UNIVERSITE DE BRETAGNE OCCIDENTALE
Département de Mathématiques

Année universitaire 2003-2004
DEUG MIAS-MASS 1ère année
ALG 11F - M11
Septembre 2003

Cours d'algèbre

P. Cardaliaguet

Table des matières

Notations

Dans toute la suite, nous utilions les notations suivantes :

- $\mathbb{N}$ désigne l'ensemble des entiers naturels, $\mathbb{N}^*$ l'ensembles des entiers naturels non nuls,
- $\mathbb{Z}$ désigne l'ensemble des entiers relatifs, $\mathbb{Z}^*$ l'ensembles des entiers relatifs non nuls,
- $\mathbb{Q}$ désigne l'ensemble des rationnels, $\mathbb{Q}^*$ l'ensembles des rationnels non nuls,
- $\mathbb{R}$ désigne l'ensemble des réels, $\mathbb{R}^*$ l'ensembles des réels non nuls,
- $\mathbb{C}$ désigne l'ensemble des nombres complexes, $\mathbb{C}^*$ l'ensembles des nombres complexes non nuls,
- $\mathbb{R}[X]$ désigne l'ensemble des polynômes à coefficients réels,
- $\mathbb{C}[X]$ désigne l'ensemble des polynômes à coefficients complexes.

1 Les nombres complexes

1.1 Définitions élémentaires

Vocabulaire et notations :

1. On appelle **nombre complexe** toute expression de la forme $x+iy$, où x et y sont des réels. Dans toute la suite, les nombres complexes seront le plus souvent désignés par la lettre z.
2. Si $z = x + iy$ est un nombre complexe, on appelle
   - la **partie réelle** de z, noté $\mathcal{R}e(z)$, le nombre réel x :
   $$\text{si } z = x + iy \quad \text{alors} \quad \mathcal{R}e(z) = x \ .$$
   - la **partie imaginaire** de z, noté $\mathcal{I}m(z)$, le nombre réel y :
   $$\text{si } z = x + iy \quad \text{alors} \quad \mathcal{I}m(z) = y \ .$$
3. On dit qu'un nombre complexe $z = x + iy$ est nul si $x = y = 0$.
4. On dit que deux nombres complexes $z = x + iy$ et $z' = x' + iy'$ sont égaux si leurs parties réelles et leurs parties imaginaires sont égales :
   $$z = z' \qquad \Leftrightarrow \qquad x = x' \text{ et } y = y'$$
5. Un nombre complexe est **imaginaire pur** si sa partie réelle est nulle. On note alors $z = iy$ au lieu de $z = 0 + iy$.
6. Un nombre complexe est dit **réel** si sa partie imaginaire est nulle. On note alors $z = x$ au lieu de $z = x + i0$.
7. L'ensemble des nombres complexes est noté $\mathbb{C}$.

Remarque importante : Contrairement à l'ensemble des réels, dans lequel deux éléments se comparent, il n'y a pas d'ordre naturel sur $\mathbb{C}$. On ne comparera donc **jamais** deux nombres complexes. On dit que $\mathbb{C}$ n'est pas ordonné.

Dans $\mathbb{C}$ on définit les opérations suivantes :

1. **Addition :** Si $z = x + iy$ et $z' = x' + iy'$ sont deux nombres complexes, la somme $z + z'$ est le nombre complexe défini par

$$z + z' = (x + x') + i(y + y')$$

2. **Produit :** Si $z = x + iy$ et $z' = x' + iy'$ sont deux nombres complexes, le produit $z.z'$ est le nombre complexe défini par

$$(*) \qquad z.z' = (xx' - yy') + i(xy' + x'y)$$

Remarque : Notons d'abord que, si $z = z' = i$, alors on obtient $i^2 = i.i = -1$. Un moyen mnémotechnique pour se souvenir de la formule $(*)$ est le suivant : il suffit de développer formellement le produit $(x + iy)(x' + iy')$ (nous verrons plus loin que ce calcul est légitime) :

$$(x + iy)(x' + iy') = xx' + iyx' + ixy' + i^2yy'$$

ce qui donne le résultat annoncé compte tenu de l'égalité $i^2 = -1$.

Voici quelques propriétés élémentaires de l'addition :

Proposition 1.1 *Supposons que z, z' et z'' sont des nombres complexes. Alors*

1. **Associativité :** $z + (z' + z'') = (z + z') + z''$
2. **Commutativité :** $z + z' = z' + z$
3. **Existence d'un élément neutre :** 0 *est l'élément neutre pour l'addition :* $0+z = z+0 = z$.
4. **Existence d'un opposé :** *si $z = x + iy$, alors le nombre complexe $(-z) = (-x) + i(-y)$ vérifie :* $z + (-z) = (-z) + z = 0$.

Ces résultats sont de simples applications de résultats symétriques dans $\mathbb{R}$. Nous ne les démontrerons donc pas.

Dans la suite, on notera $-z = -x - iy$ au lieu de $-z = (-x) + i(-y)$.

Nous énonçons maintenant les propriétés élémentaires du produit :

Proposition 1.2 *Supposons que z, z' et z'' sont des nombres complexes.*

1. **Associativité :** $z.(z'.z'') = (z.z').z''$
2. **Commutativité :** $z.z' = z'.z$
3. **Distributivité :** $(z + z').z'' = z.z'' + z'.z''$
4. **Existence d'un élément neutre :** *le nombre complexe* 1 *est l'élément neutre pour le produit :* $1.z = z.1 = z$.
5. **Existence d'un inverse :** *tout nombre complexe* **non nul** z *admet un inverse pour le produit, noté* $\frac{1}{z}$.
6. 0 **est un élément absorbant :** $0.z = z.0 = 0$.

Preuve : Nous nous contentons de démontrer l'existence d'un inverse, le reste étant immédiat. Soit $z = x + iy$ un complexe non nul. On prétend que le complexe $z' = x' + iy'$ avec

$$x' = x/(x^2 + y^2) \text{ et } y' = -y/(x^2 + y^2)$$

est un inverse de z. En effet,

$$\begin{aligned} z.z' &= (xx' - yy') + i(xy' + yx') \\ &= (x^2/(x^2 + y^2) + y^2/(x^2 + y^2)) + i(xy/(x^2 + y^2) - xy/(x^2 + y^2)) = 1 \ . \end{aligned}$$

Montrons maintenant qu'un tel inverse est unique. Si z_1 et z_2 sont deux inverses de z, alors on a $z.z_1 = 1$, ce qui entraîne, en multipliant par z_2 à gauche, que

$$z_2 = z_2.1 = z_2.(z.z_1) = (z_2.z).z_1 = 1.z_1 = z_1 \ .$$

Donc l'inverse est unique.

QED

Un conséquence très importante de l'existence d'un inverse est la suivante :

Corollaire 1.3 *Si z et z' sont deux nombres complexes, et si $z.z' = 0$ alors soit $z = 0$ soit $z' = 0$.*

On dit que $\mathbb{C}$ est intègre.

Preuve : Il suffit de supposer par exemple que z est non nul, et de multiplier l'égalité $z.z' = 0$ par $1/z$, ce qui donne $z' = 0$. Donc soit $z = 0$, soit $z' = 0$.

QED

1.2 Conjugué d'un nombre complexe

Définition 1.4 *Soit $z = x+iy$ un nombre complexe. On appelle conjugué de z le nombre complexe noté $\bar{z}$ de même partie réelle que z et de partie imaginaire opposée :*

$$\text{si } z = x + iy, \quad \text{alors} \quad \bar{z} = x - iy$$

Rappelons que, par convention, $x - iy = x + i(-y)$.

Proposition 1.5 *Soient z et z' deux nombres complexes. Alors*

1. $\overline{\bar{z}} = z$
2. $\overline{z + z'} = \bar{z} + \bar{z'}$
3. $\overline{z.z'} = \bar{z}.\bar{z'}$
4. *z est réel si et seulement si $z = \bar{z}$*
5. *z est imaginaire pur si et seulement si $\bar{z} = -z$.*
6. $\mathcal{R}e(z) = \frac{z+\bar{z}}{2}$ *et* $\mathcal{I}m(z) = \frac{z-\bar{z}}{2i}$.

Preuve : La première assertion est évidente.
Montrons la troisième. Si $z = x + iy$ et $z' = x' + iy'$, alors

$$\overline{z.z'} = \overline{xx' - yy' + i(xy' + yx')} = xx' - yy' - i(xy' + yx') \ ,$$

tandis que

$$\bar{z}.\bar{z'} = (x - iy)(x' - iy') = xx' - yy' - i(xy' + yx') \ ,$$

d'où l'égalité annoncée.
Nous laissons les assertions suivantes en exercice.

QED

1.3 Module d'un nombre complexe

Définition 1.6 *Soit $z = x + iy$ un nombre complexe. Le module de z est le réel, noté $|z|$, défini par*

$$|z| = \sqrt{x^2 + y^2}\ .$$

Proposition 1.7 *Soient z et z' deux nombres complexes. Alors*

1. *$|z| \geq 0$ et on a l'équivalence : $|z| = 0$ si et seulement si $z = 0$.*
2. *$|z|^2 = z.\bar{z}$ et, si $z \neq 0$, $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$*
3. *$|z.z'| = |z|\,|z'|$*
4. *$|-z| = |z|$, $|\bar{z}| = |z|$ et, si $z \neq 0$, $\left|\frac{1}{z}\right| = \frac{1}{|z|}$.*
5. *$|\mathcal{R}e(z)| \leq |z|$ et $|\mathcal{I}m(z)| \leq |z|$*
6. *(Inégalité triangulaire) $|z + z'| \leq |z| + |z'|$*
7. *$||z| - |z'|| \leq |z - z'|$*

Preuve : Dans toute la preuve on note $z = x + iy$ et $z' = x' + iy'$.

1. Comme $|z| = \sqrt{x^2 + y^2}$ et que, par définition, une racine est positive, $|z| \geq 0$.
   Si $z = 0$ alors il est clair que $|z| = \sqrt{0^2 + 0^2} = 0$. Réciproquement, si $|z| = 0$, alors on a $x^2 + y^2 = 0$. La somme du réel positif x^2 et du réel positif y^2 étant égale à zéro, on en déduit que $x = y = 0$. Donc $z = 0$.
2. $z.\bar{z} = (x + iy).(x - iy) = x^2 - i^2y^2 = x^2 + y^2 = |z|^2$.
3. On a, d'une part,
   $$|z.z'|^2 = (xx' - yy')^2 + (xy' + yx')^2 = x^2(x')^2 + y^2(y')^2 + x^2(y')^2 + y^2(x')^2$$
   car les termes croisés se simplifient. D'autre part, on a
   $$(|z|\,|z'|)^2 = (x^2 + y^2)((x')^2 + (y')^2) = x^2(x')^2 + y^2(y')^2 + x^2(y')^2 + y^2(x')^2\ .$$
   D'où l'égalité désirée.
4. Laissé au lecteur en exercice
5. idem
6. On a
   $$\begin{aligned} |z + z'|^2 &= (z + z').(\overline{z + z'}) \\ &= (z + z').(\bar{z} + \bar{z'}) \\ &= z.\bar{z} + z.\bar{z'} + \bar{z}.z' + z'.\bar{z'} \\ &= |z|^2 + 2\mathcal{R}e(z\bar{z'}) + |z'|^2 \\ &\leq |z|^2 + 2|\mathcal{R}e(z\bar{z'})| + |z'|^2 \end{aligned}$$
   car $z.\bar{z'} + \bar{z}.z' = z.\bar{z'} + \overline{z.\bar{z'}}$. Or
   $$|\mathcal{R}e(z\bar{z'})| \leq |z\bar{z'}| = |z||\bar{z'}| = |z||z'|\ .$$
   Donc
   $$|z + z'|^2 \leq |z|^2 + 2|z||z'| + |z'|^2 = (|z| + |z'|)^2\ ,$$
   ce qui donne l'inégalité demandée.

7. On a $|z| = |(z-z')+z'| \leq |z-z'|+|z'|$ d'après l'inégalité triangulaire. Donc $|z|-|z'| \leq |z-z'|$. En inversant les rôles de z et z', on obtient de même que $|z'| - |z| \leq |z - z'|$. Ces deux inégalités impliquent le résultat désiré : $||z| - |z'|| \leq |z - z'|$.

QED

Notation : On note $\mathbf{U}$ l'ensemble des complexes z de module 1.

Exercice 1.7.1 Montrer que $\mathbf{U}$ vérifie :
i) si z et z' appartiennent à $\mathbf{U}$, alors $z.z'$ aussi,
ii) si z appartient à $\mathbf{U}$, alors $z \neq 0$ et $1/z$ appartient aussi à $\mathbf{U}$.

On dit que $\mathbf{U}$ est un groupe.

Exercice 1.7.2 Montrer que, si $z \in \mathbb{C}$ avec $z \neq 0$, alors $z/|z|$ appartient à $\mathbf{U}$.

Preuve : En effet, $|\, z/|z|\,| = |z|/|z| = 1$. Donc $z/|z|$ appartient à $\mathbf{U}$.

1.4 Argument d'un nombre complexe

Définition 1.8 (Exponentielle complexe) *Pour tout nombre réel t, on note*

$$e^{it} = \cos(t) + i\sin(t) \ .$$

Remarque : L'application ainsi définie est *a priori* une application de $\mathbb{R}$ dans $\mathbb{C}$.

Proposition 1.9 *Soient z et z' deux nombres complexes. Alors, pour tout $t \in \mathbb{R}$, on a :*

1. *e^{it} appartient à $\mathbf{U}$.*
2. *$\dfrac{1}{e^{it}} = \overline{e^{it}} = e^{-it}$*
3. *$e^{it} = 1$ si et seulement si il existe un entier relatif k tel que $t = 2k\pi$.*
4. *pour tout réel t', $e^{i(t+t')} = e^{it}.e^{it'}$*
5. **Formules de Moivre :** *pour tout entier relatif n, on a $(e^{it})^n = e^{int}$*

Remarques : 1) Les propriétés précédentes expliquent, par analogie avec les propriétés de l'exponentielle dans $\mathbb{R}$, la notation e^{it}.
2) Les deux relations suivantes, très souvent utiles, sont appelées **formules d'Euler** :

$$\forall t \in \mathbb{R},\ \cos(t) = \frac{e^{it} + e^{-it}}{2} \text{ et } \sin(t) = \frac{e^{it} - e^{-it}}{2i} \ .$$

Preuve de la proposition 1.9 : C'est une application directe des formules de trigonométrie.

1. $|e^{it}| = \sqrt{\cos^2(t) + \sin^2(t)} = \sqrt{1} = 1$.
2. Notons d'abord que $e^{-it} = \cos(-t) + i\sin(-t) = \cos(t) - i\sin(t) = \overline{e^{it}}$ car $\cos(-t) = \cos(t)$ et $\sin(-t) = -\sin(t)$. Montrons maintenant que $e^{it}.e^{-it} = 1$, ce qui prouvera que $e^{-it} = 1/e^{it}$. En effet, $e^{it}.e^{-it} = e^{it}\overline{e^{it}} = |e^{it}|^2 = 1^2 = 1$.
3. $e^{it} = 1$ équivaut à $\cos(t) = 1$ et $\sin(t) = 0$. Or il est bien connu que, si $\cos(t) = 1$ et $\sin(t) = 0$, alors $t = 0$ modulo 2π, c'est-à-dire qu'il existe un entier relatif k tel que $t = 2k\pi$.

4. Calculons $e^{it}.e^{it'}$:

$$\begin{aligned} e^{it}.e^{it'} &= (\cos(t)\cos(t') - \sin(t)\sin(t')) + i(\cos(t)\sin(t') + \sin(t)\cos(t')) \\ &= \cos(t+t') + i\sin(t+t') = e^{i(t+t')} \ . \end{aligned}$$

5. Cela se démontre par récurrence, en utilisant le résultat précédent.

QED

Théorème 1.10 (Admis) *Pour tout nombre complexe z appartenant à $\mathbf{U}$, il existe un réel t tel que*

$$z = e^{it}$$

Autrement dit, l'application exponentielle, définie de $\mathbb{R}$ dans $\mathbf{U}$ est **surjective**.

Définition 1.11 *Soit z un nombre complexe non nul. On appelle argument de z tout réel t tel que*

$$\frac{z}{|z|} = e^{it} \ .$$

Remarque : Cette définition a bien un sens car nous avons vu dans un exercice ci-dessus que $z/|z|$ appartient à $\mathbf{U}$.

Forme trigonométrique : On dit qu'un nombre complexe non nul z est mis sous forme trigonométrique si on écrit z sous la forme : $z = |z|e^{it}$, avec t un argument de z. La forme $z = x + iy$ s'appelle la **forme algébrique**.

Proposition 1.12 *Soient z un complexe non nul et t un argument de z. Alors un réel t' est un argument de z si et seulement s'il existe un entier relatif k tel que*

$$t' = t + 2k\pi \ .$$

Remarque : On dit alors que $t' = t$ modulo 2π. Ce qui est noté : $t' = t \ (mod\ 2\pi)$.

Preuve : Supposons d'abord que t' soit un argument de z. Alors, par définition de l'argument, on a

$$\frac{z}{|z|} = e^{it} = e^{it'} \ .$$

En divisant cette égalité par e^{it}, on obtient $1 = e^{i(t'-t)}$. Cette égalité implique l'existence d'un entier relatif k tel que $t' = t + 2k\pi$ (cf. la proposition 1.9).

Réciproquement, s'il existe un entier relatif k tel que $t' = t + 2k\pi$, alors

$$e^{it'} = e^{it} = \frac{z}{|z|} \ ,$$

et t' est un argument de z.

QED

Notation : Pour tout complexe non nul z, on note $arg(z)$ n'importe quel argument de z.

Proposition 1.13 *Soient z et z' deux nombres complexes non nuls. Alors*

1. $arg(-z) = \pi + arg(z) \ (mod\ 2\pi)$ *et* $arg(\bar{z}) = -arg(z) \ (mod\ 2\pi)$,
2. $arg(1/z) = -arg(z) \ (mod\ 2\pi)$,

3. $arg(z.z') = arg(z) + arg(z')$ *(mod* 2π*)*

Attention à la façon de lire ces égalités : l'égalité $arg(-z) = \pi + arg(z)$ signifie : pour tout t argument de $-z$ et pour tout t' argument de z, on a l'égalité suivante : $t = \pi + t'$ (mod 2π), c'est-à-dire qu'il existe un entier $k \in \mathbb{Z}$ avec $t = \pi + t' + 2k\pi$.

Preuve :

1. Soit t un argument de $-z$ et t' un argument de z. Montrons que $t = \pi + t'$ (mod 2π). En effet, par définition de l'argument, on a :

$$e^{it} = \frac{-z}{|-z|} = -\frac{z}{|z|} = -e^{it'} = e^{i(t'+\pi)} .$$

Donc $t' = t + \pi$ (mod 2π) (cf. Proposition 1.9, 3).

Montrons que $arg(\bar{z}) = -arg(z)$ (mod 2π). Soit t un argument de $\bar{z}$ et t' un argument de z. Alors

$$e^{it} = \frac{\bar{z}}{|\bar{z}|} = \overline{\left(\frac{z}{|z|}\right)} = \overline{e^{it'}} = e^{-it'}$$

(on a utilisé le fait que $|\bar{z}| = |z|$). Donc $t = -t'$ (mod 2π).

2. Soit t un argument de $1/z$ et t' un argument de z. Alors

$$e^{it} = \frac{1/z}{|1/z|} = \frac{1/z}{1/|z|} = \frac{1}{z/|z|} = \frac{1}{e^{it'}} = e^{-it'}$$

(on a utilisé le fait que $|1/z| = 1/|z|$). Donc $t = -t'$ (mod 2π).

3. Soient t un argument de z, t' un argument de z' et t" un argument de $z.z'$. On a alors

$$e^{it"} = \frac{z.z'}{|z.z'|} = \frac{z}{|z|}.\frac{z'}{|z'|} = e^{it}.e^{it'} = e^{i(t+t')}$$

(on a utilisé le fait que $|z.z'| = |z|\,|z'|$). Donc $t" = t + t'$ (mod 2π).

QED

1.5 Racines $n$ièmes d'un nombre complexe

Dans toute cette partie, n désigne un entier naturel non nul.

Définition 1.14 *On dit qu'un nombre complexe z est une racine nième de l'unité (ou de 1) si* $z^n = 1$.

Exemple : Le nombre complexe i est racine quatrième de l'unité car $i^4 = (-1)^2 = 1$.

Théorème 1.15 *Il y a exactement n racines nièmes de l'unité. Ce sont les nombres complexes de la forme*

$$z_k = e^{\frac{2ik\pi}{n}} \qquad \text{où } k \in \{0, \ldots, n-1\} .$$

Preuve : D'abord il est clair que les z_k définis ci-dessus sont des racines $n$ièmes de l'unité. En effet,

$$z_k^n = \left(e^{\frac{2ik\pi}{n}}\right)^n = e^{2ik\pi} = 1 .$$

Notons de plus que, si $0 \leq k, k' \leq n-1$, avec $k \neq k'$, alors $z_k \neq z_{k'}$. Il y a donc au moins n racines distinctes de l'unité.

Réciproquement, supposons qu'un nombre complexe z soit racine $n$ième de l'unité. Montrons d'abord que z appartient à $\mathbf{U}$. En effet, on a

$$1 = |z^n| = |z|^n \ .$$

Or le module est un nombre réel positif. Donc $|z| = 1$, i.e., $z \in \mathbf{U}$.

Comme $z \in \mathbf{U}$, il existe un nombre réel t tel que $z = e^{it}$. Choisissons un entier k' tel que $t + 2k'\pi$ soit positif. Notons que $t' = t + 2k'\pi$ est un argument de z. Comme z est racine $n$ième de l'unité, on a : $z^n = 1 = e^{int'}$. On déduit de la proposition 1.9 qu'il existe un entier relatif k tel que

$$nt' = 2k\pi \ .$$

Par conséquent, comme $n \neq 0$, cela donne $t' = \frac{2k\pi}{n}$. Comme t' est positif, k l'est aussi. Effectuons la division euclidienne de k par n : il existe deux entiers naturels p et r, tels que $r \in \{0, \ldots, n-1\}$ et $k = pn + r$. Alors, comme $t' = 2p\pi + \frac{2r\pi}{n}$ est un argument de z, on déduit de la proposition 1.12 que $\frac{2r\pi}{n}$ est un argument de z. D'où $z = e^{\frac{2ir\pi}{n}}$ avec $r \in \{0, \ldots, n-1\}$, ce qui est bien le résultat désiré.

QED

Définition 1.16 *Soit a un nombre complexe non nul. On dit qu'un nombre complexe z est une racine nième de a si $z^n = a$.*

Remarque : Dans le cas $n = 2$ on parle de "racine carrée" ou même simplement de "racine" de a. Par contre, on n'écrit **jamais** cette racine sous la forme $\sqrt{a}$ ni $a^{\frac{1}{2}}$. En effet, comme dans $\mathbb{R}$, il y a toujours 2 nombres complexes vérifiant $z^2 = a$, mais, contrairement à $\mathbb{R}$, il n'y a aucun moyen de choisir de façon naturelle une de ces racines (rappelons que, si $a \in \mathbb{R}$, $\sqrt{a}$ désigne la racine positive).

Corollaire 1.17 *Pour tout nombre complexe non nul a il existe exactement n racines nièmes de a. Ce sont les nombres complexes de la forme*

$$z_k = |a|^{1/n} e^{\frac{it+2ik\pi}{n}} \qquad \text{où } k \in \{0, \ldots, n-1\} \ ,$$

et où t désigne un argument de a.

Remarque : Dans le cas des racines carrées, si δ est une racine de $a \neq 0$ alors l'autre racine est $-a$.

Preuve : Il est aisé de voir que, si $z_k = |a|^{1/n} e^{\frac{it+2ik\pi}{n}}$ avec $k \in \{0, \ldots, n-1\}$, alors z_k est une racine $n$ième de a.

Réciproquement, supposons que z soit une racine $n$ième de a. Alors le nombre complexe $ze^{-it/n}/|a|^{\frac{1}{n}}$ est une racine $n$ième de l'unité, car

$$\left(\frac{ze^{-it/n}}{|a|^{\frac{1}{n}}}\right)^n = \frac{z^n e^{-it}}{|a|} = \frac{ae^{-it}}{|a|} = \frac{|a|e^{it}e^{-it}}{|a|} = 1 \ ,$$

car $a = |a|e^{it}$ (forme trigonométrique). Donc, d'après le théorème 1.15, il existe un entier $k \in \{0, \ldots, n-1\}$ tel que

$$\frac{ze^{-it/n}}{|a|^{\frac{1}{n}}} = e^{\frac{ik\pi}{n}} \ .$$

En multipliant l'égalité par $e^{it/n}|a|^{\frac{1}{n}}$, on obtient que z se met sous la forme désirée :

$$z = |a|^{1/n} e^{\frac{it+2ik\pi}{n}} \qquad \text{où } k \in \{0, \ldots, n-1\} \ .$$

QED

1.6 Equation du second degré dans $\mathbb{C}$

On considère une équation du second degré dans $\mathbb{C}$:

$$(*) \qquad az^2 + bz + c = 0$$

où a, b et c sont des nombres complexes donnés, et z est l'inconnue. On suppose que $a \neq 0$, de sorte que l'équation est vraiment du second degré.

Théorème 1.18 *Soit $\Delta = b^2 - 4ac$. Alors*

- *si $\Delta \neq 0$, alors l'équation (*) admet exactement deux solutions distinctes z_1 et z_2 avec*

$$z_1 = \frac{-b + \delta_1}{2a} \text{ et } z_2 = \frac{-b + \delta_2}{2a} ,$$

  où δ_1 et δ_2 sont les deux racines carrées du nombre complexe Δ.

- *si $\Delta = 0$, alors l'équation admet une solution unique $z = \frac{-b}{2a}$.*

Remarque : Rappelons que $\delta_2 = -\delta_1$.

Preuve : Montrons d'abord qu'un nombre complexe z est solution de (*) si et seulement si $2az + b$ est une racine carrée de Δ.

En effet, si z est solution de (*), alors

$$(2az + b)^2 = 4a^2z^2 + 4abz + b^2 = 4a(az^2 + bz) + b^2 = 4a(-c) + b^2 = \Delta .$$

Réciproquement, si $2az + b$ est une racine carrée de Δ, alors

$$(2az + b)^2 = 4a^2z^2 + 4abz + b^2 = b^2 - 4ac ,$$

ce qui implique, en simplifiant d'abord par b^2 puis en divisant par $4a$, que

$$az^2 + bz + c = 0 .$$

Donc z est bien solution de (*).

Supposons maintenant que $\Delta \neq 0$. Alors il existe deux racinces distinctes de Δ, notées respectivement δ_1 et δ_2. Un nombre complexe z est alors solution de (*) si et seulement si $2az + b$ est une racine carrée de Δ, i.e., si et seulement si $2az + b = \delta_j$ (avec $j = 1$ ou $j = 2$). En soustrayant b à cette égalité, puis en divisant par $2a$ on obtient le résultat annoncé.

Si au contraire $\Delta = 0$, alors la seule racine carrée de Δ est 0. Donc un nombre complexe z est solution de (*) si et seulement si $2az + b$ est nul. Ce qui donne bien une seule solution $z = -b/2a$.

QED

Exercice 1.18.1 Si a, b et c sont des réels, alors les solutions z_1 et z_2 sont conjuguées : $z_2 = \overline{z_1}$.

1.7 Interprétation géométrique des nombres complexes

1.7.1 Généralités

Dans toute la suite, on considère le plan $\mathcal{P}$ orienté muni d'une base orthonormée directe $(O, \vec{\imath}, \vec{\jmath})$.

Définition 1.19 *Soit $z = x + iy$ un nombre complexe.*

- Le point d'affixe z est le point M du plan de coordonnées (x, y).

- Le vecteur d'affixe z est le vecteur $\vec{v}$ de coordonnées (x, y).

Réciproquement,

- A tout point M du plan, de coordonnées (x, y), on peut associer le nombre complexe $z = x+iy$. Le point M a alors pour affixe z.

- De même, à tout vecteur $\vec{v}$ de coordonnées (x, y), on peut associer le nombre complexe $z = x + iy$. Le vecteur $\vec{v}$ a alors pour affixe z.

Interprétation de la somme de nombres complexes :

- Si le vecteur $\vec{v}_1$ a pour affixe z_1 et le vecteur $\vec{v}_2$ a pour affixe z_2, alors le vecteur $\vec{v}_1 + \vec{v}_2$ a pour affixe $z_1 + z_2$.
- Si le point M_1 a pour affixe z_1 et le point M_2 a pour affixe z_2, alors le vecteur $\overrightarrow{M_1M_2}$ a pour affixe $z_2 - z_1$.

La preuve de ces assertions est immédiate.

Interprétation du module d'un nombre complexe :

- Soit M le point d'affixe z. Alors $|z| = |OM|$ (où $|OM|$ signifie la distance de O à M).
- Si le point M_1 a pour affixe z_1 et le point M_2 a pour affixe z_2, alors $|z_2 - z_1| = |M_1M_2|$.

Interprétation de l'argument d'un nombre complexe :

- Si le vecteur $\vec{v}$, non nul, a pour affixe le nombre complexe z, alors $arg(z) = (\widehat{\vec{i}, \vec{v}}) \pmod{2\pi}$ (où $(\widehat{\vec{i}, \vec{v}})$ est une mesure de l'angle orienté entre $\vec{i}$ et $\vec{v}$).
- Si les vecteurs non nuls $\vec{v}_1$ et $\vec{v}_2$ ont pour affixe respective les nombres complexes z_1 et z_2, alors
$$(\widehat{\vec{v}_1, \vec{v}_2}) = arg(z_2) - arg(z_1) \qquad (\text{mod } 2\pi)$$
et
$$(\widehat{\vec{v}_1, \vec{v}_2}) = arg\left(\frac{z_2}{z_1}\right) \qquad (\text{mod } 2\pi)\ .$$
- Soit M le point d'affixe z. Alors $arg(z) = (\widehat{\vec{i}, \vec{v}})$ avec $\vec{v} = \overrightarrow{OM}$.

1.7.2 Exemples d'applications des nombres complexes à la géométrie plane

Exemple 1.20 (Points alignés) Soient M_1, M_2 et M_3 trois points distincts du plan, d'affixe respective z_1, z_2 et z_3. Les points M_1, M_2 et M_3 sont alignés si et seulement si l'expression suivante : $\frac{z_2-z_1}{z_3-z_1}$ est un réel.

En effet, les points M_1, M_2 et M_3 sont alignés si et seulement si l'angle $(\widehat{\vec{v}_1, \vec{v}_2})$, avec $\vec{v}_1 = \overrightarrow{M_1M_2}$ et $\vec{v}_2 = \overrightarrow{M_1M_3}$, vaut 0 ou π (à $2k\pi$ près). Or cet angle a pour expression

$$(\widehat{\vec{v}_1, \vec{v}_2}) = arg\left(\frac{z_2 - z_1}{z_3 - z_1}\right)\ .$$

Or l'argument du nombre complexe $\frac{z_2-z_1}{z_3-z_1}$ est 0 ou π si et seulement si ce nombre un réel.

En conclusion, les points M_1, M_2 et M_3 sont alignés si et seulement si nombre complexe $\frac{z_2-z_1}{z_3-z_1}$ est un réel.

Exemple 1.21 (Translation) A toute translation du plan de vecteur $\vec{v}$, on peut associer de façon biunivoque un nombre complexe a, l'affixe de $\vec{v}$.

L'image par la translation de vecteur $\vec{v}$ d'un point M d'affixe z est alors le point M' d'affixe $z + a$.

Preuve : Exercice.

Exemple 1.22 (Similitudes) A toute similitude plane $S(O, k, \alpha)$ de centre O, de rapport $k > 0$ et d'angle α, on peut associer de façon biunivoque l'unique nombre complexe $ke^{i\alpha}$.

L'image par la similitude $S(O, k, \alpha)$ d'un point M d'affixe z est alors le point M' d'affixe $ke^{i\alpha}z$.

Preuve : Exercice.

Exemple 1.23 (Equation d'un cercle) Soient un point A d'affixe a et un rayon $r > 0$. Alors le cercle de centre A et de rayon r est l'ensemble des points M d'affixe z avec $|z - a| = r$.

Preuve : Exercice.

Exemple 1.24 (Droites et cercles) Soient a et b deux nombres complexes distincts, et $k > 0$.

L'ensembles des points M d'affixe z vérifiant $\left|\frac{z-a}{z-b}\right| = k$ est

- un cercle si $k \neq 1$, et
- une droite si $k = 1$ (c'est la médiatrice du segment $[A, B]$, avec A le point d'affixe a et B le point d'affixe b).

Preuve : Exercice (faire par exemple une preuve analytique).

1.8 Quelques exercices

Exercice 1.24.1 Simplifier les expressions suivantes : $(3 + 2i)(1 - 3i)$ et $\dfrac{3 + 2i}{1 - 3i}$.

Exercice 1.24.2 Calculer le module et un argument pour les nombres complexes suivants :

$$1 - \cos(\theta) + i\sin(\theta) \text{ où } \theta \in \mathbb{R}\,.$$

Exercice 1.24.3 Montrer que, pour tout réel t, $\cos^3(t) = \frac{1}{4}\cos(3t) + \frac{3}{4}\cos(t)$. Donner une formule similaire pour $\sin^3(t)$.

Exercice 1.24.4 Pour tout réel t, calculer $\cos(5t)$ et $\sin(5t)$ en fonction de $\cos(t)$ et de $\sin(t)$.

Déduire du fait que $\cos(5\frac{\pi}{10}) = 0$ la valeur de $\cos(\pi/10)$.

Exercice 1.24.5

i) Calculer les racines carrées des nombres complexes suivants : $\frac{1}{2} + \frac{\sqrt{3}}{2}i$ et $z = 8(i + \sqrt{3})$.
ii) Calculer les racines carrées du nombre complexe $z = 4ab + 2(a^2 - b^2)i$ (avec $a, b \in \mathbb{R}$).
iii) Calculer les racines quatrièmes de -4.

Exercice 1.24.6 Résoudre l'équation du second degré suivante : $z^2 - 2iz - 1 + 2i$.

Exercice 1.24.7 Soit $\theta \in \mathbb{R}$. Résoudre l'équation : $z^2 - 2e^{i\theta}z + 2i\sin(\theta)e^{i\theta} = 0$.

Exercice 1.24.8 Déterminer l'ensemble des points du plan dont l'affixe est un nombre complexe z tels que les points d'affixes respectives i, z et iz sont alignés.

2 Les nombres entiers et les nombres rationnels

Pour des raisons de temps, nous ne ferons pas la construction de $\mathbb{N}, \mathbb{Z}$ ou $\mathbb{Q}$. Nous supposerons donc connues les règles de calcul sur $\mathbb{N}, \mathbb{Z}$ et $\mathbb{Q}$, ainsi que les propriétés de l'ordre sur ces ensembles.

Rappelons la propriété très importante suivante : $\mathbb{N}$ (respectivement $\mathbb{Z}$ ou $\mathbb{Q}$) est **intègre** : si p_1 et p_2 appartiennent à $\mathbb{N}$ (resp. à $\mathbb{Z}$ ou à $\mathbb{Q}$), et si $p_1 p_2 = 0$, alors $p_1 = 0$ ou $p_2 = 0$.

2.1 Le principe de récurrence

Définition 2.1 *Soit A une partie* **non vide** *de $\mathbb{N}$. On dit que $\bar{a}$ est* **le plus petit élément** *de A si :*

i) $\bar{a}$ appartient à A,

ii) $\forall a \in A$, on a : $\bar{a} \leq a$ (i.e., $\bar{a}$ minore A)

Remarques :

1. Un tel élément, s'il existe, est nécessairement unique.
2. Si $\bar{a}$ est le plus petit élément de A, alors

$$\forall a \in \mathbb{N}, \text{ avec } a < \bar{a}, \text{ on a } a \notin A .$$

Une propriété très importante de l'ensemble des entiers est la suivante :

Théorème 2.2 (Admis) *Soit A une partie* **non vide** *de $\mathbb{N}$. Alors A possède un plus petit élément.*

Définition 2.3 *On dit qu'une partie non vide A de $\mathbb{N}$ est* **majorée** *s'il existe un entier M tel que*

$$\forall a \in A, \ a \leq M .$$

On dit que M est un majorant de A.

On dit qu'une partie non vide A de $\mathbb{N}$ possède **un plus grand élément** *$\bar{a}$ si*

i) $\bar{a}$ appartient à A,

ii) $\forall a \in A$, on a : $\bar{a} \geq a$.

Remarque : On montre facilement qu'un plus grand élément, s'il existe, est unique. Notons que le plus grand élément de A est un majorant de A.

Corollaire 2.4 *Toute partie non vide et majorée de $\mathbb{N}$ possède un plus grand élément.*

Preuve : Soit B le sous-ensemble de $\mathbb{N}$ composé des majorants de A :

$$B = \{b \in \mathbb{N} \mid \forall a \in A, \ b \geq a\} .$$

Comme A est majoré, B est une partie non vide de $\mathbb{N}$. Donc, d'après le théorème 2.2, B possède un plus petit élément noté $\bar{a}$.

Montrons que $\bar{a}$ est bien le plus grand élément de A. Pour cela, montrons d'abord que $\bar{a}$ appartient à A. Raisonnons par l'absurde en supposant au contraire que $\bar{a}$ n'appartient pas à A. Nous allons montrer qu'alors $b = \bar{a} - 1$ appartient à B, ce qui contredit le fait que $\bar{a}$ est le plus petit élément de B. En effet, comme $\bar{a}$ appartient à B, on a : pour tout $a \in A$, $a \leq \bar{a}$. Or $\bar{a}$ n'appartient pas à A, donc en fait $a < \bar{a}$, ce qui montre que $a \leq \bar{a} - 1 = b$. On a donc prouvé que, pour tout $a \in A$, $a \leq b$. Ceci montre que b appartient à B, et contredit le fait que $\bar{a}$ est le plus petit élément de B.

Par conséquent, on a démontré que $\bar{a}$ appartient à A. Comme $\bar{a}$ appartient à B, il est clair que $\bar{a}$ est un majorant de A. En conclusion, $\bar{a}$ est bien le plus grand élément de A.

QED

Voici le résultat le plus important de cette partie :

Théorème 2.5 (Principe de récurrence) *Soit $\mathcal{P} : \mathbb{N} \to \{0,1\}$ une application possédant les propriétés suivantes :*
a) $\mathcal{P}(0) = 1$
b) pour tout $n \in \mathbb{N}$, si $\mathcal{P}(n) = 1$, alors $\mathcal{P}(n+1) = 1$.
Alors $\mathcal{P}(n) = 1$ pour tout $n \in \mathbb{N}$.

Remarque : En pratique, $\mathcal{P}(n)$ désigne une propriété, dépendant de l'entier n, dont on veut montrer qu'elle est vraie pour tout entier n. L'expression $\mathcal{P}(n) = 1$ signifie que la propriété est vraie, tandis que $\mathcal{P}(n) = 0$ qu'elle est fausse.

Le théorème précédent signifie donc que, pour montrer une propriété $\mathcal{P}(n)$ (qui dépend de $n \in \mathbb{N}$) pour tout $n \in \mathbb{N}$, il suffit
- de montrer que $\mathcal{P}(0)$ est vraie,
- de montrer que, si $\mathcal{P}(n)$ est vraie pour un certain n, alors $\mathcal{P}(n+1)$ est également vraie.

Preuve du théorème 2.5 : On raisonne par l'absurde en supposant qu'il existe $n_0 \in \mathbb{N}$ tel que $\mathcal{P}(n_0) = 0$. Soit

$$A = \{n \in \mathbb{N} \mid \mathcal{P}(n) = 0\} .$$

Par hypothèse, A est une partie non vide de $\mathbb{N}$ car n_0 appartient à A.

Donc A possède un plus petit élément $\bar{a}$. Notons que $\bar{a}$ appartient à A, donc $\mathcal{P}(\bar{a}) = 0$, et que $\bar{a} \geq 1$ car $\mathcal{P}(0) = 1$ par hypothèse (a).

De plus, comme $\bar{a}$ est le plus petit élément de A, $n = \bar{a} - 1$ (qui appartient à $\mathbb{N}$) n'appartient pas à A. D'où $\mathcal{P}(n) = 1$. Mais l'hypothèse (b) implique alors que $\mathcal{P}(n+1) = 1$. On a trouvé une contradiction puisque $n + 1 = \bar{a}$.

Ceci prouve que, pour tout $n \in \mathbb{N}$, $\mathcal{P}(n) = 1$.

QED

On montre exactement de la même façon le principe de récurrence généralisé, qui est souvent utile :

Théorème 2.6 (Principe de récurrence généralisé) *Soit $\mathcal{P} : \mathbb{N} \to \{0,1\}$ une application possédant les propriétés suivantes :*
a) $\mathcal{P}(0) = 1$
b) pour tout $n \in \mathbb{N}$, si $\{\forall k \leq n,\ \mathcal{P}(k) = 1\}$, alors $\mathcal{P}(n+1) = 1$.
Alors $\mathcal{P}(n) = 1$ pour tout $n \in \mathbb{N}$.

Preuve : Exercice.

2.2 La division euclidienne

Définition 2.7 *Soient a et b deux entiers relatifs. On dit que a divise b si*
a) a n'est pas nul,
b) il existe un entier relatif $k \in \mathbb{Z}$ tel que $b = ka$.

Remarque : L'entier k est alors unique, et noté $\frac{b}{a}$.

Notation : l'expression "$a|b$" signifie " a divise b".

Proposition 2.8 *Soient a, b et c trois entiers relatifs.*

1. *si* $c \neq 0$, *alors* $a|b$ *si et seulement si* $ac|bc$,

2. *si* $a|b$, *alors* $(-a)|b$ *et* $a|(-b)$,

3. *si* $a|b$ *et* $a|c$, *alors* $a|(b+c)$.

4. *si* $a|b$ *et* $b|a$, *alors* $a = b$ *ou* $a = -b$.

5. *si* $ab|c$ *alors* $a|c$ *et* $b|c$.

6. *si* $a \in \mathbb{N}^*$ *et* $b \in \mathbb{N}$, *avec* $a|b$, *alors soit* $b = 0$ *soit* $a \leq b$.

Preuve : Cette proposition est une conséquence immédiate de la définition de la division. Nous la laissons en exercice.

QED

Théorème 2.9 (Division euclidienne) *Soient* a *et* b *deux entiers naturels,* **avec** a **non nul**. *Il existe alors un unique couple* $(q, r) \in \mathbb{N}^2$ *tel que*

$$b = qa + r \quad \text{et} \quad 0 \leq r < a \ .$$

Vocabulaire : q est appelé **quotient** de la division euclidienne tandis que r s'appelle **le reste**.

Preuve de l'unicité : Montrons d'abord que le couple (q, r), s'il existe, est unique. Pour cela, on suppose qu'il existe deux couples $(q_1, r_1) \in \mathbb{N}^2$ et $(q_2, r_2) \in \mathbb{N}^2$ tels que l'égalité suivante soit satisfaite : pour $j = 1$ et $j = 2$,

$$b = q_j a + r_j \quad \text{et} \quad 0 \leq r_j < a \ .$$

Sans perte de généralité, on peut supposer que $r_1 \leq r_2$ (dans le cas contraire, on échange le rôle de (q_1, r_1) et (q_2, r_2)). Comme

$$b = q_1 a + r_1 = q_2 a + r_2 \ , \qquad \text{on a : } r_2 - r_1 = a(q_1 - q_2) \ .$$

Donc $r_2 - r_1$ est un entier naturel divisible par a. Mais, d'autre part, $r_2 - r_1 \leq r_2$ (car $r_1 \geq 0$) et $r_2 < a$. Comme $a > 0$, $a|(r_1 - r_2)$ et $a > (r_1 - r_2)$, on a $r_2 = r_1$. Cette égalité, conjuguée avec l'égalité $r_2 - r_1 = a(q_1 - q_2)$ et le fait que $a \neq 0$ implique que $q_1 = q_2$. En conclusion, nous avons prouvé que, si le couple (q, r) existe, il est unique.

Preuve de l'existence : Nous montrons maintenant son existence. Pour cela, on considère le sous-ensemble A de $\mathbb{N}$ défini par

$$A = \{p \in \mathbb{N} \mid ap > b\} \ .$$

Notons d'abord que l'ensemble A n'est pas vide. En effet, le nombre entier $b + 1$ appartient à A car $a \geq 1$, et donc $a(b + 1) \geq b + 1 > b$.

Par conséquent, l'ensemble A possède un plus petit élément $\bar{p}$. Posons $q = \bar{p} - 1$ et $r = b - aq$. Comme 0 n'appartient pas à A, on a $q \geq 0$. Comme l'égalité $b = aq + r$ est évidente d'après la définition de q et r, il reste à montrer que $0 \leq r < a$.

Notons d'abord que $r \geq 0$. En effet, comme $\bar{p}$ est le plus petit élément de A, $q = \bar{p} - 1$ n'appartient pas à A, i.e., $aq \leq b$. D'où $r \geq 0$.

Montrons enfin que $r < a$. En effet, comme $\bar{p}$ appartient à A, on a $a\bar{p} > b$. D'où $a(q + 1) > b$, ce qui implique que $r = b - aq < a$.

QED

2.3 Le ppcm d'une famille d'entiers

Définition 2.10 (PPCM) *Soit $\{a_1, \ldots, a_n\}$ un sous-ensemble de $\mathbb{Z}^*$. On appelle plus petit commun multiplicateur (ppcm) de $\{a_1, \ldots, a_n\}$ l'unique entier $\mu \in \mathbb{N}^*$ tel que*

a) $\forall i = 1, \ldots, n,\ a_i | \mu$,

b) $\forall k \in \mathbb{N}^*$, si $\{\forall i = 1, \ldots, n,\ a_i | k\}$, alors $\mu | k$.

Notation : Le ppcm de $\{a_1, \ldots, a_n\}$ est noté $ppcm\{a_1, \ldots, a_n\}$.

Terminologie : Soit $k \in \mathbb{N}^*$ tel que : $\forall i = 1, \ldots, n,\ a_i | k$. On dit alors que k est un multiple commun à $a_1, \ldots, a_n$.

Le ppcm de $\{a_1, \ldots, a_n\}$ est l'entier naturel non nul qui est un multiple commun à $a_1, \ldots, a_n$, et qui divise tous les autres multiples communs à $a_1, \ldots, a_n$.

Montrons l'existence du **ppcm**$\{a_1, \ldots, a_n\}$.

Théorème 2.11 *Soit $\{a_1, \ldots, a_n\}$ un sous-ensemble de $\mathbb{Z}^*$. Le ppcm de $\{a_1, \ldots, a_n\}$ existe et est unique. C'est le plus petit multiple commun à $a_1, \ldots, a_n$.*

Remarque : Ce résultat justifie donc la terminologie de **plus petit** multiple commun.

Preuve : Soit A l'ensemble des entiers naturels non nuls multiples communs à tous les a_i :

$$A = \{k \in \mathbb{N}^* \mid \forall i = 1, \ldots, n,\ a_i | k\} .$$

L'ensemble A est non vide car il contient l'entier $|a_1 \ldots . a_n|$. Donc A possède un plus petit élément noté μ. Montrons que μ est bien le ppcm de $\{a_1, \ldots, a_n\}$.

Comme μ appartient à A, μ est non nul et vérifie la condition (a) de la définition. Pour montrer que μ vérifie aussi (b), il suffit de montrer que μ divise k pour tout k appartenant à A.

On raisonne par l'absurde en supposant qu'il existe k dans A qui n'est pas divisible par μ. Soient q et r respectivement le quotient et le reste de la division euclidienne de k par μ. On a $k = q\mu + r$ et $0 < r < \mu$. Comme, pour tout $i = 1, \ldots, n$, a_i divise k et μ, a_i divise r. Donc r appartient à A, ce qui contredit le fait que μ est le plus petit élément de A. Donc μ divise k pour tout k dans A. On a montré l'existence du ppcm de $\{a_1, \ldots, a_n\}$.

Montrons l'unicité du ppcm. Si μ_1 et μ_2 sont deux ppcm de $\{a_1, \ldots, a_n\}$, alors μ_1 divise μ_2 et μ_2 divise μ_1 (c'est la propriété (b) de la définition). Donc, d'après la proposition 2.8, on a $\mu_1 = \mu_2$ ou $\mu_1 = -\mu_2$. Comme μ_1 et μ_2 sont strictement positifs, la seule égalité possible est $\mu_1 = \mu_2$. Le ppcm est donc unique.

QED

Voici quelques propriétés du ppcm :

Proposition 2.12

i) Soit $\{a_1, \ldots, a_n\}$ un sous-ensemble de $\mathbb{Z}^*$ et $\alpha \in \mathbb{Z}^*$. Alors

$$ppcm\{\alpha a_1, \ldots, \alpha a_n\} = |\alpha|\, ppcm\{a_1, \ldots, a_n\} .$$

ii) Si a et b sont deux entiers relatifs non nuls, avec $a|b$, alors

$$ppcm\{a, b\} = |b| .$$

Preuve : i) Appelons μ le ppcm de $\{a_1, \ldots, a_n\}$. Il faut montrer que $|\alpha|\mu$ est le ppcm de $\{\alpha a_1, \ldots, \alpha a_n\}$.

Comme, pour tout $i = 1, \ldots, n$, a_i divise μ, on a que αa_i divise $|\alpha|\mu$. Donc $|\alpha|\mu$ vérifie le (a) de la définition du ppcm.

Soit $k \in \mathbb{N}^*$ tel que, pour tout $i = 1, \ldots, n$, αa_i divise k. Alors α divise k (cf proposition 2.8), et donc $|\alpha|$ divise aussi k. Posons $k' = \frac{k}{|\alpha|}$. Notons que k' appartient à $\mathbb{N}^*$ car $k \in \mathbb{N}^*$.

Comme, pour tout $i = 1, \ldots, n$, αa_i divise $k = |\alpha| k'$, on en déduit que a_i divise k'. De plus, μ étant le ppcm de $\{a_1, \ldots, a_n\}$, la propriété (b) de la définition du ppcm implique que μ divise k'. Donc $\alpha\mu$ divise $k = |\alpha| k'$. Par conséquent, $|\alpha|\mu$ vérifie la condition (b) de la définition du ppcm.

ii) Pour montrer que $ppcm\{a, b\} = |b|$, posons $\mu = |b|$. Alors a et b divisent clairement μ, qui vérifie (a) de la définition du ppcm.

Soit maintenant k tel que a et b divisent k. Alors $\mu = |b|$ divise aussi k. D'où μ vérifie le (b) de la définition du ppcm.

QED

Nous apprendrons plus loin à calculer le ppcm.

2.4 Le pgcd d'une famille d'entiers

Définition 2.13 (PGCD) *Soit $\{a_1, \ldots, a_n\}$ un sous-ensemble de $\mathbb{Z}^*$. On appelle plus grand commun diviseur (pgcd) de $\{a_1, \ldots, a_n\}$ l'unique entier $\mu \in \mathbb{N}^*$ tel que*

a) $\forall i = 1, \ldots, n$, $\mu | a_i$,

b) $\forall k \in \mathbb{N}^*$, si $\{\forall i = 1, \ldots, n,\ k | a_i\}$, alors $k | \mu$.

Remarques : 1) Bien noter que le pgcd de $\{a_1, \ldots, a_n\}$ est le même que celui de $\{|a_1|, \ldots, |a_n|\}$. On peut donc toujours se restreindre au cas où $a_1, \ldots, a_n$ sont des entiers naturels.

2) En ce qui concerne la terminologie, il faut remarquer que le pgcd est non seulement **le plus grand** diviseur commun à $a_1, \ldots, a_n$, mais également est divisé par tout autre diviseur commun à $a_1, \ldots, a_n$.

Notation : Le pgcd de $\{a_1, \ldots, a_n\}$ est noté $pgcd\{a_1, \ldots, a_n\}$

Comme pour le ppcm, cette définition est justifiée par le théorème suivant :

Théorème 2.14 *Soit $\{a_1, \ldots, a_n\}$ un sous-ensemble de $\mathbb{Z}^*$. Le pgcd de $\{a_1, \ldots, a_n\}$ existe et est unique.*

L'unicité du pgcd est claire puisque, si μ_1 et μ_2 sont deux pgcd de $\{a_1, \ldots, a_n\}$, alors μ_1 et μ_2 se divisent l'un l'autre, et, étant positifs, sont donc égaux.

Le lemme suivant montre l'existence du pgcd :

Lemme 2.15 *Soient $\{a_1, \ldots, a_n\}$ un sous-ensemble de $\mathbb{Z}^*$ et $\mathcal{I}$ le sous-ensemble de $\mathbb{N}^*$ défini par*

$$\mathcal{I} = \{m \in \mathbb{N}^* \mid \exists (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n \text{ tels que } m = \alpha_1 a_1 + \ldots + \alpha_n a_n\} .$$

Alors $\mathcal{I}$ est non vide, et le plus petit élément de $\mathcal{I}$ est le pgcd de $\{a_1, \ldots, a_n\}$.

Preuve : L'ensemble $\mathcal{I}$ est non vide car, par exemple a_1^2 appartient à $\mathcal{I}$ (prendre $\alpha_1 = a_1$, $\alpha_2 = \ldots = \alpha_n = 0$). Notons μ le plus petit élément de la partie $\mathcal{I}$.

Comme μ appartient à $\mathcal{I}$, il existe $\alpha_1, \ldots, \alpha_n$ tels que $\mu = \alpha_1 a_1 + \ldots + \alpha_n a_n$. Vérifions que μ satisfait (a) de la définition du pgcd. Pour cela, on raisonne par l'absurde en supposant qu'il existe $i \in \{1, \ldots, n\}$ tel que μ ne divise pas a_i. Soit q et r respectivement le quotient et le reste de la division euclidienne de a_i par μ : $a_i = q\mu + r$ et $0 < r < \mu$. Alors r appartient à $\mathcal{I}$ car $r \in \mathbb{N}^*$ et

$$\begin{aligned} r = a_i - q\mu = \ & (-\alpha_1 q) a_1 + \ldots + (-\alpha_{i-1} q) a_{i-1} + (1 - \alpha_i q) a_i \\ & + (-\alpha_{i+1} q) a_{i+1} + \ldots + (-\alpha_n q) a_n . \end{aligned}$$

Mais d'autre part $\mu > r$ et μ est le plus petit élément de A. On a donc trouvé une contradiction. Par conséquent μ divise tous les a_i, $i = 1, \ldots, n$.

Reste à prouver que μ satisfait la partie (b) de la définition du pgcd. Pour cela, considérons k un diviseur commun à tous les a_i. Il est clair alors que k divise tous les éléments de $\mathcal{I}$. Comme μ appartient à $\mathcal{I}$, k divise donc μ.

QED

Le lemme que nous venons de montrer montre aussi le corollaire suivant, qui sera très important pour prouver le théorème de Bezout :

Corollaire 2.16 *Soit $\{a_1, \ldots, a_n\}$ un sous-ensemble de $\mathbb{Z}^*$. Il existe alors des entiers relatifs $\alpha_1, \ldots, \alpha_n$ tels que*

$$pgcd(a_1, \ldots, a_n) = \alpha_1 a_1 + \ldots + \alpha_n a_n \ .$$

Voici maintenant quelques propriétés du pgcd qui seront utiles plus tard :

Proposition 2.17
i) Soient $\{a_1, \ldots, a_n\}$ un sous-ensemble de $\mathbb{Z}^*$ et α un entier relatif non nul. Alors

$$pgcd\{\alpha a_1, \ldots, \alpha a_n\} = |\alpha| \, pgcd\{a_1, \ldots, a_n\} \ .$$

ii) Si a et b sont deux entiers relatifs non nuls tels que $a|b$, alors

$$pgcd(a, b) = |a| \ .$$

Preuve : i) Posons $\mu = pgcd\{a_1, \ldots, a_n\}$ et $\mu' = \{\alpha a_1, \ldots, \alpha a_n\}$. Il faut montrer que $|\alpha|\mu = \mu'$.

On remarque d'abord que $|\alpha|\mu$ est un diviseur commun à $\alpha a_1, \ldots, \alpha a_n$, car μ est un diviseur commun à $a_1, \ldots, a_n$. Donc $|\alpha|\mu$ divise μ'. Il existe donc $k \in \mathbb{N}^*$ avec $\mu' = |\alpha|\mu k$.

Comme μ' est le pgcd de $\{\alpha a_1, \ldots, \alpha a_n\}$, $\mu' = |\alpha|\mu k$ est un diviseur commun à $\alpha a_1, \ldots, \alpha a_n$, ce qui implique que μk est un diviseur commun à $a_1, \ldots, a_n$. Or μ étant le pgcd à $\{a_1, \ldots, a_n\}$, cela entraîne que μk divise μ. Or $\mu > 0$ et $\mu k > 0$, donc $k = 1$. On a donc prouvé que $\mu' = |\alpha|\mu$.

ii) Posons $\mu = pgcd\{a, b\}$. Comme $|a|$ divise à la fois a et b, $|a|$ divise μ. De plus, μ divise a, donc divise $|a|$. Ceci prouve que $\mu = |a|$.

QED

La proposition suivante affirme que l'on peut toujours ramener le calcul du pgcd de n entiers à n calculs du pgcd de 2 entiers.

Proposition 2.18 *Soient $\{a_1, \ldots, a_n\}$ un sous-ensemble de $\mathbb{Z}^*$, avec $n \geq 3$. Alors*

$$pgcd\{a_1, \ldots, a_n\} = pgcd\left\{a_1, pgcd\{a_2, \ldots, a_n\}\right\} \ .$$

Preuve : Posons $\mu = pgcd\{a_1, \ldots, a_n\}$, $\mu' = pgcd\{a_2, \ldots, a_n\}$ et $\mu" = pgcd\{a_1, \mu'\}$. On veut montrer que $\mu = \mu"$.

Montrons d'abord que μ divise $\mu"$. Comme μ est un diviseur commun à $a_2, \ldots, a_n$, μ divise μ'. Comme de plus, μ divise a_1, μ divise le pgcd de a_1 et de μ', i.e., divise $\mu"$.

Réciproquement, $\mu"$ divise à la fois a_1 et μ'. Or μ' étant un diviseur commun à $a_2, \ldots, a_n$, $\mu"$ est également un diviseur commun à $a_2, \ldots, a_n$. Donc $\mu"$ divise tous les a_i, avec $i = 1, \ldots, n$, donc $\mu"$ divise le pgcd de $\{a_1, \ldots, a_n\}$, c'est-à-dire μ.

En conclusion, les entiers naturels μ et $\mu"$ se divisent l'un l'autre, et sont donc égaux.

QED

Voici maintenant le résultat principal de cette partie, qui justifie l'algorithme d'Euclide de calcul du pgcd, que nous introduisons après.

Théorème 2.19 *Soient a_1 et a_2 deux entiers naturels non nuls. Si a_2 ne divise pas a_1, alors*

$$pgcd\{a_1, a_2\} = pgcd\{a_2, r\}$$

où r est le reste de la division euclidienne de a_1 par a_2.

Preuve : Soient q et r respectivement le quotient et le reste de la division euclidienne de a_1 par a_2 : $a_1 = qa_2 + r$ et $0 < r < a_2$. Notons μ le pgcd de a_2 et r et μ' le pgcd de a_1 et a_2. Montrons que $\mu = \mu'$.

(a) Par définition, $\mu | a_2$. Comme $\mu | r$ et $\mu | a_2$, on a aussi $\mu | qa_2 + r = a_1$. Donc μ est un diviseur commun de a_2 et de a_1. Donc μ divise μ' qui est le pgcd de a_1 et a_2.

(b) Réciproquement, μ' divise a_1 et a_2, donc μ' divise aussi $a_1 - qa_2 = r$. Par conséquent, μ' divise le pgcd de a_2 et de r, i.e., divise μ.

En conclusion, les entiers naturels μ et μ" se divisent l'un l'autre, et sont donc égaux.

QED

Décrivons maintenant **l'algorithme d'Euclide**. L'objet de l'algorithme est de calculer le pgcd de deux entier naturels non nuls a_1 et a_2.

- **Initialisation :** Posons $r_1 = a_1$ et $r_2 = a_2$
- tant que $r_i > 0$, on définit r_{i+1} comme étant le reste de la division euclidienne de r_{i-1} par r_i.

Proposition 2.20 *Soit (r_i) la suite définie par l'algorithme d'Euclide. Alors il existe un indice $i_0 \leq a_2 + 2$ tel que $r_{i_0} = 0$ et*

$$pgcd\{a_1, a_2\} = r_{i_0 - 1} \ .$$

Exemple : Si $a_1 = 48$ et $a_2 = 30$, alors $r_1 = a_1 = 48$, $r_2 = a_2 = 30$, $r_3 = 48 - 1.30 = 18$, $r_4 = 30 - 1.18 = 12$, $r_5 = 18 - 1.12 = 6$, $r_6 = 12 - 2.6 = 0$. Donc $i_0 = 6$ et $pgcd\{48, 30\} = r_5 = 6$.

Preuve de la proposition 2.20 : Par définition du reste de la division euclidienne, la suite (r_i) est strictement décroissante à partir du rang $i = 2$. On montre donc facilement par récurrence que $r_i \leq a_2 - i + 2$ pour $i \geq 2$. Or r_i est positif pour tout i. L'algorithme s'arrête donc au plus tard en temps $i_0 \leq r_2 + 2$.

On démontre également par récurrence, en utilisant le théorème 2.19, que, pour tout $i < i_0 - 1$,

$$pgcd\{a_1, a_2\} = pgcd\{r_{i-1}, r_i\} \ . \tag{1}$$

Or, par définition de i_0, l'entier $r_{i_0 - 1}$ divise $r_{i_0 - 2}$. La proposition 2.17 affirme alors que

$$pgcd\{r_{i_0-2}, r_{i_0-1}\} = r_{i_0-1} \ . \tag{2}$$

En mettant ensembles les égalités (1) et (2), on obtient le résultat désiré : $pgcd\{a_1, a_2\} = r_{i_0 - 1}$.

QED

2.5 Nombres premiers entre eux

Définition 2.21 *Soit $\{a_1, \ldots, a_n\}$ un sous-ensemble de $\mathbb{Z}^*$. On dit que les nombres $a_1, \ldots, a_n$ sont premiers entre eux si leur pgcd est 1.*

Exemple : Les nombres 30, 35 et 14 sont premiers entre eux. En effet, on a d'une part : $pgcd\{35, 14\} = pgcd\{14, 7\} = 7$ d'après l'algorithme d'Euclide. D'autre part, on a

$$pgcd\{30, 35, 14\} = pgcd\{30, pgcd\{35, 14\}\} = pgcd\{30, 7\},$$

où $pgcd\{30, 7\} = pgcd\{7, 2\} = pgcd\{2, 1\} = 1$ d'après l'algorithme d'Euclide. Donc on a montré que $pgcd\{30, 35, 14\} = 1$.

Le théorème le plus important de cette partie, et un des plus importants de ce cours, est le théorème de Bezout :

Théorème 2.22 (Bezout) *Soit $\{a_1, \ldots, a_n\}$ un sous-ensemble de $\mathbb{Z}^*$. Alors les nombres $a_1, \ldots, a_n$ sont premiers entre eux si et seulement si il existe n entiers relatifs $\alpha_1, \ldots, \alpha_n$ tels que*

$$\alpha_1 a_1 + \ldots + \alpha_n a_n = 1 \,. \tag{3}$$

On appelle **relation de Bezout une relation du type (3)**.

Preuve : Supposons d'abord que $a_1, \ldots, a_n$ sont premiers entre eux. Comme le pgcd de $a_1, \ldots, a_n$ est 1, le corollaire 2.16 affirme qu'il existe n entiers relatifs $\alpha_1, \ldots, \alpha_n$ tels que $\alpha_1 a_1 + \ldots + \alpha_n a_n = 1$.

Réciproquement, supposons qu'il existe n entiers relatifs $\alpha_1, \ldots, \alpha_n$ tels que $\alpha_1 a_1 + \ldots + \alpha_n a_n = 1$. Soit μ le pgcd de $a_1, \ldots, a_n$. Comme μ est un diviseur commun de $a_1, \ldots, a_n$, μ divise également $\alpha_1 a_1 + \ldots + \alpha_n a_n$, i.e., μ divise 1. Comme $\mu > 0$, μ ne peut être égal qu'à 1. En conclusion, $a_1, \ldots, a_n$ sont premiers entre eux.

QED

Comment trouver une relation de Bezout ?

En pratique, pour trouver une relation de Bezout, on utilise l'algorithme d'Euclide, en écrivant à chaque étape le quotient et le reste de la division euclidienne de r_{i+1} par r_i (cf les notations de l'algorithme).

Par exemple, pour les entiers $n_1 = 48$ et $n_2 = 30$, cela donne :

- $n_1 = r_1 = 48$, $n_2 = r_2 = 30$, $r_1 = 1.r_2 + 18$, d'où $r_3 = 18 = n_1 - n_2$.
- $r_2 = 1.r_3 + 12$, d'où $r_4 = 12 = r_2 - r_3 = n_2 - (n_1 - n_2) = 2n_2 - n_1$.
- $r_3 = 1.r_4 + 6$ d'où $r_5 = 6 = r_3 - r_4 = (n_1 - n_2) - (2n_2 - n_1) = 2n_1 - 3n_2$.
- $r_4 = 2n_5$ d'où $r_6 = 0$.
- On en conclut que $pgcd\{n_1, n_2\} = r_5 = 6$. Une relation de Bezout est donc : $2n_1 - 3n_2 = 6$.

Théorème 2.23 (Gauss) *Soient a, b et c trois entiers naturels non nuls. Si a divise bc et est premier avec b, alors a divise c.*

Preuves : Nous donnons deux démonstrations de ce résultat :

Première démonstration : Comme a et b sont premiers entre eux, le théorème de Bezout affirme qu'il existe α_1 et α_2 tels que

$$\alpha_1 a + \alpha_2 b = 1 \,. \qquad \text{D'où } \alpha_1 ac + \alpha_2 bc = c \,.$$

Comme a divise à la fois ac et bc, a divise $\alpha_1 ac + \alpha_2 bc$, c'est-à-dire, a divise c.

Seconde démonstration : D'après la première partie de la proposition 2.17, on a :

$$pgcd\{ac, bc\} = c\,pgcd\{a, b\} = c.1 = c\ .$$

Comme a est un diviseur commun de ac et de bc, et que c est le pgcd de ac et bc, on en déduit que a divise c.

QED

Une conséquence cruciale du théorème de Gauss est le corollaire suivant :

Corollaire 2.24 *Soient a, b, c trois entiers naturels, avec a et b non nuls et premiers entre eux. Si $a|c$ et $b|c$ alors $ab|c$.*

Preuve : Comme $a|c$, il existe un entier c' tel que $c = ac'$. Or $b|c$, donc $b|(ac')$. Comme a et b sont premiers entre eux, le théorème de Gauss affirme que $b|c'$. Donc $ab|c$.

QED

Une autre application du théorème de Bezout est la suivante :

Proposition 2.25 *Soit $\{a_1, \ldots, a_n\}$ un sous-ensemble de $\mathbb{Z}^*$. Alors un entier naturel μ est le pgcd de $a_1, \ldots, a_n$ si et seulement si μ est un diviseur commun de $a_1, \ldots, a_n$ et les entiers $\frac{a_1}{\mu}, \ldots, \frac{a_n}{\mu}$ sont premiers entre eux.*

Preuve : Supposons d'abord que μ est le pgcd de $a_1, \ldots, a_n$. Alors on sait que μ est un diviseur commun de $a_1, \ldots, a_n$. De plus, le corollaire 2.16 affirme qu'il existe des entiers $\alpha_1, \ldots, \alpha_n$ tels que $\alpha_1 a_1 + \ldots + \alpha_n a_n = \mu$. En divisant cette égalité par μ, on obtient :

$$\alpha_1 \frac{a_1}{\mu} + \ldots + \alpha_n \frac{a_n}{\mu} = 1\ .$$

Le théorème de Bezout affirme alors que $\frac{a_1}{\mu}, \ldots, \frac{a_n}{\mu}$ sont premiers entre eux.

Réciproquement, supposons que μ est un diviseur commun de $a_1, \ldots, a_n$ et les entiers $\frac{a_1}{\mu}, \ldots, \frac{a_n}{\mu}$ sont premiers entre eux. Notons d le pgcd de $a_1, \ldots, a_n$. Comme μ est un diviseur commun de $a_1, \ldots, a_n$, μ divise d par définition du pgcd. De plus, comme $\frac{a_1}{\mu}, \ldots, \frac{a_n}{\mu}$ sont premiers entre eux, le théorème de Bezout affirme qu'il existe des entiers $\alpha_1 \ldots, \alpha_n$ tels que $\alpha_1 \frac{a_1}{\mu} + \ldots \alpha_n \frac{a_n}{\mu} = 1$, ce qui implique que $\alpha_1 a_1 + \ldots \alpha_n a_n = \mu$. Comme d est un diviseur commun de $a_1, \ldots, a_n$, d divise $\alpha_1 a_1 + \ldots \alpha_n a_n$, et donc divise μ. Nous avons prouvé que les entiers naturels d et μ se divisent l'un l'autre. Ils sont donc égaux.

QED

Nous expliquons maintenant comment calculer le ppcm de deux nombres à partir de leur pgcd : pour cela, commençons par un résultat intermédiaire.

Proposition 2.26 *Soient a et b deux entiers naturels non nuls premiers entre eux. Alors le ppcm de a et b est égal à ab.*

Preuve : Posons $\mu = ppcm\{a, b\}$. Comme ab est un multiple commun de a et de b, μ divise ab (condition (b) de la définition du ppcm).

Comme a divise μ, il existe un entier k tel que $\mu = ak$. Or b divise également μ, donc divise ak. Or a et b sont premiers entre eux. Le théorème de Gauss affirme alors que b divise k. Donc il existe un entier $k' \in \mathbb{N}^*$ tel que $k = bk'$. D'où $\mu = abk'$. On en déduit que ab divise μ.

Les entiers naturels μ et ab se divisent l'un l'autre, donc sont égaux.

QED

Voici maintenant la relation entre ppcm et pgcd dans le cas général :

Théorème 2.27 *Soient a et b deux entiers naturels non nuls. Alors*

$$pgcd\{a,b\}\, ppcm\{a,b\} = ab\ .$$

Preuve : Posons $d = pgcd\{a,b\}$. La proposition 2.25 affirme que d divise a et b et que $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux. D'après la proposition 2.26, le ppcm de $\frac{a}{d}$ et $\frac{b}{d}$ est égal à $\frac{ab}{d^2}$.

Donc

$$ppcm\{a,b\} = ppcm\{d\frac{a}{d}, d\frac{b}{d}\} = d\, ppcm\{\frac{a}{d}, \frac{b}{d}\} = d\,\frac{ab}{d^2} = \frac{ab}{d}\ .$$

On en déduit l'égalité désirée.

QED

On conclut cette partie par la mise sous forme irréductible d'un nombre rationnel. Rappelons qu'un nombre rationnel est un nombre réel r pour lequel il existe $(p,q) \in \mathbb{Z} \times \mathbb{Z}^*$ avec $r = p/q$.

Théorème 2.28 (Forme irréductible d'un nombre rationnel) *Soit r un nombre rationnel non nul. Il existe un unique couple $(a,b) \in \mathbb{Z}^* \times \mathbb{N}^*$ tel que*

$$r = \frac{a}{b} \qquad \text{et} \qquad a \text{ et } b \text{ premiers entre eux}\ .$$

Preuve : *Existence :* On suppose que r est positif (sinon, faire le même travail avec $-r$). Comme r est rationnel, il existe $(p,q) \in \mathbb{Z} \times \mathbb{Z}^*$ avec $r = p/q$. On peut choisir p et q strictement positifs car r l'est. Posons $d = pgcd\{p,q\}$, $a = p/d$ et $b = q/d$. Alors la proposition 2.25 affirme que a et b sont premiers entre eux. De plus, on a bien $r = a/b$ car

$$r = \frac{p}{q} = \frac{ad}{bd} = \frac{a}{b}\ .$$

Unicité : Supposons qu'il existe deux couples $(a_1,b_1) \in \mathbb{Z}^* \times \mathbb{N}^*$ et $(a_2,b_2) \in \mathbb{Z}^* \times \mathbb{N}^*$ tels que, pour $j = 1, 2$, $r = \frac{a_j}{b_j}$ et a_j et b_j sont premiers entre eux. Alors

$$r = \frac{a_1}{b_1} = \frac{a_2}{b_2}$$

D'où $a_1 b_2 = a_2 b_1$. Alors b_2 divise $a_2 b_1$. Comme b_2 et a_2 sont premiers entre eux, le théorème de Gauss affirme que b_2 divise b_1. On obtient de même que b_1 divise b_2. Les entiers naturels b_1 et b_2 se divisant l'un l'autre, ils sont égaux. L'égalité $a_1 b_2 = a_2 b_1$ et le fait que $b_1 = b_2 \neq 0$ impliquent alors que $a_1 = a_2$. D'où l'unicité de la mise sous forme irréductible.

QED

2.6 Nombres premiers

Définition 2.29 *On appelle nombre premier tout nombre entier naturel p, tel que $p \geq 2$ et dont les seuls diviseurs dans $\mathbb{N}^*$ sont 1 et p, i.e., :*

$$\text{si } q \in \mathbb{N}^* \text{ avec } q|p\ ,\ \text{alors } q = 1 \text{ ou } q = p\ .$$

Le théorème suivant affirme que tout entier naturel possède des diviseurs premiers :

Théorème 2.30 *Soit n un entier naturel, avec $n \geq 2$. Il existe un nombre premier qui divise n.*

Preuve : Soit A le sous-ensemble des entiers naturels supérieurs à 2 et diviseurs de n :

$$A = \{q \in \mathbb{N}^* \mid q \geq 2 \text{ et } q|n\} .$$

Alors A est une partie non vide de $\mathbb{N}$ (car $n \in A$) et donc possède un plus petit élément p.

Montrons que p est premier. Soit k un nombre entier naturel qui divise p. Alors k divise aussi n, car p divise n. Il y a alors deux possibilités :

- soit $k < 2$, c'est-à-dire $k = 1$,

- soit $k \geq 2$, et donc k appartient à A. Or p est le plus petit élément de A. Donc $k \geq p$. Mais k divise p, donc $k = p$.

On a prouvé que, si k divise p, alors soit $k = 1$, soit $k = p$. Donc p est un diviseur premier de n.

QED

Le théorème d'Euclide affirme qu'il existe une infinité de nombres premiers :

Théorème 2.31 (Euclide) *Pour tout entier naturel n, il existe un nombre premier p supérieur à n.*

Preuve : Fixons un entier $n \geq 2$, et considérons le nombre $q = n! + 1 = (1.2.3 \ldots n) + 1$. D'après le théorème 2.30, il existe un nombre premier p qui divise q.

Montrons que p est supérieur à n. En effet, si, raisonnant par l'absurde, on suppose que $p < n$, alors p divise $n!$. Donc p ne peut pas diviser q car p ne divise pas 1 (rappelons que $p \geq 2$). On a donc trouvé une contradiction. Par conséquent, p est supérieur à n.

QED

2.7 Décomposition d'un entier en facteurs premiers

Théorème 2.32 *Tout entier naturel $a \geq 2$ peut s'écrire d'une manière unique sous la forme :*

$$a = (p_1)^{k_1} \ldots (p_m)^{k_m}$$

où $p_1, \ldots, p_m$ sont des nombres premiers distincts et $k_1, \ldots, k_m$ sont des entiers strictement positifs.

Remarque : L'unicité signifie ici que si on a deux expressions de cette forme :

$$a = (p_1)^{k_1} \ldots (p_m)^{k_m} = (q_1)^{r_1} \ldots (q_n)^{r_n}$$

avec $p_1, \ldots, p_m$ (respectivement $q_1, \ldots, q_n$) des nombres premiers distincts et $k_1, \ldots, k_m$ (respectivement $r_1, \ldots, r_n$) des entiers strictement positifs, alors $m = n$ et, pour tout $i \in \{1, \ldots, n\}$, il existe un indice $j \in \{1, \ldots, n\}$ tel que $p_i = q_j$ et $k_i = r_j$.

Preuve : Nous ne démontrons que l'existence, la preuve de l'unicité étant un peu plus délicate. On raisonne par récurrence généralisée sur le nombre a. Si $a = 2$, le résultat est évident.

Supposons le résultat vrai jusqu'au nombre $a \geq 2$. Montrons qu'il est encore vrai pour $a + 1$. D'après le théorème 2.30, le nombre $a + 1$ possède un diviseur premier, noté p. Posons $b = \frac{a+1}{p}$.

Il y a alors 2 cas : soit $b = 1$, et alors le résultat est démontré. Soit $b > 1$, et on a alors $2 \leq b \leq a$. Par hypothèse de récurrence, il existe alors des nombres premiers distincts $p_1, \ldots, p_m$ et des entiers strictement positifs $k_1, \ldots, k_m$ tels que

$$b = (p_1)^{k_1} \ldots (p_m)^{k_m} .$$

Donc

$$a + 1 = p(p_1)^{k_1} \ldots (p_m)^{k_m}$$

et $a + 1$ possède une décomposition en facteurs premiers.

Par récurrence, on en déduit l'existence de la décomposition pour tout entier a.

Application au calcul du pgcd et du ppcm : Soient a et b deux entiers naturels non nuls supérieurs à 2. On suppose que

$$a = (p_1)^{k_1} \dots (p_m)^{k_m} \text{ et } b = (p_1)^{r_1} \dots (p_m)^{r_m}$$

avec $p_1, \dots, p_m$ des nombres premiers distincts et $k_1, \dots, k_m$ (respectivement $r_1, \dots, r_m$) des *entiers positifs ou nuls* (de façon à avoir une écriture commune pour a et b). Alors

$$pgcd\{a,b\} = (p_1)^{\min\{k_1,r_1\}} \dots (p_m)^{\min\{k_m,r_m\}} \text{ et } ppcm\{a,b\} = (p_1)^{\max\{k_1,r_1\}} \dots (p_m)^{\max\{k_m,r_m\}} .$$

2.8 Quelques exercices

Exercice 2.32.1 Soit k un entier naturel. Montrer que $9k+4$ et $2k+1$ sont premiers entre eux.

Exercice 2.32.2 Calculer $pgcd(1863, 368, 14375)$ et $ppcm(1863, 368, 14375)$.

Exercice 2.32.3 Quel est le pgcd de $17^{63} - 1$ et $17^{42} - 1$?

Exercice 2.32.4 Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation $27x + 45y = 63$.

Exercice 2.32.5 1) A partir de l'algorithme d'Euclide, déterminer deux entiers relatifs u_0 et v_0 tels que $35u_0 + 13v_0 = 1$.
2) Déterminer tous les couples d'entiers relatifs (u, v) tels que $35u + 13v = 1$.

Exercice 2.32.6 Déterminer tous les couples d'entiers n, m tels que

$$1 \leq n \leq m,\ m + n = 256 \text{ et } pgcd\{n,m\} = 16 .$$

Exercice 2.32.7 Soit $n \geq 1$ un nombre entier. En s'inspirant de l'algorithme d'Euclide, montrer que la fraction rationnelle $\frac{15n^2+8n+6}{30n^2+21n+13}$ est irreductible.

3 Les polynômes

Avertissement : L'ensemble des polynômes partage de nombreuses propriétés communes avec l'ensemble des entiers (division euclidienne, existence d'un ppcm, d'un pgcd, notion de nombres ou de polynômes premiers, etc...) C'est pourquoi plusieurs parties de ce chapitre sont redondantes par rapport au chapitre précédent. C'est en particulier le cas des parties 3.3 à 3.7 qui ne figurent ici que par commodité du lecteur.

3.1 Définitions et vocabulaire

Définition 3.1

- *Un polynôme P est une expression de la forme $P(X) = a_0 + a_1X + a_2X^2 + \dots a_nX^n$.*
- *$a_0, a_1, \dots, a_n$ sont les* **coefficients** *du polynôme. Si $a_0, a_1, \dots, a_n$ sont des nombres réels, le polynôme est* **réel**. *Si $a_0, a_1, \dots, a_n$ sont des nombres complexes, le polynôme est* **complexe**.
- *L'ensemble des polynômes réels est noté $\mathbb{R}[X]$, tandis que l'ensemble des polynômes complexes est noté $\mathbb{C}[X]$.*
- *Le polynôme P est nul si tous ses coefficents sont nuls.*
- *Si P est un polynôme non nul, avec $P(X) = a_0 + a_1X + a_2X^2 + \dots a_nX^n$, le* **degré** *du polynôme P, noté $deg(P)$, est le plus grand entier $k \in \{0, \dots, n\}$ tel que $a_k \neq 0$.*

  Par convention, le degré du polynôme nul est $-\infty$.
- *Si P est un polynôme non nul, avec $P(X) = a_0 + a_1X + a_2X^2 + \dots a_nX^n$ et $n = deg(P)$, alors a_n est appelé* **coefficient directeur** *de P.*

  Si ce coefficient directeur est égal à 1, on dit que le polynôme P est **normalisé**.
- *Deux polynômes P_1 et P_2 sont égaux si P_1 et P_2 ont même degré et si les coefficients de P_1 et P_2 sont égaux.*

Somme de deux polynômes : Soient $P_1(X) = a_0 + a_1X + \dots + a_nX^n$ et $P_2(X) = b_0 + b_1X + \dots + b_mX^m$. Le polynôme $P_1 + P_2$ est le polynôme $(P_1 + P_2)(X) = c_0 + c_1X + \dots + c_kX^k$, avec

- l'entier k est défini par $k = \max\{n, m\}$,
- les coefficients c_i sont définis par :

$$\forall i \in \{1, \dots, k\}\ ,\ c_i = \begin{cases} a_i + b_i & \text{si } i \leq \min\{n, m\} \\ a_i & \text{si } m + 1 < i \leq n \\ b_i & \text{si } n + 1 < i \leq m \end{cases}$$

Remarque : La somme des deux polynômes réels (respectivement complexe) est un polynôme réel (respectivement complexe).

Produit de deux polynômes : Soient $P_1(X) = a_0 + a_1X + \dots + a_nX^n$ et $P_2(X) = b_0 + b_1X + \dots + b_mX^m$. Le polynôme P_1P_2 est le polynôme $(P_1P_2)(X) = c_0 + c_1X + \dots + c_kX^k$, avec

- l'entier k est défini par $k = n + m$,
- les coefficients c_i sont définis par :

$$\forall i \in \{1, \dots, k\}\ ,\ c_i = \sum_{j+l=i} a_jb_l\ .$$

Remarque : Cette formule correspond au developpement formel du produit

$$(a_0 + a_1X + \ldots + a_nX^n)(b_0 + b_1X + \ldots + b_mX^m) .$$

Il est facile de montrer que la somme et le produit de polynômes possèdent les propriétés habituelles (associativité, commutativité, le polynôme nul est un élément neutre pour l'addition, existence d'un opposé, distributivité).

Sauf mention contraire, dans toute la suite nous travaillerons indifféremment dans $\mathbb{R}[X]$ ou dans $\mathbb{C}[X]$. Un **scalaire** sera alors, dans le premier cas, un élément de $\mathbb{R}$, et dans le second, un élément de $\mathbb{C}$.

Théorème 3.2 *Soient P_1 et P_2 deux polynômes. Alors*

- *$deg(P_1 + P_2) \leq \max\{deg(P_1), deg(P_2)\}$. De plus, il y a inégalité stricte si et seulement si $deg(P_1) = deg(P_2)$ et le coefficient dominant de P_1 est l'opposé de celui de P_2.*
- *$deg(P_1P_2) = deg(P_1) + deg(P_2)$. De plus, si P_1 et P_2 sont non nuls, le coefficient dominant de P_1P_2 est le produit du coefficient dominant de P_1 et de celui de P_2.*

Remarques :

1. Si P_1 ou P_2 est le polynôme nul, le résultat est encore valable à condition d'utiliser la convention $-\infty + k = -\infty$ pour tout entier k.
2. Notons que, si P_1 et P_2 sont non nuls et normalisés, alors P_1P_2 est non nul et normalisé.

Preuve du théorème : C'est une conséquence directe des définitions de la somme et du produit.

QED

Ceci implique que l'ensemble des polynômes est intègre :

Corollaire 3.3 *Si P_1 et P_2 sont deux polynômes, et si $P_1P_2 = 0$ alors soit $P_1 = 0$, soit $P_2 = 0$.*

Preuve : En effet, $deg(P_1P_2) = deg(P_1) + deg(P_2) = -\infty$ car $P_1P_2 = 0$. Donc $deg(P_1) = -\infty$ ou $deg(P_2) = -\infty$, c'est-à-dire que $P_1 = 0$ ou $P_2 = 0$.

QED

3.2 Division euclidienne

Définition 3.4 *Soient A et B deux polynômes. On dit que A divise B si*
a) A n'est pas nul,
b) il existe un polynôme Q tel que $B = QA$.

Remarque : Le polynôme Q est alors unique, et noté $\frac{B}{A}$.

Notation : l'expression "$A|B$" signifie " A divise B".

Proposition 3.5 *Soient A, B et C trois polynômes.*

1. *si $C \neq 0$, alors $A|B$ si et seulement si $AC|BC$,*
2. *si $A|B$, alors $(-A)|B$ et $A|(-B)$,*
3. *si $A|B$ et $A|C$, alors $A|(B + C)$.*

4. *si $A|B$ et $B|A$, alors il existe un scalaire non nul α tel que $B = \alpha A$.*

5. *si $AB|C$ alors $A|C$ et $B|C$.*

6. *si $A \neq 0$ et $A|B$, alors, soit $B = 0$, soit $deg(A) \leq deg(B)$.*

Preuve : Cette proposition est une conséquence immédiate de la définition de la division. Nous la laissons en exercice.

QED

Théorème 3.6 *Soient A et B deux polynômes avec $B \neq 0$. Il existe alors un unique couple (Q, R) de polynômes, avec*

$$A = QB + R \text{ et } deg(R) < deg(B) .$$

Terminologie : Le polynôme Q s'appelle le quotient de la division euclidienne de A par B, tandis que le polynôme R s'appelle le reste.

Preuve de l'unicité : Supposons que (Q_1, R_1) et (Q_2, R_2) soient deux couples de polynômes tels que

$$A = Q_1B + R_1 = Q_2B + R_2 \text{ avec } deg(R_1) < deg(B) \text{ et } deg(R_2) < deg(B) .$$

Alors, comme $(Q_1 - Q_2)B = R_2 - R_1$, le polynôme B divise le polynôme $R_1 - R_2$ qui est de degré strictement inférieur à celui de B. Donc $R_1 = R_2$, ce qui implique, puisque $B \neq 0$, que $Q_1 = Q_2$.

Nous avons donc prouvé qu'il existe au plus un couple (Q, R) de polynômes vérifiant la relation désirée.

Preuve de l'existence : On suppose que B ne divise pas A, car sinon le résultat est évident. Notons

$$E = \{n \in \mathbb{N} \mid \exists \text{ un polynôme } C \text{ avec } deg(A - BC) = n\} .$$

L'ensemble E n'est pas vide car il contient par exemple $deg(A)$ (prendre $C = 0$). Donc E contient un plus petit élément r. Comme $r \in E$, il existe un polynôme Q tel que le polynôme $R = (A - BQ)$ a pour degré r. Montrons que $r < deg(B)$.

Pour cela, on raisonne par l'absurde en supposant au contraire que $r = deg(R) \geq deg(B)$. Posons $n = deg(B)$ et appelons b_n et c_r respectivement le coefficient dominant de B et de R. Alors on affirme que le polynôme $Q_1 = Q + \frac{c_r}{b_n}X^{r-n}$ (avec la convention $X^0 = 1$) vérifie : $deg(A - BQ_1) < r$. En effet,

$$A - BQ_1 = A - B(Q + \frac{c_r}{b_n}X^{r-n}) = R - \frac{c_r}{b_n}X^{r-n}B .$$

Les polynômes R et $\frac{c_r}{b_n}X^{r-n}B$ sont de même degré r et ont même coefficient dominant c_r. Donc $A - BQ_1$ a un degré strictement inférieur à r. Comme $deg(A - BQ_1)$ appartient à E par définition de E (notons que $A - BQ_1 \neq 0$ car B ne divise pas A), on a trouvé une contradiction car r est le plus petit élément de E et $deg(A - BQ_1) < r$. Par conséquent, on a prouvé que $r = deg(R) < deg(B)$. Ceci achève la démonstration de l'existence du couple (Q, R) tel que $A = QB + R$ et $deg(R) < deg(B)$.

QED

3.3 Le ppcm d'un famille de polynômes

Définition 3.7 (PPCM) *Soit $\{A_1, \ldots, A_n\}$ une famille de polynômes non nuls. On appelle plus petit commun multiplicateur (ppcm) de $\{A_1, \ldots, A_n\}$ l'unique polynôme non nul et normalisé P tel que*

a) $\forall i = 1, \ldots, n,\ A_i | P$,

b) Pour tout polynôme non nul Q, si $\{\forall i = 1, \ldots, n,\ A_i | Q\}$, alors $P | Q$.

Notation : Le ppcm de $\{A_1, \ldots, A_n\}$ est noté $ppcm\{A_1, \ldots, A_n\}$.

Terminologie : Soit Q un polynôme tel que : $\forall i = 1, \ldots, n,\ A_i | Q$. On dit alors que Q est un multiple commun à $A_1, \ldots, A_n$.

Le ppcm de $\{A_1, \ldots, A_n\}$ est le polynôme non nul et normalisé qui est un multiple commun à $A_1, \ldots, A_n$, et qui divise tous les autres polynômes multiples communs à $A_1, \ldots, A_n$.

Montrons l'existence du $ppcm\{A_1, \ldots, A_n\}$.

Théorème 3.8 *Soit $\{A_1, \ldots, A_n\}$ une famille de polynômes non nuls. Le ppcm de $\{A_1, \ldots, A_n\}$ existe et est unique. C'est le polynôme de plus petit degré parmi les polynômes non nuls et normalisés qui sont multiples commun de $A_1, \ldots, A_n$.*

Preuve : Soit E l'ensemble des entiers naturels non nuls défini par

$$E = \{k \in \mathbb{N}^* \mid \exists \text{ un polynôme } Q \text{ tel que } \forall i = 1, \ldots, n,\ A_i | Q \text{ et } k = deg(Q)\} .$$

L'ensemble E est non vide car il contient l'entier $k = deg(A_1 \ldots . A_n)$. En effet, $A_1 \ldots . A_n$ est un multiple commun de $A_1, \ldots, A_n$. Donc E possède un plus petit élément noté p. Comme p appartient à E, il existe un polynôme P (que l'on peut choisir normalisé) qui est multiple commun à tous les A_i et tel que $deg(P) = p$. Montrons que P est le ppcm de $\{A_1, \ldots, A_n\}$.

Par construction, P est non nul et vérifie la condition (a) de la définition. Pour montrer que P vérifie aussi (b), il suffit de montrer que P divise A pour tout A multiple commun à $A_1, \ldots, A_n$.

On raisonne par l'absurde en supposant qu'il existe A multiple commun à $A_1, \ldots, A_n$ qui n'est pas divisible par P. Soient Q et R respectivement le quotient et le reste de la division euclidienne de A par P. On a $A = QP + R$ et $0 \leq deg(R) < deg(P)$. Comme, pour tout $i = 1, \ldots, n$, A_i divise A et P, A_i divise R. Donc R est un multiple commun à tous les A_i et $deg(R)$ appartient à E. Ceci contredit le fait que $p = deg(P)$ est le plus petit élément de E. Donc P divise A pour tout A multiple commun à tous les A_i. On a montré l'existence du ppcm de $\{A_1, \ldots, A_n\}$.

Montrons l'unicité du ppcm. Si P_1 et P_2 sont deux ppcm de $\{A_1, \ldots, A_n\}$, alors P_1 divise P_2 et P_2 divise P_1. Comme P_1 et P_2 sont normalisés, cela implique que $P_1 = P_2$. Le ppcm est donc unique.

QED

Voici quelques propriétés du ppcm :

Proposition 3.9

i) Soit $\{A_1, \ldots, A_n\}$ une famille de polynômes non nuls et B un polynôme non nul et de coefficient dominant b. Alors

$$ppcm\{BA_1, \ldots, BA_n\} = \frac{1}{b} B\, ppcm\{A_1, \ldots, A_n\} .$$

ii) Si A et B sont deux polynômes non nuls, avec $A | B$, et si b est le coefficient dominant de B, alors

$$ppcm\{A, B\} = \frac{1}{b} B .$$

Preuve : i) Quitte à remplacer B par $\frac{1}{b}B$, on peut supposer que B est normalisé. Appelons P le ppcm de $\{A_1, \ldots, A_n\}$. Il faut montrer que BP (qui est alors normalisé) est le ppcm de $\{BA_1, \ldots, BA_n\}$.

Comme, pour tout $i = 1, \ldots, n$, A_i divise P, on a que BA_i divise BP. Donc BP vérifie le (a) de la définition du ppcm.

Soit Q un polynôme non nul tel que, pour tout $i = 1, \ldots, n$, BA_i divise Q. Alors B divise Q et on note $Q_1 = \frac{Q}{B}$. Remarquons que $Q_1 \neq 0$ car $Q \neq 0$.

Comme, pour tout $i = 1, \ldots, n$, BA_i divise $Q = BQ_1$, on en déduit que A_i divise Q_1. De plus, P étant le ppcm de $\{A_1, \ldots, A_n\}$, la propriété (b) de la définition du ppcm implique que P divise Q_1. Donc BP divise $Q = BQ_1$. Par conséquent, BP vérifie la condition (b) de la définition du ppcm.

ii) On suppose encore que B est normalisé. Comme A et B divisent clairement B, B vérifie (a) de la définition du ppcm.

Le polynôme B vérifie le (b) de la définition du ppcm de façon évidente. Donc $B = ppcm\{A, B\}$.

QED

Nous apprendrons plus loin à calculer le ppcm d'une famille de polynômes.

3.4 Le pgcd d'une famille de polynômes

Définition 3.10 (PGCD) *Soit $\{A_1, \ldots, A_n\}$ une famille de polynômes non nuls. On appelle plus grand commun diviseur (pgcd) de $\{A_1, \ldots, A_n\}$ l'unique polynôme non nul et normalisé P tel que*

a) $\forall i = 1, \ldots, n$, $P|A_i$,

b) pour tout polynôme non nul Q, si $\{\forall i = 1, \ldots, n,\ Q|A_i\}$, alors $Q|P$.

Remarque : Le pgcd est **le plus grand** diviseur commun à $A_1, \ldots, A_n$ au sens où il a le plus grand degré.

Notation : Le pgcd de $\{A_1, \ldots, A_n\}$ est noté $pgcd\{A_1, \ldots, A_n\}$

Théorème 3.11 *Soit $\{A_1, \ldots, A_n\}$ une famille de polynômes non nuls. Le pgcd de $\{A_1, \ldots, A_n\}$ existe et est unique.*

L'unicité du pgcd est claire puisque, si P_1 et P_2 sont deux pgcd de $\{A_1, \ldots, A_n\}$, alors P_1 et P_2 se divisent l'un l'autre, et, étant normalisés, sont donc égaux.

Le lemme suivant montre l'existence du pgcd :

Lemme 3.12 *Soient $\{A_1, \ldots, A_n\}$ une famille de polynômes non nuls et $\mathcal{I}$ l'ensemble des polynômes défini par :*

$$\mathcal{I} = \{A \neq 0 \mid \exists Z_1, \ldots, Z_n \text{ des polynômes tels que } A = Z_1A_1 + \ldots + Z_nA_n\} .$$

Alors cet ensemble est non vide et possède un polynôme normalisé P de plus petit degré dans $\mathcal{I}$. Ce polynôme est le pgcd de $\{A_1, \ldots, A_n\}$.

Preuve : L'ensemble $\mathcal{I}$ est non vide car, par exemple A_1^2 appartient à $\mathcal{I}$ (prendre $Z_1 = A_1$, $Z_2 = \ldots = Z_n = 0$). Soit

$$E = \{n \in \mathbb{N} \mid \exists A \in \mathcal{I} \text{ avec } deg(A) = n\} .$$

Comme E est une partie non vide de $\mathbb{N}$, E possède un plus petit élément noté p. Comme p appartient à E, il existe un polynôme P, que l'on peut choisir normalisé, tel que $deg(P) = p$. Montrons que P est le pgcd de $A_1, \ldots, A_n$.

Comme $P \in \mathcal{I}$, il existe des polynômes $Z_1, \ldots, Z_n$ tels que $P = Z_1A_1 + \ldots + Z_nA_n$. Vérifions que P satisfait (a) de la définition du pgcd. Pour cela, on raisonne par l'absurde en supposant qu'il existe $i \in \{1, \ldots, n\}$ tel que P ne divise pas A_i. Soit Q et R respectivement le quotient et le reste de la division euclidienne de A_i par P : $A_i = QP + R$ et $0 \leq deg(R) < deg(P)$. Alors R appartient à $\mathcal{I}$ car $R \neq 0$ par hypothèse et

$$\begin{aligned} R = A_i - QP = \quad & (-Z_1Q)A_1 + \ldots + (-Z_{i-1}Q)A_{i-1} + (1 - Z_iQ)A_i \\ & +(-Z_{i+1}Q)A_{i+1} + \ldots + (-Z_nQ)A_n \ . \end{aligned}$$

Donc $deg(R)$ appartient à E. Mais d'autre part $deg(R) < p$ et p est le plus petit élément de E. On a donc trouvé une contradiction. Par conséquent P divise tous les A_i, $i = 1, \ldots, n$.

Reste à prouver que P satisfait la partie (b) de la définition du pgcd. Pour cela, considérons Q un diviseur commun à tous les A_i. Il est clair alors que Q divise tous les éléments de $\mathcal{I}$. Comme P appartient à $\mathcal{I}$, Q divise donc P.

QED

On déduit de la démonstration le corollaire suivant :

Corollaire 3.13 *Soit $\{A_1, \ldots, A_n\}$ une famille de polynômes non nuls. Il existe alors des polynômes $Z_1, \ldots, Z_n$ tels que*

$$pgcd(A_1, \ldots, A_n) = Z_1A_1 + \ldots + Z_nA_n \ .$$

Voici maintenant quelques propriétés du pgcd qui seront utiles plus tard :

Proposition 3.14
i) Soient $\{A_1, \ldots, A_n\}$ une famille de polynômes non nuls et B un polynôme non nul de coefficient dominant b. Alors

$$pgcd\{BA_1, \ldots, BA_n\} = \frac{B}{b}\, pgcd\{A_1, \ldots, A_n\} \ .$$

ii) Si A et B sont deux polynômes non nuls tels que $A|B$, et si a est le coefficient dominant de A, alors

$$pgcd(A, B) = \frac{A}{a} \ .$$

Preuve : i) On suppose pour simplifier les notations que B est normalisé. Posons $P_1 = pgcd\{A_1, \ldots, A_n\}$ et $P_2 = pgcd\{BA_1, \ldots, BA_n\}$. Il faut montrer que $BP_1 = P_2$.

On remarque d'abord que BP_1 est un diviseur commun à $BA_1, \ldots, BA_n$, car P est un diviseur commun à $A_1, \ldots, A_n$. Donc BP_1 divise P_2. Il existe donc un polynôme Q non nul avec $P_2 = QBP_1$.

Comme P_2 est le pgcd de $\{BA_1, \ldots, BA_n\}$, $P_2 = QBP_1$ est un diviseur commun à $BA_1, \ldots, BA_n$, ce qui implique que QP_1 est un diviseur commun à $A_1, \ldots, A_n$. Or P_1 étant le pgcd de $\{A_1, \ldots, A_n\}$, cela entraîne que QP_1 divise P_1. Or $P_1 \neq 0$ et $Q \neq 0$, donc Q est un scalaire non nul. On a donc prouvé que $P_2 = QBP_2$, avec Q scalaire non nul. Comme P_1, B et P_2 sont normalisés, on en déduit que $Q = 1$ et que $P_2 = BP_1$.

ii) On suppose que A est normalisé. Posons $P = pgcd\{A, B\}$. Comme A divise à la fois A et B, A divise P. De plus, P divise A par définition du pgcd. Comme A et P sont normalisés et se divisent l'un l'autre, on a $P = A$.

QED

La proposition suivante affirme que l'on peut toujours ramener le calcul du pgcd de n polynômes à n calculs du pgcd de 2 polynômes.

Proposition 3.15 *Soient $\{A_1, \ldots, A_n\}$ une famille de polynômes non nuls, avec $n \geq 3$. Alors*

$$pgcd\{A_1, \ldots, A_n\} = pgcd\,\{A_1, pgcd\{A_2, \ldots, A_n\}\} \ .$$

Preuve : Posons $P_1 = pgcd\{A_1, \ldots, A_n\}$, $P_2 = pgcd\{A_2, \ldots, A_n\}$ et $P_3 = pgcd\{A_1, P_2\}$. On veut montrer que $P_1 = P_3$.

Montrons d'abord que P_1 divise P_3. Comme P_1 est un diviseur commun à $A_2, \ldots, A_n$, P_1 divise P_2. Comme de plus, P_1 divise A_1, P_1 divise le pgcd de A_1 et de P_2, i.e., divise P_3.

Réciproquement, P_3 divise à la fois A_1 et P_2. Or P_2 étant un diviseur commun à $A_2, \ldots, A_n$, P_3, divisant P_2, est également un diviseur commun à $A_2, \ldots, A_n$. Donc P_3 divise tous les A_i, avec $i = 1, \ldots, n$, ce qui implique que P_3 divise le pgcd de $\{A_1, \ldots, A_n\}$, c'est-à-dire P_1.

En conclusion, les polynômes normalisés P_1 et P_3 se divisent l'un l'autre, et sont donc égaux.

QED

Voici maintenant le résultat principal de cette partie, qui justifie l'algorithme d'Euclide de calcul du pgcd, que nous introduisons après.

Théorème 3.16 *Soient A_1 et A_2 deux polynômes non nuls. Si A_2 ne divise pas A_1, alors*

$$pgcd\{A_1, A_2\} = pgcd\{A_2, R\}$$

où R est le reste de la division euclidienne de A_1 par A_2.

Preuve : Soient Q et R respectivement le quotient et le reste de la division euclidienne de A_1 par A_2 : $A_1 = QA_2 + R$ et $0 \leq deg(R) < deg(A_2)$. Posons $P_1 = pgcd\{A_2, R\}$ et $P_2 = pgcd\{A_1, A_2\}$. Montrons que $P_1 = P_2$.

(a) Par définition, $P_1 | A_2$. Comme $P_1 | R$ et $P_1 | A_2$, on a aussi $P_1 | QA_2 + R = A_1$. Donc P_1 est un diviseur commun de A_2 et de A_1. Donc P_1 divise P_2 qui est le pgcd de A_1 et A_2.

(b) Réciproquement, P_2 divise A_1 et A_2. Donc P_2 divise aussi $R = A_1 - QA_2$. Par conséquent, P_2 divise le pgcd de A_2 et de R, i.e., divise P_1.

En conclusion, les polynômes normalisés P_1 et P_2 se divisent l'un l'autre, et sont donc égaux.

QED

Décrivons maintenant **l'algorithme d'Euclide**. Comme dans $\mathbb{Z}$, l'objet de l'algorithme est de calculer le pgcd de polynômes non nuls A_1 et A_2.

- **Initialisation :** Posons $R_1 = A_1$ et $R_2 = A_2$
- tant que $R_i \neq 0$, on définit R_{i+1} comme étant le reste de la division euclidienne de R_{i-1} par R_i.

Proposition 3.17 *Soit (R_i) la suite de polynômes définie par l'algorithme d'Euclide. Alors il existe un indice $i_0 \leq deg(A_2) + 2$ tel que $R_{i_0} = 0$ et*

$$pgcd\{A_1, A_2\} = \frac{1}{r_{i_0-1}} R_{i_0-1} \ ,$$

où r_{i_0-1} est le coefficient dominant de R_{i_0-1}.

Exemple : Si $A_1 = X^3 + X + 2$ et $A_2 = X^2 - 1$, on a

- $R_1 = A_1 = X^3 + X + 2$ et $R_2 = A_2 = X^2 - 1$,
- $R_3 = 2X + 2$ car $R_1 = XR_2 + 2X + 2$
- $R_4 = 0$ car R_3 divise R_2.
- Conclusion : $pgcd(A_1, A_2) = \frac{1}{2} R_3 = X + 1$

Preuve de la proposition 3.17 : Par définition du reste de la division euclidienne, la suite $(deg(R_i))$ est strictement décroissante à partir du rang $i = 2$. On montre donc facilement par récurrence que $deg(R_i) \leq deg(R_2) - i + 2$ pour $i \geq 2$. Or $deg(R_i) \geq 0$ est positif pour tout $i < i_0$. L'algorithme s'arrête donc au plus tard en temps $i_0 \leq deg(R_2) + 2$.

On démontre également par récurrence, en utilisant le théorème 3.16, que, pour tout $i < i_0 - 1$,

$$pgcd\{A_1, A_2\} = pgcd\{R_{i-1}, R_i\} \ . \tag{4}$$

Or, par définition de i_0, le polynôme R_{i_0-1} divise R_{i_0-2}. La proposition 3.14 affirme alors que

$$pgcd\{R_{i_0-2}, R_{i_0-1}\} = \frac{1}{r_{i_0-1}} R_{i_0-1} \ . \tag{5}$$

En mettant ensembles les égalités (4) et (5), on obtient le résultat désiré : $pgcd\{A_1, A_2\} = \frac{1}{r_{i_0-1}} R_{i_0-1}$.

QED

3.5 Polynômes premiers entre eux

Définition 3.18 *Soit $\{A_1, \ldots, A_n\}$ une famille de polynômes non nuls. On dit que les polynômes $A_1, \ldots, A_n$ sont premiers entre eux si leur pgcd est 1.*

Exemple : Par exemple, les polynômes $A_1(X) = X^4 + X^2 + 1$ et $A_2(X) = X^2 + 1$ sont premiers entre eux car $pgcd(A_1, A_2) = pgcd(A_2, 1) = 1$ car 1 est le reste de la division euclidienne de A_1 par A_2.

Théorème 3.19 (Bezout) *Soit $\{A_1, \ldots, A_n\}$ une famille de polynômes non nuls. Alors les polynômes $A_1, \ldots, A_n$ sont premiers entre eux si et seulement si il existe n polynômes $Z_1, \ldots, Z_n$ tels que*

$$Z_1 A_1 + \ldots + Z_n A_n = 1 \ . \tag{6}$$

On appelle **relation de Bezout une relation du type (6)**.

Preuve : Supposons d'abord que $A_1, \ldots, A_n$ sont premiers entre eux. Comme le pgcd de $A_1, \ldots, A_n$ est 1, le corollaire 3.13 affirme qu'il existe n polynômes $Z_1, \ldots, Z_n$ tels que $Z_1 A_1 + \ldots + Z_n A_n = 1$.

Réciproquement, supposons qu'il existe n polynômes $Z_1, \ldots, Z_n$ tels que $Z_1 A_1 + \ldots + Z_n A_n = 1$. Soit P le pgcd de $A_1, \ldots, A_n$. Comme P est un diviseur commun de $A_1, \ldots, A_n$, P divise également $Z_1 A_1 + \ldots + Z_n A_n$, i.e., P divise 1. Comme P est normalisé, P ne peut être égal qu'à 1. En conclusion, $A_1, \ldots, A_n$ sont premiers entre eux.

QED

Comment trouver une relation de Bezout ?

Comme dans$\mathbb{Z}$, pour trouver une relation de Bezout, on utilise l'algorithme d'Euclide, en écrivant à chaque étape le quotient et le reste de la division euclidienne de R_{i+1} par R_i (cf les notations de l'algorithme).

Par exemple, soit $A_1 = X^4 + 1$ et $A_2 = X^3 + 1$.

- Posons $R_1 = A_1$ et $R_2 = A_2$.
- Effectuons la division euclidienne de R_1 par R_2. Alors $R_1 = XR_2 + (-X + 1)$, donc $R_3 = (-X + 1) = A_1 - XA_2$.

- Effectuons maintenant la division euclidienne de R_2 par R_3. Alors $R_2 = R_3(-X^2 - X - 1) + 2$ et on pose $R_4 = 2$.

- D'où

$$\begin{aligned} 1 &= \tfrac{1}{2}A_2 + \tfrac{1}{2}(X^2 + X + 1)(-X + 1) = \tfrac{1}{2}A_2 + \tfrac{1}{2}(X^2 + X+)(A_1 - XA_2) \\ &= \tfrac{1}{2}(X^2 + X + 1)A_1 - \tfrac{1}{2}(X^3 + X^2 + X - 1)A_2 \ . \end{aligned}$$

  On a donc trouvé la relation de Bezout suivante : $\frac{1}{2}(X^2+X+1)A_1 - \frac{1}{2}(X^3+X^2+X-1)A_2 = 1$.

Théorème 3.20 (Gauss) *Soient A, B et C trois polynômes non nuls. Si A divise BC et est premier avec B, alors A divise C.*

Preuves : Comme A et B sont premiers entre eux, le théorème de Bezout affirme qu'il existe Z_1 et Z_2 tels que

$$Z_1 A + Z_2 B = 1 \ . \qquad \text{D'où } Z_1 AC + Z_2 BC = C \ .$$

Comme A divise à la fois AC et BC, A divise $Z_1AC + Z_2BC$, c'est-à-dire que A divise C.

QED

Une conséquence cruciale du théorème de Gauss est le corollaire suivant :

Corollaire 3.21 *Soient A, B et C trois polynômes, avec A et B non nuls et premiers entre eux. Si $A|C$ et $B|C$ alors $(AB)|C$.*

Preuve : Comme $A|C$, il existe un polynôme D tel que $C = AD$. Or $B|C$, donc $B|(AD)$. Comme A et B sont premiers entre eux, le théorème de Gauss affirme que $B|D$. Donc $(AB)|C$.

QED

Une autre application du théorème de Bezout est la suivante :

Proposition 3.22 *Soit $\{A_1, \ldots, A_n\}$ une famille de polynômes non nuls. Alors un polynôme non nul et normalisé P est le pgcd de $A_1, \ldots, A_n$ si et seulement si P est un diviseur commun de $A_1, \ldots, A_n$ et les polynômes $\frac{A_1}{P}, \ldots, \frac{A_n}{P}$ sont premiers entre eux.*

Preuve : Supposons d'abord que P est le pgcd de $A_1, \ldots, A_n$. Alors on sait que P est un diviseur commun de $A_1, \ldots, A_n$. De plus, le corollaire 3.13 affirme qu'il existe des polynômes $Z_1, \ldots, Z_n$ tels que $Z_1A_1 + \ldots + Z_nA_n = P$. En divisant cette égalité par P, on obtient :

$$Z_1 \frac{A_1}{P} + \ldots + Z_n \frac{A_n}{P} = 1 \ .$$

Le théorème de Bezout affirme alors que les polynômes $\frac{A_1}{P}, \ldots, \frac{A_n}{P}$ sont premiers entre eux.

Réciproquement, supposons que P est un diviseur commun de $A_1, \ldots, A_n$ et les polynômes $\frac{A_1}{P}, \ldots, \frac{A_n}{P}$ sont premiers entre eux. Notons D le pgcd de $A_1, \ldots, A_n$. Comme P est un diviseur commun de $A_1, \ldots, A_n$, P divise D par définition du pgcd. De plus, comme $\frac{A_1}{P}, \ldots, \frac{A_n}{P}$ sont premiers entre eux, le théorème de Bezout affirme qu'il existe des polynômes $Z_1 \ldots, Z_n$ tels que $Z_1 \frac{A_1}{P} + \ldots Z_n \frac{A_n}{P} = 1$, ce qui implique que $Z_1A_1 + \ldots Z_nA_n = P$. Comme D est un diviseur commun de $A_1, \ldots, A_n$, D divise $Z_1A_1 + \ldots Z_nA_n$, et donc divise P. Nous avons prouvé que les polynômes normalisés D et P se divisent l'un l'autre. Ils sont donc égaux.

QED

Nous expliquons maintenant comment calculer le ppcm de deux polynômes à partir de leur pgcd : pour cela, commençons par un résultat intermédiaire.

Proposition 3.23 *Soient A et B deux polynômes non nuls premiers entre eux, de coefficients dominant respectif a et b. Alors le ppcm de A et B est égal à $\frac{1}{ab}AB$.*

Preuve : On suppose pour simplifier, que A et B sont normalisés. Posons $P = ppcm\{A, B\}$. Comme AB est un multiple commun de A et de B, P divise AB (condition (b) de la définition du ppcm).

Comme A divise P, il existe un polynôme K tel que $P = AK$. Or B divise également P, donc divise AK. Or A et B sont premiers entre eux. Le théorème de Gauss affirme alors que B divise K. Donc il existe un polynôme R tel que $K = BR$. D'où $P = ABR$. On en déduit que AB divise P.

Les polynômes normalisés P et AB se divisent l'un l'autre, donc sont égaux.

QED

Voici maintenant la relation entre ppcm et pgcd dans le cas général :

Théorème 3.24 *Soient A et B deux polynômes non nuls de coefficient dominant respectivement a et b. Alors*

$$ab\, pgcd\{A, B\}\, ppcm\{A, B\} = AB\ .$$

Preuve : On suppose pour simplifier que A et B sont normalisés. Posons $D = pgcd\{A, B\}$. La proposition 3.22 affirme que D divise A et B et que les polynômes $\frac{A}{D}$ et $\frac{B}{D}$ sont premiers entre eux. D'après la proposition 3.23, le ppcm de $\frac{A}{D}$ et $\frac{B}{D}$ est égal à $\frac{AB}{D^2}$.

Donc

$$ppcm\{A, B\} = ppcm\{D\frac{A}{D}, D\frac{B}{D}\} = D\, ppcm\{\frac{A}{D}, \frac{B}{D}\} = D\,\frac{AB}{D^2} = \frac{AB}{D}\ .$$

On en déduit l'égalité désirée.

QED

3.6 Polynômes premiers

Définition 3.25 *On appelle polynôme premier tout polynôme P non nul, de degré supérieur ou égal à 1, qui n'est divisible que par les polynômes constants ou par les polynômes de la forme λP où λ est un scalaire non nul.*

Voici un exemple fondamental :

Proposition 3.26 *Soit P un polynôme de degré 1. Alors P est premier.*

Preuve : Si Q est un diviseur de P, comme $P \neq 0$, $deg(Q) = 0$ ou $deg(Q) = 1$. Dans le premier cas, Q est un polynôme constant. Dans le second, Q est un polynôme de degré 1, et le quotient de P par Q est un polynôme constant. Donc Q est de la forme λP avec $\lambda \neq 0$. Par conséquent, P est un polynôme premier.

QED

Le théorème suivant affirme que tout polynôme possède des diviseurs premiers :

Théorème 3.27 *Soit A un polynôme, avec $deg(A) \geq 1$. Il existe un polynôme premier qui divise A.*

Preuve : Notons $\mathcal{I}$ l'ensemble des polynômes de degré supérieur ou égal à 1 qui divisent A. Notons que $\mathcal{I}$ est non vide car A appartient à $\mathcal{I}$. Soit maintenant

$$E = \{n \in \mathbb{N}^* \mid \exists B \in \mathcal{I} \text{ avec } n = deg(B)\} .$$

Comme A appartient à $\mathcal{I}$, $n = deg(A)$ appartient à E. Donc E est une partie non vide de $\mathbb{N}$ et possède un plus petit élément, noté p. Par définition de E, il existe un polynôme $P \in \mathcal{I}$ de degré p. Comme $P \in \mathcal{I}$, $p = deg(P) \geq 1$.

Montrons que P est premier. Soit Q un polynôme qui divise P. Alors Q divise aussi A, car, comme $P \in \mathcal{I}$, P divise A. Il y a alors deux possibilités :

- soit $deg(Q) = 0$, c'est-à-dire que Q est constant,
- soit $deg(Q) \geq 1$, et donc $deg(Q)$ appartient à E. Or $p = deg(P)$ est le plus petit élément de E. Donc $deg(Q) \geq deg(P)$. Comme Q divise P, il existe un scalaire non nul λ tel que $Q = \lambda P$.

On a prouvé que, si Q divise P, alors soit Q est constant, soit Q est de la forme λP avec $\lambda \neq 0$. Donc P est un diviseur premier de A.

QED

3.7 Décomposition d'un polynôme en facteurs premiers

Théorème 3.28 *Tout polynôme non nul A peut s'écrire d'une manière unique sous la forme :*

$$A = \lambda (P_1)^{k_1} \dots (P_m)^{k_m}$$

où λ est un scalaire non nul, $P_1, \dots, P_m$ sont des polynômes premiers et normalisés distincts et $k_1, \dots, k_m$ sont des entiers strictement positifs.

Remarque : L'unicité signifie ici que si on a deux expressions de cette forme :

$$A = \lambda_1 (P_1)^{k_1} \dots (P_m)^{k_m} = \lambda_2 (Q_1)^{r_1} \dots (Q_n)^{r_n}$$

avec λ_1 et λ_2 des scalaires non nuls, $P_1, \dots, P_m$ (respectivement $Q_1, \dots, Q_n$) des polynômes premiers et normalisés distincts et $k_1, \dots, k_m$ (respectivement $r_1, \dots, r_n$) des entiers strictement positifs, alors $m = n$, $\lambda_1 = \lambda_2$ et, pour tout $i \in \{1, \dots, n\}$, il existe un indice $j \in \{1, \dots, n\}$ tel que $P_i = Q_j$ et $k_i = r_j$.

Preuve : On ne démontre que l'existence. On raisonne par récurrence généralisée sur le degré de A. Si $deg(A) = 1$, le résultat est évident car A est premier.

Supposons le résultat vrai pour tous les polynômes de degré inférieur ou égal à n, $n \geq 1$. Montrons qu'il est encore vrai pour les polynômes de degré $n+1$. Soit A un polynôme de degré $n+1$. D'après le théorème 3.27, le polynôme A possède un diviseur premier, noté P. Posons $B = \frac{A}{P}$.

Il y a alors 2 cas : soit B est constant, et alors le résultat est démontré. Soit $deg(B) \geq 1$, et on a alors $1 \leq deg(B) < deg(A) = n+1$. Par hypothèse de récurrence, il existe alors un scalaire $\lambda \neq 0$, des polynômes premiers et normalisés distincts $P_1, \dots, P_m$ et des entiers strictement positifs $k_1, \dots, k_m$ tels que

$$B = \lambda (P_1)^{k_1} \dots (P_m)^{k_m} .$$

Donc

$$A = \lambda P (P_1)^{k_1} \dots (P_m)^{k_m}$$

et A possède une décomposition en facteurs premiers.

Par récurrence, on en déduit l'existence de la décomposition pour tout polynôme A.

QED

Application au calcul du pgcd et du ppcm : Soient A et B deux polynômes non nuls de degré supérieurs à 1. On suppose que

$$A = \lambda_1 (P_1)^{k_1} \dots (P_m)^{k_m} \text{ et } b = \lambda_2 (P_1)^{r_1} \dots (P_m)^{r_m}$$

avec λ_1 et λ_2 des scalaires non nuls, $P_1, \dots, P_m$ des polynômes premiers et normalisés distincts et $k_1, \dots, k_m$ (respectivement $r_1, \dots, r_m$) des *entiers positifs ou nuls* (de façon à avoir une écriture commune pour A et B). Alors

$$pgcd\{A, B\} = (P_1)^{\min\{k_1, r_1\}} \dots (P_m)^{\min\{k_m, r_m\}} \text{ et } ppcm\{A, B\} = (P_1)^{\max\{k_1, r_1\}} \dots (P_m)^{\max\{k_m, r_m\}} .$$

3.8 Racine d'un polynôme

A partir de maintenant, nous sommes obligés de faire une nette distinction entre le cas réel et le cas complexe. Afin de ne pas trop alourdir les énoncés, on introduit la notation $\mathbf{k}$ qui signifie indifféremment $\mathbb{R}$ ou $\mathbb{C}$, et $\mathbf{k}[X]$ qui signifie $\mathbb{R}[X]$ ou $\mathbb{C}[X]$. La notation $\mathbf{k}$ signifie toujours la même chose à l'intérieur d'un même énoncé.

Définition 3.29 (Racine) *Soit P un polynôme de $\mathbf{k}[X]$ et $\alpha \in \mathbf{k}$ un scalaire. On dit que α est une racine de P si $P(\alpha) = 0$.*

Par exemple, le polynôme $P(X) = X^2 + 1$ n'a pas de racine réelle, mais a pour racines complexes i et $-i$.

Notons qu'un polynôme de degré 1 possède toujours une et une seule racine :

Lemme 3.30 *Soit $P(X) = aX + b$ un polynôme de $\mathbf{k}[X]$ avec $a \neq 0$. Alors P possède une, et une seule, racine dans $\mathbf{k}$.*

Preuve : Il est clair que la seule racine de P est $-b/a$.

QED

Lemme 3.31 *Si $P|Q$ et α est une racine de P, alors α est une racine de Q.*

Preuve : En effet, comme P divise Q, il existe un polynôme A tel que $Q = AP$. Alors $Q(\alpha) = A(\alpha)P(\alpha) = 0$ car $P(\alpha) = 0$.

QED

La caractérisation suivante des racines joue un rôle essentiel dans toute la suite :

Théorème 3.32 *Soit $P \in \mathbf{k}[X]$ et $\alpha \in \mathbf{k}$. Alors α est une racine de P si et seulement si $(X - \alpha)$ divise P dans $\mathbf{k}[X]$.*

Preuve : On suppose d'abord que α est une racine de P. Pour montrer que $(X - \alpha)$ divise P, notons Q et R le quotient et le reste de la division euclidienne de P par $(X - \alpha)$:

$$P(X) = Q(X)(X - \alpha) + R(X) \text{ et } deg(R) < deg(X - \alpha) = 1 .$$

Comme $deg(X - \alpha) = 1$, R est un polynôme constant. Or

$$0 = P(\alpha) = Q(\alpha).0 + R(\alpha) = R(\alpha)$$

car α est une racine de P. Donc le polynôme constant R est nul, ce qui prouve que $(X - \alpha)$ divise P.

Réciproquement, si $(X - \alpha)$ divise P, alors comme α est une racine de $(X - \alpha)$, α est aussi une racine de P.

QED

Corollaire 3.33 *Soient n un entier naturel et P un polynôme de degré inférieur ou égal à n. Si P a au moins $n+1$ racines distinctes, alors P est égal au polynôme nul.*

Preuve : On fait la preuve par récurrence sur n. Pour $n = 0$, c'est vrai car un polynôme constant qui s'annule en au moins un point est identiquement nul.

On suppose que le résultat est vrai pour n. Montrons-le pour $n+1$. Soit P un polynôme de degré au plus $(n+1)$, qui possède au moins $(n+2)$ racines distinctes $\alpha_1, \ldots, \alpha_{n+2}$. On sait alors que P est divisible par $(X - \alpha_{n+2})$. Soit Q tel que $P(X) = Q(X)(X - \alpha_{n+2})$. Comme le degré de P est au plus $n+1$, le degré de Q est au plus n. Montrons que $\alpha_1, \ldots, \alpha_{n+1}$ sont des racines de Q. En effet

$$\forall i \in \{1, \ldots, n+1\},\ P(\alpha_i) = 0 = (\alpha_i - \alpha_{n+2})Q(\alpha_i)\ .$$

Comme $\alpha_i \neq \alpha_{n+2}$ si $i \in \{1, \ldots, n+1\}$, cette dernière égalité montre que $Q(\alpha_i) = 0$. Donc, pour tout $i \in \{1, \ldots, n+1\}$, α_i est une racine de Q. Nous avons montré que le polynôme Q, de degré au plus n, possède au moins $n+1$ racines distinctes. L'hypothèse de récurrence affirme alors que Q est nul. Donc $P = (X - \alpha_{n+2})Q$ l'est aussi.

QED

Le théorème suivant est souvent appelé **théorème fondamental de l'algèbre** :

Théorème 3.34 (dit de d'Alembert) *Soit $P \in \mathbb{C}[X]$ un polynôme non constant. Alors P possède au moins une racine complexe.*

On dit aussi que $\mathbb{C}$ est *algébriquement clos*. La démonstration de ce résultat est difficile et hors programme.

Remarque : En particulier, tout polynôme non constant de $\mathbb{R}[X]$ possède au moins une racine réelle ou complexe.

Corollaire 3.35 *Les polynômes premiers de $\mathbb{C}[X]$ sont les polynômes de degré 1.*

Preuve : Soit P un polynôme de degré 1. Alors nous avons déjà montré que P est premier.

Réciproquement, soit P un polynôme premier de $\mathbb{C}[X]$. Comme $deg(P) \geq 1$, P n'est pas constant. Donc le théorème de d'Alembert affirme que P possède au moins une racine $\alpha \in \mathbb{C}$. Donc $(X - \alpha)$ divise P. Comme P est premier, cela implique qu'il existe une constante $\beta \in \mathbb{C}^*$ telle que $P(X) = \beta(X - \alpha)$ et prouve que P est un polynôme de degré 1.

QED

On en déduit la factorisation en facteurs premiers d'un polynôme de $\mathbb{C}[X]$.

Théorème 3.36 *Soit P un polynôme de $\mathbb{C}[X]$, $\alpha_1, \ldots, \alpha_n$ les racines distinctes de P dans $\mathbb{C}$. Il existe alors une constante $\beta \in \mathbb{C}^*$, et des entiers strictement positifs $k_1, \ldots, k_n$ tels que*

$$P(X) = \beta(X - \alpha_1)^{k_1} \ldots (X - \alpha_n)^{k_n}\ .$$

De plus, le degré de P est $k_1 + k_2 + \ldots + k_n$, c'est-à-dire que P possède exactement $deg(P)$ racines à condition de les compter avec leur ordre de multiplicité.

Preuve : C'est une conséquence immédiate du théorème de factorisation en facteurs premiers d'un polynôme et de la caractérisation des polynômes premiers de $\mathbb{C}[X]$.

QED

Nous cherchons maintenant à caractériser les polynômes premiers de $\mathbb{R}[X]$. Pour cela, nous avons besoin de deux résultats préliminaires :

Lemme 3.37 *Soit P un polynôme de $\mathbb{R}[X]$ et $\alpha \in \mathbb{C}$ une racine de P dans $\mathbb{C}[X]$.*
Alors le conjugué de α, noté $\bar{\alpha}$, est aussi une racine de P.

Preuve : En effet, si $P(X) = a_0 + a_1 X + \ldots + a_n X^n$, α est une racine de P signifie que $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$. Prenons le conjugué de cette expression :

$$0 = \overline{a_0 + a_1\alpha + \ldots + a_n\alpha^n} = \overline{a_0} + \overline{a_1\alpha} + \ldots + \overline{a_n\alpha^n} = a_0 + a_1\bar{\alpha} + \ldots + a_n\bar{\alpha}^n = P(\bar{\alpha})$$

car les coefficients a_i sont réels. Ceci prouve que $\bar{\alpha}$ est une racine de P.

QED

Lemme 3.38 *Soient P et Q deux polynômes de $\mathbb{R}[X]$. On suppose que Q divise P dans $\mathbb{C}[X]$. Alors Q divise P dans $\mathbb{R}[X]$.*

Preuve : Par hypothèse, il existe un polynôme $R \in \mathbb{C}[X]$ tel que $P = QR$. Montrons que les coefficients de R sont en fait réels. En effet, comme P et Q sont des polynômes réels,

$$\bar{P} = P = \overline{QR} = \bar{Q}\bar{R} = Q\overline{R}\,.$$

Donc $\overline{R}$ est également le quotient de P par Q. Ce quotient étant unique, cela prouve que $\overline{R} = R$, c'est-à-dire que R est à coefficients réels.

QED

Nous décrivons maintenant les polynômes premiers de $\mathbb{R}[X]$.

Théorème 3.39 *Soit P un polynôme de $\mathbb{R}[X]$. Alors P est premier si et seulement si, soit $deg(P) = 1$, soit $deg(P) = 2$ et P n'a pas de racine réelle.*

Preuve : Montrons d'abord que, $deg(P) = 1$, ou si $deg(P) = 2$ et P n'a pas de racine réelle, alors P est premier. Si $deg(P) = 1$, nous avons vu que c'est bien le cas. Supposons maintenant que $deg(P) = 2$ et que P n'a pas de racine réelle. Si $Q \in \mathbb{R}[X]$ est un diviseur de P, alors, comme $P \neq 0$, on a $deg(Q) = 0$, 1 ou 2. Supposons un instant que $deg(Q) = 1$. Alors Q possède une racine réelle $\alpha \in \mathbb{R}$. Or Q divise P, donc α est aussi une racine de P. C'est impossible car P n'a pas de racine réelle par hypothèse. Donc soit $deg(Q) = 0$, et Q est alors constant, soit $deg(Q) = 2 = deg(P)$, et, comme Q divise P, il existe un réel non nul λ tel que $Q = \lambda P$. Ceci prouve que P est premier.

Réciproquement, supposons que P soit un polynôme premier. Comme $deg(P) \geq 1$, P possède au moins une racine α, réelle ou complexe (cf théorème de d'Alembert). Si α est réel, alors le polynôme réel $(X - \alpha)$ divise P. Comme P est premier, il existe $\beta \in \mathbb{R}^*$ tel que $P(X) = \beta(X - \alpha)$. Donc P est de degré 1. Supposons maintenant que $\alpha \notin \mathbb{R}$. Alors le conjugué de α, noté $\bar{\alpha}$, est différent de α et est aussi une racine de P. Les polynômes $(X - \alpha)$ et $(X - \bar{\alpha})$ divise P dans $\mathbb{C}[X]$. Ces polynômes sont premiers (car de degré 1), et distincts, car $\alpha \neq \bar{\alpha}$. Donc ces polynômes sont premiers entre eux. Comme chacun d'eux divise P dans $\mathbb{C}[X]$, leur produit $(X - \alpha)(X - \bar{\alpha})$ divise aussi P dans $\mathbb{C}[X]$. Or

$$(X - \alpha)(X - \bar{\alpha}) = X^2 - 2\mathcal{R}e(\alpha)X + |\alpha|^2$$

est un polynôme réel. Donc $X^2 - 2\mathcal{R}e(\alpha)X + |\alpha|^2$ divise P dans $\mathbb{R}[X]$. Comme P est premier, il existe une constante $\beta \in \mathbb{R}^*$ telle que $P(X) = \beta(X^2 - 2\mathcal{R}e(\alpha)X + |\alpha|^2)$, et P est un polynôme de degré 2 sans racine réelle.

QED

3.9 Dérivée d'un polynôme et formule de Taylor

Définition 3.40 (Dérivée) *Soit P un polynôme de $\mathbf{k}[X]$, $P(X) = a_0 + a_1X + \dots a_nX^n = \sum_{k=0}^n X^k$. Le polynôme dérivé de P, noté P', est le polynôme*

$$P'(X) = a_1 + 2a_2X + 3a_3X^2 + \dots + na_nX^{n-1} = \sum_{k=1}^{n} ka_kX^{k-1} .$$

Notons en particulier que :

Proposition 3.41 *Si $P \in \mathbf{k}[X]$ et si $deg(P) \geq 1$, alors $deg(P') = deg(P) - 1$.*

Proposition 3.42 *Si P_1 et P_2 sont deux polynômes de $\mathbf{k}[X]$, et si $\lambda \in \mathbf{k}$, alors*

1. **Dérivée d'une somme :** $(P_1 + P_2)' = P_1' + P_2'$,
2. **Dérivée du produit par un scalaire :** $(\lambda P)' = \lambda P'$,
3. **Dérivée d'un produit de polynômes :** $(P_1P_2)' = P_1'P_2 + P_1P_2'$.

Preuve : Seule la dernière assertion pose vraiment une difficulté de démonstration, c'est donc elle seule que nous démontrons. Remarquons d'abord que le résultat est vrai si $P_1(X) = X^m$ et $P_2(X) = X^n$. En effet,

$$(P_1P_2)'(X) = (X^{m+n})' = (m+n)X^{n+m-1}$$

tandis que

$$P_1'(X)P_2(X)+P_1(X)P_2'(X) = mX^{m-1}X^n+X^m(nX^{n-1}) = mX^{m+n-1}+nX^{m+n-1} = (m+n)X^{n+m-1} .$$

Démontrons maintenant le résultat dans le cas général. Soient $P_1(X) = \sum_{k=0}^n a_kX^k$ et $P_2(X) = \sum_{i=0}^n b_iX^i$. Alors

$$\begin{aligned}
(P_1P_2)'(X) &= \left(\sum_{k=0}^n \sum_{i=0}^n a_kb_iX^{k+i}\right)' \\
&= \sum_{k=0}^n \sum_{i=0}^n a_kb_i(X^{k+i})' \\
&= \sum_{k=0}^n \sum_{i=0}^n a_kb_i\left((X^k)'X^i + X^k(X^i)'\right) \\
&= \left(\sum_{k=0}^n \sum_{i=0}^n a_kb_i(X^k)'X^i\right) + \left(\sum_{k=0}^n \sum_{i=0}^n a_kb_iX^k(X^i)'\right) \\
&= \left(\sum_{k=0}^n a_k(X^k)'\right)\left(\sum_{i=0}^n b_iX^i\right) + \left(\sum_{k=0}^n a_kX^k\right)\left(\sum_{i=0}^n b_i(X^i)'\right) \\
&= P_1'(X)P_2(X) + P_1(X)P_2'(X)
\end{aligned}$$

QED

Définition 3.43 (Dérivées *n*ièmes) *Pour $n \in \mathbb{N}^*$, on définit par récurrence la dérivée nième d'un polynôme, notée $P^{(n)}$:*

$P^{(1)}(X) = P'(X)$ et, si $P^{(n)}$ a été défini, alors $P^{(n+1)} = \left(P^{(n)}\right)'$.

Par convention, on notera $P^{(0)} = P$.

Exemple fondamental : Si $P(X) = X^m$ (avec $m \geq 1$), alors

$$\forall k \in \{0, \dots, m\},\ P^{(k)}(X) = \frac{m!}{(m-k)!}X^{m-k} ,$$

et

$$\forall k \geq m+1,\ P^{(k)}(X) = 0 .$$

Preuve : On fait la preuve par récurrence sur k. Pour $k = 0$ et $k = 1$, c'est évident.

On suppose le résultat vrai pour $k \geq 1$, et on le montre pour $k+1$. L'hypothèse de récurrence affirme que, si $k \leq m$, alors $P^{(k)}(X) = \frac{m!}{(m-k)!}X^{m-k}$, et si $k > m$, alors $P^{(k)}(X) = 0$.

Supposons d'abord $k+1 \leq m$. On dérive l'égalité $P^{(k)}(X) = \frac{m!}{(m-k)!}X^{m-k}$:

$$P^{(k+1)}(X) = \frac{m!}{(m-k)!}(m-k)X^{m-k-1} = \frac{m!}{(m-k-1)!}X^{m-k-1} ,$$

ce qui est le résultat désiré. Si $k = m$, alors $P^{(k)}(X)$ est un polynôme constant. Donc sa dérivée est nulle : $P^{(k+1)}(X) = 0$. Finalement, si $k > m$, alors $P^{(k)}(X)$ est nul, donc $P^{(k+1)}(X) = 0$. Nous avons montré le résultat au rang $k+1$.

Par récurrence, on en déduit le résultat pour tout k.

QED

Théorème 3.44 (Formules de Taylor) *Soient n un entier naturel et P un polynôme de $\mathbf{k}[X]$ de degré au plus n. Alors, pour tout $\alpha \in \mathbf{k}$, on a*

$$P(X) = \sum_{k=0}^{n} \frac{(X-\alpha)^k}{k!}P^{(k)}(\alpha) .$$

Preuve : Démontrons d'abord la formule pour les polynômes $P_i(X) = X^i$ $(i \in \{0, \ldots, n\})$:

$$\sum_{k=0}^{n} \frac{(X-\alpha)^k}{k!}P_i^{(k)}(\alpha) = \sum_{k=0}^{i} \frac{(X-\alpha)^k}{k!}\frac{i!}{(i-k)!}\alpha^{(i-k)} = \sum_{k=0}^{i} \frac{i!}{k!(i-k)!}(X-\alpha)^k\alpha^{(i-k)}$$

Appliquons la formule du binôme de Newton à cette égalité :

$$\sum_{k=0}^{i} \frac{i!}{k!(i-k)!}(X-\alpha)^k\alpha^{(i-k)} = (X-\alpha+\alpha)^i = X^i = P_i(X) .$$

Donc la formule est démontrée pour les polynômes $P_i(X) = X^i$.

Montrons-la maintenant pour un polynôme P quelconque de degré inférieur ou égal à n : $P(X) = \sum_{i=0}^{n} a_i X^i = \sum_{i=0}^{n} a_i P_i(X)$.

$$\sum_{k=0}^{n} \frac{(X-\alpha)^k}{k!}P^{(k)}(\alpha) = \sum_{k=0}^{n} \frac{(X-\alpha)^k}{k!}\left(\sum_{i=0}^{n} a_i P_i^{(k)}(\alpha)\right) = \sum_{i=0}^{n} a_i \left(\sum_{k=0}^{n} \frac{(X-\alpha)^k}{k!}P_i^{(k)}(\alpha)\right)$$

Or nous avons déjà montré la formule de Taylor pour les polynômes P_i. Donc

$$\sum_{k=0}^{n} \frac{(X-\alpha)^k}{k!}P^{(k)}(\alpha) = \sum_{i=0}^{n} a_i P_i(X) = P(X) .$$

QED

3.10 Multiplicité d'une racine

Théorème 3.45 (Multiplicité d'une racine) *Soit P un polynôme non nul de $\mathbf{k}[X]$ et $\alpha \in \mathbf{k}$ une racine de P.*

Il existe un unique entier $k \in \mathbb{N}^*$ tel que

a) $(X-\alpha)^k$ divise P,

b) $(X-\alpha)^{k+1}$ ne divise pas P.

On dit que la racine α est de multiplicité k.

Preuve : Montrons d'abord qu'il existe un entier $k \geq 1$ tel que $(X-\alpha)^k$ divise P et $(X-\alpha)^{k+1}$ ne divise pas P. Soit A l'ensemble des entiers naturels n tels que $(X-\alpha)^{n+1}$ ne divise pas P. Alors A est non vide car, comme P est non nul, $n = deg(P)$ appartient à A. Soit k le plus petit élément de A. Alors $k \geq 1$ car $(X-\alpha)$ divise P, et donc $0 \notin A$. De plus, comme k appartient à A, $(X-\alpha)^{k+1}$ ne divise pas P. Enfin, comme k est le plus petit élément de A, l'entier naturel $k-1$ n'appartient pas à A, et donc $(X-\alpha)^k$ divise P. Donc nous avons prouvé l'existence d'un entier k possédant les propriétés désirées.

Montrons maintenant que cet entier est unique. Soit $n \geq 1$ un autre entier tel que $(X-\alpha)^n$ divise P et $(X-\alpha)^{n+1}$ ne divise pas P. Notons que n appartient à l'ensemble A défini plus haut. De plus, pour tout entier $m < n$, le polynôme $(X-\alpha)^{m+1}$ divise $(X-\alpha)^n$, et donc divise P. On a donc montré que, pour tout entier $m < n$, m n'appartient pas à A. Donc n est le plus petit élément de A, et $n = k$.

QED

Terminologie : Une racine de multiplicité 1 est également appelée **racine simple**, une racine de multiplicité 2, **racine double**, etc...

Théorème 3.46 *Soient P un polynôme non nul de $\mathbf{k}[X]$, $\alpha \in \mathbf{k}$ une racine de P et k un entier naturel non nul.*

Alors α est de multiplicité k si et seulement si

$$\forall n \in \{0, \ldots, k-1\},\ P^{(n)}(\alpha) = 0 \text{ et } P^{(k)}(\alpha) \neq 0\ .$$

Par exemple, α est une racine simple de P si et seulement si $P(\alpha) = 0$ et $P'(\alpha) \neq 0$. De même, α est une racine double de P si et seulement si $P(\alpha) = P'(\alpha) = 0$ et $P''(\alpha) \neq 0$.

Preuve : Soit $r \geq 1$ le plus grand entier tel que $\forall n \in \{0, \ldots, r-1\},\ P^{(n)}(\alpha) = 0$. Un tel entier existe car, si P est de degré d, alors $P^{(d)}$ est un polynôme constant et non nul. Donc $P^{(d)}(\alpha) \neq 0$. Notre objectif est de montrer que r est la multiplicité de la racine α.

Notons d'abord que $P^{(r)}(\alpha) \neq 0$. Ecrivons la formule de Taylor en α : si $deg(P) = m$ (avec $m \geq r$), alors

$$P(X) = \sum_{n=0}^{m} \frac{(X-\alpha)^n}{n!} P^{(n)}(\alpha) = \sum_{n=r}^{m} \frac{(X-\alpha)^n}{n!} P^{(n)}(\alpha) = (X-\alpha)^r \left(\sum_{n=r}^{m} \frac{(X-\alpha)^{n-r}}{n!} P^{(n)}(\alpha) \right) .$$

Notons $Q(X)$ le polynôme $\sum_{n=r}^{m} \frac{(X-\alpha)^{n-r}}{n!} P^{(n)}(\alpha)$. On peut remarquer que $Q(\alpha) = \frac{P^{(r)}(\alpha)}{r!}$ est non nul.

Donc $(X-\alpha)^r$ divise P mais $(X-\alpha)^{r+1}$ ne divise pas P car sinon, $(X-\alpha)$ diviserait Q, ce qui est en contradiction avec le fait que $Q(\alpha) \neq 0$.

On a donc prouvé que r est la multiplicité de α.

QED

3.11 Applications aux fractions rationnelles

Définition 3.47 *On appelle fraction rationnelle toute expression de la forme $\frac{P}{Q}$ où $P \in \mathbf{k}[X]$, $Q \in \mathbf{k}[X]$ et $Q \neq 0$.*

Notation : L'ensembles des fractions rationnelles sur $\mathbf{k}$ (avec $\mathbf{k} = \mathbb{R}$ ou $\mathbf{k} = \mathbb{C}$) est noté $\mathbf{k}(X)$.

Proposition 3.48 (Forme irréductible d'une fraction rationnelle) *Soit $R \in \mathbf{k}(X)$ une fraction rationnelle non nulle. Il existe alors un unique couple de polynômes $(P, Q) \in \mathbf{k}[X] \times \mathbf{k}[X]$ tels que*

i) $Q \neq 0$ est normalisé,
ii) $R = \frac{P}{Q}$,
iii) P et Q sont premiers entre eux.

Terminologie : Lorsque l'on écrit la fraction rationnelle R sous la forme $\frac{P}{Q}$ avec P et Q comme si dessus, on dit que la fraction rationnelle R est mise **sous forme irréductible**.

La preuve du théorème étant identique à celle du théorème correspondant dans $\mathbb{Q}$, nous l'omettons.

L'objectif du reste du chapitre est d'écrire une fraction rationnelle comme somme de fractions rationnelles dont le dénominateur est "simple" (c'est-à-dire une puissance d'un polynôme premier).

Nous allons pour cela procéder en plusieurs étapes.

Lemme 3.49 *Soit P, Q_1 et Q_2 trois polynômes de $\mathbf{k}[X]$ avec Q_1 et Q_2 non nuls. Si Q_1 et Q_2 sont premiers entre eux, il existe des polynômes P_1 et P_2 dans $\mathbf{k}[X]$ tels que*

$$\frac{P}{Q_1 Q_2} = \frac{P_1}{Q_1} + \frac{P_2}{Q_2} \, .$$

Preuve : Comme Q_1 et Q_2 sont premiers entre eux, le théorème de Bezout affirme qu'il existe deux polynômes A_1 et A_2 dans $\mathbf{k}[X]$ tels que $A_1 Q_1 + A_2 Q_2 = 1$. Alors

$$\frac{P}{Q_1 Q_2} = \frac{P(A_1 Q_1 + A_2 Q_2)}{Q_1 Q_2} = \frac{P A_1 Q_1}{Q_1 Q_2} + \frac{P A_2 Q_2}{Q_1 Q_2} = \frac{P A_1}{Q_2} + \frac{P A_2}{Q_1} \, .$$

Pour obtenir le résultat annoncé, il suffit donc de poser $P_1 = P A_2$ et $P_2 = P A_1$.

QED

Lemme 3.50 *Soient D un polynôme non nul de $\mathbf{k}[X]$ de degré d, P un polynôme de $\mathbf{k}[X]$ et n un entier naturel. Il existe alors un unique $(n+1)-$uplet de polynômes $(Q_0, \ldots, Q_{n-1}, R)$ tel que*

$$P = Q_0 + Q_1 D + \ldots + Q_{n-1} D^{n-1} + R D^n = \left(\sum_{i=0}^{n} Q_i D^i \right) + R D^n \, ,$$

avec, pour tout $i \in \{0, \ldots, n-1\}$, $deg(Q_i) < d$.

Preuve : On fait la preuve de l'existence et de l'unicité par récurrence sur n.

Pour $n = 1$, le résultat est une application directe de la division euclidienne du polynôme P par le polynôme D, Q_0 étant le reste de cette division euclidienne et R le quotient.

On suppose maintenant le résultat vrai pour l'entier n. Montrons-le pour $n+1$. D'après l'hypothèse de récurrence, il existe un unique $(n+1)-$uplet de polynômes $(Q_0, \ldots, Q_{n-1}, R)$ tel que

$$P = Q_0 + Q_1 D + \ldots + Q_{n-1} D^{n-1} + R D^n \, , \tag{7}$$

avec, pour tout $i \in \{0, \ldots, n-1\}$, $deg(Q_i) < d$. Effectuons la division euclidienne de R par D : il existe un unique couple de polynômes (S, Q_n) tel que $R = SD + Q_n$ et $deg(Q_n) < d$. Alors l'égalité (7) devient

$$P = Q_0 + Q_1 D + \ldots + Q_{n-1} D^{n-1} + (SD + Q_n) D^n = Q_0 + Q_1 D + \ldots + Q_{n-1} D^{n-1} + Q_n D^n + S D^{n+1} \, .$$

Nous avons prouvé l'existence du $(n+2)-$uplet remplissant les conditions du théorème au rang $n+1$.

Montrons maintenant l'unicité au rang $n+1$. Supposons que le $(n+2)$-uplet $(A_0, \ldots, A_n, B)$ vérifie :

$$P = A_0 + A_1 D + \ldots + A_n D^n + B D^{n+1}$$

avec, pour tout $i \in \{1, \ldots, n\}$, $deg(A_i) < d$. Notons d'abord que l'égalité précédente se réécrit

$$P = A_0 + A_1 D + \ldots + A_{n-1} D^{n-1} + (A_n + BD) D^n$$

D'après l'hypothèse de récurrence au rang n, l'unicité du $(n+1)-$uplet $(Q_0, \ldots, Q_{n-1}, R)$ implique que $A_0 = Q_0$, $A_1 = Q_1$, ..., $(A_n + BD) = R$. De plus, comme $deg(A_n) < d$ par hypothèse, le couple (B, A_n) est nécessairement le quotient et le reste de la division euclidienne de R par D. D'où $A_n = Q_n$ et $B = S$. On a donc montré l'unicité au rang $n+1$.

Par récurrence, on en déduit le résultat pour tout entier n.

QED

Corollaire 3.51 *Soient P et D deux polynômes de $\mathbf{k}[X]$, avec $D \neq 0$ et n un entier naturel non nul. Il existe alors un unique $(n+1)-$uplet de polynômes $(Q_0, \ldots, Q_{n-1}, R)$ tel que*

$$\frac{P}{D^n} = R + \frac{Q_{n-1}}{D} + \ldots + \frac{Q_1}{D^{n-1}} + \frac{Q_0}{D^n},$$

avec, pour tout $i \in \{0, \ldots, n-1\}$, $deg(Q_i) < d$.

Preuve : C'est une application immédiate du lemme précédent.

QED

Nous pouvons maintenant énoncer le théorème le plus important du chapitre :

Théorème 3.52 (Décomposition en éléments simples d'une fraction rationnelle) *Soit $\frac{P}{Q}$ une fraction rationnelle de $\mathbf{k}(X)$ mise sous forme irréductible. On suppose que la décomposition en facteur premiers de Q s'écrit sous la forme*

$$Q = \beta P_1^{k_1} \ldots P_n^{k_n}$$

où les P_i sont des polynômes premiers tous distincts, $k_1, \ldots, k_n$ sont des entiers naturels non nuls, et $\beta \neq 0$ appartient à $\mathbf{k}$.

Il existe alors des polynômes Q_{ij} avec $i \in \{1, \ldots, n\}$ et $j \in \{1, \ldots, k_i\}$ et un polynôme R tels que

$$\frac{P}{Q} = R + \left(\frac{Q_{11}}{P_1} + \ldots + \frac{Q_{1,k_1}}{P_1^{k_1}} \right) + \ldots + \left(\frac{Q_{n1}}{P_n} + \ldots + \frac{Q_{n,k_n}}{P_n^{k_n}} \right) = R + \sum_{i=1}^{n} \sum_{j=1}^{k_i} \frac{Q_{ij}}{P_i^j}$$

et, pour tout $i \in \{1, \ldots, n\}$ et $j \in \{1, \ldots, k_i\}$, $deg(Q_{ij}) < deg(P_i)$.

Remarques :

1. Une telle décomposition est unique à l'ordre près. La preuve de l'unicité (ainsi que son énoncé précis) étant un peu délicate, nous ne la ferons pas.

2. Pour une fraction rationnelle de $\mathbb{R}(X)$, il existe *a priori* deux décompositions, l'une dans $\mathbb{C}$ et l'autre dans $\mathbb{R}$. En pratique (par exemple en intégration), on se sert le plus souvent de celle dans $\mathbb{R}$.

Preuve : En utilisant le lemme 3.49, on montre sans difficulté, par récurrence, qu'il existe des polynômes $Q_1, \ldots, Q_n$ tels que

$$\frac{P}{Q} = \frac{Q_1}{P_1^{k_1}} + \ldots + \frac{Q_n}{P_n^{k_n}}$$

car les polynômes $P_1^{k_1}, \ldots, P_n^{k_n}$ sont premiers entre eux.

A chaque fraction $\frac{Q_i}{P_i^{k_i}}$, on applique le corollaire 3.51, ce qui donne le résultat du théorème.

QED

3.12 Quelques exercices

Exercice 3.52.1

On considère le polynôme $P(X) = X^4 + 6X^3 + 16X^2 + 22X + 15$.

i) Déterminer deux scalaires λ et μ tels que

$$P(X) = (X^2 + 3X + \lambda)^2 - (X + \mu)^2 \ .$$

ii) En déduire la décomposition de P en produit de facteurs irréductibles dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

Exercice 3.52.2

On considère les deux polynômes $P(X) = X^4 + 1$ et $Q(X) = X^3 + 1$.

i) Calculer les racines de P et Q (dans $\mathbb{C}$) sous forme algébrique et sous forme trigonométrique.

ii) Décomposer P et Q en produit de polynôme irréductibles de $\mathbb{R}[X]$.

iii) Calculer le pgcd de P et Q.

iv) En déduire un couple (U, V) de polynômes de $\mathbb{R}[X]$ de degré ≤ 3 tel que $PU + QV = 1$.

Exercice 3.52.3

Soit $A(X) = X^6 + aX^4 + bX^3 + c$ un polynôme de $\mathbb{C}[X]$.

i) Déterminer a, b, c tels que 1 soit racine double de A et j soit racine de A.

ii) Montrer alors que $A \in \mathbb{R}[X]$ et que j est racine double.

iii) Décomposer A en produits de facteurs irréductibles dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

Exercice 3.52.4

Décomposer dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$ les polynômes suivants en facteurs irréductibles :

$$X^3 + 1 \qquad X^3 - 1 \qquad X^3 + 2X^2 + 2X + 1$$

$$X^4 + 1 \qquad X^4 + X^2 + 1 \qquad 1 + X + X^2 + X^3 + X^4 + X^5$$

Exercice 3.52.5

Décomposer en éléments simples sur $\mathbb{R}$ les fractions rationnelles suivantes :

$$\frac{X+1}{X+2} \qquad \frac{2X-3}{X^2-3X+2} \qquad \frac{4X^3}{X^4-1}$$

$$\frac{X^3+8X^2+8X+1}{(X^2+X+1)(X+1)^2} \qquad \frac{X+5}{(X+1)(X+2)(X+3)}$$

Exercice 3.52.6

1. Montrer *sans calcul* que le polynôme $(X+1)$ divise les polynômes X^5+1 et X^3+1.
2. Calculer explicitement les polynômes $P_1(X) = \frac{X^5+1}{X+1}$ et $P_2(X) = \frac{X^3+1}{X+1}$.
3. Montrer que P_1 et P_2 sont premiers entre eux.
4. En déduire le pgcd de X^5+1 et X^3+1.
5. Calculer le ppcm de X^5+1 et X^3+1.

4 Quelques examens des années précédentes

UNIVERSITE DE BRETAGNE OCCIDENTALE
Département de Mathématiques

Année universitaire 2000-2001
DEUG MIAS-MASS 1ère année
Epreuve de ALG 11F - M11
Mardi 23 Janvier 2001 - Durée 2h

Epreuve sans document ni calculatrice
Les exercices sont indépendants

Question de cours (5 points)

1. Soit $\mathbb{R}[X]$ l'ensemble des polynômes à coefficients réels, et P et Q deux polynômes non nuls de $\mathbb{R}[X]$. Rappeler la définition du p.g.c.d. de P et Q.
2. Enoncer le théorème de Bezout dans $\mathbb{R}[X]$.
3. Soient P, Q et D trois polynômes non nuls de $\mathbb{R}[X]$. On suppose que D divise à la fois P et Q et que les polynômes P/D et Q/D sont premiers entre eux. Démontrer, en utilisant le théorème de Bezout, que D est le p.g.c.d. de P et Q.

Exercice 1 (2 points) Calculer le module et l'argument de toutes les racines troisièmes de $z = 4\sqrt{2}(i-1)$.

Exercice 2 (5 points)

1. A partir de l'algorithme d'Euclide, déterminer deux polynômes P_1 et P_2 de $\mathbb{R}[X]$ tels que $(X^2+X+1)P_1 + (X^2+1)P_2 = 1$.
2. En déduire tous les polynômes Q_1 et Q_2 de $\mathbb{R}[X]$ vérifiant $(X^2+X+1)Q_1 + (X^2+1)Q_2 = 1$.

Exercice 3 (3 points) Pour tout réel λ, on considère le polynôme $P_\lambda(X) = X^4 + 2\lambda X^2 + 1$. Déterminer toutes les valeurs de λ pour lesquelles les polynômes P_λ et P'_λ sont premiers entre eux dans $\mathbb{R}[X]$.

Exercice 4 (5 points) Décomposer en éléments simples les fractions rationnelles

$$R_1 = \frac{1}{X(X^2-1)} \quad \text{et} \quad R_2 = \frac{4X^2-2X}{(X^2+1)(X-1)^2}\ .$$

UNIVERSITE DE BRETAGNE OCCIDENTALE
Département de Mathématiques

Année universitaire 2000-2001
DEUG MIAS-MASS 1ère année
Epreuve de ALG 11F - M11
Mercredi 5 Septembre 2001 - Durée 2h

Epreuve sans document ni calculatrice
Les exercices sont indépendants

Question de cours (5 points) L'objectif de cette question est de retrouver la démonstration de l'existence d'une division euclidienne pour les entiers.

Dans toute la question, on suppose que n_1 et n_2 sont deux entiers naturels, avec n_2 non nul.

1. Montrer que l'ensemble
$$A = \{k \in \mathbb{N} \text{ tel que } \ kn_2 > n_1\}$$
possède un plus petit élément, noté $\bar{k}$.

2. Montrer que l'entier r défini par $r = n_1 - (\bar{k} - 1)n_2$ vérifie $0 \leq r < n_2$ (on pourra raisonner par l'absurde).

3. Montrer finalement qu'il existe un couple d'entiers (q, r) tels que $n_1 = qn_2 + r$ avec $0 \leq r < n_2$.

Exercice 1 (2 points) Calculer le module et l'argument de toutes les racines quatrièmes de $z = 8(i + \sqrt{3})$.

Exercice 2 (5 points)

1. A partir de l'algorithme d'Euclide, déterminer deux entiers relatifs n_1 et n_2 tels que
$$93n_1 + 71n_2 = 1 \ .$$

2. En déduire tous les entiers relatifs q_1 et q_2 vérifiant $93q_1 + 71q_2 = 1$.

Exercice 3 (3 points) Trouver toutes les racines du polynôme
$$P(X) = X^4 + 2X^3 - 36X^2 - 162X - 189$$
sachant que ce polynôme P possède une racine triple.

Exercice 4 (5 points) Décomposer en éléments simples dans $\mathbb{R}[X]$ les fractions rationnelles
$$R_1(X) = \frac{1}{X^2 - X} \quad \text{et} \quad R_2(X) = \frac{1}{X^3 - 1} \ .$$

UNIVERSITE DE BRETAGNE OCCIDENTALE
Département de Mathématiques

Année universitaire 2001-2002
DEUG MIAS-MASS 1ère année
Epreuve de ALG 11F - M11
Mardi 15 Janvier 2002 - Durée 2h

Epreuve sans document ni calculatrice
Les exercices sont indépendants

Question de cours

1. Rappeler la définition d'un nombre entier premier.
2. Démontrer que pour tout nombre entier $n \geq 2$, il existe un nombre premier qui divise n (Indication : on pourra raisonner par récurrence sur n).

Exercice 1 Déterminer le module et l'argument du nombre complexe $z = \dfrac{1 + i\sqrt{3}}{1 - i}$, et donner toutes les racines septièmes de z.

Exercice 2 Calculer $pgcd\{1360, 1224, 510\}$.

Exercice 3 Décomposer en éléments simples dans $\mathbb{R}[X]$ les fractions rationnelles suivantes :

$$R_1(X) = \frac{X+1}{X^2-4} \quad \text{et} \quad R_2(X) = \frac{X+1}{X^4+X^2}\,.$$

Exercice 4 On considère le polynôme $P(X) = X^5 - X^4 + X^3 + X^2 + 2$.

1. Démontrer que si un nombre complexe z est une racine de P, alors son conjugué $\bar{z}$ l'est aussi.
2. Montrer que $z = (1 + i)$ est racine de P.
3. En déduire la factorisation de P en facteurs premiers dans $\mathbb{R}[X]$.

UNIVERSITE DE BRETAGNE OCCIDENTALE
Département de Mathématiques

Année universitaire 2001-2002
DEUG MIAS-MASS 1ère année
Epreuve de ALG 11F - M11
Mercredi 4 Septembre 2002 - Durée 2h

Epreuve sans document ni calculatrice
Les exercices sont indépendants

Question de cours Soient P_1 et P_2 deux polynômes réels, avec P_2 non nul.

1. Rappeler ce qu'est la division euclidienne de P_1 par P_2.
2. Démontrer l'unicité du quotient et du reste de la division euclidienne de P_1 par P_2.

Exercice 1 Déterminer l'ensemble des nombres complexes $z \neq 0$ tels que

$$\frac{1}{\bar{z}} = 32\, i\, z^4 \ .$$

Exercice 2

1. A partir de l'algorithme d'Euclide, déterminer deux polynômes P_1 et P_2 tels que

$$P_1(X)\,(X^3+1) + P_2(X)\,(X^2+2) = 1 \ .$$

2. En déduire tous les couples (Q_1, Q_2) de polynômes tels que

$$Q_1(X)\,(X^3+1) + Q_2(X)\,(X^2+2) = 1 \ .$$

Exercice 3 Décomposer en éléments simples dans $\mathbb{R}[X]$ les fractions rationnelles suivantes :

$$R_1(X) = \frac{3X}{X^2 - X - 2} \quad \text{et} \quad R_2(X) = \frac{X^2 + X - 1}{X^4 + X^3} \ .$$

Exercice 4 On considère le polynôme $P(X) = X^4 + 2X^3 - 2X^2 + 8$.

1. Trouver toutes les racines de P sachant que P possède une racine double.
2. En déduire la factorisation de P en facteurs premiers dans $\mathbb{R}[X]$.