiple de f.*
(3) *d est un diviseur commun de f et de g si et seulement si m est un multiple commun de f et de g.*
(4) *$d = \mathrm{Pgcd}(f, g)$ si et seulement si $m = \mathrm{Ppcm}(f, g)$.*

Démonstration. 1) Si d divise f on peut écrire $f = pd$, donc (remplaçant f par pd dans la relation $fg = dm$) on a $pdg = dm$. On peut simplifier par d qui est non nul [proposition I.2.5]. Donc $m = pg$ est multiple de g. Inversement, si $m = pg$, alors $fg = dpg$ et $f = dp$.
2) Il suffit d'échanger les rôles de f et de g.
3) Si d divise f **et** g, il en résulte que m est multiple de g **et** de f.
4) La somme $\deg(d) + \deg(m)$ est constante (égale à $\deg(f) + \deg(g)$). Ainsi d est de degré maximal si et seulement si m est de degré minimal. □

On sait calculer un Pgcd (par l'algorithme d'Euclide). Si d est un Pgcd, c'est un diviseur commun et on a alors

$$f = pd \quad \text{et} \quad g = qd.$$

Avec ces notations, on obtient une expression pour un Ppcm :

COROLLAIRE I.6.5. *Le polynôme $m = dpq$ est un Ppcm de f et de g.*

Démonstration. On a en effet $md = dpqd = (pd)(qd) = fg$. □

CHAPITRE II

Facteurs irréductibles

II.1. Racines

Valeurs.

Définition II.1.1. Soient $f = a_0 + a_1x + \ldots + a_nx^n$ un polynôme à coefficients dans un corps K et α un élément de K. On appelle *valeur de f en α*, on note $f(\alpha)$ l'élément de K défini par

$$f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n.$$

Remarque II.1.2. Le plus souvent K est pour nous le corps des réels ou des complexes. Comme les réels sont des complexes particuliers, on peut aussi calculer la valeur d'un polynôme réel en un complexe. Ainsi, pour $f = x^2 + 1$, on a $f(i) = 0$.

Remplaçant *la chose* x par un nombre α, "les règles de calcul sont en tout point les mêmes" :

Proposition II.1.3. *Soient f et g deux polynômes. Alors, pour tout α on a*

- $(f + g)(\alpha) = f(\alpha) + g(\alpha)$,
- $(fg)(\alpha) = f(\alpha)g(\alpha)$.

Corollaire II.1.4. *Soient f un polynôme à coefficients dans K et α un élément de K. Alors le reste de la division euclidienne de f par $(x - \alpha)$ est $f(\alpha)$.*

Démonstration. Le diviseur $(x - \alpha)$ étant de degré 1, le reste est une constante a. Écrivant $f = (x - \alpha)q + a$, on a $f(\alpha) = (\alpha - \alpha)q(\alpha) + a$, soit $f(\alpha) = a$. □

Racines.

Définition II.1.5. On dit que α est une *racine* ou un *zéro* de f si $f(\alpha) = 0$.

Remarque II.1.6. Nous avons noté [Remarque II.1.2] qu'un polynôme réel peut toujours être considéré comme un polynôme complexe particulier. Ainsi le polynôme $f = x^2 + 1$ n'a pas de racine réelle, mais il a deux racines complexes, i et $-i$.

Lemme II.1.7. *Soit $f = gh$ un produit de deux polynômes. Alors α est une racine de f si et seulement si c'est une racine de g ou de h.*

Démonstration. On a $f(\alpha) = g(\alpha)h(\alpha)$ et le produit $g(\alpha)h(\alpha)$ est nul si et seulement si (au moins) un des facteurs est nul. □

Comme le reste de la division de f par $(x-\alpha)$ est $f(\alpha)$ [Corollaire II.1.4], on tire

PROPOSITION II.1.8. *Soit f. Alors α est une racine de f si et seulement si $(x-\alpha)$ divise f.*

COROLLAIRE II.1.9. *Un polynôme f de degré n à coefficients dans un corps K a au plus n racines distinctes dans K.*

Démonstration. On raisonne par récurrence sur n. Si $f = ax + b$ est de degré $n = 1$, il a exactement une racine : $\alpha = -(b/a)$. Soit maintenant f de degré n. Si f n'a aucune racine, le résultat est vérifié. Si f admet une racine α, on peut écrire $f = (x-\alpha)q$ où q est de degré $n-1$. Si $\beta \neq \alpha$ est une autre racine, comme ce n'est pas une racine de $(x-\alpha)$ c'est une racine de q [Lemme II.1.7]. Par hypothèse de récurrence, q admet au plus $n-1$ racines donc f en admet au plus n (celles de q et α). □

II.2. Polynôme irréductible

Lorsqu'on décompose un polynôme f en un produit de facteurs, soit $f = gh$, il peut s'agir d'une *fausse* décomposition du type $f = a(a^{-1}f)$, où le premier facteur est une constante, le second est associé à f (une telle décomposition est en effet toujours possible). En revanche, il peut s'agir d'une *vraie* décomposition si chaque facteur est de degré strictement inférieur à celui de f (et non constant).

DÉFINITION II.2.1. On dit qu'un polynôme f *non constant* à coefficients dans un corps K est *irréductible* (sur K) s'il ne peut se décomposer en produit de facteurs de degré strictement inférieur à celui de f (à coefficients dans K).

Notons bien qu'on écarte les constantes. Lorsqu'on décompose un polynôme de degré 1, l'un des facteurs est nécessairement une constante :

PROPOSITION II.2.2. *Les polynômes de degré 1 sont irréductibles.*

Les polynômes de degré 1 ont toujours une (et une seule) racine. En revanche on va établir que les polynômes irréductibles de degré supérieur n'ont pas de racine (condition nécessaire mais non suffisante).

PROPOSITION II.2.3. *Soit f un polynôme de degré $n \geq 2$.*

(1) *Si f est irréductible alors f n'a pas de racine.*
(2) *Si $n = 2$ ou 3 et si f n'a pas de racine alors f est irréductible.*

Démonstration. 1) Si f a une racine α, il résulte de la proposition II.1.8 qu'on a la *vraie* décomposition $f = (x-\alpha)g$, où le premier facteur est de degré 1 et le second de degré $n-1$.

2) Si $n = 2$ ou 3 et si $f = gh$, où g et h sont non constants et de degré strictement inférieur à n, alors l'un de ces facteurs est nécessairement de degré 1. Celui-ci a donc une racine, laquelle est aussi une racine de f [Lemme II.1.7]. □

Remarques II.2.4. 1) En fait, un polynôme réel de degré 3 a toujours une racine (il prend toutes valeurs de $-\infty$ à $+\infty$ — ou l'inverse — et *passe* donc par la valeur 0). Sur les complexes, nous verrons même plus bas que tout polynôme non constant admet une racine (théorème de d'Alembert).
2) Sur le corps $\mathbb{Q}$ des nombres rationnels, on peut montrer qu'il existe des polynômes irréductibles de tout degré n (donc sans racines pour $n \geq 2$).
3) Il faut bien préciser sur quel corps on se place. Par exemple le polynôme $f = x^2 + 1$, est irréductible sur $\mathbb{R}$, mais sur $\mathbb{C}$ il admet la décomposition $f = (x + i)(x - i)$.
4) L'exemple ci-dessous montre qu'à partir du degré 4 un polynôme peut n'avoir aucune racine et cependant ne pas être irréductible.

Exemple II.2.5. Le polynôme $f = x^4 + 2x^2 + 1$ n'a pas de racine réelle. En effet, il prend en tout $\alpha \in \mathbb{R}$ une valeur strictement positive. En revanche, il admet la décomposition $f = (x^2 + 1)(x^2 + 1)$.

Terminons par une remarque simple mais utile. Si $f = gh$ admet une vraie décomposition, multipliant par une constante $a \neq 0$, on obtient la vraie décomposition $af = (ag)h$. On a donc le résultat suivant.

Proposition II.2.6. *Tout polynôme associé à un polynôme irréductible et lui-même irréductible.*

Nombres premiers. La notion de polynôme irréductible correspond à celle de *nombre premier*. On dit qu'un entier $n \geq 2$ est premier s'il n'est pas produit de facteurs strictement plus petits. Ainsi $6 = 2 \times 3$, n'est pas premier, mais $2, 3, 5, 7, 11, \ldots$ le sont. Nous verrons que tout polynôme (non constant) admet un diviseur irréductible. Cela correspond au fait bien connu que tout entier naturel $n \geq 2$ admet un diviseur premier.

Pour trouver tous les nombres premiers jusqu'à n, le grec Eratosthène (qui fut le premier à calculer la circonférence de la Terre, au IV$^{\text{ème}}$ siècle avant Jésus-Christ) a proposé la méthode suivante, dite *du crible*. On dresse la liste des entiers jusqu'à n parmi lesquels 2 est le plus petit nombre premier. Les multiples de 2 (sauf 2 lui-même) ne sont pas premiers, on barre tous ces multiples. Le premier entier non barré est 3, il est premier (il n'est divisible par aucun nombre premier plus petit). On barre tous les multiples de 3 (sauf 3). L'entier suivant non barré est 5. On barre tous les multiples de 5. Ainsi de suite. Finalement, les entiers qui ne sont pas barrés sont premiers.

En fait, pour examiner si un entier est premier, il suffit de tester s'il est divisible par un nombre (premier) inférieur à sa racine carrée. En effet si $n = ab$ alors $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$. Ainsi, pour établir le crible sur les 24 premiers entiers, il suffit de barrer les multiples de 2 et 3.

	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24

Les Éléments d'Euclide, rédigés au III$^{\text{ème}}$ siècle avant Jésus-Christ, contiennent plusieurs résultats sur les nombres premiers (par exemple que tout entier admet un facteur premier). On y trouve aussi le joli théorème suivant.

THÉORÈME II.2.7. *Il existe une infinité de nombres premiers.*

Démonstration. Il suffit de montrer que, pour tout entier n, il existe un nombre premier supérieur à n. On pose $N = n! + 1$. On note que N n'est divisible par aucun entier $k, 2 \leq k \leq n$, en effet le reste de la division par k est 1. Mais N admet au moins un facteur premier p qui est donc tel que $p > n$. □

II.3. Unique décomposition

On dit qu'on décompose un polynôme f en *produit de facteurs irréductibles* lorsqu'on écrit

$$f = p_1 p_2 \dots p_n,$$

où les polynômes p_i sont irréductibles. Noter que les facteurs peuvent être répétés (les p_i ne sont pas supposés distincts) et qu'il peut n'y en avoir qu'un seul (si $n = 1$).

LEMME II.3.1. *Tout polynôme non constant se décompose en produit de facteurs irréductibles.*

Démonstration. Soit f un polynôme non constant. S'il est irréductible, il admet une décomposition avec un seul facteur. En particulier le résultat est donc vrai pour les polynômes de degré 1. On raisonne par récurrence sur le degré de f. Considérant le cas où f n'est pas irréductible, on peut écrire $f = gh$, où g et h sont non constants et de degré inférieur à celui de f. Par hypothèse de récurrence, g et h sont produits de facteurs irréductibles et f est le produit de tous ces facteurs (ceux de g et ceux de h). □

On s'intéresse maintenant à l'unicité de cette décomposition. En fait on peut toujours changer l'ordre des facteurs. On peut aussi multiplier un facteur par une constante non nulle et un autre par l'inverse de cette constante. Par exemple $x(x+1) = (2x+2)\left(\frac{1}{2}x\right)$. Cela revient à remplacer certains facteurs par des polynômes associés. On montrera que la décomposition est unique à l'ordre près et à associés près.

Lemme de Gauss.

LEMME II.3.2 (Lemme de Gauss). *Si un polynôme f divise un produit gh et est étranger avec g, alors il divise h.*

Démonstration. Comme f et g sont étrangers, on a une relation de Bézout $1 = pf + qg$ [Corollaire I.5.6]. Multipliant cette relation par h, on tire

$$h = pfh + qgh = (ph)f + q(gh).$$

Donc h est une combinaison de deux multiples de f (f lui-même, et gh que f divise par hypothèse). Ainsi, f divise h. □

LEMME II.3.3. *Soient p un polynôme irréductible et g un polynôme. Alors ou bien p divise g ou bien p et g sont étrangers.*

Démonstration. Si p ne divise pas g, alors g est non nul et le reste de la division de g par p est de degré strictement inférieur à celui de p. A fortiori, l'algorithme d'Euclide conduit à un Pgcd de degré encore inférieur. Comme le Pgcd divise p, il n'a donc d'autre choix que d'être une constante. □

PROPOSITION II.3.4. *Si un polynôme irréductible divise un produit de polynômes, alors il divise l'un des facteurs.*

Démonstration. Supposons qu'un polynôme irréductible p divise le produit $g_1 g_2 \dots g_n$ de n polynômes. Si p divise g_n, il divise bien l'un des facteurs. Sinon p est premier avec g_n. D'après le lemme de Gauss, p divise alors le produit $g_1 g_2 \dots g_{n-1}$. Par récurrence sur le nombre de facteurs, on conclut que p divise l'un des g_i, pour $i \leq n-1$. □

Unicité.

THÉORÈME II.3.5. *Tout polynôme f à coefficients dans un corps K peut se décomposer en un produit*

$$f = a p_1 p_2 \dots p_n$$

où a et une constante et les n polynômes p_i ($n \geq 0$) sont irréductibles et unitaires. En outre, si f est non nul, cette décomposition est unique à l'ordre près des facteurs.

Démonstration. Existence. Si $f = a$ est constant, la décomposition se fait alors sans facteurs irréductibles ($n = 0$). Sinon on sait qu'on peut écrire

$$f = q_1 q_2 \dots q_n$$

où les q_i sont irréductibles [Lemme II.3.1]. Si le coefficient directeur de q_i est a_i, on a $q_i = a_i p_i$ où p_i est unitaire. Comme p_i est associé à q_i, il est irréductible [Proposition II.2.6]. Prenant pour a le produit des a_i, on obtient la décomposition voulue.
Unicité. Si f est nul, la constante a est nulle. Le produit de cette constante par n'importe quel polynôme est donc nul et dans ce cas, mais dans ce cas seulement la décomposition n'est évidemment pas unique. Sinon, on montre

que la décomposition est unique par récurrence sur le degré. Tout d'abord, la constante a est le coefficient directeur du produit $ap_1p_2\dots p_r$ (puisque les p_i sont unitaires), elle est donc uniquement déterminée. En particulier, la décomposition est donc unique pour les polynômes de degré 0. Pour un polynôme de degré $n > 0$, considérons alors deux décompositions

$$f = ap_1p_2\dots p_r = bq_1q_2\dots q_s.$$

Comme on vient de le dire, $a = b$ et, simplifiant par cette constante, on a

$$p_1p_2\dots p_r = q_1q_2\dots q_s.$$

Mais alors p_1 divise l'un des q_j [Corollaire II.3.4]. Quitte à réarranger les facteurs, on peut supposer que p_1 divise q_1. Comme q_1 est irréductible, il ne peut s'agir que d'une *fausse* factorisation, de la forme $q_1 = up_1$, où u est une constante. Mais comme p_1 et q_1 sont unitaires, alors $p_1 = q_1$. Simplifiant par p_1 on tire

$$p_2\dots p_r = q_2\dots q_s,$$

deux décompositions d'un même polynôme g de degré inférieur à celui de f. Par hypothèse de récurrence, ces décompositions sont les mêmes (à l'ordre près des facteurs). □

II.4. Théorème de d'Alembert

Donnons sans démonstration le théorème de d'Alembert (démontré par Gauss) annoncé plus haut [Remarque II.2.4 (1)].

THÉORÈME II.4.1. *Tout polynôme non constant admet* (*au moins*) *une racine complexe.*

Il en résulte que les seuls polynômes irréductibles sur les complexes sont les polynômes de degré 1 (les polynômes de degré $n > 1$ ne peuvent être irréductibles lorsqu'ils ont une racine [Proposition II.2.3]).

COROLLAIRE II.4.2. *Sur les complexes, tout polynôme f se décompose* (*de manière unique*) *en produit de la forme*

$$f = a(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n).$$

Polynômes réels irréductibles. Les polynômes de degré 1 sont toujours irréductibles ainsi que les polynômes de degré 2 qui n'ont pas de racine [Proposition II.2.3]. Sur les réels, ces derniers sont les polynômes de la forme $f = ax^2 + bx + c$ dont le *discriminant* $\Delta = b^2 - 4ac$ est strictement négatif. En s'appuyant sur le théorème de d'Alembert on montre qu'il n'y en a pas d'autre :

COROLLAIRE II.4.3. *Sur les réels, les polynômes irréductibles sont*

- *les polynômes de degré 1* (*dits* de première espèce,)
- *les polynômes de degré 2 de discriminant* $\Delta < 0$, (*dits* de deuxième espèce,)

Il suffit d'établir que les polynômes de degré $n \geq 3$ ne sont jamais irréductibles. On commence par un lemme.

LEMME II.4.4. *Si un polynôme réel admet une racine complexe, il admet alors aussi la racine complexe conjuguée.*

Démonstration. Soit $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Supposons que $f(\alpha) = 0$, pour $\alpha \in \mathbb{C}$. Prenant le conjugué de $f(\alpha)$, on obtient

$$\overline{f(\alpha)} = a_n\overline{\alpha}^n + a_{n-1}\overline{\alpha}^{n-1} + \ldots + a_1\overline{\alpha} + a_0 = 0.$$

En effet, le conjugué d'une somme (resp. d'un produit) est la somme (resp. le produit) des conjugués et on ne change pas les coefficients (réels) en prenant leur conjugué. Donc $\overline{\alpha}$ est une racine de f. □

On peut maintenant montrer qu'un polynôme f de degré $n \geq 3$ n'est pas irréductible sur les réels. On sait que f admet une racine complexe α [Théorème II.4.1] et on considère deux cas :
1) α est réel. Dans ce cas $(x - \alpha)$ est un diviseur de f sur $\mathbb{R}$, et f n'est pas irréductible.
2) α n'est pas réel. Dans ce cas $(x - \alpha)$ divise f sur $\mathbb{C}$. A priori on peut simplement conclure que f n'est pas irréductible sur $\mathbb{C}$. Mais d'après le lemme, f admet aussi la racine $\overline{\alpha}$ et donc $(x - \overline{\alpha})$ est un autre facteur de f. Dans l'unique décomposition de f on a ces deux facteurs et on peut écrire

$$f = (x - \alpha)(x - \overline{\alpha})q = \big(x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}\big)q.$$

Notant que $\alpha + \overline{\alpha}$ et $\alpha\overline{\alpha}$ sont réels, $g = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}$ est donc un polynôme réel de degré 2. Par ailleurs, q est (l'unique) quotient de la division euclidienne de f par g, ainsi q est réel, de degré $n-2$. Comme f est de degré $n \geq 3$, la décomposition $f = gq$ est donc une vraie décomposition sur $\mathbb{R}$.

II.5. Multiplicité

Racines multiples. Dans l'unique décomposition d'un polynôme en produit de facteurs irréductibles [Théorème II.3.5], les facteurs de la forme $(x - \alpha)$ correspondent aux racines. Il se peut qu'un tel facteur intervienne plusieurs fois :

DÉFINITION II.5.1. Soit f un polynôme à coefficients dans un corps K. On dit que $\alpha \in K$ est une *racine d'ordre* k de f si k est le plus grand entier tel que $(x - \alpha)^k$ divise f. Si $k = 1$, on dit que α est une *racine simple* et, si $k > 1$, que c'est une *racine multiple* (*racine double* si $k = 2$, *triple* si $k = 3$).

On peut préciser le corollaire II.1.9 sur le nombre des racines en prenant en compte les multiplicités :

COROLLAIRE II.5.2. *Soit f un polynôme de degré n admettant les racines $\alpha_1, \ldots, \alpha_r$ respectivement de multiplicité $k_1, \ldots, k_r$. Alors*

$$k_1 + \ldots + k_r \leq n.$$

Sur les complexes, il résulte du théorème de d'Alembert [Théorème II.4.1] que f est produit de facteurs de la forme $(x-\alpha)$. Regroupant les facteurs correspondant à une même racine, on peut écrire

$$f = a(x-\alpha_1)^{k_1}\dots(x-\alpha_r)^{k_r}.$$

COROLLAIRE II.5.3. *Soit f un polynôme complexe de degré n admettant les racines (complexes) $\alpha_1,\dots,\alpha_r$ respectivement de multiplicités $k_1,\dots,k_r$. Alors*

$$k_1+\dots+k_r = n.$$

Dérivée. Sans référence aux fonctions, on peut définir la dérivée d'un polynôme de manière formelle :

DÉFINITION II.5.4. Soit

$$f = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$$

un polynôme à coefficients dans un corps K. On appelle *dérivée* de f, on note f', le polynôme

$$f' = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \dots + a_1.$$

REMARQUE II.5.5. Si f est un polynôme réel ou complexe de degré n on voit que sa dérivée f' est de degré $n-1$. En particulier $f'=0$ si et seulement si f est une constante.

On a les règles de calcul suivantes :

PROPOSITION II.5.6. *Soient f et g deux polynômes à coefficients dans K et a une constante. Alors*

(i) $(f+g)' = f'+g'$.
(i) $(af)' = af'$.
(iii) $(fg)' = f'g+fg'$.

Démonstration. Les formules pour la dérivée de la somme ou du produit par une constante sont faciles à établir. Pour le produit, on peut considérer que f et g sont sommes de monômes. Appliquant les résultats précédents, on peut se ramener au cas où $f=x^n$ et $g=x^m$. On a alors

$$(fg)' = (x^{n+m})' = (n+m)x^{n+m-1} = nx^{n-1}x^m + mx^{m-1}x^n = f'g+fg'.$$

□

Une récurrence sur n donne le corollaire suivant

COROLLAIRE II.5.7. *Soient f un polynôme à coefficients dans un corps K et n un entier. Alors*

$$(f^n)' = nf^{n-1}f'.$$

En particulier, pour tout $\alpha\in K$, on a $[(x-\alpha)^n]' = n(x-\alpha)^{n-1}$.

Compte tenu de la remarque II.5.5 on peut aussi tirer le résultat suivant de la dérivée de la somme (ou d'une différence) :

COROLLAIRE II.5.8. *Soient f et g deux polynômes réels ou complexes. Alors $f'=g'$ si et seulement si la différence $f-g$ est une constante.*

Formule de Taylor. On peut définir la dérivée seconde (dérivée de la dérivée) et, par itération, les dérivées successives de f :

DÉFINITION II.5.9. Soit f un polynôme à coefficients dans un corps K. Pour tout entier k on appelle *dérivée d'ordre k* de f, on note $f^{(k)}$, la dérivée de $f^{(k-1)}$.

En particulier, $f^{(0)} = f$, la *dérivée première* $f^{(1)}$ n'est autre que la dérivée f' de f et la *dérivée seconde* $f^{(2)}$ peut aussi se noter f".

REMARQUE II.5.10. Comme le fait de dériver abaisse le degré, il est clair que pour f de degré n et $k > n$, on a $f^{(k)} = 0$.

On établit maintenant la formule dite *formule de Taylor* :

THÉORÈME II.5.11. *Soit f un polynôme (réel ou complexe) de degré n. Pour toute constante a on a alors*

$$f = f(a) + (x-a)f'(a) + \ldots + \frac{(x-a)^n}{n!} f^{(n)}(a).$$

Démonstration. On raisonne par récurrence sur n. Pour f constant, on a de manière triviale $f = f(a)$. On pose

$$g = f(a) + (x-a)f'(a) + \ldots + \frac{(x-a)^n}{n!} f^{(n)}(a).$$

Dérivant g, il résulte des règles de calcul [Proposition II.5.6] et du corollaire II.5.7 (donnant la dérivée de $(x-a)^k$) qu'on a

$$g' = f'(a) + \ldots + \frac{(x-a)^{n-1}}{(n-1)!} f^{(n)}(a).$$

Par hypothèse de récurrence, on voit que g' est l'expression de la formule de Taylor pour la dérivée f' de f (de degré $n-1$). Ainsi $f' = g'$ et donc $f = g + C$, où C est une constante [Corollaire II.5.8]. Comme par ailleurs, $g(a) = f(a)$, alors $C = 0$, soit $f = g$. □

Calculant f en $x = a + h$, donc faisant $x - a = h$, on tire :

COROLLAIRE II.5.12. *Soit f un polynôme de degré n (réel ou complexe). Pour tout a et tout h on a alors*

$$f(a+h) = f(a) + hf'(a) + \ldots + \frac{h^n}{n!} f^{(n)}(a).$$

Dérivées et multiplicité.

THÉORÈME II.5.13. *Soient f un polynôme (réel ou complexe), α un nombre (réel ou complexe) et k un entier. Alors les assertions suivantes sont équivalentes :*

(i) *α est une racine d'ordre k de f.*
(ii) *$f(\alpha) = f^{(1)}(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$ et $f^{(k)}(\alpha) \neq 0$.*

En particulier,
• α est une racine simple si et seulement si $f(\alpha) = 0$ et $f'(\alpha) \neq 0$,
• α est une racine double si et seulement si $f(\alpha) = f'(\alpha) = 0$ et $f"(\alpha) \neq 0$,
ainsi de suite.

On pourrait dire que α est une racine d'ordre 0 si $f(\alpha) \neq 0$ (α *n'est pas* racine de f).

Démonstration. Montrons d'abord que $(x-\alpha)^k$ divise f si et seulement si $f(\alpha) = f^{(1)}(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$.
— Supposons que $f(\alpha) = f^{(1)}(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$. Dans la formule de Taylor [Théorème II.5.11], les k premiers termes sont nuls. On peut donc mettre $(x-\alpha)^k$ en facteur.
— Inversement, supposons que $(x-\alpha)^k$ divise f. Alors $f = (x-\alpha)^k g$. Dérivant cette égalité, on obtient, d'après les règles de calculs [Proposition II.5.6] :

$$f' = k(x-\alpha)^{k-1} g + (x-\alpha)^k g'.$$

Alors $(x-\alpha)^{k-1}$ divise f'. Par le même raisonnement, $(x-\alpha)^{k-2}$ divise $f"$, ainsi de suite, et donc $f(\alpha) = f^{(1)}(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$.

Le plus grand entier k tel que $f(\alpha) = f^{(1)}(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$ est donc le plus grand entier k tel que $(x-\alpha)^k$ divise f. □

CHAPITRE III

Équations et racines

III.1. Quadratiques et cubiques

Équations quadratiques. On dispose de *formules* pour la résolution des équations quadratiques (c'est à dire du second degré). En fait, la résolution de ces équations remonte à la Babylone antique, et est liée à divers problèmes de carrés.

Partons d'un problème simple (et classique) : trouver deux nombres connaissant leur somme et leur produit. On sait le résoudre a priori, en utilisant une des plus anciennes identités remarquable :

$$\left(\frac{x+y}{2}\right)^2 = \left(\frac{x-y}{2}\right)^2 + xy.$$

Connaissant la somme $S = x + y$ et le produit $P = xy$, on tire la différence $D = x - y$ par la formule

$$\frac{D}{2} = \sqrt{\left(\frac{S}{2}\right)^2 - P},$$

puis les valeurs de $x = \frac{S}{2} + \frac{D}{2}$ et $y = \frac{S}{2} - \frac{D}{2}$ soit

$$x = \frac{S}{2} + \sqrt{\left(\frac{S}{2}\right)^2 - P} \quad \text{et} \quad y = \frac{S}{2} + \sqrt{\left(\frac{S}{2}\right)^2 - P}. \tag{III.1.1}$$

Notons qu'il est tout aussi facile de trouver deux nombres connaissant leur *différence* et leur produit.

Soit maintenant une équation quadratique :

$$ax^2 + bx + c = 0. \tag{III.1.2}$$

On peut multiplier (plutôt que diviser) par a, on obtient

$$a^2x^2 + bax + ca = 0.$$

Posant $y = ax$, on se ramène alors à une équation du type

$$y^2 + by + ca = 0.$$

En fait dans l'Antiquité, on ne considère que des égalités entre nombres positifs. Donc par exemple, une équation du type "carré plus nombre égal *chose*" soit

$$y^2 + P = Sy. \tag{III.1.3}$$

On voit le lien avec le problème précédent : si $S = x + y$ est la somme de deux nombres, et $P = xy$ leur produit alors

$$Sy = xy + y^2 = P + y^2.$$

Trouver x et y dont on connaît la somme S et le produit P revient donc à résoudre l'équation III.1.3.

De nos jours (et de manière équivalente), on présente les racines de l'équation générale III.1.2 sous la forme

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Formules de Cardan. Les racines d'une équation *cubique* (c'est à dire de degré 3) séxpriment de même par des formules publiées par Cardan en 1545 (dites *formules de Cardan*), découvertes plus tôt par Scipione Del Ferro puis par Tartaglia (qui les avait montrées à Cardan sous la condition de ne pas les divulguer!).

On cherche à résoudre l'équation

$$ax^3 + bx^2 + cx + d = 0.$$

On peut d'abord multiplier par a^2 et se ramener à l'équation

$$a^3x^3 + ba^2x^2 + ca^2x + da^2 = 0$$

puis noter que les deux premiers termes $a^3x^3 + ba^2x^2$ sont ceux du développement de $(ax + b/3)^3$. Si on fait le changement de variable $y = ax + b/3$ on obtient alors l'équation

$$y^3 + (ca - b^2/3)y + da^2 + 2b^3/27 - (abc)/3 = 0.$$

Si on sait résoudre cette équation en y on sait alors résoudre l'équation initiale, en revenant à $x = y/a - b/3a$.

Tout revient donc à résoudre une équation sans terme carré, qu'on écrira sous *forme réduite*

$$y^3 - py - q = 0. \tag{III.1.4}$$

On cherche une solution sous la forme $y = u + v$. On doit alors avoir

$$(u + v)^3 - p(u + v) - q = 0. \tag{III.1.5}$$

Rappelant l'identité remarquable

$$(u + v)^3 = u^3 + 3u^2v + 3uv^2 + v^3 = u^3 + v^3 + 3uv(u + v)$$

et reportant dans l'équation III.1.5, on tire

$$u^3 + v^3 + (u + v)(3uv - p) - q = 0.$$

Mais alors il suffit que u et v vérifient les relations

$$\begin{cases} 3uv = p \\ \\ u^3 + v^3 = q \end{cases}$$

Soit encore

$$\begin{cases} u^3v^3 = (p/3)^3 \\ \\ u^3 + v^3 = q \end{cases}$$

On retrouve le problème classique de trouver deux nombres connaissant leur somme et leur produit! On pose

$$\Delta = \left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3$$

c'est le *discriminant* de l'équation. Des formules III.1.1 rappelées plus haut, on tire

$$u^3 = \frac{q}{2} + \sqrt{\Delta} \quad \text{et} \quad v^3 = \frac{q}{2} - \sqrt{\Delta}.$$

D'où la formule qui donne la racine $y = u + v$ de l'équation cubique :

$$y = \sqrt[3]{\frac{q}{2} + \sqrt{\Delta}} + \sqrt[3]{\frac{q}{2} - \sqrt{\Delta}}.$$

Remarques III.1.1. 1) En général, il y trois racines cubiques dans le corps des complexes donc trois choix pour u connaissant $u^3 = \frac{q}{2} + \sqrt{\Delta}$. Ayant choisi une racine cubique pour u, alors v est uniquement déterminé puisque u et v sont liés par la relation $3uv = p$. Aux trois racines cubiques pour u correspondent donc les trois racines (distinctes ou confondues) de l'équation de degré 3.
2) Une équation de degré 4 peut se ramener à une cubique ainsi que l'a montré Ludovico Ferrari, un disciple de Cardan. On dit que les équations de degré 2, 3 et 4 sont *résolubles par radicaux* : les racines s'expriment par des formules faisant intervenir des radicaux (racine carrées, cubiques ou quatrièmes). Paolo Ruffini en 1799, puis le norvégien Niels Abel et enfin le français Evariste Galois ont montré que de telles formules n'existaient pas pour les équations de degré 5 ou plus.

Apparition des nombres complexes. Cardan a noté que l'équation

$$x^3 = 15x + 4$$

avait la racine évidente $\alpha = 4$. Or les formules donnent

$$\begin{cases} u^3v^3 = (p/3)^3 = 125 \\ \\ u^3 + v^3 = 4 \end{cases}$$

soit $\Delta = \left(\frac{4}{2}\right)^2 - \left(\frac{15}{3}\right)^3 = -121$. Le calcul de u^3 et v^3 était donc réputé impossible. Notant que $121 = (11)^2$, on serait amené à écrire

$$u^3 = 2 + 11\sqrt{-1} \quad \text{et} \quad v^3 = 2 - 11\sqrt{-1}.$$

Cardan a alors introduit la notion de *nombre sophistique*. Si on pouvait calculer avec $\sqrt{-1}$ on retrouverait bien

$$\begin{cases} u^3v^3 = (2+11\sqrt{-1})(2-11\sqrt{-1}) = 4-(11\sqrt{-1})^2 = 4+121 = 125 \\ \\ u^3+v^3 = (2+11\sqrt{-1})+(2-11\sqrt{-1}) = 4 \end{cases}$$

Cette approche a été reprise par Rafaelle Bombelli (1526-1573) dans l'*Algebra*.

Ainsi il serait faux de dire que les nombres complexes ont été créés pour "inventer des racines imaginaires" : au contraire, ils sont apparus pour interpréter des formules devant conduire à des racines bien réelles.

III.2. Coefficients et racines

On a vu le lien entre somme et produit des racines pour l'équation quadratique, il remonte à l'Antiquité. Cardan avait aussi noté certaines relations entre la somme des racines d'une cubique et ses coefficients ; des résultats dans le même sens furent obtenus par François Viète qui fut l'un des premiers à considérer les équations avec *paramètres*, c'est à dire dont les coefficients eux-mêmes sont des lettres et non des nombres. Les théorèmes généraux sont pour une grande part dus à Isaac Newton.

Fonctions symétriques élémentaires des racines.

Définition III.2.1. Soient $(x_1,\dots,x_n)$ n éléments (distincts ou confondus) d'un corps K. On appelle *fonctions symétriques élémentaires* de ces éléments les expressions

$\sigma_1(x_1,\dots,x_n) = \sum_i x_i$, somme des x_i,
$\sigma_2(x_1,\dots,x_n) = \sum_{i<j} x_ix_j$, somme des produits deux à deux des x_i,
...
$\sigma_n(x_1,\dots,x_n) = \prod_i x_i$, produit des x_i.

Considérons maintenant les n racines complexes (distinctes ou répétées chacune autant de fois que leur multiplicité) d'un polynôme de degré n.

Théorème III.2.2. *Soit $f = a_nx^n + a_{n-1}x^{n-1} + \dots + a_0$ un polynôme complexe de degré n. Alors les fonctions symétriques élémentaires de ses racines sont liées aux coefficients par les relations :*

$$\sigma_1 = -\frac{a_{n-1}}{a_n}, \dots, \sigma_k = (-1)^k\frac{a_{n-k}}{a_n}, \dots, , \sigma_n = (-1)^n\frac{a_0}{a_n}.$$

Démonstration. Si les racines de f sont $x_1,\dots,x_n$, on a

$$f = a_nx^n + a_{n-1}x^{n-1} + \dots + a_0 = a_n\prod_i(x-x_i).$$

Divisant par a_n on se ramène à un polynôme unitaire

$$f = x^n + \frac{a_{n-1}}{a_n}x^{n-1} + \dots + \frac{a_0}{a_n} = \prod_i(x-x_i).$$

On peut alors développer le produit et identifier les coefficients et pour se convaincre des relations, raisonner par récurrence sur n.

— Pour $n = 2$, on a bien

$$(x - x_1)(x - x_2) = x^2 - (x_1 + x_2)x + x_1x_2.$$

— Notons $\sigma'_1, \ldots, \sigma'_{n-1}$ les fonctions symétriques élémentaires des $n-1$ premières racines $x_1, \ldots, x_{n-1}$. Par hypothèse de récurrence, on a

$$\prod_{i \leq n-1} (x - x_i) = x^{n-1} + \ldots + (-1)^{k-1}\sigma'_{k-1}x^{n-k} + (-1)^k\sigma'_k x^{n-k-1} + \ldots.$$

Multipliant $\prod_{i \leq n-1}(x - x_i)$ par $(x - x_n)$ on obtient un polynôme dont le terme de degré $n - k$ à pour coefficient

$$(-x_n)(-1)^{k-1}\sigma'_{k-1} + (-1)^k\sigma'_k = (-1)^k \left(x_n\sigma'_{k-1} + \sigma'_k\right).$$

Il reste à vérifier qu'on a bien

$$\sigma_k = x_n\sigma'_{k-1} + \sigma'_k.$$

En effet, σ_k est la somme des produits k à k des racines, et donc des produits k à k des $n-1$ premières racines (de somme σ'_k) et des produits de x_n avec les produits $k-1$ à $k-1$ des $n-1$ premières racines (de somme σ'_{k-1}). □

Identités de Newton. Les identités de Newton permettent de calculer par récurrence les sommes des puissances des racines. On note $S_k = \sum_i x_i^k$ la somme des puissances k-ièmes des racines. (On note en particulier qu'on a $S_0 = \sum_i x_i^0 = n$.)

THÉORÈME III.2.3. *Soit $f = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0$ un polynôme complexe de degré n. Alors, pour $k \leq n$, on a les relations*

$$a_nS_k + a_{n-1}S_{k-1} + \ldots + a_{n-k+1}S_1 + ka_{n-k} = 0$$

et pour $k \geq n$, les relations

$$a_nS_k + a_{n-1}S_{k-1} + \ldots + a_0S_{k-n} = 0.$$

Démonstration. 1) Pour $k \geq n$, il suffit de noter que pour toute racine x_i on a

$$a_nx_i^n + a_{n-1}x_i^{n-1} + \ldots + a_0.$$

Multipliant par x_i^{k-n}, on obtient

$$a_nx_i^k + a_{n-1}x_i^{k-1} + \ldots + a_0x_i^{k-n}.$$

Ajoutant terme à terme les n relations (pour chacune des racines), on obtient les relations de Newton.
2) Pour $k \leq n$, on exprime de deux manières différentes la dérivée f' de f. On a d'abord

$$f' = na_nx^{n-1} + \ldots + (n-k)a_{n-k}x^{n-k-1} + \ldots. \tag{III.2.1}$$

Ensuite, écrivant $f = a_n\prod_i(x - x_i)$, on montre par récurrence sur n, en appliquant la formule de la dérivée d'un produit, qu'on a

$$f' = \sum_i f_i \quad \text{où} \quad f_i = \frac{f}{x - x_i}.$$

Comme $f(x_i) = 0$, on peut écrire, pour tout i

$$f_i = \frac{f(x) - f(x_i)}{x - x_i} = a_n \frac{x^n - x_i^n}{x - x_i} + a_{n-1} \frac{x^{n-1} - x_i^{n-1}}{x - x_i} + \ldots + a_1 \frac{x - x_i}{x - x_i}.$$

Appliquant les identités remarquables

$$x^k - x_i^k = (x - x_i)(x^{k-1} + x_i x^{k-2} + \ldots + x_i^{k-1})$$

on obtient

$$f_i = a_n x^{n-1} + \ldots + [a_n x_i^k + a_{n-1} x_i^{k-1} + \ldots + a_{n-k}] x^{n-k-1} + \ldots.$$

Ajoutant entre-eux tous les f_i, on arrive à

$$f' = n a_n x^{n-1} + \ldots + [a_n S_k + a_{n-1} S_{k-1} + \ldots + n a_{n-k}] x^{n-k-1} + \ldots. \quad \text{(III.2.2)}$$

Identifiant les coefficients de degré $n-k-1$ entre III.2.1 et III.2.2, on obtient

$$(n - k) a_{n-k} = a_n S_k + a_{n-1} S_{k-1} + \ldots + n a_{n-k}$$

dont on tire les relations de Newton. □

Coefficients entiers, solutions entières.

PROPOSITION III.2.4. *Soit $f = x^n + a_{n-1} x^{n-1} + \ldots + a_0$, un polynôme unitaire à coefficients entiers. Si f admet une racine rationnelle α, alors α est un entier et il divise le terme constant a_0.*

Démonstration. Soit $\alpha = a/b$ une racine rationnelle qu'on peut supposer sous forme irréductible (et de dénominateur positif). On a

$$f(\alpha) = (a/b)^n + a_{n-1}(a/b)^{n-1} + \ldots + a_0 = 0$$

multipliant par b^n on tire

$$a^n = -b\big(a_{n-1} a^{n-1} + \ldots + a_0 b^{n-1}\big).$$

Tout facteur premier p de b divise a^n donc divise aussi a. Ayant supposé la fraction sous forme irréductible, b n'admet aucun tel facteur p. Autrement dit, $b = 1$ et $\alpha = a$ est un entier (relatif). Par ailleurs on peut aussi écrire

$$a_0 = -a\big(a^{n-1} + a_{n-1} a^{n-2} + \ldots + a_1\big)$$

donc $\alpha = a$ divise a_0. □

EXEMPLE III.2.5. Le polynôme $f = x^3 - 2$ n'admet aucune racine rationnelle. En effet une telle racine serait un entier diviseur de 2. Il suffit de vérifier que $1, -1, 2, -2$ ne sont pas racines de f. Comme il est de degré 3, ce polynôme est donc irréductible sur $\mathbb{Q}$ [Proposition II.2.3].

III.3. La règle et le compas

Constructions géométriques. Avec une règle et un compas, on peut réaliser des constructions géométriques. On connaît les plus classiques : médiatrice d'un segment, bissectrice d'un angle, parallèle à une droite, etc. on peut aussi citer la construction du pentagone régulier (dont on dit que les pythagoriciens avaient fait leur emblème).

Trois problèmes fameux ont été posés dès l'Antiquité :

— *La trisection de l'angle* : donné un angle θ, le partager en trois angles égaux (chacun de valeur $\theta/3$).

— *La duplication du cube* : donné un cube, construire un segment qui soit le côté du cube de volume double (de même que le carré construit sur la diagonale d'un carré a une surface double que le carré donné).

— *La quadrature du cercle* : donné un cercle, construire un carré de même surface que le disque ainsi considéré.

Pour résoudre certains de ces problèmes, les grecs ont parfois utilisé d'autres outils que la règle (la droite) et le compas (le cercle). Ainsi, au IV^{ème} siècle avant Jésus Christ, Menechme avait déjà montré comment réaliser la duplication du cube par intersection de deux coniques : à l'intersection d'une parabole (d'équation $y = x^2$) et d'une hyperbole (d'équation $y = 2/x$) est le point A d'abcisse $\sqrt[3]{2}$. Cette approche a été systématiquement développée par le mathématicien et poète Omar Khayyam au XII^{ème} siècle pour la résolution des équations cubiques.

Néanmoins, on cherche ici à déterminer quels problèmes ont une solution à la règle et au compas seuls : partant d'un ensemble de points qui définissent la figure initiale, on ne s'autorise qu'à joindre deux de ces points par une droite ou à tracer un cercle de centre un point donné et passant par un autre de ces points. L'intersection de deux droites, de deux cercles ou d'un cercle et d'une droite est alors un point obtenu par construction à la règle et au compas. Ce nouveau point peut ensuite être utilisé dans une étape suivante, selon les mêmes principes.

Usage de coordonnées et nombres constructibles. René Descartes, dans le célèbre *Discours de la Méthode*, ramène les problèmes géométriques de construction à la détermination des nombres qui peuvent mesurer les "lignes" construites (par *ligne* il désigne ce qu'on appelle aujourd'hui un segment de droite). Il explique comment, à partir de segments de longueur α et β, on peut (facilement) construire à la règle et au compas des segments de longueur $\alpha + \beta, \alpha - \beta, \alpha\beta, \alpha/\beta$. Il explique aussi comment passer de x à $\sqrt{x}$.

En fait, partant d'un segment OA de longueur unité, on peut mener la droite portant O et A et construire la perpendiculaire en O, autrement dit, on peut considérer un système d'axes orthonormé.

LEMME III.3.1. *A partir d'un système orthonormé, on peut construire le point B de coordonnées (x, y) à la règle et au compas si et seulement si on peut construire des segments de longueurs $|x|$ et $|y|$.*

Démonstration. Ayant B on peut construire ses projections H et Q sur les axes et les segments OH et OK sont respectivement de longueur $|x|$ et $|y|$. Inversement, on peut reporter les grandeurs $|x|$ et $|y|$ sur les axes, donc obtenir H et Q et construire B (à l'intersection de perpendiculaires à chacun des axes). □

DÉFINITION III.3.2. On dit qu'un nombre réel x est *constructible* si, étant donné un système orthonormé (son origine, ses axes et l'unité), on peut construire un point à la règle et au compas dont x est une coordonnée.

Il résulte des travaux de Descartes que les nombres constructibles forment une partie de $\mathbb{R}$ qui est fermée pour les quatre opérations arithmétiques (somme, différence, produit, quotient). On dit qu'ils forment un *corps*. En outre ce corps est fermé pour la racine carrée : si x est constructible, $\sqrt{x}$ l'est aussi. En particulier, se donnant l'unité, on obtient tous les entiers, mais aussi tous les rationnels et aussi les racines carrées de rationnels, et ainsi de suite, on peut ajouter, multiplier, diviser et prendre des racines carrées de nombres constructibles pour en obtenir de nouveaux. Par exemple $\sqrt{\frac{1}{2} + \sqrt{3}}$ est constructible.

Corps quadratiques, extensions quadratiques. Étendant la notion aux complexes, on dit qu'une partie K de $\mathbb{C}$ est un *sous-corps* de $\mathbb{C}$ si elle est fermée pour les quatre opérations arithmétiques : si α et β sont dans K, alors $\alpha+\beta, \alpha-\beta, \alpha\beta$ sont dans K ainsi que α/β pour $\beta \neq 0$. On en connaît déjà trois exemples : la partie formée par l'ensemble $\mathbb{Q}$ des rationnels, la partie formée par l'ensemble $\mathbb{R}$ des réels ainsi que $\mathbb{C}$ lui-même (la partie toute entière).

On peut obtenir d'autres sous-corps par "adjonction" d'une racine carrée. Si d est un complexe, il résulte du théorème de d'Alembert [Théorème II.4.1] que l'équation $x^2 = d$ a toujours au moins une racine dans $\mathbb{C}$. Notant $\sqrt{d}$ une racine, on dit que c'est une *racine carrée de d*.

PROPOSITION III.3.3. *Soient K un sous corps de $\mathbb{C}, d \in K$ et $\sqrt{d}$ une racine carrée de d dans $\mathbb{C}$. La partie L de $\mathbb{C}$ définie par*

$$L = \{\alpha + \beta\sqrt{d} \mid \alpha \in K, \beta \in K\}$$

est un sous corps de $\mathbb{C}$ contenant K et $\sqrt{d}$.

Démonstration. — L contient K : pour $x \in K$, on a $x = \alpha + \beta\sqrt{d}$ en prenant $\alpha = x$ et $\beta = 0$.
— L contient $\sqrt{d}$: on a $\sqrt{d} = \alpha + \beta\sqrt{d}$ en prenant $\alpha = 0$ et $\beta = 1$.
— Si $\sqrt{d}$ est dans K, autrement dit si d est un carré dans K, alors $L = K$ et L est bien un sous corps de $\mathbb{C}$ contenant K.

— Si $\sqrt{d}$ n'est pas dans K, il faut vérifier que L est fermé pour les quatre opérations arithmétiques. Par exemple que l'inverse d'un élément non nul de L est dans L. C'est clair s'il s'agit d'un élément de K, considérons donc l'inverse de $\alpha + \beta\sqrt{d}$ où $\beta \neq 0$. On a

$$\frac{1}{\alpha + \beta\sqrt{d}} = \frac{\alpha - \beta\sqrt{d}}{\alpha^2 - d\beta^2} = \alpha_1 + \beta_1\sqrt{d}$$

où $\alpha_1 = \frac{\alpha}{\alpha^2 - d\beta^2}$ et $\beta_1 = \frac{-\beta}{\alpha^2 - d\beta^2}$ sont bien dans K si toutefois ces expressions ont un sens, c'est à dire si le dénominateur $\alpha^2 - d\beta^2$ n'est pas nul. Mais c'est le cas, sinon $\alpha^2 = d\beta^2$ et $d = \left(\frac{\alpha}{\beta}\right)^2$ serait un carré dans K. □

Définitions III.3.4. Soient K un sous corps de $\mathbb{C}, d$ un élément de K qui n'est pas un carré dans K et $\sqrt{d}$ une racine carrée de d dans $\mathbb{C}$. On note $K[\sqrt{d}]$ le sous corps de $\mathbb{C}$ défini par

$$K[\sqrt{d}] = \{\alpha + \beta\sqrt{d} \mid \alpha \in K, \beta \in K\}.$$

On dit que $K[\sqrt{d}]$ est une *extension quadratique de* K. On dit en particulier qu'une extension quadratique de $\mathbb{Q}$ est un *corps quadratique*.

Exemples III.3.5. Il est d'usage de noter i (plutôt que $\sqrt{-1}$) une racine carrée de (-1) dans $\mathbb{C}$. Le corps $\mathbb{C}$ des complexes n'est rien d'autre que l'extension quadratique $\mathbb{R}[i]$ des réels :

$$\mathbb{C} = \mathbb{R}[i] = \{\alpha + i\beta \mid \alpha \in \mathbb{R}, \beta \in \mathbb{R}\}.$$

On peut de même considérer le corps quadratique $\mathbb{Q}[i]$:

$$\mathbb{Q}[i] = \{\alpha + i\beta \mid \alpha \in \mathbb{Q}, \beta \in \mathbb{Q}\}.$$

On a aussi le corps quadratique $\mathbb{Q}[\sqrt{2}]$:

$$\mathbb{Q}[\sqrt{2}] = \{\alpha + \beta\sqrt{2} \mid \alpha \in \mathbb{Q}, \beta \in \mathbb{Q}\}.$$

Suite d'extensions quadratiques. On a vu que les rationnels sont des nombres constructibles. La racine carrée d'un nombre rationnel est constructible, donc les éléments un corps quadratique réel (contenu dans $\mathbb{R}$) sont constructibles. Plus généralement, comme la racine carrée d'un nombre constructible est constructible, si on a une suite de sous-corps de $\mathbb{R}$

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n$$

tels que chacun est une extension quadratique du précédent, alors les éléments de K_n sont constructibles. En fait, il s'agit d'une caractérisation des nombres constructibles :

Théorème III.3.6. *Un nombre x est constructible si et seulement si il existe une suite de sous-corps de $\mathbb{R}$:*

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n$$

tels que chacun est une extension quadratique du précédent et $x \in K_n$.

Démonstration. S'il existe une telle suite, on a vu que les éléments de K_n sont constructibles, il nous reste à montrer que si x est constructible alors il existe une telle suite. La figure dont on part est formée de l'origine O et du point A d'abcisse 1 sur l'axe des x. Leurs coordonnées sont des éléments de $\mathbb{Q}$ (en fait, 0 et 1). Supposons, par récurrence, qu'après un certain nombre de constructions (intersections de droites et de cercles), tous les points qu'on a obtenu ont leur coordonnées dans un corps $K = K_{n-1}$ obtenu par $n-1$ extensions quadratiques successives. Faisons une nouvelle construction, à partir de ces points, en distinguant les cas :

1) Intersection de deux droites. Joignant deux points A_1 et A_1' de coordonnées respectives (a_1, b_1) et (a_1', b_1'), on considère une droite d'équation

$$(x - a_1)(b_1' - b_1) - (y - b_1)(a_1' - a_1) = 0.$$

De même la droite joignant A_2 et A_2' de coordonnées (a_2, b_2) et (a_2', b_2') a pour équation

$$(x - a_2)(b_2' - b_2) - (y - b_2)(a_2' - a_2) = 0.$$

Par hypothèse les coordonnées des points donnés sont dans K_{n-1}. Trouver les coordonnées de l'intersection de ces droites revient donc à résoudre un système d'équations linéaires à coefficients dans K_{n-1} de la forme

$$\begin{cases} \alpha_1 x + \beta_1 y = \gamma_1 \\ \\ \alpha_2 x + \beta_2 y = \gamma_2 \end{cases}$$

Les solutions s'obtiennent par des opérations arithmétiques élémentaires sur les coefficients, elles sont donc encore dans $K = K_{n-1}$.

2) Intersection d'une droite et d'un cercle. Supposons construits le point Ω de coordonnées (p, q), ainsi qu'un segment de longueur r. Par hypothèse de récurrence, p, q et r sont dans K. Le cercle de centre Ω et de rayon r a pour équation

$$(x - p)^2 + (y - q)^2 - r^2 = 0.$$

Trouver les coordonnées de l'intersection de ce cercle et d'une droite passant par deux points déjà construits, c'est résoudre un système de la forme

$$\begin{cases} \alpha x + \beta y = \gamma \\ \\ x^2 + y^2 + \alpha' x + \beta' y + \gamma' = 0 \end{cases}$$

Éliminant y, on arrive à une équation quadratique $ax^2 + bx + c = 0$ où a, b et c sont dans K, car ils s'obtiennent par des opérations arithmétiques élémentaires sur les coefficients des équations de la droite et du cercle. Dire que la droite coupe le cercle, c'est dire que cette équation a des solutions réelles, donc que son discriminant $\Delta = b^2 - 4ac$ est positif. Les solutions de l'équation, à savoir $\frac{-b \pm \sqrt{\Delta}}{2a}$ appartiennent alors à l'extension quadratique $K_n = K[\sqrt{\Delta}]$ de $K = K_{n-1}$.

3) Intersection de deux cercles. Cette fois on doit résoudre le système

$$\begin{cases} x^2+y^2+\alpha x+\beta y+\gamma=0 \\ \\ x^2+y^2+\alpha' x+\beta' y+\gamma'=0 \end{cases}$$

Soustrayant les deux équations, on se ramène au problème de l'intersection d'un cercle et de la droite d'équation

$$(\alpha-\alpha')x+(\beta-\beta')y+(\gamma-\gamma')=0.$$

□

Constructions impossibles.

PROPOSITION III.3.7. *Si x est un nombre constructible et racine d'une équation cubique à coefficients rationnels, alors cette équation admet au moins une racine rationnelle.*

Démonstration. On raisonne sur une équation cubique réduite, c'est à dire qu'on suppose x racine d'un polynôme f de la forme

$$f=x^3-px-q.$$

D'après le théorème III.3.6, comme x est constructible, il existe une suite de sous-corps de $\mathbb{R}$:

$$\mathbb{Q}=K_0\subset K_1\subset\ldots\subset K_n$$

tels que chacun est une extension quadratique du précédent et $x\in K_n$. On montre que f admet au moins une racine dans K_{n-1}. On montrerait de même que f admet une racine dans K_{n-2} et ainsi de suite, jusqu'à $K_0=\mathbb{Q}$. Pour simplifier, on note $K=K_{n-1}$. Alors $K_n=K[\sqrt{d}]$ où $d\in K$ n'est pas un carré dans K et $x=\alpha+\beta\sqrt{d}$, avec α,β dans K.
— Si $\beta=0$, alors la racine $x=\alpha$ est elle même dans K.
— Si $\beta\neq 0$, montrons que $y=\alpha-\beta\sqrt{d}$ est une autre racine de l'équation. Comme x est racine de f on a

$$f(x)=(\alpha+\beta\sqrt{d})^3-p(\alpha+\beta\sqrt{d})-q=\alpha_1+\beta_1\sqrt{d}=0$$

où $\alpha_1=\alpha^3+3d\alpha\beta^2-p\alpha-q$, et $\beta_1=3\alpha^2\beta+d\beta^3-p\beta$ sont dans K. En fait $\beta_1=0$. Sinon $\alpha_1+\beta_1\sqrt{d}=0$ et $\sqrt{d}=\frac{-\alpha_1}{\beta_1}$, soit $d=\left(\frac{\alpha_1}{\beta_1}\right)^2$ et d serait un carré dans K. Mais alors on a aussi $\alpha_1=0$ (puisque $\alpha_1+\beta_1\sqrt{d}=0$). On peut donc conclure qu'on a

$$f(y)=(\alpha-\beta\sqrt{d})^3-p(\alpha-\beta\sqrt{d})-q=\alpha_1-\beta_1\sqrt{d}=0.$$

Par ailleurs, comme le polynôme f n'a pas de terme de degré 2, la somme de ses racines est nulle [Théorème III.2.2]. Dans $\mathbb{C}$, le polynôme f admet trois racines : x,y et une troisième racine z. Pour finir, on peut voir que cette troisième racine est en fait dans le corps K, en effet

$$z=-(x+y)=-\big((\alpha+\beta\sqrt{d})+(\alpha-\beta\sqrt{d})\big)=-2\alpha.$$

□

On peut maintenant conclure à l'impossibilité des constructions fameuses de l'Antiquité :

— *La trisection de l'angle* : il est par exemple impossible de réaliser la trisection des angles d'un triangle équilatéral. Donné un segment OA de longueur unité, on sait construire un triangle équilatéral de côté OA, ce qui revient, étant donné le cercle trigonométrique (de centre 0 de rayon 1), à construire la droite qui fait avec l'axe des x l'angle $\frac{\pi}{3}$. Réaliser la trisection reviendrait à construire la droite qui fait avec l'axe des x l'angle $\frac{\pi}{9}$. Les coordonnées du point correspondant sur le cercle, soient $\cos(\frac{\pi}{9}), \sin(\frac{\pi}{9})$, seraient alors des nombres constructibles. On rappelle la relation

$$\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta).$$

Comme $\cos(\frac{\pi}{3}) = \frac{1}{2}$, on voit que $\cos(\frac{\pi}{9})$ est racine de l'équation cubique

$$8x^3 - 6x - 1 = 0.$$

Posons $\xi = 2\cos(\frac{\pi}{9}), \xi$ est racine du polynôme

$$f = x^3 - 3x - 1.$$

Si ξ était constructible, f devrait avoir une racine rationnelle, mais il résulte de la proposition III.2.4 que ce n'est pas le cas (il suffit de vérifier que ni 1 ni -1 ne sont racines de f).

— *La duplication du cube* : si la duplication du cube était possible, le nombre $\sqrt[3]{2}$ serait constructible. Le polynôme $x^3 - 2$ devrait alors avoir une racine rationnelle. On a vu que ce n'était pas le cas [Exemple III.2.5].

— *La quadrature du cercle* : C'est à Pierre-Laurent Wantzel qu'on doit d'avoir montré l'impossibilité de la trisection de l'angle et de la duplication du cube dans la "Recherche sur les moyens de reconnaître si un problème de géométrie peut se résoudre à la règle et au compas" publiée en 1837. L'impossibilité de la quadrature du cercle est plus difficile. Donné un cercle de rayon 1, il faut construire un carré de même aire donc de côté $\sqrt{\pi}$. Cela revient à dire que $\sqrt{\pi}$ est un nombre constructible. Si c'était le cas, π serait également constructible. Johann Heinrich Lambert (1728-1777), collègue d'Euler et Lagrange à l'académie des sciences de Berlin, avait montré que π n'est pas un nombre rationnel, ni la racine carrée d'un nombre rationnel. En fait π n'est pas d'avantage une racine carrée de racine carrée ni une racine cubique, ni même la racine d'aucune équation algébrique à coefficients rationnels, on dit que c'est un *nombre transcendant*. Ce résultat à été établi par Ferdinand von Lindemann (1852-1939) en 1882. On peut en déduire que π n'est pas constructible et mettre ainsi fin à une quête de près de 25 siècles!

CHAPITRE IV

Géométrie (Notes de cours)

IV.1. Courbes du plan

Trois systèmes de représentations pour une courbe dans le plan.

- Représentation paramétrique :

$$\begin{cases} x = & f(t) \\ y = & g(t) \end{cases}$$

- Équation polaire :

$$r = f(\theta)$$

- Equation implicite :

$$\Phi(x, y) = 0.$$

On a les relations $\begin{cases} x = & r\cos(\theta) \\ y = & r\sin\theta) \end{cases}$ et inversement $\begin{cases} r^2 = & x^2 + y^2 \\ \theta = & \arctan(\frac{y}{x}) \end{cases}$

IV.2. Droites du plan

La droite passant par $A = (a, b)$ de vecteur directeur $\vec{V} = (\alpha, \beta)$ admet pour représentation paramétrique

$$\begin{cases} x = & a + t\alpha \\ y = & b + t\beta \end{cases}$$

Donc, pour la droite joignant deux points $A = (a, b)$ et $A' = (a', b')$,

$$\begin{cases} x = & a + t(a' - a) \\ y = & b + t(b' - b) \end{cases}$$

On obtient les équations implicites

$$x(b' - b) + y(a - a') + b(a' - a)a(b - b') = 0$$

ou

$$\beta x - \alpha y + (\alpha b - \beta a) = 0.$$

IV.3. Le cercle

Le cercle de centre $A = (a, b)$ de rayon R est l'ensemble des points $P = (x, y)$ tels que $AP = R$, soit

$$(x - a)^2 + (y - b)^2 = R^2.$$

Il a donc pour équation implicite

$$x^2 + y^2 - 2ax - 2by + a^2 + b^2 - R^2 = 0 \tag{IV.3.1}$$

Puissance d'un point par rapport un cercle.

PROPOSITION IV.3.1. *Si une droite passant par un point P coupe un cercle $\mathcal{C}$ en deux points A et B le produit algébrique $\overline{PA}.\overline{PB}$ ne dépend pas de cette droite : on a toujours*

$$\overline{PA}.\overline{PB} = d^2 - R^2$$

où d est la distance de P au centre du cercle, R le rayon.

Le produit (constant) $\overline{PA}.\overline{PB}$ s'appelle *puissance de P par rapport à $\mathcal{C}$.*

COROLLAIRE IV.3.2. *La puissance de P par rapport à un cercle s'obtient en reportant les coordonnées de P dans l'équation (IV.3.1) du cercle.*

IV.4. Droites et sphères dans l'espace

La droite passant par $A = (a, b, c)$ de vecteur directeur $\vec{V} = (\alpha, \beta, \gamma)$ admet pour représentation paramétrique

$$\begin{cases} x = & a + t\alpha \\ y = & b + t\beta \\ z = & c + t\gamma \end{cases}$$

Donc, pour la droite joignant deux points $A = (a, b, c)$ et $A' = (a', b', c')$,

$$\begin{cases} x = & a + t(a' - a) \\ y = & b + t(b' - b) \\ z = & c + t(c' - c) \end{cases}$$

Mais attention , une équation implicite de la forme

$$ax + by + cz + d = 0$$

ne représente pas une droite mais un plan.

La sphère de centre $A = (a, b, c)$ de rayon R a pour équation

$$(x - a)^2 + (y - b)^2 + (z - c)^2 = R^2.$$

ou encore

$$x^2 + y^2 + z^2 - 2ax - 2by - 2cz + a^2 + b^2 + c^2 - R^2 = 0.$$