ESTIA 1^{e}Année - Mathématiques
Cours d'algèbre

Xavier Dussau, Jean Esterle, Fouad Zarouf et Rachid Zarouf [1]

3 novembre 2008

[1]I.Harlouchet-en eskuhartzearekin

Introduction

Ce cours d'algèbre se compose de 4 chapitres. Au Chapitre 1 on rappelle les notions de Groupe, d'Anneau et de Corps. Au Chapitre 2 on présente, essentiellement sans démonstration, les notions et résultats usuels d'arithmétique : p.g.c.d., théorème de Bezout, algorithme d'Euclide, théorème de Gauss, théorème chinois, p.p.c.m., nombres premiers, décomposition en facteurs premiers. Au chapitre 3 on développe, avec des démonstrations détaillées, **"l'arithmétique des polynômes"**, où on retrouve les mêmes notions, les polynômes irréductibles jouant le rôle des nombres premiers. Au Chapitre 4 on donne la décomposition des fractions en éléments simples et ses applications au calcul intégral.

Toutes les notions et tous les résultats sont illustrés par de nombreux exemples concrets, où les calculs sont détaillés. D'autre part les objets présentés dans ce cours, à l'exception de la factorisation des polynômes de degré supérieur à 4, peuvent être **effectivement calculés**. La mise au point d'algorithmes de calcul efficaces (dans des situations beaucoup plus complexes que celles abordées dans ce modeste cours) est d'ailleurs l'objet d'une branche importante des Mathématiques contemporaines, **l'Algorithmique Arithmétique**, représentée à Bordeaux par l'équipe de réputation internationale animée par le Professeur H.Cohen. On n'abordera évidemment pas ici ce domaine des mathématiques, mais on montrera sur de nombreux exemples comment le logiciel de calcul formel **MUPAD** peut être utilisé pour mener à bien des calculs qui seraient inaccessibles sans l'usage de l'ordinateur.

Aitzin solasa Algebra ikasgai hauek lau kapitulutan moldatuak dira. I. Kapituluan Talde, Eraztun eta Gorputzaren nozioak oroitarazten dira. II. Kapituluan aritmetikako ohiko ezaguera eta emaitzak : z.k.h.-a, Bezout-en teorema, Euklides-en algoritmoa, Gauss-en teorema, teorema txinoa, m.k.t.-a, zenbaki lehenak, faktore lehenetako deskonposaketa, funtsean frogarik gabe aurkeztuak dira. III. Kapituluan, froga zehatzekin, **"polinomioen aritmetika"** azaltzen da , non, polinomio laburtezinek zenbaki lehenen papera jokatuz, ezaguera berak kausitzen diren. IV. Kapituluan elementu sinpleetako frakzioen deskonposaketa aurkezten da, eta honen aplikazioak kalkulu integralean. Ezaguera eta emaitza guziak kalkulu xehez lagunduriko anitz adibide konkreturekin argituak dira. Gainera, ikasgai hauetan aurkeztu objektuak, maila 4 baino handiagoa duten polinomioen faktorizazioa ezik, **eraginkorki kalkula daitezke**. Bestalde, kalkulu-algoritmoen lanketa (ikasgai xume honetan aipatuak diren baino egoera askoz korapilatsuagoetakoa), Matematika garaikideen adar garrantzitsu baten aztergaia da, **Algoritmika Aritmetikoa**, H. Cohen Irakasleak animatzen duen Bordaleko nazioarteko ospeko taldeak ordezkatua. Ez gara hemen nehondik ere matematika alor horretan sartuko, baina, anitz adibideren gainean, erakutsiko dugu nola **MUPAD** kalkulu formalaren programa, ordenagailurik gabe lortu ezinak izango liratekeen kalkuluak bururatzeko erabil daitekeen.

Table des matières

Chapitre 1

Groupes, Anneaux, Corps

1.1 Groupes

Nous commencons par rappeler des définitions classiques

Definition 1.1.1 *Un groupe est une ensemble non vide G muni d'une loi de composition interne $(x, y) \longmapsto x \circ y$ possédant les propriétés suivantes*

(1.1) $x \circ (y \circ z) = (x \circ y) \circ z$ pour tout triplet (x, y, z) d'éléments de G.

(1.2) Il existe un élément e de G tel que $x \circ e = e \circ x = x$ pour tout $x \in G$.

(1.3) Pour tout $x \in G$, il existe $y \in G$ tel que $x \circ y = y \circ x = e$.

On dira qu'une loi de composition interne sur un ensemble E vérifiant la condition (1.1) est *associative*. Si $(G, \circ)$ est un groupe, l'élément e de G vérifiant la condition (1.2) ci-dessus est appelé *élément neutre* de G. On vérifie (exercice) que cet élément neutre est unique. L'élément y de G tel que $x \circ y = y \circ x = e$ est appelé *inverse* de x. Il est également unique. On vérifie plus généralement (exercice) que si $(E, \circ)$ est un ensemble muni d'une loi de composition associative pour laquelle il existe un élément neutre e, et si trois éléments x, y_1 et y_2 de E vérifient $x \circ y_1 = y_2 \circ x = e$ alors $y_1 = y_2$.

Definition 1.1.2 *On dit qu'un groupe $(G, \circ)$ est commutatif , ou abélien , si on a la condition suivante*

(1.4) $x \circ y = y \circ x$ pour tout couple (x, y) d'éléments de G.

La loi de composition d'un groupe abélien G sera souvent notée $+$. Dans ce cas l'élément neutre de G sera noté 0 , et l'inverse d'un élément x de G sera noté $-x$ et appelé l'*opposé de x.*

Exemple 1.1.3 *Notons $\mathbb{Z}$ l'ensemble des entiers relatifs, $\mathbb{Q}$ l'ensemble des rationnels, $\mathbb{R}$ l'ensemble des réels et $\mathbb{C}$ l'ensemble des nombres complexes. Alors $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes abéliens.*

Exemple 1.1.4 *Soit $p \geq 2$ un entier. Pour $0 \leq a \leq p-1$ on pose $\bar{a} = \{a + pn\}_{n\in\mathbb{Z}}$, et on pose $\bar{a} + \bar{b} = \bar{r}$ où r est le reste de la division de $a + b$ par p (d'après le cours de CM1 , on a bien $0 \leq r \leq p-1$). On vérifie que $(\mathbb{Z}/p\mathbb{Z}, +)$ est un groupe abélien.*

On peut illustrer ceci par les tables d'addition de $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$.

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Ces deux exemples sont un cas particulier de la théorie des *groupes quotient* qu'il n'y a pas lieu de développer ici. On notera que la nature mathématique exacte des éléments $\bar{0}, \bar{1}, \ldots, p-1$ de $\mathbb{Z}/p\mathbb{Z}$ ne joue guère de rôle en pratique. Ce qui compte est de pouvoir utiliser la table de l'addition (à laquelle on ajoutera plus loin une table de multiplication)

On peut également utiliser la notation multiplicative pour certains groupes abéliens ou non. On note alors $x.y$ au lieu de $x \circ y$. L'élément unité est noté 1 (ou I s'il s'agit de matrices), et l'inverse de $x \in G$ est noté x^{-1} (la notation x^{-1} est utilisée dans tous les cas où la loi du groupe n'est pas notée additivement).

On notera $\mathbb{Q}^*$ l'ensemble des rationnels non nuls. On notera de même $\mathbb{R}^*$ l'ensemble des réels non nuls et $\mathbb{C}^*$ l'ensemble des nombres complexes non nuls. On pose d'autre part $\Gamma = \{z \in \mathbb{C} \mid |z| = 1\}$. Le produit de deux éléments x et y de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ sera noté $x.y$ (ou xy si aucune confusion n'est à craindre).

Exemple 1.1.5 *$(\mathbb{Q}^*, .)$, $(\mathbb{R}^*, .)$, $(\mathbb{C}^*, .)$ et $(\Gamma, .)$ sont des groupes abéliens pour le produit usuel.*

L'ensemble $GL(2, \mathbb{R})$ des matrices à deux lignes et deux colonnes à coefficients réels de déterminant non nul est un groupe non abélien pour le produit matriciel (dont la définition est rappellée plus loin).

Notons que si $(G, \circ)$ est un groupe, on a les propriétés suivantes (exercice facile)

$$(x^{-1})^{-1} = x \qquad \forall x \in G. \tag{1.5}$$

$$(xy)^{-1} = y^{-1} \circ x^{-1} \qquad \forall x, y \in G. \tag{1.6}$$

Une notion importante en théorie des groupes est la notion de sous-groupe, donnée par la définition suivante.

Definition 1.1.6 *Soit $(G, \circ)$ un groupe. On dit qu'une partie H de G est un sous-groupe de G si les deux conditions suivantes sont vérifiées*

(i) H est non vide , et $x \circ y \in H$ pour tout couple (x, y) déléments de H.

(ii) $(H, \circ)$ est un groupe.

La proposition suivante est utile pour éviter des vérifications fastidieuses.

Proposition 1.1.7 *Soit $(G, \circ)$ un groupe et soit $H \subset G$. Les deux conditions suivantes sont équivalentes*

(i) H est un sous-groupe de G.

(ii) H est non vide, et $a \circ b^{-1} \in H$ pour tout couple (a, b) d'éléments de H.

Démonstration : Il est clair que tout sous-groupe de G vérifie (ii). Réciproquement soit $H \subset G$ vérifiant (ii) , et soit $a \in H$. On a $e = a \circ a^{-1} \in H$, donc H contient l'élément neutre e de G. On a $b^{-1} = e \circ b^{-1} \in H$ pour tout $b \in H$. Enfin d'après la propriété 1.6 on $a \circ b = a \circ (b^{-1})^{-1} \in H$ pour tout couple (a, b) d'éléments de H. ♣

1.2 Anneaux

On va maintenant s'intéresser aux ensembles munis de deux lois de composition interne.

Definition 1.2.1 *Soit $(A, +, .)$ un ensemble non vide possédant au moins deux éléments muni de deux lois de composition internes. On dit que $(A, +, .)$ est un anneau si les conditions suivantes sont vérifiées*

(i) $(A, +)$ est un groupe abélien.

(ii) $x.(y + z) = x.y + x.z et (y + z).x = y.x + z.x$ pour tout triplet (x, y, z) d' éléments de A.

(iii) $x.(y.z) = (x.y).z$ pour tout triplet (x, y, z) d' éléments de A.

(iv) Il existe un élément 1 de A tel que $x.1 = 1.x = x$ pour tout $x \in A$.

On dit qu'un anneau $(A, +, .)$ est commutatif si on a de plus la propriété suivante

(v) $x.y = y.x$ pour tout couple (x, y) d'éléments de A.

Pour éviter d'alourdir les notations on écrira "l'anneau A" au lieu de "l'anneau $(A, +, .)$" quand aucune confusion n'est à craindre.De même on écrira souvent xy au lieu de $x.y$. L'élément noté 1 dans la définition ci dessus est appellé *unité* de l'anneau A. On dit qu'un élément x de A est inversible s'il existe $y \in A$ tel que $xy = yx = 1$. Cet élément y, appelé *inverse de* x, est alors noté x^{-1}. La formule 1.6 reste valable dans ce contexte , et on vérifie (exercice) que $(Inv(A), 1)$ est un groupe, $Inv(A)$ désignant l'ensemble des éléments inversibles d'un anneau A.

Il est clair que $(\mathbb{Z}, +, .)$, $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$ et $(\mathbb{C}, +, .)$ sont des anneaux commutatifs. On peut également munir $\mathbb{Z}/p\mathbb{Z}$ d'une structure d'anneau commutatif naturelle

Exemple 1.2.2 *Soit $p \geq 2$ un entier. Pour $0 \leq a \leq p-1, 0 \leq b \leq p-1$, on pose $\bar{a}.\bar{b} = r$ où r désigne le reste de la division de $a.b$ par p. Alors $(\mathbb{Z}/p\mathbb{Z}, +, .)$ est un anneau commutatif.*

Nous illustrons ceci en donnant les tables d'addition et de multiplication de $\mathbb{Z}/4\mathbb{Z}$.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$.$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Soit maintenant $\mathcal{M}(2,\mathbb{R})$ l'ensemble des matrices carrées à deux lignes et deux colonnes à coefficients réels.On pose

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} . \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$$

Exemple 1.2.3 $(\mathcal{M}(2,\mathbb{R}),+,.)$ *est un anneau non commutatif qui a pour unité* $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Soit n un entier positif.On pose $C_n^0 = 1, C_n^1 = n$, et $C_n^p = \frac{n(n-1)...(n-p+1)}{p!}$ pour $2 \leq p \leq n$. Si A est un anneau , et si $ab = ba$, avec $a, b \in A$, on a , avec la convention $a^0 = b^0 = 1$, la *formule du binôme de Newton*

$$(1.7) \qquad (a+b)^n = \sum_{0 \leq p \leq n} C_n^p a^p b^{n-p}$$

On peut introduire la notion de sous-anneau, mais elle joue un rôle moins important que la notion de sous-groupe. Pour les anneaux commutatifs la notion importante est la notion d'*idéal*, que nous détaillerons pour les anneaux de polynômes.

1.3 Corps

Nous introduisons une dernière notion importante.

Definition 1.3.1 *Soit $(K,+,.)$ un ensemble muni de deux lois de composition internes. On dit que $(K,+,.)$ est un corps si $(K,+,.)$ est un anneau commutatif dans lequel tout élément non nul possède un inverse.*

Soit $(K,+,.)$ un corps, et soit K^* l'ensemble des éléments non nuls de K, 0 désignant l'élément neutre de l'addition.On vérifie que $(K^*,.)$ est un groupe abélien, et que $1 \neq 0$.

Exemple 1.3.2 $(\mathbb{Q},+,.),(\mathbb{R},+,.),(\mathbb{C},+,.)$ *sont des corps.On verra plus loin que $\mathbb{Z}/p\mathbb{Z}$ est un corps si p est un nombre premier.*

Il est clair que $\mathbb{Z}$ n'est pas un corps puisque 1 et -1 sont les seuls éléments inversibles de $\mathbb{Z}$. La table de mutiplication de $\mathbb{Z}/4\mathbb{Z}$ montre que $\bar{2}$ n'a pas d'inverse, donc $\mathbb{Z}/4\mathbb{Z}$ n'est pas un corps (on verra plus généralement que $\mathbb{Z}/p\mathbb{Z}$ n'est pas un corps si p n'est pas premier). Notons que le corps $\mathbb{Z}/2\mathbb{Z}$ ne possède que deux éléments.

On peut dans les corps se livrer à des calculs analogues aux calculs usuels dans $\mathbb{R}$. On peut noter $\frac{1}{a}$ l'inverse d'un élément non nul d'un corps K , et l'équation $ax = b$ a pour unique solution dans K $x = \frac{b}{a}$. De même la règle "*pour qu'un produit de facteurs soit nul il faut et il suffit que l'un des facteurs soit nul*" est valable dans un corps quelconque (mais pas dans un anneau quelconque puisque $\bar{2}.\bar{2} = 0$ dans $\mathbb{Z}/4\mathbb{Z}$).

1.4 Calculs dans $\mathbb{Z}/n\mathbb{Z}$ sous MUPAD

On peut utiliser MUPAD pour faire des calculs dans $\mathbb{Z}/n\mathbb{Z}$

Exemple 1.4.1 *Calculer* $\overline{3174667}+\overline{257985}$, $-\overline{3174667}+\overline{257985}$ *et* $\overline{3174667}.\overline{257985}$ *dans* $\mathbb{Z}/8786543\mathbb{Z}$.

On utilise la commande **modp**

```
modp(3174667 + 257985, 8786543);
```

```
modp(-3174667 + 257985, 8786543);
```

```
modp(3174667 * 257985, 8786543);
```

```
3432652
```

```
5869861
```

```
5219879
```

On a donc $\overline{3174667} + \overline{257985} = \overline{3432652}$, $\quad -\overline{3174667} + \overline{257985} = \overline{5869861}$, $\overline{3174667.257985} = \overline{5219879}$.

On peut également calculer dans $\mathbb{Z}/n\mathbb{Z}$ des inverses, et des produits du type $\bar{a}.\bar{b}^{-1}$, mais il faut faire attention.

Exemple 1.4.2 *Calculer l'inverse de* $\bar{8}$ *dans* $\mathbb{Z}/48\mathbb{Z}$.

```
modp(1/6,48);
```

```
Error: impossible inverse modulo
```

MUPAD a raison : $\bar{6}.\bar{8} = \bar{0}$, donc $\bar{6}$ n'est pas inversible dans $\mathbb{Z}/48\mathbb{Z}$. Pour éviter cet écueil on va choisir n premier, car dans ce cas, comme on le verra au chapitre suivant , $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Exemple 1.4.3 *Calculer* $(\overline{317465})^{-1}$ *et* $\overline{317465}.(\overline{257985})^{-1}$ *dans* $\mathbb{Z}/nZ$, *où* n *est le* 34567^{e} *nombre premier.*

```
ithprime(34567);
```

```
409463
```

On voit donc que le nombre premier cherché est 409463, et on peut faire les calculs

```
modp(1/317465,409463);
```

```
modp(317465/257985,409463);
```

```
180813
```

```
335955
```

Donc $(\overline{317465})^{-1} = \overline{180813}$ et $\overline{317465}.(\overline{257985})^{-1} = \overline{335955}$ dans $\mathbb{Z}/409463\mathbb{Z}$.

1.5 Exercices pour le Chapitre 1

exercice 1

Vérifier que $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif pour $n \geq 2$.

exercice 2

Donner les tables d'addition et de multiplication de $\mathbb{Z}/7\mathbb{Z}$ et $\mathbb{Z}/9\mathbb{Z}$. Quels sont les éléments inversibles de ces deux anneaux ?

exercice 3

Montrer que l'ensemble $\mathbb{T} = \{z \in \mathbb{C}^* | \ |z| = 1\}$ est un sous-groupe de $\mathbb{C}^*$. Montrer que $\mathbb{U}_n = \{z \in \mathbb{C}^* | \ z^n = 1\}$ est un sous-groupe de $\mathbb{T}$ pour $n \in \mathbb{Z}$.

exercice 4

Montrer que $GL_2(\mathbb{R})$, l'ensemble des matrices carrées d'ordre 2 inversibles, est un groupe (la loi du groupe étant la multiplication des matrices). Montrer que
$H := \{M \in GL_2(\mathbb{R}) \mid \det M = 1\}$ et $K := \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \ , \ \theta \in \mathbb{R} \right\}$
sont des sous-groupes de $GL_2(\mathbb{R})$.

exercice 5

Soit G l'ensemble des quatre fonctions numériques

$$f_1(x) = x, \ f_2(x) = \frac{1}{x}, \ f_3(x) = -x, \ f_4(x) = -\frac{1}{x},$$

définies sur $\mathbb{R}^*$, muni de la composition des applications. Montrer que G est un groupe.

exercice 6

Soit $\mathcal{F}$ l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Montrer que $(\mathcal{F}, +, *)$ est un anneau commutatif, où $(f+g)(x) = f(x) + g(x)$ et $(f * g)(x) = f(x).g(x)$ pour $x \in \mathbb{R}$,$f, g \in \mathcal{F}$.

exercice 7

Prouver que tous les sous-groupes de $\mathbb{Z}$ sont de la forme $a\mathbb{Z}$, avec $a \in \mathbb{N}$.

exercice 8

Montrer que $A = \left\{a + b\sqrt{3}, a, b \in \mathbb{R}\right\}$ est un sous-anneau de $\mathbb{R}$. Est-ce que A est un sous-corps de $\mathbb{R}$?

exercice 9

Soit $(G, \circ)$ un groupe tel que $a \circ a = e$ pour $a \in G$. Montrer que G est commutatif et donner un exemple de groupe vérifiant cette propriété.

exercice 10 (sous MUPAD)

a) Déterminer le 456917^e nombre premier

b) Effectuer dans $\mathbb{Z}/n\mathbb{Z}$, n désignant le nombre trouvé à la question précédente, les opérations suivantes

$\overline{1723497} + \overline{5255675}$, $\overline{1723497} - \overline{5255675}$, $\overline{1723497}.\overline{5255675}$.

c) Résoudre dans $\mathbb{Z}/n\mathbb{Z}$ l'équation $\overline{5255675}x = \overline{1723497}$.

Chapitre 2

Un peu d'arithmétique

2.1 La division du CM

On se propose ici de donner sans démonstration quelques résultats classiques d'arithmétique. Une démarche analogue permettra de developper en détail au Chapitre suivant *" l' arithmétique des polynômes"* qui joue un rôle important en algèbre linéaire.

Dans toute la suite $\mathbb{Z}$ désignera l'ensemble des entiers relatifs, $\mathbb{N} = \{n \in \mathbb{Z} \mid n \geq 0\}$ l'ensemble des entiers naturels, et $\mathbb{N}^*$ l'ensemble des entiers positifs, munis des opérations usuelles.

Théorème 2.1.1 *Soit $a \in \mathbb{Z}$, et soit $b \in \mathbb{N}^*$. Il existe un couple unique (q, r) d'entiers possédant les deux proprités suivantes*

(i) $a = bq + r$

(ii) $0 \leq r \leq b - 1$.

Ce résultat , souvent appelé "division euclidienne dans $\mathbb{Z}$", a été vu en CM1 pour $a > 0$ et l'extension aux entiers négatifs est évidente. L'unicité provient du fait que si $r - r' = b(q' - q)$, avec $q \neq q'$, alors $|r - r'| \geq b$, tandis que $|r - r'| \leq b - 1$ si r et r' vérifient (ii).

On dispose d'un moyen effectif pour calculer q et r

1	3	2	9
	4	2	14
		6	

qui donne $q = 14$ et $r = 6$ si $a = 132$, $b = 9$.

Definition 2.1.2 *Soient m et n deux entiers relatifs.On dit que m divise n s'il existe $p \in \mathbb{Z}$ tel que $n = mp$. On dit alors que n est un multiple de m.*

On a l'importante notion de plus grand commun diviseur (p.g.c.d.)

Théorème 2.1.3 *Soit $(a_1, \ldots, a_p)$ une famille finie d'entiers naturels non tous nuls. Il existe un unique entier positif d possédant les propriétés suivantes*

(i) d divise a_i pour $1 \leq i \leq p$.

(ii) Si un entier relatif δ divise a_i pour $1 \leq i \leq p$, alors δ divise d.

Cet entier positif d est appelé le p.g.c.d. de la famille $(a_1, \ldots, a_p)$.

Il est clair que le p.g.c.d. de $(a_1, \ldots, a_p)$ est égal à celui de $(|a_1|, \ldots, |a_p|)$, et que le p.g.c.d. d'une famille d'entiers ne change pas si on lui retire ses éléments nuls.

Pour calculer le p.g.c.d. d'une famille $(a_1, \ldots, a_p)$ on peut procéder par récurrence finie : si on note b_k le p.g.c.d de $(a_1, \ldots, a_k)$ alors b_{k+1} est le p.g.c.d de a_{k+1} et b_k. Il est clair que le p.g.c.d. de $(a_1, \ldots, a_p)$ est égal à celui de $(|a_1|, \ldots, |a_p|)$. Il suffit donc de savoir calculer le p.g.c.d. de deux entiers positifs a et b, ce qui se fait par *l'algorithme d'Euclide*. Celui-ci consiste à faire des *divisions successives*. Soient a et b deux entiers positifs , avec $a \geq b$, et soit d leur p.g.c.d. On procède de la manière suivante.On commence par écrire

$a = bq_1 + r_1$ avec $0 \leq r \leq b - 1$. Si $r = 0, d = b$.

Sinon on recommence
$b = r_1 q_2 + r_2$ avec $0 \leq r_2 \leq r_1 - 1$. Si $r_2 = 0, d = r_1$.

Sinon on recommence
$r_1 = r_2 q_3 + r_3$ avec $0 \leq r_3 \leq r_2 - 1$. Si $r_3 = 0, d = r_2$.

Sinon on recommence
....
$r_k = r_{k+1} q_{k+2} + r_{k+2}$ avec $0 \leq r_{k+2} \leq r_{k+1} - 1$. Si $r_{k+2} = 0, d = r_{k+1}$.

Sinon on recommence
...
On finit par avoir, à un certain rang p
$r_p = r_{p+1} q_{p+2} + r_{p+2}$ avec $0 \leq r_{p+2} \leq r_{p+1} - 1$, $r_{p+2} \neq 0$

$r_{p+1} = r_{p+2} q_{p+3} + r_{p+3}$ avec $r_{p+3} = 0$. On a alors $d = r_{p+2}$.

Autrement dit **"le p.g.c.d. est égal au dernier reste non nul dans l'algorithme d'Euclide."** Comme $r_k > r_{k+1}$ pour tout k , il est clair avec les notations ci-dessus que l'algorithme s'arrête avec $p + 2 \leq b - 1$. Le fait que le p.g.c.d. de a et b est bien égal au dernier reste non nul provient du fait que si u et v sont deux entiers positifs alors le p.g.c.d. de u et v est égal au p.g.c.d. de v et du reste de la division de u par v.

On a donc

$p.g.c.d.(a, b) = p.g.c.d.(b, r_1) = p.g.c.d.(r_1, r_2) = \ldots = p.g.c.d.(r_{p+2}, 0) = r_{p+2}$.

Exemple 2.1.4 *p.g.c.d. de 132 et 55*
132 = 55 × 2 + 22
55 = 22 × 2 + 11
22 = 11 × 2 + 0
Le p.g.c.d. de 132 et 55 est égal à 11.

On va maintenant énoncer le théorème de Bezout

Théorème 2.1.5 *Soit $(a_1, \ldots, a_p)$ une famille finie d'entiers naturels non tous nuls et soit d le p.g.c.d. de $(a_1, \ldots, a_p)$.Il existe une famille $(u_1, \ldots, u_p)$ d'éléments de* $\mathbf{Z}$ *vérifiant*

$$a_1u_1 + \ldots a_pu_p = d$$

Plus généralement l'équation $a_1v_1 + \ldots a_pv_p = n$ admet une solution $(v_1, \ldots, v_p)$ dans $\mathbf{Z}^p$ si et seulement si n est un multiple de d.

On dispose d'une *méthode effective* pour calculer deux entiers u et v tels que $au + bv = d$, d désignant le p.g.c.d. de deux entiers positifs a et b. Il suffit de **"remonter l'algorithme d'Euclide"**. On peut en effet utiliser l'avant dernière ligne de l'algorithme pour exprimer $d = r_{p+2}$ en fonction de r_{p+1} et r_p. En utilisant la ligne précedente on exprime r_{p+1} en fonction de r_p et r_{p-1} et en substituant on exprime d en fonction de r_p et r_{p-1}. En itérant ce procédé ligne par ligne vers le haut on obtient les coefficients u et v cherchés.

Exemple 2.1.6 *Trouver deux entiers u et v tels que* $132u + 55v = 11$.
11 = 55 − 22 × 2
22 = 132 − 55 × 2
11 = 55 − (132 − 55 × 2) × 2
55 × 5 − 132 × 2 = 11
Le couple (-2, 5) est donc solution

En fait on dispose d'une méthode rapide pour calculer u et v, en faisant des calculs intermédiaires pendant le déroulement de l'algorithme. L'idée est la suivante : si $r_{n+2} = au_{n+2} + bv_{n+2}$, en remontant l'algorithme on obtient $r_n = r_{n+1}q_{n+2} + r_{n+2}$, $r_{n+2} = -r_{n+1}q_{n+2} + r_n = a(q_{n+2}u_{n+1} - u_n) + b(q_{n+2}v_{n+1} - v_n)$. On obtient les relations de récurrence

$$\begin{cases} u_{n+2} = -q_{n+2}u_{n+1} + u_n \\ v_{n+2} = -q_{n+2}v_{n+1} + v_n \end{cases} \tag{2.1}$$

Avec les notations ci-dessus on peut alors écrire en colonne les valeurs successives de u_n et v_n. On a $u_1 = 1 = 1 - q_1 \times 0, v_1 = -q_1 = -q_1 + 0$, et on peut écrire "l'algorithme d'Euclide étendu"

	q_n	u_n	v_n
		1	0
		0	1
132 = 55 × 2 + 22	2	1	-2
55 = 22 × 2 + 11	2	-2	5
22 = 11 × 2 + 0			

On retrouve ainsi le fait que $(-2) \times 132 + 5 \times 55 = 11$.

2.2 Applications du théorème de Bezout

Definition 2.2.1 *Soient a et b deux entiers relatifs.On dit que a et b sont premiers entre eux si leur p.g.c.d. est égal à 1.*

On va maintenant donner deux conséquences importantes du théorème de Bezout.

Théorème 2.2.2 *(Gauss) Soient a, b, c trois entiers relatifs non nuls. Si a divise bc, et si a est premier avec b, alors a divise c.*

Démonstration : Il existe $u, v \in \mathbf{Z}$ tels que $au + bv = 1$. Donc $c = auc + bcv$. Comme a divise bc , il existe $w \in \mathbf{Z}$ tel que $bc = aw$. Donc $c = a(uc + vw)$, ce qui montre que a divise c. ♣

Corollaire 2.2.3 *Soient a et b deux entiers relatifs non nuls et soit d le p.g.c.d. de a et b. Soit $\mathcal{S} = \{(u, v) \in \mathbf{Z}^2 \mid au + bv = 0\}$. On a $\mathcal{S} = \{-nb', na'\}_{n \in \mathbf{Z}}$, où $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$*

Démonstration : Il résulte du théorème de Bezout que a' et b' sont premiers entre eux, et $\mathcal{S} = \{(u, v) \in \mathbf{Z}^2 \mid a'u + b'v = 0\}$. Il est clair que si $u = -nb'$ et si $v = na'$ alors $(u, v) \in \mathcal{S}$. Réciproquement si $a'u + b'v = 0$ alors a' divise $b'v$, donc a' divise v d'après le théorème de Gauss. Donc il existe $n \in \mathbf{Z}$ tel que $v = na'$. On a alors $ua' = -b'na'$, donc $u = -nb'$. ♣

On a alors le résultat suivant concernant l'équation de Bezout, dont la démonstration est laissée en exercice.

Corollaire 2.2.4 *Soient a et b deux entiers positifs premiers entre eux. Il existe alors un unique couple (u_0, v_0) d'entiers relatifs vérifiant les deux conditions suivantes*

(i) $au_0 + bv_0 = 1$

(ii) $0 \leq u_0 < b$.

De plus dans ce cas on a $v_0 \leq 0$ et $|v| < a$.

D'autre part les solutions entières de l'équation $au + bv = 1$ sont données par les couples de la forme $u = u_0 - nb, v = v_0 + na$ avec $n \in \mathbf{Z}$.

Ces résultats ont diverses applications pratiques. On peut par exemple les utiliser pour déterminer les points à coordonnées entières d'une droite dont les coefficients de l'équation sont entiers.

Exemple 2.2.5 *Déterminer les points a coordonnées entières de la droite Δ d'équation $55x + 132y = 13$.*

Pour que de tels points existent, il faudrait que 13 soit un multiple du p.g.c.d. de 55 et 132, qui est égal à 11, ce qui est visiblement faux. Donc cette droite n'a pas de points à coordonnées entières.

Exemple 2.2.6 *Déterminer les points à coordonnées entières de la droite D d'équation 55x + 132y = 22.*

Ici 22 est un multiple de 11, donc l'équation $55x + 132y = 22$ a des solutions entières. Comme $55 \times 5 - 2 \times 132 = 1$ on obtient une solution particulière en posant $x_0 = 10, y_0 = -4$. Soient maintenant $(x, y) \in Z^2$. On a $55x+132y-22 = 55(x - x_0) + 132(y - y_0)$. On voit donc que $55x + 132y = 22$ si et seulement si $x = 10+u$ et $y = -4+v$, avec $55u+132v = 0$. Comme $\frac{55}{11} = 5$ et $\frac{132}{11} = 12$ on voit que les points à coordonnées entières de D sont les points donc les coordonnées sont de la forme $(10 - 12n, -4 + 5n)$ avec $n \in \mathbf{Z}$.

On a la variante suivante du théorème de Gauss, dont la démonstration est laissée en exercice.

Théorème 2.2.7 *Soient $a, b_1, \ldots, b_p$ des entiers non nuls. Si a est premier avec b_k pour $1 \leq k \leq p$, alors a est premier avec le produit $b_1 \ldots b_k$.*

Corollaire 2.2.8 *Soient $a_1, ..., a_k$ des entiers premiers entre eux deux à deux. Si $x \in \mathbf{Z}$ est divisible par a_j pour $1 \leq j \leq k$, alors x est divisible par le produit $a_1...a_k$.*

Démonstration : Si $k = 1$, il n'y a rien à démontrer. Supposons maintenant que le résultat est vrai pour $k - 1$, avec $k \geq 2$. Soient $a_1, ..., a_k$ des entiers premiers entre eux deux à deux et supposons que $x \in \mathbf{Z}$ est divisible par a_j pour $1 \leq j \leq k$. Alors x est divisible par le produit $a_1...a_{k-1}$, donc x s'écrit sous la forme $x = a_1...a_{k-1}y$, avec $y \in \mathbf{Z}$. Il résulte du théorème ci-dessus que a_k est premier avec $a_1...a_{k-1}$, et on déduit alors du théorème de Gauss que a_k divise y. Donc x est divisible par $a_1...a_k$, et la propriété est vraie pour k. Le résultat est donc démontré par récurrence. ♣

2.3 Le théorème chinois

Soit p un entier positif. On dira que deux entiers relatifs a et b sont *congrus modulo p* , et on écrira $a \equiv b \ \ (p)$, quand $a - b$ est divisible par p.On v'erifie facilement que si $a \equiv a' \ \ (p)$ et si $b \equiv b' \ \ (p)$ alors $a + b \equiv a' + b' \ \ (p)$ et $ab \equiv a'b' \ \ (p)$.

On a le théorème suivant , dû à un mathématicien chinois anonyme.

Théorème 2.3.1 *Soient $p_1, \ldots, p_k$ des entiers positifs tels que p_i et p_j soient premiers entre eux pour $i \neq j$.Alors pour toute famille $(q_1, \ldots, q_k)$ dans $\mathbf{Z}^k$ le système d'équations de congruence*

$x \equiv q_1 \quad (p_1)$
$\ldots$
$\ldots$
$x \equiv q_k \quad (p_k)$
possède des solutions dans $\mathbf{Z}$. *De plus si* x_0 *est une solution, alors la solution générale du système est donnée par la formule*

$$x = x_0 + np_1...p_k,$$

avec $n \in \mathbf{Z}$.

Notons que si x_0 est une solution particulière alors $x \in \mathbf{Z}$ est solution du système si et seulement si $x - x_0 \equiv 0 \pmod{p_j}$ pour $1 \leq j \leq k$. Donc si $x = x_0 + np_1...p_k$, avec $n \in \mathbf{Z}$, alors x est solution du système. Réciproquement, si x est solution du système, alors $x - x_0$ est divisible par $p_1, p_2, ...$ et p_k, qui sont premiers entre eux deux à deux, donc il est divisible par le produit $p_1...p_k$ et on a $x = x_0 + np_1...p_k$ avec $n \in \mathbf{Z}$.

Pour démontrer l'existence d'une solution on procède par récurrence sur k et on est ramené à chaque étape à résoudre dans $\mathbf{Z}^2$ une équation du type $ax + by = c$, avec a , b , c entiers relatifs , a et b premiers entre eux. Ceci donne un moyen effectif de trouver des solutions pour ce type de systèmes d'équations de congruence, que nous décrivons dans l'exemple suivant

Exemple 2.3.2 *Trouver* $x \in \mathbf{Z}$ *vérifiant*
$x \equiv 1 \quad (2)$
$x \equiv -1 \quad (3)$
$x \equiv 2 \quad (5)$

Les solutions de la première équation sont de la forme $x = 1 + 2m, m \in \mathbf{Z}$. En reportant dans la seconde équation on obtient $1+2m = -1+3n$, avec $n \in \mathbf{Z}$, qui donne $3n - 2m = 2$. L'équation $3u - 2v = 1$ admet pour solution triviale $u = 1, v = 1$. Donc on peut prendre $m = n = 2$, ce qui fait que $x = 1 + 4 = 5$ est solution du système formé par les deux premières équations.

La solution générale de ce système est de la forme $x = 5+6p$, avec $p \in \mathbf{Z}$. En reportant dans la dernière équation on trouve $5+6p = 2+5q$, soit $6p-5q = -3$. L'équation $6u-5v = 1$ a pour solution triviale $u = v = 1$. Donc on peut prendre $p = q = -3$, ce qui donne $x_0 = -13$ comme solution du système proposé.On voit facilement que la solution générale est de la forme $x = -13 + 2 \times 3 \times 5n = -13 + 30n$, avec $n \in \mathbf{Z}$.

La méthode utilisée ci-dessus est valable pour tous les systèmes d'équations de congruence vérifiant les hypothèses du théorème chinois, mais il faut en général utiliser l'algorithme d'Euclide étendu pour résoudre les équations du type Bezout rencontrées à chaque étape des calculs.

2.4 Décomposition en produit de nombres premiers

La notion de p.g.c.d. a pour pendant celle de plus grand commun multiple (p.p.c.m.). Nous nous limiterons au cas de deux entiers.

Théorème 2.4.1 *Soient a et b deux entiers relatifs. Il existe un unique entier $m \geq 0$, appelé p.p.c.m. de a et b, possédant les deux propriťés suivantes*

(i) m est un mutiple commun à a et b

(ii) Si n est un multiple commun à a et b, alors n est un multiple de m.

De plus si on note $a \wedge b$ le p.g.c.d. de a et b et $a \vee b$ le p.p.c.m. de a et b on a la relation$(a \wedge b)(a \vee b) = ab$ (avec la convention $0 \wedge 0 = 0$).

Exemple 2.4.2 *Comme le p.g.c.d. de* 55 *et* 132 *est égal à* 11*, le p.p.c.m. de* 55 *et* 132 *est égal à* 660.

Une autre notion importante est la notion de nombre premier.

Definition 2.4.3 *Soit $p \geq 2$ un entier. On dit que p est premier si* 1 *et p sont les seuls diviseurs positifs de p.*

Il est clair que si p est premier, et si q n'est pas un multiple de p, alors p et q sont premiers entre eux. En utilisant le théorème de Gauss, on obtient le résultat suivant

Théorème 2.4.4 *Soit $a \geq 2$ un entier. Il existe une unique suite finie croissante $(p_1, \ldots, p_k)$ de nombres premiers et une unique suite $(n_1, \ldots, n_k)$ d'entiers positifs telles que $a = p_1^{n_1} \ldots p_k^{n_k}$. Cette formule est appellée décomposition en facteurs premiers de n.*

En utilisant la décomposition en facteurs premiers de deux entiers on obtient le résultat suivant.

Proposition 2.4.5 *Soient $a \geq 2$ et $b \geq 2$ deux entiers. Le p.g.c.d. de a et b est égal au produit des diviseurs premiers communs à a et b, affectés du plus petit de leurs exposants dans les décompositions de a et b, et le p.p.c.m. de a et b est égal au produit des diviseurs premiers de a ou b, affectés du plus grand de leurs exposants dans les décompositions de a et b.*

Exemple 2.4.6 *Les décompositions en facteurs premiers de* 110 *et* 132 *sont* $110 = 2 \times 5 \times 11$ *et* $132 = 2^2 \times 3 \times 11$. *Les seuls diviseurs premiers communs à* 55 *et* 132 *sont* 2 *(avec l'exposant* 1 *pour* 110 *et l'exposant* 2 *pour* 132*) et* 11 *(avec l'exposant* 1 *dans les deux cas). Donc* $110 \wedge 132 = 2 \times 11 = 22$*, et* $110 \vee 132 = 2^2 \times 3 \times 5 \times 11 = 660$.

Cette deuxième méthode de calcul du p.g.c.d. est à première vue plus simple que l'algorithme d'Euclide mais pour les grands nombres le coût du calcul de la décomposition en facteurs premiers est élevé, et les logiciels de calcul utilisent des variantes de l'algorithme d'Euclide.

Pour dresser la liste des nombres premiers on utilise le "*crible d'Eratosthène*" que nous mettons en oeuvre pour déterminer les nombres premiers inférieurs ou égaux à 30.

On écrit la liste $2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30$

On garde 2 et on raye les mutiples de 2.

$2, 3, ., 5, ., 7, ., 9, ., 11, ., 13, ., 15, ., 17, ., 19, ., 21, ., 23, ., 25, ., 27, ., 29, .$

Le premier nombre non rayé après 2 est 3. On le garde et on raye les multiples de 3.

$2, 3, ., 5, ., 7, ., ., ., 11, ., 13, ., ., ., 17, ., 19, ., ., ., 23, ., 25, ., ., ., 29, .$

Le premier nombre non rayé après 3 est 5. On le garde et on retire tous les multiples de 5.

$\mathbf{2}, \mathbf{3}, ., \mathbf{5}, ., \mathbf{7}, ., ., ., \mathbf{11}, ., \mathbf{13}, ., ., ., \mathbf{17}, ., \mathbf{19}, ., ., ., \mathbf{23}, ., ., ., ., ., \mathbf{29}, .$

Comme tout nombre non premier $n \geq 30$ admet un diviseur premier $p \leq \sqrt{30} < 6$, on vient d'écrire la liste des nombres premiers inférieurs ou égaux à 30.

Le plus grand nombre premier connu est $2^{6972593}-1$ qui a 2.098.960 chiffres.Ce résultat a rapporté en 1999 $ 50.000 à ses auteurs. Une prime de $ 100.000 sera attribuée à ceux qui construiront un nombre premier de plus de dix millions de chiffres (les grands nombres premiers jouent un rôle important en cryptographie).

Nous concluons ce chapitre par le résultat suivant.

Théorème 2.4.7 *Soit $p \geq 2$ un entier. Alors $\mathbf{Z}/p\mathbf{Z}$ est un corps si et seulement si p est premier.*

Démonstration : Si p n'est pas premier il existe un diviseur d de p tel que $1 < d < p$. On a alors $p = dq$ avec $1 < q < p$. Donc $\bar{0} = \bar{d}\bar{q}$ avec $\bar{d} \neq 0$, $\bar{q} \neq 0$, et $\mathbf{Z}/p\mathbf{Z}$ n'est pas un corps.

Par contre si p est premier soit α un élément non nul de $\mathbf{Z}/p\mathbf{Z}$. On a $u = \bar{a}$ avec $1 \leq a < p$. Donc a et p sont premiers entre eux. D'après le théorème 2.1.5 il existe $u, v \in \mathbf{Z}$ tels que $au + pv = 1$ et $0 \leq u \leq p-1$, et le reste de la division de au par p est égal à 1. Donc $\alpha\bar{u} = \bar{1}$ et tout élément non nul de $\mathbf{Z}/p\mathbf{Z}$ est inversible, ce qui prouve que $\mathbf{Z}/p\mathbf{Z}$ est un corps. ♣

2.5 Arithmétique sous MUPAD

On peut facilement calculer des p.g.c.d. sous MUPAD

Exemple 2.5.1 *Calculer le p.g.c.d. de* 298765435678976 *et* 34567891345298766.

On utilise la commande **igcd**.

```
igcd(298765435678976,34567891345298766);
```

```
14
```

Le p.g.c.d. cherché est donc 14, et MUPAD calcule aussi les coefficients de l'équation de Bezout.

Exemple 2.5.2 *Trouver deux entiers relatifs* u *et* v *tels que* $298765435678976.u + 34567891345298766.v = 14$.

On utilise la commande **igcdex**

```
igcdex(298765435678976,34567891345298766);
```

```
14, -276327850495985, 2388262848289
```

On peut donc prendre $u = -276327850495985$ et $v = 2388262848289$.

On peut s'aider de MUPAD pour résoudre des équations de congruence à gros coefficients.

Exemple 2.5.3 *Trouver un entier relatif* x *vérifiant le système d'équations de congruence suivant*

$x \equiv 23467 \quad (5139204473593)$
$x \equiv 34567 \quad (3710417184184751041)$
$x \equiv 345921 \quad (19214672689)$

Conformément au cours, on va chercher x de la forme $x = 23467 + 5139204473593.n$, avec $n \in \mathbf{Z}$, et on va chercher à déterminer n de facon que x vérifie la seconde équation. On doit donc avoir $x - 34567 = 3710417184184751041.m$, avec $m \in \mathbf{Z}$. On obtient $-11100 + 5139204473593.n = 3710417184184751041.m$ soit $5139204473593.n - 3710417184184751041.m = 11100$.

On vérifie que 5139204473593 et 3710417184184751041 sont premiers entre eux et on cherche une solution de l'équation de Bezout $5139204473593.u + 3710417184184751041.v = 1$.

```
igcdex(5139204473593,3710417184184751041);
```

```
1, 211774982003123841, -293324141432
```

On peut donc prendre $u = 211774982003123841$. On multiplie par 11100

```
211774982003123841*11100;
```

```
2350702300234674635100
```

Donc $x = 23467 + 5139204473593 \times 2350702300234674635100$ est solution des deux premières équations.

```
23467 + 5139204473593 *
  2350702300234674635100;
```

```
120807397774513952984447248609377 67
```

Donc 120807397774513952984447248609377 67 est solution des deux premières équations.

Pour avoir une solution des trois équations on cherche x de la forme $x = 120807397774513952984447248609377 67+5139204473593\times3710417184184751041\times p$, avec $p \in \mathbf{Z}$. On doit avoir $x - 345921 = 19214672689 \times q$, avec $q \in \mathbf{Z}$, soit $120807397774513952984447248609377 67-345921+5139204473593\times3710417184184751041\times p = 19214672689 \times q$. Après calculs on obtient finalement

-92006627297481846863667070278609332417751150140596221093869947051494040521 7

Pour obtenir un nombre plus raisonnable on va remplacer le nombre trouvé par le reste de sa division par $5139204473593\times3710417184184751041\times19214672689$ avec la commande modp

```
    5139204473593* 3710417184184751041*
19214672689;
```

```
366396765292453449518496628221093743191657
```

```
modp(-92006627297481846863667070278609332417751150140596221093869947051494040521 7,
366396765292453449518496628221093743191657);
```

```
215557658403617465722583570562398169549197
```

On trouve donc que **21555765840361746572258357056239816954919 7 est solution de l'équation proposée.**

En fait la bibliothèque de MUPAD **permettait d'obtenir directement le résultat en une fraction de seconde avec la commande numlib : :ichrem**

```
numlib::ichrem([ 23467, 34567,345921],[5139204473593,3710417184184751041,19214672689]);
```

```
215557658403617465722583570562398169549197
```

On peut trouver aussi avec MUPAD la décomposition en facteurs premiers.Le premier nombre donné est le signe, et ensuite on trouve les facteurs premiers suivis de l'ordre de multiplicité.MUPAD peut bien sûr aussi calculer le p.p.c.m.

Exemple 2.5.4 *Décomposition en facteurs premiers et p.p.c.m. de 286439140625 et 9240262625.*

Pour la décomposition en facteurs premiers on utilise la commande **ifactor**.

```
ifactor( 286439140625);
```

```
[1, 5, 7, 11, 2, 157, 1, 193, 1]
```

```
ifactor( 9240262625);
```

```
[1, 5, 3, 11, 1, 6720191, 1]
```

Les décompositions en facteurs premiers sont donc $286439140625 = 5^7 \times 11^2 \times 157 \times 193$ et $9240262625 = 5^3 \times 11 \times 6720191$. Ceci montre que le p.g.c.d. est égal à $5^3 \times 11 =$ **1375** et le p.p.c.m. à $5^7 \times 11^7 \times 157 \times 193 \times 6720191$ que l'on calcule sous MUPAD :

```
   5^7* 11^2*
157 * 193 * 6720191;
```

```
1924925734875859375
```

Le p.p.c.m. de 286439140625 et 9240262625 est donc égal à **1924925734875859375**.

On retrouve directement ces deux résultats en utilisant la commande **igcd** pour le p.g.c.d. et la commande **ilcm** pour le p.p.c.m.

```
igcd(286439140625 , 9240262625);
```

```
                                    1375
```

```
ilcm(286439140625 , 9240262625);
```

```
                              1924925734875859375
```

2.6 Exercices pour le Chapitre 2

exercice 1

a) En utilisant l'algorithme d'Euclide étendu, d'eterminer le p.g.c.d. de 90 et 72 et déterminer deux entiers relatifs u et v tels que $90u + 72v = 18$.

b) Décomposer 72 et 18 en facteurs premiers. Utiliser ces décompositions pour retrouver le p.g.c.d. de 90 et 72 et trouver leur p.p.c.m.

exercice 2

Trouver un entier n vérifiant les 3 propriétés suivantes

a) $n - 1$ est divisible par 4

b) $n + 3$ est divisible par 5

c) $n - 2$ est divisible par 7.

exercice 3

Vérifier que si $a, b \in \mathbf{Z}$, $a\mathbf{Z} + b\mathbf{Z}$ et $a\mathbf{Z} \cap b\mathbf{Z}$ sont des sous-groupes de $\mathbf{Z}$. Montrer que $a\mathbf{Z} + b\mathbf{Z} = (a \wedge b)\mathbf{Z}$ et $a\mathbf{Z} \cap b\mathbf{Z} = (a \vee b)\mathbf{Z}$.

exercice 4

Prouver que $\sqrt{2}$ et $\sqrt{5}$ ne sont pas pas rationnels.

exercice 5

Soit $n \geq 1$; montrer que si $2^n - 1$ est premier alors n est premier.

exercice 6

a) Démontrer que pour tout $(x, n) \in \mathbf{N}^2$, $1 + x$ divise $1 + x^{2n+1}$.

b) En déduire si $2^m + 1$ est premier alors m est une puissance de 2.

exercice 7
Déterminer le reste de la division euclidienne de $(7077)^{377}$ par 11.

exercice 8
Soit $x = \overline{a_n a_{n-1} \cdots a_1 a_0}$ un entier écrit en système décimal.
a) Prouver que x est divisible par 11 si et seulement si $\sum_{k=0}^{n}(-1)^k a_k \equiv 0 \quad (11)$.
b) Prouver que x est divisible par 6 si et seulement si $4\sum_{k=1}^{n} a_k + a_0 \equiv 0 \quad (6)$.

exercice 9
Chercher l'ensemble des couples $(x, y) \in \mathbf{Z}^2$ tels que :
a) $11x + 41y = 4$.
b) $8x + 30y = 7$.
c) $12x + 3y = 21$.

exercice 10
Résoudre dans $\mathbf{N}^2$, les deux équations suivantes :
(i) $a \vee b + 10\ a \wedge b = 142$.
(ii) $a \vee b + a \wedge b = b + 9$.

exercice 11
a) Déterminer les éléments inversibles de $\mathbf{Z}\backslash 20\mathbf{Z}$ et préciser leurs inverses.
b) Résoudre dans $\mathbf{Z}\backslash 20\mathbf{Z} \times \mathbf{Z}\backslash 20\mathbf{Z}$ le système ci-dessous :
$\bar{4}x + \bar{7}y = \overline{10}$
$\bar{5}x + \overline{14}y = \overline{18}$

exercice 12
Résoudre l'équation $\bar{x}^2 = \bar{1}$ dans $\mathbf{Z}\backslash 19\mathbf{Z}$ et $\mathbf{Z}\backslash 58\mathbf{Z}$.

exercice 13 [Petit théorème de Fermat]
Si p est un nombre premier et $n \geq 1$, montrer que $n^p \equiv n \quad (p)$.

exercice 14 [cryptographie à clef publique]
Elaborer un algorithme qui calcule les diviseurs d'un entier naturel quelconque n. Est-ce que votre algorithme est utilisable en pratique (i.e. avec un ordinateur) si n est très grand ?

exercice 15 (sous MUPAD)
a) Déterminer le p.g.c.d. et le p.p.c.m. de 10987654654983 et 13987673897659876 et trouver deux entiers relatifs u et v tels que $10987654654983 \times u + 13987673897659876 \times v = 1$.
b)D'ecomposer 10987654654983 et 13987673897659876 en facteurs premiers et retrouver à partir de cette décomposition leur p.g.c.d. et leur p.p.c.m.

exercice 16 (sous MUPAD)
Trouver le plus petit entier positif x véifiant les trois équations suivantes

$$x \equiv 123 \qquad (10987654654983)$$

$$x \equiv -24567 \qquad (13987673897659876)$$

$$x \equiv 3456298 \qquad (6720227)$$

Chapitre 3

Polynômes

3.1 Polynômes sur un corps K

On va commencer par définir l'anneau $K[x]$ des polynômes sur un corps K.

Definition 3.1.1 *Soit K un corps. Un polynôme à coefficients dans K est une suite $(a_k)_{k\geq 0}$ d'éléments de K nulle à partir d'un certain rang. L'ensemble des polynômes à coefficients dans k est noté $K[x]$. On définit la somme et le produit de deux polynômes $(a_k)_{k\geq 0}$ et $(b_k)_{k\geq 0}$ par les formules*

$(a_k)_{k\geq 0} + (b_k)_{k\geq 0} = (a_k + b_k)_{k\geq 0}$

$(a_k)_{k\geq 0}.(b_k)_{k\geq 0} = (\sum_{j=0}^{k} a_j b_{k-j})_{k\geq 0}$.

On définit également le produit d'un élément λ de k et d'un polynôme $(a_k)_{k\geq 0}$ par la formule

$\lambda.(a_k)_{k\geq 0} = (\lambda a_k)_{k\geq 0}$.

Des vérifications de routine montrent que $(K[x], +, .)$ est un anneau commutatif. L'élément neutre de l'addition est le polynôme nul $\tilde{0} := (0, 0, 0, \ldots)$ et l'élément neutre de la multiplication est le polynôme $\tilde{1} := (0, 1, 0, 0, \ldots)$.

Definition 3.1.2 *Soit $P = (a_k)_{k\geq 0}$ un polynôme non nul. On appelle degré de P, et on note $d^\circ(P)$, le plus grand entier $n \geq 0$ tel que $a_n \neq 0$. On pose par convention $d^\circ(\tilde{0}) = -\infty$.*

Si m et n sont deux entiers naturels on définit le symbole de Kronecker $\delta_{m,n}$ par la formule

$\delta_{m,n} = 0$ si $m \neq n$

$\delta_{m,n} = 1$ si $m = n$

Posons $e_p = (\delta_{p,k})_{k\geq 0}$, de sorte que $e_0 = \tilde{0}$ et $e_1 = \tilde{1}$. On a $e_p e_q = (\sum_{j=0}^{k} \delta_{p,j}\delta_{q,k-j})_{k\geq 0}$. La seule possibilité pour que $\delta_{p,j}\delta_{q,k-j} \neq 0$ est que l'on ait à la fois $j = p$ et $k - j = q$. Ceci ne se produit que si $k = p + q$ et on voit donc que $e_p e_q = e_{p+q}$.

Posons $x^p = e_p$ pour $p \geq 1$.

Soit $P = (a_k)_{k\geq 0} \in K[x]$, et soit $n \in \mathbf{N}$ tel que $n \geq d^\circ(P)$. On a $(a_k)_{k\geq 0} = a_0\tilde{1} + \ldots + a_n x^n$. Par un abus d'écriture on écrira 0 au lieu de $\tilde{0}$, 1 au lieu de $\tilde{1}$, et on supprimera $\tilde{1}$ dans l'écriture ci-dessus, ce qui revient à identifier a au polynôme $(a, 0, 0, 0, \ldots)$ pour $a \in k$ (on dira alors que le polynôme $(a, 0, 0, 0, \ldots) \simeq a$ est un *polynôme constant).* On obtient, avec la convention $x^0 = 1$, l'écriture usuelle

$P = a_0 + \ldots a_n x^n = \sum_{k=0}^{n} a_k x^k$ pour $P \in K[x]$, $n \geq d^\circ(P)$.

Avec les conventions $n > -\infty$ et $n + (-\infty) = -\infty + (-\infty) = -\infty$ pour $n \in \mathbf{N}$ on vérifie que l'on a , pour $P \in k[x], Q \in k[x]$:

(3.1) $d^\circ(P+Q) \leq max(d^\circ(P), d^\circ(Q))$, et $d^\circ(P+Q) = max(d^\circ(P), d^\circ(Q))$ si $d^\circ(P) \neq d^\circ(Q)$.

(3.2) $d^\circ(PQ) = d^\circ(P) + d^\circ(Q)$

Soient A et B deux polynômes non nuls. Il résulte de la formule (3.2) que $AB \neq 0$. En particulier on a le *principe de simplification* suivant

(3.3) Si $AB = AC$ avec $A, B, C \in K[x]$, $A \neq 0$, alors $B = C$.

3.2 Division euclidienne

Le résultat suivant a été vu en Terminale pour les polynômes à coefficients réels.

Théorème 3.2.1 *Soient $P \in K[x], B \in K[x]$, avec $B \neq 0$. Il existe alors un unique couple (Q, R) d'éléments de $K[x]$ vérifiant les deux propriétés suivantes*

(i) $P = BQ + R$

(ii) $d^\circ(R) < d^\circ(B)$.

Démonstration : L'existence du couple (Q,R) est évidente si $d^\circ(B) = 0$, car dans ce cas il suffit de poser $Q = \frac{A}{B}, R = 0$. Supposons maintenant que $n := d^\circ(B) \geq 1$. On a $B = b_0 + \ldots + b_n x^n$, avec $b_n \neq 0$. On va raisonner par récurrence sur le degré de P. Si $d^\circ(P) < n$ il suffit de poser $Q = 0, R = P$. Supposons qu'un couple (Q, R) vérifiant les propriétés (i) et (ii) existe pour tous les polynômes P tels que $d^\circ(P) \leq k$, avec $k \geq n - 1$, et soit $P \in K[x]$ tel que $d^\circ(P) \leq k + 1$. On a $P = a_0 + \ldots + a_{k+1} x^{k+1}$, et le degré de $P - \frac{a_{k+1}}{b_n} B x^{k+1-n}$ est inférieur ou égal à k . Donc il existe $Q, R \in K[x]$, avec $d^\circ(R) < d^\circ(B)$, tels que $P - \frac{a_{k+1}}{b_n} B x^{k+1-n} = BQ + R$. On a alors $P = B(Q + \frac{a_{k+1}}{b_n} x^{k+1-n}) + R$, avec $d^\circ(R) < d^\circ(B)$, ce qui donne la décomposition cherchée. On voit donc par récurrence qu'un couple (Q, R) vérifiant les propriétés (i) et (ii) existe pour tout $P \in K[x]$.

Soient maintenant (Q, R) et (Q', R') deux couples de polynômes vérifiant (i) et (ii). On a $R - R' = B(Q' - Q)$. Si $Q' \neq Q$ on aurait $d^\circ(B) > max(d^\circ(R), d^\circ(R')) \geq d^\circ(R - R') = d^\circ(B) + d^\circ(Q' - Q) \geq d^\circ(B)$, ce qui est absurde.Donc $Q = Q'$ et $R = R'$. ♣

Notons que la démonstration formelle ci-dessus donne en fait un algorithme explicite pour calculer Q et R. Nous illustrons cet algorithme dans le cas où $P = x^3 + 1$, $B = x^2 + 2x + 1$.

$\mathbf{x^3}$			$\mathbf{+1}$	$\mathbf{x^2}$	$\mathbf{+2x}$	$+1$
$-x^3$	$-2x^2$	$-x$		$\mathbf{x}$	$\mathbf{-2}$	
	$\mathbf{-2x^2}$	$\mathbf{-x}$	$\mathbf{+1}$			
	$2x^2$	$+4x$	$+2$			
		$\mathbf{3x}$	$\mathbf{+3}$			

On obtient donc la décomposition $x^3 + 1 = (x^2 + 2x + 1)(x - 2) + 3x + 3$. Dans ce cas $Q = x - 2, R = 3x + 3$.

Pour $P = a_0 + \ldots + a_n x^n \in K[x], \lambda \in K$, on définit $P(\lambda) \in K$ par la formule

(3.4) $\quad P(\lambda) = a_0 + \ldots + a_n \lambda^n$

On vérifie immédiatement que l'on a les propriétés suivantes, pour $P, Q \in K[x], \lambda \in K$:

(3.5) $\quad (P + Q)(\lambda) = P(\lambda) + Q(\lambda)$.

(3.6) $\quad (PQ)(\lambda) = P(\lambda)Q(\lambda)$.

Definition 3.2.2 *Soit $P \in K[x]$, et soit $\lambda \in K$. On dit que λ est une racine de P quand $P(\lambda) = 0$.*

De même que pour les entiers relatifs on introduit la notion de *diviseur* d'un polynôme.

Definition 3.2.3 *Soient $P, Q \in K[x]$. On dit que P est un diviseur de Q s'il existe $U \in K[x]$ tel que $Q = PU$. On dit alors que Q est un multiple de P.*

On a alors le résultat suivant, déjà vu en Terminale pour les polynômes à coefficients réels.

Corollaire 3.2.4 *Soit $P \in K[x]$ et soit $\lambda \in K$. Alors λ est une racine de P si et seulement si P est divisible par $x - \lambda$.*

Démonstration : On a $P = (x - \lambda)Q + R$, avec $d^\circ(R) < 1$. Donc il existe $a \in K$ tel que $R = a$, et $P(\lambda) = (\lambda - \lambda)Q(\lambda) + a = a$. Ceci montre que $P = (x - \lambda)Q + P(\lambda)$, et on voit que $x - \lambda$ est un diviseur de P si et seulement si $P(\lambda) = 0$. ♣

3.3 Idéaux de l'anneau des polynômes

On va maintenant introduire la notion d'*idéal*, qui joue un rôle central dans la théorie des anneaux.

Definition 3.3.1 *On dit que $I \subset K[x]$ est un idéal de $K[x]$ quand les deux conditions suivantes sont vérifiées*
(i) I est un sous-groupe de $(K[x], +)$
(ii) $PQ \in I \quad \forall P \in I, \forall Q \in K[x]$.

Pour $P \in K[x]$, on pose $PK[x] = \{PQ\}_{Q \in K[x]}$. Il est clair que $PK[x]$ est un idéal de $K[x]$. Réciproquement on a le résultat suivant, qui est la base de "l'arithmétique des polynômes."

Théorème 3.3.2 *Pour tout idéal I de $K[x]$ il existe $B \in K[x]$ tel que $I = BK[x]$.*

Démonstration : Si $I = \{0\}$ il suffit de prendre $B = 0$. Si $I \neq 0$ notons I^* l'ensemble des éléments non nuls de I. Il existe $B \in I^*$ tel que $d^\circ(B) \leq d^\circ(P)$ pour tout $P \in I^*$.

On a $BQ \in I$ pour tout $Q \in K[x]$, donc $BK[x] \subset I$. Soit maintenant $P \in I$. Il existe $Q, R \in K[x]$, avec $d^\circ(R) < d^\circ(B)$, tels que $A = BQ + R$. Comme $B \in I$, $BQ \in I$, et comme $P \in I$, $R = P - BQ \in I$. Si $R \neq 0$, on aurait $R \in I^*$ et $d^\circ(R) \geq d^\circ(B)$, ce qui n'est pas le cas. Donc $R = 0$ et $P \in I$, ce qui prouve que $I = BK[x]$. ♣

3.4 La notion de p.g.c.d

On va maintenant introduire la notion de *plus grand commun diviseur (p.g.c.d.)* pour une famille de polynômes.On dira qu'un polynôme $P \in K[x]$ est *unitaire* s'il existe $n \geq 0$ tel que $P = \sum_{k<n} a_k x^k + x^n$ (on a alors $d^\circ(P) = n$).

Théorème 3.4.1 *Soit $(A_1, \ldots, A_p)$ une famille d' éléments de $K[x]$ non tous nuls. Il existe un unique polynôme unitaire $D \in K[x]$,appelé le p.g.c.d. de la famille $(A_1, \ldots, A_p)$, possédant les propriétés suivantes*

(i) D est un diviseur de A_i pour $1 \leq i \leq p$.
(ii) Si $\Delta \in K[x]$ est un diviseur de A_i pour $1 \leq i \leq k$, alors Δ est un diviseur de D.

D'autre part il existe une famille $(U_1, \ldots, U_{p)})$ d'éléments de $K[x]$ vérifiant

(iii) $A_1U_1 + \ldots A_pU_p = D$ (identité de Bezout).

De plus si $P \in K[x]$, alors l'équation $A_1V_1 + \ldots + A_pV_p = P$ possède des solutions $(V_1, \ldots, V_p)$ dans $K[x]^p$ si et seulement si P est un multiple de D.

Démonstration : Soit I l'ensemble des polynômes de la forme $P = A_1Q_1 + \ldots + A_pQ_p$, où $Q_1, \ldots, Q_p \in K[x]$. En posant $Q_j = 0$ pour $1 \leq j \leq p, j \neq i$, $Q_i = 1$, on voit que $A_i \in I$ pour $1 \leq i \leq p$, et $I \neq \{0\}$.

Soient $P = A_1Q_1 + \ldots + A_pQ_p, P' = A_1Q'_1 + \ldots + A_pQ'_p$ deux éléments de I. On a $P - P' = A_1(Q_1 - Q'_1) + \ldots + A_p(Q_p - Q'_p) \in I$, et par conséquent I est un sous-groupe de $(K[x], +)$.

Soit maintenant $P = A_1Q_1 + \ldots + A_pQ_p \in I$, et soit $Q \in K[x]$. On a $PQ = A_1Q_1Q + \ldots + A_pQ_pQ \in I$, et on voit que I est un idéal de $K[x]$. Il existe donc $D \in K[x]$ tel que $I = DK[x]$. Comme $I \neq \{0\}$, $D \neq 0$, et , quitte à multiplier D par un élément non nul de K, on peut supposer que D est unitaire.

Comme $A_i \in I$, il existe $Q_i \in K[x]$ tel que $A_i = DQ_i$, et on voit que D est un diviseur de A_i pour $1 \leq i \leq p$. Comme $D = D.1 \in I$, il existe $U_1, \ldots, U_p \in K[x]$ tels que $D = A_1U_1 + \ldots + A_pU_p$, et D vérifie (iii). Soit maintenant $\Delta \in K[x]$ tel que Δ divise A_i pour $1 \leq i \leq p$. Il existe $B_1, \ldots, B_p \in K[x]$ tels que $A_i = \Delta B_i$ pour $1 \leq i \leq p$, et on a $D = \Delta(B_1U_1 + \ldots + B_pU_p)$. Donc Δ divise D, et D vérifie (ii). Soit $D' \in K[x]$ un polynôme unitaire vérifiant (i) et (ii). Alors D' divise D et D divise D' , donc il existe $B, B' \in K[x]$ tels que $D' = DB$ et $D = D'B'$. Donc $D = DBB'$. Comme $D \neq 0$, $d^\circ(B) + d^\circ(B') = 0$. Donc $d^\circ(B) = d^\circ(B') = 0$, et il existe $b \in K, b \neq 0$ tel que $D' = bD$. Donc D' est de la forme $D' = b(\sum_{k<n} d_kx^k + x^n) = \sum_{k<n} bd_kx^k + bx^n$. Comme $b \neq 0$, et comme D' est unitaire, on a $b = 1, D' = D$, ce qui prouve l'unicité du p.g.c.d..

Soit $P \in K[x]$.Il résulte de la définition de D que P est un multiple de D si et seulement si $P \in I$. Il résulte alors de la définition de I que la propriété (iv) est vérifiée. ♣

Il est clair que le p.g.c.d. d'une famille $(A_1, \ldots, A_p)$ de polynômes ne change pas si on retire de cette famille des polynômes nuls. D'autre part si on note B_k le p.g.c.d. de la famille $(A_1, \ldots, A_k)$ alors le p.g.c.d. de la famille $(A_1, \ldots, A_{k+1})$ est égal au p.g.c.d. de B_k et A_{k+1}. Donc pour calculer le p.g.c.d. d'une famille finie quelconque de polynômes il suffit de savoir calculer le p.g.c.d. de deux polynômes non nuls.

On peut pour cela utiliser l'**algorithme d'Euclide**, de même que dans le cas du p.c.c.d. de deux entiers. On dira que deux polynômes U et V à coefficients dans K sont *équivalents* , et on écrira $U \approx V$, s'il existe $\lambda \in K$, avec $\lambda \neq 0$, tel que $U = \lambda V$.

Pour calculer le p.g.c.d. D de deux polynômes non nuls A et B, on procède de la manière suivante.On commence par écrire

$A = BQ_1 + R_1$ avec $d^\circ(R_1) \leq d^\circ(B) - 1$. Si $R_1 = 0, D \approx B$.
Sinon on recommence
$B = R_1Q_2 + R_2$ avec $d^\circ(R_2) \leq d^\circ(R_1) - 1$. Si $R_2 = 0, D \approx R_1$.
Sinon on recommence
$R_1 = R_2Q_3 + R_3$ avec $d^\circ(R_3) \leq d^\circ(R_2) - 1$. Si $R_3 = 0, D \approx R_2$.
Sinon on recommence
....
$R_k = R_{k+1}Q_{k+2} + R_{k+2}$ avec $d^\circ(R_{k+2}) \leq d^\circ(R_{k+1}) - 1$. Si $R_{k+2} = 0, D \approx R_{k+1}$.

Sinon on recommence

...

On finit par avoir, à un certain rang p

$R_p = R_{p+1}Q_{p+2} + R_{p+2}$ avec $d^\circ(R_{p+2}) \leq d^\circ(R_{p+1}) - 1$, $R_{p+2} \neq 0$
$R_{p+1} = R_{p+2}Q_{p+3} + R_{p+3}$ avec $R_{p+3} = 0$. On a alors $D \approx R_{p+2}$.

Autrement dit **"le p.g.c.d. est égal au dernier reste non nul dans l'algorithme d'Euclide."** Comme $d^\circ(R_k) > d^\circ(R_{k+1})$ pour tout k , il est clair avec les notations ci-dessus que l'algorithme s'arrête avec $p + 2 \leq b - 1$. Le fait que le p.g.c.d. de A et B est bien équivalent au dernier reste non nul provient du fait que si U et V sont deux polynômes alors le p.g.c.d. de U et V est égal au p.g.c.d. de V et du reste de la division de U par V.

On a donc

$p.g.c.d.(A, B) = p.g.c.d.(B, R_1) = p.g.c.d.(R_1, R_2) = \ldots = p.g.c.d.(R_{p+2}, 0) \approx R_{p+2}$. Notons que **le p.g.c.d. de deux polynômes ne change pas si on remplace ces deux polynômes par des polynômes équivalents.** Cette remarque évidente permet de simplifier les calculs.

Exemple 3.4.2 *p.g.c.d. de* $x^3 + 1$ *et* $x^4 + x^2 + 3x + 1$.

Un calcul simple donne

$$x^4 + x^2 + 3x + 1 = (x^3 + 1)x + x^2 + 2x + 1.$$

Un calcul déjà vu donne

$x^3+1 = (x^2+2x+1)(x-2)+\mathbf{3x+3}$. On remplace à la ligne suivante $3x+3$ par le polynôme équivalent $x + 1$.

$$x^2 + 2x + 1 = (x + 1)^2 = (x + 1)(x + 1) + \mathbf{0}.$$

Le p.g.c.d. de x^3+1 et x^2+2x+1 est donc le polynôme unitaire équivalent à $3x + 3$. Il est donc égal à $\mathbf{x + 1}$.

Soient A et B deux polynômes non nuls, et soit D leur p.g.c.d.. Pour trouver deux polynômes U et V vérifiant l'équation de Bezout $AU + BV = D$ il suffit , de même que dans le cas des entiers, de "**remonter l'algorithme d'Euclide**." On exprime R_{p+2} en fonction de R_{p+1} et R_p en utilisant l'avant-dernière ligne de l'algorithme. Avec la ligne précédente on exprime R_{p+1} en fonction de R_p et R_{p-1} , ce qui permet d'exprimer R_{p+2} en fonction de R_p et R_{p-1} , etc...En continuant ce procédé on trouve les polynômes U et V cherchés. En fait pour ce type de calculs le plus simple est d'utiliser un "algorithme d'Euclide étendu" analogue à celui utilisé pour les entiers. En écrivant $R_n = AU_n + BV_n$, on obtient les relations

$$U_{n+2} = -Q_{n+2}U_{n+1} + U_n, \quad V_{n+2} = -Q_{n+2}V_{n+1} + V_n,$$

ce qui permet d'effecuer les calculs en posant $U_0 = 0$, $V_0 = 1$, $U_1 = 1 = Q_1 \times 0 + 1$, $V_1 = -Q_1 = -Q_1 \times 1 + 0$.

Nous illustrons ceci par un exemple.

Exemple 3.4.3 *Trouver deux polynômes U et V tels que $(x^4+x^2+3x+1)U+(x^3+1)V = x+1$.*

On utilise l'algorithme d'Euclide étendu :

	Q_n	U_n	V_n
		1	0
		0	1
$x^4+x^2+3x+1 = (x^3+1)x+x^2+2x+1$	x	1	$-x$
$x^3+1 = (x^2+2x+1)(x-2)+\mathbf{3x+3}$	$x-2$	$-x+2$	x^2-2x+1
$(x^2+2x+1) = \frac{1}{3}(3x+3)(x-1)+\mathbf{0}$			

On obtient

$$-(x^4+x^2+3x+1)(x-2)+(x^3+1)(x^2-2x+1) = 3x+3,$$

On peut donc prendre $U = -\frac{1}{3}(x-2), V = \frac{1}{3}(x^2-2x+1)$.

3.5 Applications du théorème de Bezout

Definition 3.5.1 *On dit que deux polynômes non nuls A et B sont premiers entre eux quand leur p.g.c.d. est égal à 1.*

Théorème 3.5.2 *(Gauss) Soient A, B, C trois polynômes non nuls. Si A divise BC, et si A est premier avec B , alors A divise C.*

Démonstration : Il existe $U, V \in K[x]$ tels que $AU+BV = 1$. Donc $C = AUC+BCV$. Comme A divise BC , il existe $W \in K[x]$ tel que $BC = AW$. Donc $C = A(UC+VW)$, ce qui montre que A divise C. ♣

Corollaire 3.5.3 *Soient A et B deux polynômes non nuls et soit D le p.g.c.d. de A et B. Soit $\mathcal{S} = \{(U,V) \in K[x]\times K[x] \mid AU+BV = 0\}$. On a $\mathcal{S} = \{-PB', PA'\}_{P\in K[x]}$, où $A' = \frac{A}{D}$ et $B' = \frac{B}{D}$*

Démonstration : Il résulte du théorème de Bezout que A' et B' sont premiers entre eux, et $\mathcal{S} = \{(U,V) \in K[x]\times K[x] \mid A'U+B'V = 0\}$. Il est clair que si $U = -PB'$ et si $V = PA'$ alors $(U,V) \in \mathcal{S}$. Réciproquement si $A'U+B'V = 0$ alors A' divise $B'V$, donc A' divise V d'après le théorème de Gauss. Donc il existe $P \in K[x]$ tel que $V = PA'$. On a alors $UA' = -B'PA'$, donc $U = -PB'$. ♣

Corollaire 3.5.4 *Soient A et B deux polynômes non nuls premiers entre eux, et soit P un polynôme. Il existe un unique couple (R,T) de polynômes vérifiant les deux conditions suivantes*

(i) $AR + BT = P$
(ii) $d^\circ(R) < d^\circ(B)$.
De plus $AU + BV = P$ *si et seulement si il existe un polynôme* Q *tel que* $U = R + BQ, V = T - AQ$.

Démonstration : On sait que l'équation de Bezout $AU + BV = 1$ possède une solution (U_1, V_1) dans $K[x] \times K[x]$. Soit R le reste de la division de U_1P par B. Il existe $Q \in K[x]$ tel que $U_1P = BQ + R$. Posons $T = V_1P + AQ$. On a $AR+BT = A(U_1P-BQ)+B(V_1P+AQ) = AU_1+BV_1 = P$, et $d^\circ(R) < d^\circ(B)$. On a $AU+BV-P = A(U-R)+B(V-T)$. Donc $AU+BV = P$ si et seulement si il existe un polynôme Q tel que $U = R + BQ, V = T - AQ$.

Soit (R', T') un autre couple de polynômes vérifiant (i) et (ii). Il existe $Q \in K[x]$ tel que $R' = BQ + R$. D'après l'unicité de la division euclidienne des polynômes on a $Q = 0$ et $R' = R$. Comme $B(T' - T) = 0$ on a alors $T' = T$. ♣

On a la variante suivante du théorème de Gauss.

Théorème 3.5.5 *Soient* $A, B_1, \ldots, B_p$ *des polynômes non nuls. Si* A *est premier avec* B_i *pour* $1 \leq i \leq p$, *alors* A *est premier avec le produit* $B_1 \ldots B_p$.

Démonstration : Si A est premier avec B_1 et B_2 , il existe $U_1, V_1, U_2, V_2 \in K[x]$ tels que $AU_1 + B_1V_1 = AU_2 + B_2V_2 = 1$. En multipliant membre à membre on obtient $(AU_1 + B_1V_1)(AU_2 + B_2V_2) = 1$ soit $A(AU_1U_2 + U_1B_2V_2 + B_1V_1U_2) + B_1B_2V_1V_2 = 1$. D'après le théorème 3.9, le p.g.c.d. D de A et B_1B_2 est un diviseur de 1. Donc $D = 1$, A est premier avec B_1B_2 et la propriété est vraie pour $p = 2$.

Supposons la propriété vraie pour p , avec $p \geq 2$, et soient $A, B_1, \ldots, B_{p+1}$ des polynômes non nuls tels que A soit premier avec B_i pour $1 \leq i \leq p + 1$. D'après l'hypothèse de récurrence, A est premier avec $B_1 \ldots B_p$. Puisque le résultat est vrai pour $p = 2$, A est premier avec $(B_1 \ldots B_p)B_{p+1} = B_1 \ldots B_{p+1}$. On voit donc par récurrence que le théorème est valable pour tout $p \geq 2$. ♣

Corollaire 3.5.6 *Soient* $P_1, ..., P_k$ *des polynômes premiers entre eux deux à deux. Si* $U \in K[x]$ *est divisible par* P_j *pour* $1 \leq j \leq k$, *alors* U *est divisible par le produit* $P_1...P_k$.

Démonstration : Si $k = 1$, il n'y a rien à démontrer. Supposons maintenant que le résultat est vrai pour $k - 1$, avec $k \geq 2$. Soient $P_1, ..., P_k$ des polynômes premiers entre eux deux à deux, et supposons que $U \in K[x]$ est divisible par P_j pour $1 \leq j \leq k$. Alors U est divisible par le produit $P_1...P_{k-1}$, donc U s'écrit sous la forme $= P_1...P_{k-1}V$, avec $P \in K[x]$. Il résulte du théorème ci-dessus que P_k est premier avec $P_1...P_{k-1}$, et on déduit alors du théorème de Gauss que P_k divise V. Donc U est divisible par le produit $P_1...P_k$, et la propriété est vraie pour k. Le résultat est donc démontré par récurrence. ♣

3.6 Le théorème chinois pour les polynômes

Soit $P \in K[x]$. On dira que deux polynômes A et B sont *congrus modulo* P, et on écrira $A \equiv B \quad (P)$, quand $A - B$ est divisible par P. On vérifie facilement que si $A_1 \equiv A_2 \quad (P)$ et si $B_1 \equiv B_2 \quad (P)$ alors $A_1 + B_1 \equiv A_2 + B_2 \quad (P)$ et $A_1 B_1 \equiv A_2 B_2 \quad (P)$. On va maintenant donner une version du "théorème chinois" valable pour les polynômes.

Théorème 3.6.1 *(théorème chinois) Soient $P_1, \ldots, P_k$ des polynômes non nuls tels que P_i et P_j soient premiers entre eux pour $i \neq j$. Alors pour toute famille $(Q_1, \ldots, Q_k)$ d'éléments de $K[x]$ le système d'équations de congruence*

$P \equiv Q_1 \quad (P_1)$

$\ldots$

$P \equiv Q_k \quad (P_k)$

possède des solutions dans $K[x]$. De plus si $B \in K[x]$ est solution, la solution générale du système est donnée par la formule

$$P = B + UP_1 ... P_k,$$

où $U \in K[x]$ est un polynôme quelconque.

Démonstration : Soit $B \in K[x]$ une solution du système. Il est clair que si $P = UP_1 ... P_k$, avec $U \in K[x]$, alors $P \equiv B \equiv Q_j \quad (P_j)$ pour $1 \leq j \leq k$, donc P est solution du système. Réciproquement si P est solution du système on a $P - B \equiv Q_j - Q_j \equiv \quad (P_j)$, donc $P - B$ est divisible par P_j pour $1 \leq j \leq k$. Il résulte alors du corollaire ci-dessus que $P - B$ est divisible par le produit $P_1 ... P_k$, et il existe $U \in K[x]$ tel que $P = B + UP_1 ... P_k$.

Il reste à établir l'existence d'une solution. Le résultat est évident si $k = 1$, car il suffit alors de prendre $P = Q_1$. Supposons que le résultat est vrai pour k, avec $k \geq 1$, et considérons une famille $P_1, \ldots, P_{k+1}$ de polynômes non nuls tels que P_i et P_j soient premiers entre eux pour $i \neq j$ ainsi qu'une famille $Q_1, \ldots, Q_{k+1}$ de polynômes quelconques.

D'après l'hypothèse de récurrence, il existe $A \in K[x]$ tel que $A \equiv Q_i \quad (P_i)$ pour $1 \leq i \leq k$. On a alors $A + P_1 \ldots P_k Q \equiv Q_i \quad (P_i)$ pour $1 \leq i \leq k$ si $Q \in K[x]$. Comme P_{k+1} est premier avec P_i pour $1 \leq i \leq k$, il résulte du théorème précédent que P_{k+1} est premier avec le produit $P_1 \ldots P_k$. Il existe donc deux polynômes U et V tels que $P_1 \ldots P_k U + P_{k+1} V = 1$. Posons $P = A - P_1 \ldots P_k U(A - Q_{k+1})$. On a $P_1 \ldots P_k U(A - Q_{k+1}) + P_{k+1} V(A - Q_{k+1}) = A - Q_{k+1}$, donc $P - Q_{k+1} = P_{k+1} V(A - Q_{k+1})$ est divisible par P_{k+1}, et par conséquent $P \equiv Q_i \quad (P_i)$ pour $1 \leq i \leq k + 1$. Le théorème est donc démontré par récurrence. ♣

Notons que cette démonstration fournit une méthode effective pour résoudre ce type d'équations de congruence, en se ramenant à chaque étape à des équations du type équation de Bezout. Nous traitons ci dessous un exemple simple.

Exemple 3.6.2 . *Soient $\lambda_1 \in \mathbf{C}$, $\lambda_2 \in \mathbf{C}$, avec $\lambda_1 \neq \lambda_2$. Trouver $P \in \mathbf{C}[x]$ tel que $P - \lambda_1$ soit divisible par $(x - \lambda_1)^2$ et tel que $P - \lambda_2$ soit divisible par $x - \lambda_2$.*

Comme $\lambda_1 \neq \lambda_2$, $x - \lambda_1$ est premier avec $x - \lambda_2$. Il résulte du théorème 3.16 que $x - \lambda_1$ est premier avec $(x - \lambda_2)^2$, et il résulte alors du théorème chinois qu'il existe bien un polynôme P vérifiant les conditions ci-dessus. On va chercher un polynôme de la forme $P = \lambda_1 + Q(x - \lambda_1)^2$. Un tel polynôme vérifie automatiquement $P \equiv \lambda_1 \quad (x - \lambda_1)^2$. On va chercher à déterminer Q de facon que $P - \lambda_2$ soit divisible par λ_2. On a $P - \lambda_2 = \lambda_1 - \lambda_2 + Q(x - \lambda_1)^2$.

On peut ici éviter le recours à l'équation de Bezout, car on sait que $P - \lambda_2$ est divisible par $x - \lambda_2$ si et seulement si λ_2 est une racine de $P - \lambda_2$. On a $(P - \lambda_2)(\lambda_2) = \lambda_1 - \lambda_2 + Q(\lambda_2)(\lambda_2 - \lambda_1)^2$. Donc λ_2 est racine de $P - \lambda_2$ si et seulement si $\lambda_1 - \lambda_2 + Q(\lambda_2)(\lambda_2 - \lambda_1)^2 = 0 \Longleftrightarrow Q(\lambda_2) = \frac{1}{\lambda_2 - \lambda_1}$. Le polynôme constant $Q = \frac{1}{\lambda_2 - \lambda_1}$ convient, et le polynôme $P = \lambda_1 + \frac{1}{\lambda_2 - \lambda_1}(x - \lambda_1)^2$ vérifie les conditions voulues.

3.7 La notion de p.p.c.m

On va maintenant introduire la notion de p.p.c.m.(plus petit commun multiple).

Théorème 3.7.1 *Soit $(P_1, \ldots, P_k)$ une famille finie de polynomes non nuls. Il existe alors un unique polynôme unitaire M, appellé le p.p.c.m. de la famille $(P_1, \ldots, P_k)$, possédant les deux propriétés suivantes*

(i) M est un multiple de P_i pour $1 \leq i \leq k$

(ii) Si Q est un multiple de P_i pour $1 \leq i \leq k$, alors Q est un multiple de M.

Démonstration : L'ensemble des multiples de P_i est égal à $P_i K[x]$. Donc l'ensemble des multiples communs à P_1 , P_2, ...et P_k est l'ensemble $I := \cap_{1 \leq i \leq k} P_i K[x]$. On vérifie immédiatement que I est un idéal de $K[x]$, et $I \neq \{0\}$ puisque $P_1 \ldots P_k \in I$. Donc il existe un polynôme unitaire $M \in K[x]$ tel que $I = MK[x]$. Par construction M vérifie (ii), et M vérifie (i) puisque $M \in I$. Si M_1 est un autre polynôme unitaire vérifiant (i) et (ii) alors M_1 divise M et M divise M_1, ce qui entraine comme on l'a déjà vu que $M = M_1$. ♣

Il est clair que si M_i désigne le p.p.c.m. de la famille $P_1, \ldots, P_i$, alors le p.p.c.m. de la famille $P_1, \ldots, P_{i+1}$ est égal au p.p.c.m. de M_i et P_{i+1}, donc les calculs de p.p.c.m. se ramènent à des calculs de p.p.c.m. de deux polynômes. Ceci peut se faire en utilisant le résultat suivant.

Théorème 3.7.2 *Soient P et Q deux polynômes unitaires, soit D leur p.g.c.d. et soit M leur p.p.c.m. On a $PQ = DM$.*

Démonstration : On a $P = DA$ et $Q = DB$ où A et B sont des polynômes premiers entre eux. Il est clair que DAB est un multiple de P et Q. Soit maintenant $U \in K[x]$ un multiple de P et Q. Il existe deux polynômes V et W tels que $U = DAV = DBW$. Donc $AV = BW$, et A divise BW. Comme A est premier avec B, il résulte du théorème de Gauss que A divise W. Il existe donc un

polynôme S tel que $U = DABS$, et U est un multiple de DAB. Comme DAB est unitaire, $DAB = M$, et $PQ = DM$. ♣

Exemple 3.7.3 *Calcul du p.p.c.m. de* $x^3 + 1$ *et* $x^4 + x^2 + 3x + 1$.

On a vu que le p.g.c.d. de ces deux polynômes est égal à $x + 1$. Comme $x^3 + 1 = (x + 1)(x^2 - x + 1)$, le p.p.c.m. de $x^3 + 1$ et $x^4 + x^2 + 3x + 1$ est égal à $(x^2 - x + 1)(x^4 + x^2 + 3x + 1) = x^6 - x^5 + 2x^4 + 2x^3 - x^2 + 2x + 1$.

On a également le résultat suivant, qui est une simple reformulation du corollaire 3.5.6

Proposition 3.7.4 *Soient* $P_1, \ldots, P_k$ *des polynômes non nuls premiers entre eux deux à deux. Alors le p.p.c.m. de la famille* $(P_1, \ldots, P_k)$ *est égal au produit* $P_1 \ldots P_k$.

3.8 Polynômes irréductibles

On va maintenant introduire la notion de *polynôme irréductible,* qui est l'analogue pour les polynômes de la notion de *nombre premier.*

Definition 3.8.1 *Soit* K *un corps.On dit que* $P \in K[x]$ *est irréductible si* P *est non constant et si les seuls diviseurs de* P *dans* $K[x]$ *sont soit constants, soit de la forme* aP *avec* $a \in K$, $a \neq 0$.

Contrairement à la notion de p.g.c.d. (le p.g.c.d. d'une famille de polynômes à coefficients dans K ne change pas si on remplace le corps K par un corps plus grand) la notion de polynôme irréductible dépend du corps considéré,comme le montrent les exemples très simples suivants.

Exemple 3.8.2 *Le polynôme* $x^2 - 5$ *est irréductible dans* $\mathbf{Q}[x]$, *mais pas dans* $\mathbf{R}[x]$. *Le polynôme* $x^2 + 1$ *est irréductible dans* $\mathbf{R}[x]$, *mais pas dans* $\mathbf{C}[x]$.

En effet un polynôme non irréductible de degré 2 doit posséder un diviseur de degré 1, qui est de la forme $ax+b$, avec $a \neq 0$, et admet $-\frac{b}{a}$ pour racine. Comme $\sqrt{5}$ est irrationnel (voir l'exercice 4 du Chapitre 2), $x^2 - 5$ est irréductible dans $\mathbf{Q}[x]$. Par contre $x^2 - 5 = (x - \sqrt{5})(x + \sqrt{5})$ n'est pas irréductible dans $\mathbf{R}[x]$. De même $x^2 + 1$ est irréductible dans $\mathbf{R}[x]$, mais $x^2 + 1 = (x + i)(x - i)$ n'est pas irréductible dans $\mathbf{C}[x]$.

On a un analogue de la décomposition des nombres entiers en produit de facteurs premiers

Théorème 3.8.3 *Soit* K *un corps. Pour tout polynôme non constant* $P \in K[x]$ *il existe un élément non nul* a *de* K *,une famille* $P_1, \ldots, P_k$ *de polynômes unitaires irréductibles distincts et une famille* $n_1, \ldots, n_k$ *d'entiers positifs tels que* $P = aP_1^{n_1} \ldots P_k^{n_k}$. *De plus cette décomposition est unique à l'ordre des facteurs près.*

Démonstration : Comme tout polynôme $Q \neq 0$ s'écrit de manière unique sous la forme $Q = aP$ avec $a \in K$ et P unitaire, il suffit de montrer que tout polynôme unitaire P de degé au moins 1 possède une décomposition en produit de polynômes unitaires irréductibles. C'est évident si $d^\circ(P) = 1$ car dans ce cas P est irréductible. Supposons cette propriété vraie pour tous les polynômes unitaires tels que $1 \leq d^\circ(P) \leq k$, avec $k \geq 1$, et soit P un polynôme unitaire de degré $k+1$. Si P est irréductible, on a la décomposition triviale $P = P$. Si P n'est pas irréductible il existe deux polynômes non constants Q et R tels que $P = QR$. Comme le produit des coefficients des termes de plus haut degré de Q et R est égal à 1 on peut en multipliant Q et en divisant R par un élément non nul de K convenable se ramener au cas où Q et R sont unitaires. On a $d^\circ(Q) < k+1$ et $d^\circ(R) < k+1$, et d'après l'hypothèse de récurrence on peut décomposer Q et R en produit de polynômes unitaires irréductible. Donc $P = QR$ se décompose en produit de polynômes irréductibles, et l'existence de la décomposition cherchée est établie par récurrence pour tout polynôme non constant P. Pour démontrer l'unicité à l'ordre près des facteurs de la décomposition du théorème on peut également se limiter au cas où P est unitaire. Notons que si deux polynômes irréductibles Q et R ne sont pas premiers entre eux alors il existe un élément non nul a de K tel que $Q = aR$, ce qui implique que $Q = R$ si Q et R sont unitaires. L'unicité de la décomposition est triviale si $d^\circ(P) = 1$. Supposons que la décomposition soit unique à l'ordre près des facteurs pour tout polynôme unitaire P tel que $1 \leq d^\circ(P) \leq k$, avec $k \geq 1$, soit P un polynôme unitaire de degré $k+1$, et soient $P = P_1^{n_1} \ldots P_k^{n_k} = Q_1^{m_1} \ldots Q_{k'}^{m_{k'}}$ deux décompositions de P en produit de puissances de polynômes unitaires irréductibles distincts. Si $P_1 \neq Q_i$ pour $1 \leq i \leq k'$ alors d'après le théorème 3.5.5 P_1 serait premier avec P, ce qui contredit le fait que P_1 divise P. Quitte à renuméroter les polynômes $Q_1, \ldots, Q_{k'}$ on peut alors supposer que $P_1 = Q_1$. Si $n_1 > m_1$ alors en simplifiant par $P_1^{m_1}$ dans les deux décompositions on obtiendrait que $P_1 = Q_i$ avec $i > 1$, ce qui est absurde. Le même argument montre que l'on ne peut avoir $m_1 > n_1$. Donc $n_1 = m_1$. Si $k = 1$ on voit en simplifiant par $P_1^{n_1}$ dans les deux décompositions que $k' = 1$. De même $k = 1$ si $k' = 1$. Dans ce cas l'unicité de la décomposition de P est établie. Supposons maintenant que $\inf(k, k') > 1$. On a $P_2^{n_2} \ldots P_k^{n_k} = Q_2^{m_2} \ldots Q_{k'}^{m_{k'}}$ et d'après l'hypothèse de récurrence on a $k = k'$ et on peut renuméroter $Q_2, \ldots, Q_k$ de sorte que $Q_i = P_i$ et $n_i = m_i$ pour $2 \leq i \leq k$. L'unicité à l'ordre près des facteurs de la décomposition donnée par le théorème est donc établie par récurrence. ♣

Le "**Théorème de d'Alembert**" (démontré en fait par Gauss) montre que tout polynôme non constant à coefficients complexes possède au moins une racine dans $\mathbf{C}$. On en déduit immédiatement que les seuls polynômes irréductibles dans $\mathbf{C}$ sont les polynômes de degré 1. Soit maintenant P un polynôme irréductible dans $\mathbf{R}[x]$, et soit λ une racine complexe de P. Si $\lambda \in \mathbf{R}$, P est divisible par $x - \lambda$ dans $\mathbf{R}[x]$, et on a $P = a(x - \lambda)$ avec $a \in \mathbf{C}$, $a \neq 0$. Si λ n'est pas réel alors $P(\bar{\lambda}) = \overline{P(\lambda)} = 0$, donc P est aussi divisible par $(x - \bar{\lambda})$ dans $\mathbf{C}[x]$. Mais $(x - \lambda)$ et $(x - \bar{\lambda})$ sont premiers entre eux dans $\mathbf{C}[x]$ donc leur p.p.c.m. est

$(x-\lambda)(x-\bar{\lambda}) = x^2+bx+c$, avec $b = -2Re(\lambda)$ et $c = \lambda\bar{\lambda} = |\lambda|^2$. Comme la division euclidienne donne les mêmes résultats dans $\mathbf{R}[x]$ et $\mathbf{C}[x]$ pour les polynômes à coefficients réels, on voit que P est divisible par x^2+bx+c dans $\mathbf{R}[x]$. On a donc $P = a(x^2+bx+c)$ avec a, b, c réels, $a \neq 0, \Delta = b^2-4c = 4Re(\lambda)^2-|\lambda|^2 < 0$. Réciproquement il est clair que tout polynôme de la forme ci dessus est irréductible dans $\mathbf{R}[x]$. Le théorème précédent prend alors la forme concrète suivante pour les polynômes à coefficients réels ou complexes.

Théorème 3.8.4 *(i) Pour tout polynôme non constant $P \in \mathbf{C}[x]$ il existe une famille $(\lambda_1, \ldots, \lambda_k)$ de nombres complexes distincts, une famille $(n_1, \ldots, n_k)$ d'entiers positifs et un complexe $a \neq 0$ tels que*

$P = a(x-\lambda_1)^{n_1} \ldots (x-\lambda_k)^{n_k}$.

Cette décomposition est unique à l'ordre près des facteurs .

(ii) Pour tout polynôme non constant $P \in \mathbf{R}[x]$ il existe une famille $(\lambda_1, \ldots, \lambda_k)$ de nombres réels distincts, une famille $((b_1, c_1) \ldots (b_{k'}, c_{k'}))$ de couples distincts de réels, avec $b_i^2 - 4c_i^2 < 0$ pour $1 \leq i \leq k'$, deux familles $(n_1, \ldots, n_k)$ et $(m_1, \ldots, m_{k'})$ d'entiers positifs et un réel $a \neq 0$ tels que
$P = a(x-\lambda_1)^{n_1} \ldots (x-\lambda_k)^{n_k}(x^2+b_1x+c_1)^{m_1} \ldots (x^2+b_{k'}x+c_{k'})^{m_{k'}}$.

L'une des familles $(\lambda_1, \ldots, \lambda_k)$ ou $((b_1, c_1) \ldots (b_{k'}, c_{k'}))$ peut être vide, et cette décomposition est unique à l'ordre près des facteurs .

Exemple 3.8.5 *La décomposition de x^3+1 dans $\mathbf{R}[x]$ est $x^3+1 = (x+1)(x^2-x+1)$. La décomposition de x^3+1 dans $\mathbf{C}[x]$ est $x^3+1 = (x+1)(x-\frac{1}{2}+i\frac{\sqrt{3}}{2})(x-\frac{1}{2}-i\frac{\sqrt{3}}{2})$.*

En effet x^2-x+1 n'a pas de racines réelles, et ses racines complexes sont $\frac{1}{2}+i\frac{\sqrt{3}}{2}$ et $\frac{1}{2}-i\frac{\sqrt{3}}{2}$.

De même que dans le cas des entiers,on peut utiliser la décomposition en produit de polynômes irréductibles pour calculer le p.g.c.d. et le p.p.c.m. d'une famille finie de polynômes non constants (les polynômes constants non nuls n'interviennent pas dans le calcul du p.p.c.m. et le p.g.c.d. d'une famille de polynômes contenant un polynôme constant est égal à 1). On vérifie que *le p.g.c.d. d'une famille $(P_1, \ldots, P_k)$ de polynômes non constants s'obtient en faisant le produit des diviseurs unitaires irréductibles communs à $P_1, \ldots, P_k$, affectés du plus petits des exposants apparraissant dans les décompositions de ces polynômes.*

D'autre part *le p.p.c.m. d'une famille $(P_1, \ldots, P_k)$ de polynômes non constants s'obtient en faisant le produit de tous les diviseurs unitaires irréductibles de $P_1, \ldots,$ ou P_k, affectés du plus grand des exposants apparaissant dans les décompositions de ces polynômes.*

Exemple 3.8.6 *Calcul du p.g.c.d. et du p.p.c.m. de x^3+1 et $(x^4-1)^2$.*

On utilise les décompositions dans $R[x]$. On a vu que la décomposition de x^3+1 est $x^3+1 = (x+1)(x^2-x+1)$, et la décomposition de $(x^4-1)^2$ est $(x^4-1)^2 = (x+1)^2(x-1)^2(x^2+1)^2$. Le seul diviseur unitaire irréductible commun est $(x+1)$, affecté de l'exposant 1 pour le premier polynôme et de

l'exposant 2 pour le second. Le p.g.c.d. de x^3+1 et $(x^4-1)^2$ est donc égal à $x+1$. Leur p.p.c.m. est égal à $(x+1)^2(x^2-x+1)(x-1)^2(x^2+1)^2 = x^{10}-x^9+x^8-2x^6+2x^5-2x^4+x^2-x+1$.

Dans le cas des entiers on est confronté à des problèmes de temps de calcul pour décomposer de grands nombres en produit de facteurs premiers. En ce qui concerne les polynômes on sait depuis l'Antiquité trouver les racines d'un polynôme de degré 2. Il a fallu attendre la deuxième moitié du XV^e siècle (formules de Cardan et Tartaglia) pour arriver à résoudre les équations de degré 3 ,puis assez rapidement celles de degré 4 (ivrognes et paillards, les mathématiciens italiens de la Renaissance gardaient secrètes leurs formules et s'affrontaient moyennant espèces sonnantes et trébuchantes dans des joutes publiques où il s'agissait devant des tiffosi passionnés de résoudre des equations concrètes de degré 3 ou 4). C'est d'ailleurs à cette occasion qu'apparait pour la première fois le mystérieux "nombre imaginaire" i, longtemps tenu en suspicion par l'Eglise, tel que $i^2=-1$. C'est seulement vers 1830 qu'Evariste Galois a démontré [1] qu'*il est impossible de trouver des formules algébriques donnant les racines des polynômes de degré supérieur ou égal à* 5, en inventant au passage la théorie des groupes (ce mathématicien de génie était malheureusement myope comme une taupe. Il est mort à vingt ans en se battant en duel au pistolet pour les beaux yeux d'une jeune femme probablement soudoyée par les sbires de Louis Philippe pour pousser les jeunes révolutionnaires républicains à s'entretuer, en cette période troublée où les polytechniciens n'avaient pas hésité à utiliser les canons de leur prestigieuse Ecole pour pilonner les troupes royales). Le manuscript laissé par Galois ne sera compris que des années plus tard.

On voit donc qu'il est en général impossible d'expliciter la décomposition exacte en produit de polynômes irréductibles d'un polynôme de degré ≥ 5. Même dans le cas du polynôme $x^4+x^2+3x+1=(x+1)(x^3-x^2+2x+1)$ les formules donnant les racines d'un polynôme de degré 3 mènent à des calculs compliqués, que nous donnerons plus loin en exercice.

3.9 Formule de Taylor pour les polynômes

On définit la *dérivée formelle* d'un polynôme $P=a_0+a_1x+\ldots+a_nx^n \in \mathbf{C}[x]$ par la formule

$$P' = a_1 + 2a_2x + \ldots + na_nx^{n-1}. \quad (3.6)$$

On définit alors par récurrence les dérivées successives $P^{(2)},\ldots,P^{(n)}$. Notons que $P^{(k)}=0$ si $k>d^\circ(P)$.

On a le résultat suivant (évidemment aussi valable pour les polynômes à coefficients réels).

[1] ce résultat a été obtenu indépendamment à la même époque par le mathématicien norvégien Abel, mort de maladie à l'âge de vingt-sept ans

Théorème 3.9.1 *(Formule de Taylor pour les polynômes) Soit $P \in \mathbf{C}[x]$, et soit $a \in \mathbf{C}$. Si $n \geq d^\circ(P)$, on a*

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

Démonstration : Soit $p \geq 1$, et posons $U = x^p$. On a $U^{(k)}(a) = p(p-1)\ldots(p-k+1)a^{p-k} = (k!)C_p^k a^{p-k}$ pour $1 \leq k \leq p$, $U^{(k)}(a) = 0$ pour $k > p$. D'après la formule du binôme (formule 1.7) on a pour $n \geq p$

$$U = (x-a+a)^p = a^p + \sum_{1\leq k\leq p} C_p^k a^{p-k}(x-a)^k = U(a) + \sum_{1\leq k\leq n} \frac{U^{(k)}(a)}{k!}(x-a)^k.$$

La formule est évidente pour les polynômes constants. Supposons la formule vraie pour les polynômes de degré $\leq m$, avec $m \geq 0$, et soit $P \in \mathbf{C}[x]$ un polynôme de degré $m+1$. On a $P = Q + bU$, avec $d^\circ(Q) \leq m, b \in \mathbf{C}, U = x^{m+1}$. Il est clair que $P^{(k)}(a) = Q^{(k)}(a) + bU^{(k)}(a)$ pour $k \geq 1$. D'après l'hypothèse de récurrence on a , pour $n \geq m+1$

$$\begin{aligned} P &= Q(a) + \sum_{1\leq k\leq n} \frac{Q^{(k)}(a)}{k!}(x-a)^k + bU(a) + b\sum_{1\leq k\leq n} \frac{U^{(k)}(a)}{k!}(x-a)^k \\ &= P(a) + \sum_{1\leq k\leq n} \frac{P^{(k)}(a)}{k!}(x-a)^k, \end{aligned}$$

et la formule est démontrée par récurrence. ♣

On définit l'*ordre de multiplicité* d'une racine a d'un polynôme non nul comme étant le plus grand entier k tel que $(x-a)^k$ divise P. On déduit de la formule de Taylor le résultat suivant.

Corollaire 3.9.2 *Soit $P \in \mathbf{C}[x]$ un polynôme non nul, et soit $a \in \mathbf{C}$ une racine de P. Alors l'ordre de multiplicité de a est égal au plus petit entier positif k tel que $P^{(k)}(a) \neq 0$.*

3.10 Utilisation de MUPAD pour des calculs concernant les polynômes

On peut utiliser MUPAD pour effectuer des divisions euclidiennes avec la commande **divide.**

Exemple 3.10.1 *Effectuer la division euclidienne de $x^{17} + 134x^{16} - 187x^{15} + 34x^{14} + 14534x^{13} - 655x^{12} + 476x^{11} - 4321x^{10} + 22346x^9 + 76584x^8 - 178596x^7 + 6789543x^6 + 453x^5 - 786x^4 + 237x^3 - 3459x^2 + 567x - 112678$ par $1277x^{10} + 98746x^9 + 55678x^8 - 596x^7 + 95437x^6 + 23451x^5 - 987x^4 + 5468x^3 - 6789x^2 + 34708x + 985132$*

```
divide(x^17
+134*x^16 - 187*x^15 + 34*x^14 +14534*x^13 - 655*x^12
+ 476*x^11 - 4321*x^10 + 22346*x^9 +76584*x^8 - 178596*x^7
+ 6789543*x^6 + 453*x^5 - 786*x^4 +237*x^3 -3459*x^2 +
567*x - 112678 , 1277*x^10 + 98746*x^9 +55678*x^8 - 596*x^7
+ 95437*x^6 + 23451*x^5 - 987*x^4 +5468*x^3 -6789*x^2 +
34708*x +985132);

                            2
708445893469244681714103 6 x    69442091132329024048213641522 6 x
---------------------------- - ------------------------------- -
    4336560239433910489             5537787425757103694453

                          3                    4               5          6
   72275707124284784293 x    737742125702560 x    7522492641 x    72372 x
   ---------------------- + ------------------ - ------------ + --------
      3395896820230157         2659277071441       2082440933     1630729

       7
      x
   + ---- + 6806736014852249451282106367947862 2/7071754542691821417816481,
     1277

                                              2
   48150644708984649911116184804625538298 7 x
   ------------------------------------------ -
           707175454269182141781648 1

   14888910104609687430899377053907979421 85 x
   ------------------------------------------ -
           707175454269182141781648 1

                                              3
   37846534779061723870625979805360704812 1 x
   ------------------------------------------ +
           707175454269182141781648 1

                                             4
   72113096301866799046921108380730157632 x
   ------------------------------------------ -
           707175454269182141781648 1
```

```
                                                 5
   1597187145888966771742513525268289844732 x
   ------------------------------------------ -
            707175454269182141781648 1

                                                 6
   6475336590611463843749200924514398573029 x
   ------------------------------------------ +
            707175454269182141781648 1

                                                7
   1249282541892634266927887386403725723 30 x
   ------------------------------------------ -
           707175454269182141781648 1

                                                 8
   3791482032010763103884484268259257245489 x
   ------------------------------------------ -
            707175454269182141781648 1

                                                 9
   6671984454903408998971321433720667667959 x
   ------------------------------------------ -
            707175454269182141781648 1

   6705533463863109322276586915840885929422 2/707175454269182141781648 1
```

Le quotient cherché est donc

$$\frac{6806736014852249451282106367947862 2}{707175454269182141781648 1}-\frac{6944209113232902404821364152 26}{5537787425757103694453}x+\frac{7084458934692446817141036}{4336560239433910489}x^2$$
$$-\frac{72275707124284784293}{3395896820230157}x^3+\frac{737742125702560}{2659277071441}x^4-\frac{7522492641}{2082440933}x^5+\frac{72372}{1630729}x^6+\frac{x^7}{1277},$$

et le reste est

$$-\frac{6705533463863109322276586915840885929422 2}{707175454269182141781648 1}-\frac{1488891010460968743089937705390797942185}{707175454269182141781648 1}x+$$
$$\frac{4815064470898464991111618480462553829 87}{707175454269182141781648 1}x^2-\frac{3784653477906172387062597980536070481 21}{707175454269182141781648 1}x^3+$$
$$\frac{7211309630186679904692110838073015763 2}{707175454269182141781648 1}x^4-\frac{1597187145888966771742513525268289844732}{707175454269182141781648 1}x^5-$$
$$\frac{6475336590611463843749200924514398573029}{707175454269182141781648 1}x^6+\frac{1249282541892634266927887386403725723 30}{707175454269182141781648 1}x^7-$$
$$\frac{3791482032010763103884484268259257245489}{707175454269182141781648 1}x^8-\frac{6671984454903408998971321433720667667959}{707175454269182141781648 1}x^9.$$

On peut également utiliser MUPAD pour calculer le p.g.c.d. et le p.p.c.m de deux polynômes avec les commandes **gcd** et **lcm**.

Exemple 3.10.2 *Calculer le p.g.c.d. et le p.p.c.m. de* $x^{12}+8x^2-29x+20$ *et* $x^{10}-8x^9-9x^8+32x^2+15x-17$.

```
gcd(x^12 +  8*x^2 + 29*x + 20,x^10 -8*x^9 -9*x^8 +32*x^2
  +15*x -17 );
```

```
                                  x + 1
```

```
lcm(x^12 +  8*x^2 + 29*x + 20,x^10 -8*x^9 -9*x^8 +32*x^2
  +15*x -17 );
```

```
            2        3        8        9       10      11       12
147 x + 792 x  + 256 x  - 180 x  - 241 x  - 43 x   + 8 x   - 17 x   +

       13      20    21
   32 x   - 9 x   + x   - 340
```

Le p.g.c.d. de ces deux polynômes est donc $x+1$, et leur p.p.c.m. est $-340+147x+792x^2+256x^3-180x^8-241x^9-43x^{10}+8x^{11}-17x^{12}+32x^{13}-9x^{20}+x^{21}$

On peut également calculer des solutions de l'équation de Bezout en utilisant la commande **gcdex**.

Exemple 3.10.3 *Trouver deux polynômes* U *et* V *tels que* $(x^{12}+8x^2-29^x+20)U+(x^{10}-8x^9-9x^8+32x^2+15x-17)V=1$.

```
   gcdex(x^12 +  8*x^2 + 29*x + 20,x^10 -8*x^9 -9*x^8 +32*x^2
  +15*x -17 );
```

```
                              2
       10226591066413994678 x    54536657733040647455 x
x + 1, ---------------------- - ---------------------- +
       646929218537545452O823    646929218537545452O823

                          3                          4
   24917896984808139752 x    37262591054937067267 x
   ---------------------- - ---------------------- +
   646929218537545452O823    646929218537545452O823

                          5                          6
```

```
2540370416875824523 x     17269057868666799603 x
---------------------- + ---------------------- -
64692921853754545208 23    64692921853754545208 23

                       7                        8
24849034822763139727 x     2549565419413859057 x
---------------------- + ---------------------- +
64692921853754545208 23    64692921853754545208 23

                                                  9857396757795882874 x
28803102298140148165 4/64692921853754545208 23, ---------------------- -
                                                  64692921853754545208 23

                       2                         3
15228966176530539013 x     26214001315256095755 x
---------------------- + ---------------------- -
64692921853754545208 23    64692921853754545208 23

                       4                         5                         6
20551163487134792 47 x     13201917364529686 36 x     20814454010360293 91 x
---------------------- - ---------------------- + ----------------------
64692921853754545208 23    64692921853754545208 23    64692921853754545208 23

                       7                         8
  7717935600074373 32 x      4595054903773392948 x
+ ---------------------- - ---------------------- +
  64692921853754545208 23    64692921853754545208 23

                       9                         10
44525114674522671 271 x    2549565419413859057 x
---------------------- - ---------------------- -
64692921853754545208 23    64692921853754545208 23

41686572102789699279/64692921853754545208 23
```

On peut donc prendre $U = \frac{2880310229814014816 54}{64692921853754545208 23} - \frac{5453656577330406474 55}{64692921853754545208 23} x + \frac{1022659106641399467 8}{64692921853754545208 23} x^2 + \frac{2491789698480813975 2}{64692921853754545208 23} x^3 - \frac{3726259105493706726 7}{64692921853754545208 23} x^4 + \frac{2540370416875824523}{64692921853754545208 23} x^5 + \frac{1726905786866679960 3}{64692921853754545208 23} x^6 - \frac{2484903482276313972 7}{64692921853754545208 23} x^7 + \frac{2549565419413859057}{64692921853754545208 23} x^8$ et $V = -\frac{4168657210278969927 9}{64692921853754545208 23} + \frac{9857396757795882874}{64692921853754545208 23} x - \frac{1522896617653053901 3}{64692921853754545208 23} x^2 + \frac{2621400131525609575 5}{64692921853754545208 23} x^3 - \frac{2055116348713479247}{64692921853754545208 23} x^4 - \frac{1320191736452968636}{64692921853754545208 23} x^5 + \frac{2081445401036029391}{64692921853754545208 23} x^6 + \frac{7717935600074373 32}{64692921853754545208 23} x^7 - \frac{4595054903773392948}{64692921853754545208 23} x^8 + \frac{4452511467452267271}{64692921853754545208 23} x^9 - \frac{2549565419413859057}{64692921853754545208 23} x^{10}$

On peut évidemment calculer $P(\lambda)$ pour $P \in \mathbf{C}[x], \lambda \in \mathbf{C}$ ou développer un produit de polynômes, en utilisant les commandes **evalp** et **expand**

Exemple 3.10.4 *Développer* $P = (x-2)^7(x+1)^9$ *et calculer* $P(5+2i)$.

```
    expand((x- 2)^7*(x+1)^9);
```

```
      4                  2         3         5         6         7         8
2072 x  - 704 x - 1248 x  - 112 x  + 1596 x  - 1274 x  - 1709 x  + 369 x  +

        9       10        11        12        13       14       15    16
   916 x  - 56 x   - 294 x   + 14 x   + 56 x   - 6 x   - 5 x   + x   - 128
```

```
unassign(x):
```

```
evalp((x- 2)^7*(x+1)^9, x = 5 +2*I);
```

```
                        95692447744 + 85393809408 I
```

On a donc $P = -128-704x-1248x^2-112x^3+2072x^4+1596x^5-1274x^6-1709x^7+369x^8+916x^9-56x^{10}-294x^{11}+14x^{12}+56x^{13}-6x^{14}-5x^{15}+x^{16}$ et $P(5+2i) = 95692447744+85393809408i$ (notons que pour MUPAD le nombre **5+2i** s'écrit **5+2*I**).

De même que dans le cas des entiers, on peut utiliser la capacité de MUPAD à résoudre des équations de Bezout pour calculer des solutions de systèmes d'équations de congruence (on pourra s'entrainer en résolvant l'exercice 13). Pour la factorisation en produit de polynômes irréductibles , impossible en général à calculer quand le degé dépasse 4, c'est beaucoup moins brillant, et la commande **factor** n'est guère efficace.

Exemple 3.10.5 *Factoriser* x^2-1 , x^3+1 , x^2-7x-5 , x^4+1 *et* x^4+x^2+3x+1.

```
    factor(x^2 -1);
```

```
                          [1, x - 1, 1, x + 1, 1]
```

```
factor(x^3 + 1);
```

```
                                  2
                [1, x + 1, 1, x  - x + 1, 1]
```

```
factor(x^2 -7*x -5);
```

```
                                2
                [1, x  - 7 x - 5, 1]
```

```
factor(x^4 +1);
```

```
                                4
                [1, x  + 1, 1]
```

```
factor(x^4 +x^2 +3*x +1);
```

```
                                    2    3
                [1, x + 1, 1, 2 x - x  + x  + 1, 1]
```

On n'avait pas besoin de MUPAD pour apprendre que $x^2-1=(x=1)(x-1)$ et que $x^3+1=(x+1)(x^2+x+1)$, et il a même refusé de résoudre une équation du second degré pour factoriser le troisième polynôme, en s'arrêtant en route dans la factorisation du dernier.

On a plus de chances de trouver les racines avec la commande **solve**.

Exemple 3.10.6 *Trouver les racines des polynômes* $x^2 - 7x - 5$ *et* $x^4 + x^2 + 3x + 1$.

```
solve(x^2 -7*x -5,x);
```

```
                    {         1/2    1/2       }
                    {       69     69          }
                    { 7/2 - -----, ----- + 7/2 }
                    {         2      2         }
```

```
solve(x^4+1,x);
```

```
             {          1/2         1/2       1/2     1/2 }
             {   (- 4 I)     (- 4 I)       4 I     4 I    }
             { - ----------, ----------, - ------, ------ }
             {       2           2           2       2    }
```

```
solve(x^4 + x^2 +3*x +1,x);
```

```
{ /   1/2         \1/3   /   1/2         \1/3
{ | 29            |      | 29            |
{ | ----- + 43/54 |      | ----- - 43/54 |
{ \   6           /      \   6           /
{ -------------------- - -------------------- -
{          2                      2

              / /   1/2         \1/3   /   1/2         \1/3 \
          1/2 | | 29            |      | 29            |    |
   1/2 I 3    | | ----- - 43/54 |    + | ----- + 43/54 |    | + 1/3,
              \ \   6           /      \   6           /    /

   /   1/2         \1/3   /   1/2         \1/3
   | 29            |      | 29            |
   | ----- + 43/54 |      | ----- - 43/54 |
```

```
\   6          /      \   6          /
------------------- - ------------------- +
         2                     2

           / /   1/2         \1/3   /   1/2         \1/3 \
       1/2 | | 29            |      | 29            |    |
1/2 I 3    | | ----- - 43/54 |    + | ----- + 43/54 |    | + 1/3, -1,
           \ \   6           /      \   6           /    /

                                                    }
                                                    }
/   1/2         \1/3   /   1/2         \1/3       }
| 29            |      | 29            |          }
| ----- - 43/54 |    - | ----- + 43/54 |    + 1/3 }
\   6           /      \   6           /          }
```

On voit donc que les racines de $x^2 - 7x - 5$ sont $\frac{7+\sqrt{69}}{2}$ et $\frac{7-\sqrt{69}}{2}$, ce qui n'est pas une grande surprise.Les racines de $x^4 + 1$, qui peuvent se calculer directement, sont données par MUPAD en utilisant des expressions (interdites aux élèves de terminale) du type $\sqrt{i}$, qu'il faut remplacer par $\frac{\sqrt{2}}{2}(1 + i)$. Par contre Mupad sait calculer les racines de polynômes de degré 3 et 4, et a trouvé les racines du dernier polynôme (pour les deux premières remplacer I par i). Les racines réelles sont -1 et $\left[\frac{\sqrt{2}29}{6} - \frac{43}{54}\right]^{1/3} - \left[\frac{\sqrt{2}9}{6} + \frac{43}{54}\right]^{1/3} + \frac{1}{3}$, et on laisse au lecteur le soin d'ecrire la décomposition en facteurs irréductibles de $x^4 + x^2 + 3x + 1$ dans $\mathbf{R}[x]$.

Il faudra se retourner vers un **logiciel de calcul numérique** pour obtenir des valeurs approchées de racines d'un polynôme de degré supérieur ou égal à 5. Même en degré 3 ou 4 des valeurs approchées précises sont souvent plus utiles que des expressions algébriques compliquées donant les valeurs exactes, mais on peut obtenir directement cette information de MUPAD.

```
 p:=x^4 +x^2 +3*x +1:
S:=solve(p=0,x):
map(S,float);
```

```
{-0.3926467817, -1.0, 0.6963233908 - 1.435949864 I,

   0.6963233908 + 1.435949864 I}
```

3.11 Interpolation de Lagrange et calcul numérique sous Matlab

Les *polynômes d'interpolation de Lagrange* permettent étant données deux familles $u_1, ..., u_{n+1}$ et $v_1, ..., v_{n+1}$ de $n+1$ nombres réels, avec $u_i \neq u_j$ pour $i \neq j$, d'exhiber un polynôme $p \in \mathbf{R}[x]$ de degré inférieur ou égal à n tel que $p(u_i) = v_i$ pour $i \leq n+1$. Ceci est un cas particulier du *théorème chinois* puisque l'équation $p(u_i) = v_i$ équivaut à l'équation $p \equiv v_i \pmod{x - u_i}$, et puisque $x - u_i$ est premier avec $x - u_j$ pour $i \neq j$. En fait on a dans ce cas une formule explicite qui donne la solution de ce problème d'interpolation.

Proposition 3.11.1 *Soient $u = (u_1, ..., u_{n+1})$ et $v = (v_1, ..., v_{n+1})$ deux familles de $n+1$ nombres réels, avec $u_i \neq u_j$ pour $i \neq j$. Posons*

$$p_{u,v} = \sum_{i=1}^{n+1} v_i \frac{\Pi_{\substack{1 \leq j \leq n+1 \\ j \neq i}} (x - u_j)}{\Pi_{\substack{1 \leq j \leq n+1 \\ j \neq i}} (u_i - u_j)}. \tag{3.1}$$

Alors le polynôme $p_{u,v}$, appelé polynôme d'interpolation de Lagrange associé aux familles u et v, est l'unique polynôme p de degré inférieur ou égal à n tel que $p(u_i) = v_i$ pour $1 \leq i \leq n+1$.

Démonstration : Posons $p_i = \frac{\Pi_{\substack{1 \leq j \leq n+1 \\ j \neq i}} (x - u_j)}{\Pi_{\substack{1 \leq j \leq n+1 \\ j \neq i}} (u_i - u_j)}$. Il est clair que $p_i(u_i) = 1$ et $p_i(u_j) = 0$ pour $1 \leq i \leq n, 1 \leq j \leq n, j \neq i$. Donc $p = \sum_{i=1}^{n+1} v_i p_i$ satisfait les conditions voulues. D'autre part si q est un polynôme distinct de p vérifiant $p(u_i) = v_i$ pour $1 \leq i \leq n+1$ alors $q - p$, qui est non nul et possède $n+1$ racines distinctes, est de degré au moins $n+1$. Comme $d^o(p) \leq n$, on a $d^o(q) = d^o(q - p) \geq n+1$, ce qui montre que p est unique. ♣

Ce résultat est important en pratique, car il permet d'obtenir des approximations raisonnables de fonctions dont on connait les valeurs $v = (v_1, ..., v_{n+1})$ en une famille de réels $u = (u_1, ..., u_{n+1})$ donnée. Si la famille comporte $n+1$ points, on peut procéder par interpolation linéaire entre les points de coordonées (u_i, v_i) et (u_{i+1}, v_{i+1}), ou par interpolation quadratique en utilisant les familles de trois points consécutifs, etc... ou en calculant la polynôme d'interpolation de Lagrange associé aux deux familles.

Dans les problèmes rencontrés en pratique on a souvent seulement besoin des valeurs approchées des quantités recherchées. Le logiciel de calcul numérique Matlab est alors en général bien préférable au logiciel de calcul formel Mupad.

Pour saisir un polynôme sous Matlab on rentre entre crochets la liste de ses coefficients, rangés en ordre décroissant par rapport au degré du monôme concerné. Par exemple pour le polynôme $x^6 + 3x^5 + 4x^2 + 7x + 1$, on écrit

```
>> p=[1 3 0 0 4 7 1]
```

```
p =

     1     3     0     0     4     7     1
```

On peut alors obtenir des valeurs approchées des 6 racines de $p = x^6 + 3x^5 + 4x^2 + 7x + 1$.

```
>> roots(p)

ans =

  -2.9314
   0.9121 + 0.9320i
   0.9121 - 0.9320i
  -0.8679 + 0.7249i
  -0.8679 - 0.7249i
  -0.1569
```

On peut également calculer le polynôme $r = pq$, où $q = x^6 + 2x^5 + x^4 + x^3 + 6x^2 + 7x + 4$.

```
>> q=[1 2 1 1 6 7 4]

q =

     1     2     1     1     6     7     4

>> r=conv(p,q)

r =

     1     5     7     4    13    40    44    25    32    71    71    35     4
```

0n a donc $r = x^{12} + 5x^{11} + 7x^{10} + 4x^9 + 13x^8 + 40x^7 + 44x^6 + 25x^5 + 32x^4 + 71x^3 + 71x^2 + 35x + 4$. On peut alors obtenir des valeurs approchées des racines de q et r, et constater sans surprise que l'ensemble des racines de r est la réunion de l'ensemble des racines de p et de l'ensemble des racines de q.

```
>> roots(q)

ans =
```

```
   0.9620 + 1.0992i
   0.9620 - 1.0992i
  -1.3735 + 0.7182i
  -1.3735 - 0.7182i
  -0.5885 + 0.6588i
  -0.5885 - 0.6588i

>> roots(r)

ans =

  -2.9314
   0.9620 + 1.0992i
   0.9620 - 1.0992i
   0.9121 + 0.9320i
   0.9121 - 0.9320i
  -1.3735 + 0.7182i
  -1.3735 - 0.7182i
  -0.8679 + 0.7249i
  -0.8679 - 0.7249i
  -0.5885 + 0.6588i
  -0.5885 - 0.6588i
  -0.1569
```

On va maintenant calculer les coefficients du polynôme d'interpolation de Lagrange p de degré 4 vérifiant les conditions $p(0) = 1 = p(1)$, $p(2) = 0,5$, $p(3) = 6.5$, $p(4) = -1$.

```
>> x=[0 1 2 3 4] ;y =[1 1 0.5 6.5 -1];
p=polyfit(x,y,4)
```

On obtient

```
p =

   -1.1250    7.9167  -16.1250    9.3333    1.0000
```

ce qui signifie que $p \equiv -1,125x^4 + 7,9167x^3 - 16,125x^2 + 9,3333x + 1$.

On va maintenant représenter graphiquement p en calculant ses valeurs en une grille de points espacés de $0,05$ entre 0 et 4 (matlab réalisera alors une interpolation linéaire entre les points de la grille).

```
>> x2=[0:0.05:4];y2=polyval(p,x2);
>> plot(x2,y2)
```

Si on cherche des polynômes de degré inférieur à n pour un problème d'interpolation faisant intervenir $n+1$ données on obtiendra seulement une "interpolation approchée." Par exemple pour $n = 1$ la commande polyfit fait apparaitre la "droite des moindres carrés" associés aux points $M_1 = (x_1, y_1), ..., M_{n+1} = (x_{n+1}, y_{n+1})$, c'est à dire la droite D pour laquelle la somme $\sum_{k=1}^{n+1} dist^2(M_k, D)$ est minimale.

```
x=[0 1 2 3 4]; y = [1 1 0.5 6.5 -1];
q=polyfit(x,y,1)
```

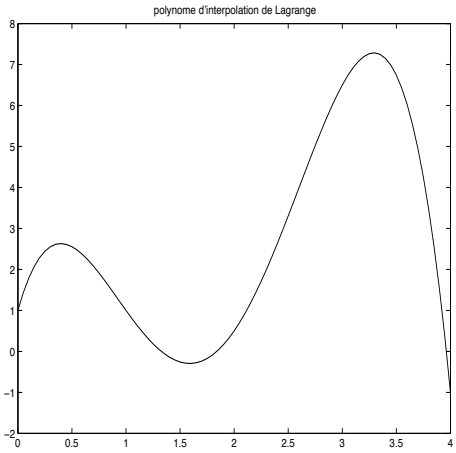
```
q =

    0.1500    1.3000
```

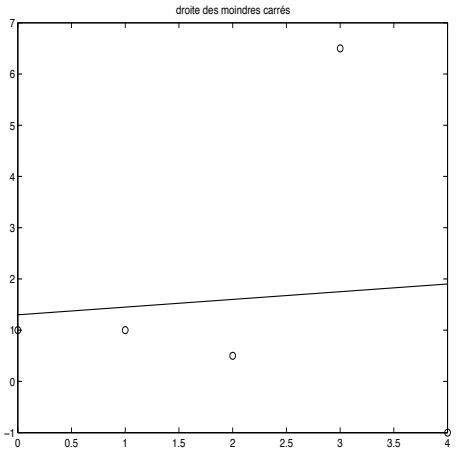
Une expression approchée de l'équation de la droite des moindres carrés est donc $y = 0,15x + 1,3$.

On peut alors obtenir une représentation graphique de la droite en question (il suffit d'une grille de deux points), à laquelle on associe la famille de points donnée au départ.

```
>> x2=[0:4:4];y2=polyval(q,x2);
plot(x2,y2)
```

```
>> hold on
>> plot(x,y,'o')
```


polynome d'interpolation de Lagrange
8
7
6
5
4
3
2
1
0
−1
−2
0
0.5
1
1.5
2
2.5
3
3.5
4


droite des moindres carrés
7
6
5
4
3
2
1
0
−1
0
0.5
1
1.5
2
2.5
3
3.5
4

3.12 Exercices sur le Chapitre 3

exercice 1

Trouver un polynôme P tel que le reste de la division euclidienne de P par $(x-1)$, $(x+1)$ ou $(x+2)$ soit égal à 3.

exercice 2

Effectuer la division euclidienne de $x^4+\frac{3}{2}x^3-\frac{15}{2}x^2+5x-1$ par $2x^3-x+1$

exercice 3

a) Soit $P=a_0+a_1x+...a_nx^n$, avec $a_k \in \mathbf{Z}$ pour $k=0,1,...,n$ et soient p et q deux entiers premiers entre eux tels que p/q soit racine de P . Montrer que p divise a_0 et q divise a_n .

b) Application : Montrer que $6x^3-2x^2+3x-4$ n'a pas de racine dans $\mathbf{Q}$.

exercice 4

Soient K un corps, a et b deux éléments de K et $P \in K[x]$ un polynôme . Déterminer, en fonction de $P(a)$ et $P(b)$, le reste de la division euclidienne de P par $(x-a)(x-b)$ dans chacun des cas suivants :

i) $a \neq b$

ii) $a=b$.

exercice 5

Soient a,b,c dans C . A quelle condition le polynôme $P=x^5+ax^2+b$ est-il divisible par $Q=x^3+x^2+cx+1$?

exercice 6

Pour quelles valeurs de $n\in N$, le polynôme $P=(x+1)^n-x^n-1$, est-il divisible par x^2+x+1 ?

exercice 7

Soit $n \in N$.

a) Montrer qu'il existe un couple unique de polynômes (A,B) de degrés strictement inférieurs à n tel que

$$(1-x)^nA+x^nB=1 \ .$$

b) Montrer que

$$A=B(1-x) \text{ et } B=A(1-x).$$

c) Montrer qu'il existe une constante a telle que

$$(1-x)A^{'}-nB=ax^{n-1}.$$

exercice 8

Déterminer les polynômes P_n de degré n tels que

$$P_n-P_n'=\frac{1}{n!}x^n.$$

exercice 9

Trouver les polynômes P tels que
$P(1) = 3, P'(1) = 4, P"(1) = 5$ et $P^{(n)} = 0 \ \ \forall n \geq 3$.

exercice 10

Soit $P = x^3 + 2$. Décomposer P en produit de polynômes irréductibles unitaires dans $K[x]$ dans chacun des cas $K = \mathbf{Q}, K = \mathbf{R}, K = \mathbf{C}, K = \mathbf{Z}/3\mathbf{Z}, K = \mathbf{Z}/5\mathbf{Z}, K = \mathbf{Z}/7\mathbf{Z}$.

exercice 11

a) Trouver tous le polynômes $P \in \mathbf{R}[x]$ tels que $P + 1$ soit divisible par $(x-1)^2$ et $P - 1$ soit divisible par $(x+1)^2$ en utilisant le théorème de Bezout.
b) Même question en remplacant P par P'.

exercice 12

Décomposer $x^4 + 1$ en produit de polynômes irréductibles dans $\mathbf{C}[x]$ et $\mathbf{R}[x]$.

exercice 13

a) Trouver deux polynômes U et V tels que $U(x^2+1) + V(x^2+x+1) = 1$.
b) Trouver un polynôme P vérifiant les trois conditions suivantes
$P - 1$ est divisible par $x^2 + 1$.
$P + x$ est divisible par $x^2 + x + 1$.
$P - x$ est divisible par $x + 3$.

exercice 14

On se propose de calculer les racines du polynôme $1 + 2x - x^2 + x^3$
a) En utilisant les outils de terminale, montrer que ce polynôme possède une racine réelle et une seule.
b) En posant $s = x - 1/3$, ramener l'équation $1+2x-x^2+x^3 = 0$ à l'équation $\frac{25}{27} + \frac{5}{3}s + s^3 = 0$.
c) On pose $s = a + b$. Ecrire l'équation obtenue pour a et b.
d) On pose à priori $ab = -\frac{5}{9}$. Calculer a^3 et b^3 en résolvant une équation du second degré (il a fallu 1700 ans pour trouver cette astuce). En déduire les racines du polynôme $1 + 2x - x^2 + x^3$ (on pourra se contenter de calculer la racine réelle).

exercice 15(sous MUPAD)

a) Effectuer la division euclidienne de B par A, avec $A = x^9 + 67x^8 + 45x^5 + 17x^4 + 25x^3 - 32x^2 + 27x - 148$ et $B = x^{12} - 35x^7 + 72x^3 - 225x^2 + 72x - 1227$.
b) Calculer le p.g.c.d. et le p.p.c.m. de A et B.
c) Calculer $A(376 - 769i)$ et $B(1906 - 3456i)$.

exercice 16(sous MUPAD)

a) Trouver deux polynômes U et V tels que $(x^9 + 7x^8 - 245x^6 + 28x^5 + 5x^3 + 321x^2 - 275x + 247)U + (x^{12} + x^9 + 7x^4 + 34678x^3 + x^2 + 2250)V = 1$.
b) Trouver un polynôme P tel que $P - x^6 + x^5 + 542x + 2371$ soit divisible par $x^9 + 7x^8 - 245x^6 + 28x^5 + 5x^3 + 321x^2 - 275x + 247$ et tel que $P + 3x^2 - 35x + 2987$ soit divisible par $x^{12} + x^9 + 7x^4 + 34678x^3 + x^2 + 2250$.

exercice 17(sous MUPAD)

Résoudre les équations $x^3 + 12x^2 + 5x + 2 = 0$ et $x^4 - x^3 + 22x + 7 = 0$.
Peut-on écrire clairement les résultats obtenus ?

exercice 18(sous Matlab)

Donner le polynôme d'interpolation de Lagrange et la droite des moindres carrés correspondant aux données $u = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]$ et $v = [1, 1, 1, -3, -3, -4, 5, 4, 3, 0, -1]$, et donner une représentation graphique des résultats obtenus.

Chapitre 4

Fractions rationnelles

4.1 Division suivant les puissances croissantes

On va maintenant s'intéresser à l'ensemble $\tilde{K}[x]$ des *fractions rationnelles* à coefficients dans un corps K. Une fraction rationnelle à coefficients dans K est un quotient de la forme $\frac{P}{Q}$ avec $P \in K[x]$, $Q \in K[x]$, $Q \neq 0$, et on identifie $\frac{P_1}{Q_1}$ et $\frac{P_2}{Q_2}$ quand $P_1Q_2 - P_2Q_1 = 0$. Les règles de calcul (réduction au même dénominateur pour l'addition, produit, simplification par un diviseur commun de P et Q) sont les mêmes que pour les fractions usuelles, et on vérifie que l'ensemble des fractions rationnelles, muni de cette addition et de ce produit est un *corps*.

Posons $R(\lambda) = \frac{P(\lambda)}{Q(\lambda)}$ pour $R = \frac{P}{Q} \in \tilde{K}[x], \lambda \in D_R := \{\lambda \in \mathbf{C} \mid Q(\lambda) \neq 0\}$. On a $R_1(\lambda) + R_2(\lambda) = (R_1 + R_2)(\lambda)$ et $R_1(\lambda)R_2(\lambda) = (R_1R_2)(\lambda)$ pour $R_1, R_2 \in \tilde{K}[x], \lambda \in D_{R_1} \cap D_{R_2}$.

On utilisera dans la suite le résultat suivant

Lemme 4.1.1 *(Division suivant les puissances croissantes)*

Soit P un polynôme et soit Q un polynôme non constant.Il existe pour tout $n \geq 1$ une unique famille $(R_0, \ldots, R_{n-1})$ de polynômes et un unique polynôme U_n vérifiant les deux conditions suivantes

(i) $d^\circ(R_i) < d^\circ(Q)$ pour $1 \leq i \leq n-1$

(ii) $P = R_0 + \ldots + R_{n-1}Q^{n-1} + Q^nU_n$.

Démonstration : Pour obtenir la décomposition ci-dessus pour $n = 1$ il suffit d'effectuer la division euclidienne de P par Q. Supposons la décomposition obtenue à l'ordre n , avec $n \geq 1$. En effectuant la division euclidienne de U_n par Q on obtient $U_n = R_n + QU_{n+1}$, avec $d^\circ(R_n) < d^\circ(Q)$, et $P = R_0 + \ldots + R_nQ^n + Q^{n+1}U_{n+1}$, ce qui établit par récurrence l'existence de la décomposition cherchée. L'unicité pour $n = 1$ provient de l'unicité de la division euclidienne. Supposons la décomposition unique à l'ordre n , avec $n \geq 1$, et soient $P = R_0 + \ldots + R_nQ^n + Q^{n+1}U_{n+1} = T_0 + \ldots + T_nQ^n + Q^{n+1}V_{n+1}$ deux décompositions de P vérifiant (ii).On a $P = R_0 + \ldots + R_{n-1}Q^{n-1} + Q^n(R_n + QU_{n+1}) =$

$T_0 + \ldots + T_{n-1}Q^{n-1} + Q^n(T_n + QV_{n+1})$. D'après l'hypothèse de récurrence, on a $R_i = T_i$ pour $1 \leq i \leq n-1$ et $R_n + QU_{n+1} = T_n + QV_{n+1}$. Le fait que $R_n = T_n$ et $U_{n+1} = V_{n+1}$ provient de l'unicité de la division euclidienne, et l'unicité de la décomposition donnée par le lemme est établie par récurrence. ♣

4.2 Décomposition en éléments simples d'une fraction rationnelle

Théorème 4.2.1 *(Décomposition en éléments simples d'une fraction rationnelle)*

Soit K un corps, soit $\frac{P}{Q}$ une fraction rationnelle à coefficients dans K, avec P et Q premiers entre eux, et soit $Q = aQ^{n_1} \ldots Q_k^{n_k}$ la décomposition de Q en produit de polynômes irréductibles unitaires dans $K[x]$.

Il existe alors $U \in K[x]$ et k familles $(A_{1,1}, \ldots, A_{1,n_1}) \ldots, (A_{k,1}, \ldots, A_{k,n_k})$ de polynômes à coefficients dans K, avec $d^\circ(A_{p,q}) < d^\circ(Q_p)$ pour $1 \leq p \leq k$, $1 \leq q \leq n_p$, vérifiant

$$\frac{P}{Q} = U + \sum_{1 \leq p \leq k} \left(\sum_{1 \leq q \leq n_p} \frac{A_{p,q}}{Q_p^q} \right).$$

De plus $A_{p,n_p} \neq 0$ pour $1 \leq p \leq k$, et la décomposition ci-dessus est unique.

Démonstration : On peut se limiter au cas où Q est unitaire. Supposons que $Q = Q_1^n$, avec Q_1 irréductible. On obtient alors la décomposition en éléments simples en effectuant la division suivant les puissances croissantes de P par Q_1 à l'ordre n.

Supposons que la décomposition en éléments simples existe quand Q possède k diviseurs unitaires irréductibles distincts, avec $k \geq 1$, et soit Q un polynôme unitaire possédant $k+1$ diviseurs irréductibles distincts $Q_1, \ldots, Q_{k+1}$. On a $Q = Q_1^{n_1} \ldots, Q_{k+1}^{n_{k+1}}$. Posons $U_1 = Q_1^{n_1} \ldots Q_{k+1}^{n_{k+1}}$, $U_2 = Q_k^{n_k}$. D'après le théorème 3.16, U_1 et U_2 sont premiers entre eux et il existe deux polynômes V_1 et V_2 tels que $U_1V_1 + U_2V_2 = 1$, ce qui donne $\frac{P}{Q} = \frac{P}{U_1U_2} = \frac{V_1P}{U_2} + \frac{V_2P}{U_1}$. D'après l'hypothèse de récurrence, $\frac{V_1P}{U_2}$ et $\frac{V_2P}{U_1}$ possèdent une décomposition en éléments simples, et la somme de ces deux décompositions donnent une décomposition en éléments simples de $\frac{P}{Q}$. L'existence de la décomposition en éléments simples est donc établie par récurrence.

Soient $P \in K[x], Q \in K[x]$ deux polynômes premiers entre eux et soit $\frac{P}{Q} = U + \sum_{1 \leq p \leq k} \left(\sum_{1 \leq q \leq n_p} \frac{A_{p,q}}{Q_p^q} \right)$, avec $U \in K[x]$, $A_{p,n_p} \neq 0$, Q_p irréductible unitaire pour $1 \leq p \leq k$, $d^\circ(A_{p,q}) < d^\circ(Q_p)$ pour $1 \leq q \leq p$ une décomposition en éléments simples de $\frac{P}{Q}$. En multipliant les deux membres de cette égalité par $QQ_1^{n_1} \ldots Q_k^{n_k}$, on obtient $PQ_1^{n_1} \ldots Q_k^{n_k} = QV$, avec $V \in K[x]$.Comme Q est premier avec P, on voit que Q divise $Q_1^{n_1} \ldots Q_k^{n_k}$.

Pour $1 \leq p \leq k$, posons $\tilde{Q}_p = \frac{Q_1^{n_1} \dots Q_k^{n_k}}{Q_p} \in K[x]$.

Multiplions les deux membres de l'égalité ci-dessus par $Q_p^{n_p} Q$. On obtient $PQ_p^{n_p} = Q(A_{p,n_p} + \frac{Q_p V}{\tilde{Q}_p})$, avec $V \in K[x]$, et $PQ_p^{n_p}\tilde{Q}_p = Q(A_{p,n_p}\tilde{Q}_p + Q_p V)$. Comme $A_{p,n_p} \neq 0$, A_{p,n_p} et Q_p sont premiers entre eux. Il résulte du théorème 3.5.5 que Q_p et $\tilde{Q}_p$ sont premiers entre eux , et il résulte également du théorème 3.5.5 que Q_p est premier avec $A_{p,n_p}\tilde{Q}_p$.Comme les diviseurs communs de Q_p et $A_{p,n_p}\tilde{Q}_p + Q_p V$ sont les mêmes que ceux de Q_p et $A_{p,n_p}\tilde{Q}_p$ on voit que Q_p et $A_{p,n_p}\tilde{Q}_p + Q_p V$ sont premiers entre eux.Il résulte alors du théorème 3.5.5 que $Q_p^{n_p}$ et $A_{p,n_p}\tilde{Q}_p + Q_p V$ sont premiers entre eux, et il résulte du théorème de Gauss que $Q_p^{n_p}$ divise Q. Comme $Q_p^{n_p}$ est premier avec $Q_q^{n_q}$ pour $p \neq q$, il résulte de la proposition 3.7.4 que le p.p.c.m. de la famille $(Q_1^{n_1}, \dots, Q_k^{n_k})$ est égal au produit $Q_1^{n_1} \dots Q_k^{n_k}$. Donc Q divise $Q_1^{n_1} \dots Q_k^{n_k}$, et $Q_1^{n_1} \dots Q_k^{n_k}$ divise Q. Comme ces deux polynômes sont unitaires, on a $Q = Q_1^{n_1} \dots Q_k^{n_k}$. Ceci prouve au passage que $A_{p,n_p} \neq 0$ dans la décomposition en éléments simples dont l'existence a été montrée plus haut. Soient maintenant $\frac{P}{Q} = U + \sum_{1 \leq p \leq k}(\sum_{1 \leq q \leq n_p} \frac{A_{p,q}}{Q_p^q}) = V + \sum_{1 \leq p \leq k}(\sum_{1 \leq q \leq n_p} \frac{B_{p,q}}{Q_p^q})$ deux décompositions en éléments simples de $\frac{P}{Q}$. Alors U et V sont égaux au quotient obtenu en effectuant la division euclidienne de P par Q. Avec les mêmes notations que ci-dessus on obtient, pour $1 \leq p \leq k$, deux polynômes W_1 et W_2 tels que

$$PQ = P\tilde{Q}_p Q_p^{n_p} = Q(A_{p,n_p}\tilde{Q}_p + Q_p W_1) = Q(B_{p,n_p}\tilde{Q}_p + Q_p W_2).$$

Donc $P = A_{p,n_p}\tilde{Q}_p + Q_p W_1 = B_{p,n_p}\tilde{Q}_p + Q_p W_2$. Comme $\tilde{Q}_p$ et Q_p sont premiers entre eux, et comme $d^\circ(A_{p,n_p}) < d^\circ(Q_p)$ et $d^\circ(B_{p,n_p}) < d^\circ(Q_p)$, il résulte du corollaire 3.5.4 que $A_{p,n_p} = B_{p,n_p}$. En appliquant ce résultat à $\frac{P}{Q} - \frac{A_{p,n_p}}{Q_p^{n_p}}$ on voit que $A_{p,q_1} = B_{p,q_1}$, où $q_1 < p$ est s'il existe le plus grand entier tel que A_{p,q_1} ou B_{p,q_1} soit non nul, et on voit par récurrence descendante que $A_{p,q} = B_{p,q}$ pour $1 \leq q \leq n_p$, ce qui prouve l'unicité de la décomposition en éléments simples. ♣

Corollaire 4.2.2 *(i) Soit $\frac{P}{Q}$ une fraction rationnelle à coefficients dans $\mathbf{C}$, avec P et Q premiers entre eux, et soit $Q = a(x-\lambda_1)^{n_1} \dots (x-\lambda_k)^{n_k}$ la décomposition de Q en produit de polynômes unitaires irréductibles dans $C[x]$.*

Il existe alors $U \in \mathbf{C}[x]$ et k familles $(a_{1,1} \dots a_{1,n_1}), \dots, (a_{k,1}, \dots, a_{k,n_k})$ de nombres complexes vérifiant

$$\frac{P}{Q} = U + \sum_{1 \leq p \leq k} \left(\sum_{1 \leq q \leq n_p} \frac{a_{p,q}}{(x-\lambda_p)^q} \right).$$

De plus $a_{p,n_p} \neq 0$ pour $1 \leq p \leq k$, et cette décomposition est unique.

(ii) Soit $\frac{P}{Q}$ une fraction rationnelle à coefficients dans $\mathbf{R}$, avec P et Q premiers entre eux, et soit $Q = a(x-\lambda_1)^{n_1} \dots (x-\lambda_k)^{n_k}(x^2+b_1x+c_1)^{m_1} \dots (x^2+b_{k'}x+c_{k'})^{m_{k'}}$ la décomposition de Q en produit de polynômes unitaires irréductibles dans $\mathbf{R}[x]$.

Il existe alors un polynôme $U \in \mathbf{R}[x]$ *, k familles* $(a_{1,1} \dots a_{1,n_1}), \dots, (a_{k,1}, \dots, a_{k,n_k})$ *de réels, et* k' *familles*

$((d_{1,1}, e_{1,1}), \dots, (d_{1,m_1}, e_{1,m_1})), \dots, ((d_{k',1}, e_{k',1}), \dots, (d_{k',m_{k'}}, e_{k',m_{k'}}))$ *de couples de réels , avec* $(b_{j,m_j}, c_{j,m_j}) \neq (0,0)$ *pour* $1 \leq j \leq k'$ *vérifiant*

$$\frac{P}{Q} = U + \sum_{1 \leq p \leq k} \left(\sum_{1 \leq q \leq n_p} \frac{a_{p,q}}{(x - \lambda_p)^q} \right) + \sum_{1 \leq p \leq k'} \left(\sum_{1 \leq q \leq m_p} \frac{d_{p,q}x + e_{p,q}}{(x^2 + b_p x + c_p)^q} \right),$$

De plus $a_{p,n_p} \neq 0$ *pour* $1 \leq p \leq k$ *,* $(b_{p,m_p}, c_{p,m_p}) \neq (0,0)$ *pour* $1 \leq p \leq k'$*, et cette décomposition est unique.*

Le terme polynômial de la décomposition en éléments simples s'obtient en prenant le quotient de la dividion euclidienne du numérateur par le dénominateur. D'autre part le coefficient a_{p,n_p} associé à une racine λ_p du dénominateur s'obtient en multipliant les deux membres de l'égalité par $(x-\lambda_p)^p$ et en remplacant après simplification x par λ_p. Ceci mène dans certains cas à des calculs rapides.

Exemple 4.2.3 *Décomposition en éléments simples de* $\frac{x^2}{(x-1)(x+1)(x+2)}$.

Le degré du numérateur étant strictement inférieur à celui du dénominateur, on sait que la décomposition est de la forme

$$\frac{x^2}{(x-1)(x+1)(x+2)} = \frac{a}{x-1} + \frac{b}{x+1} + \frac{c}{x+2}.$$

En multipliant par $x-1$ et en remplaçant x par 1, on obtient $a = \frac{1}{2\times 3} = \frac{1}{6}$. En multipliant par $x+1$ et en remplaçant x par -1, on obtient $b = \frac{1}{(-2)\times 1} = -\frac{1}{2}$. En multipliant par $x+2$ et en remplaçant x par -2, on obtient $c = \frac{4}{(-3)\times(-1)} = \frac{4}{3}$. La décomposition cherchée est donc

$$\frac{x^2}{(x-1)(x+1)(x+2)} = \frac{1}{6(x-1)} - \frac{1}{2(x+1)} + \frac{4}{3(x+2)}.$$

Dans le cas général on peut toujours après avoir effectué la division euclidienne de P par Q écrire à priori la décomposition, réduire au même dénominateur le second membre et identifier les numérateurs pour se ramener á un système d'équations linéaires, en jouant éventuellement au départ sur l'unicité de la décomposition dans le cas d'une fraction rationnelle paire ou impaire pour montrer que certains coefficients son nuls, mais ces calculs peuvent être fort compliqués. En fait la démonstration du théorème 4.1 donne une *méthode effective* pour calculer la décomposition en éléments simples d'une fraction rationnelle : en appliquant un certain nombre de fois le théorème de Bezout on se ramène à décomposer en éléments simples des fractions rationnelles de la forme $\frac{P}{Q^n}$, avec Q irréductible, et il suffit alors d'effectuer des divisions suivant les puissances croissantes. Nous illustrons cette méthode générale par un exemple

Exemple 4.2.4 *Décomposition en éléments simples de* $\frac{x^7+2x^5+4x^2-x+1}{x^2(x^2+1)^2}$.

On a $(x^2+1)^2 = x^4+2x^2+1 = x^2(x^2+2)+1$.

On en déduit que $(x^2+1)^2(x^7+2x^5+4x^2-x+1) - x^2(x^2+2)(x^7+2x^5+4x^2-x+1) = x^7+2x^5+4x^2-x+1$. On a donc

$$\frac{x^7+2x^5+4x^2-x+1}{x^2(x^2+1)^2} = \frac{x^7+2x^5+4x^2-x+1}{x^2} - \frac{(x^2+2)(x^7+2x^5+4x^2-x+1)}{(x^2+1)^2}$$

$$= x^5+2x^3+4-\frac{1}{x}+\frac{1}{x^2}-\frac{x^9+2x^7+4x^4-x^3+x^2+2x^7+4x^5+8x^2-2x+2}{(x^2+1)^2}$$

$$= x^5+2x^3+4-\frac{1}{x}+\frac{1}{x^2}-\frac{x^9+4x^7+4x^5+4x^4-x^3+9x^2-2x+2}{(x^2+1)^2}.$$

On effectue alors la division euclidienne de $x^9+4x^7+4x^5+4x^4-x^3+9x^2-2x+2$ par $(x^2+1)^2$.

$\mathbf{x^9}+$	$\mathbf{+4x^7}$	$\mathbf{+4x^5}$	$\mathbf{+4x^4}$	$\mathbf{-x^3}$	$\mathbf{+9x^2}$	$\mathbf{-2x}$	$\mathbf{+2}$	$\mathbf{x^4}$	$\mathbf{+2x^2}$	$\mathbf{+1}$	
$-x^9$	$-2x^7$	$-x^5$						$\mathbf{x^5}$	$\mathbf{+2x^3}$	$\mathbf{-x}$	$\mathbf{+4}$
	$\mathbf{2x^7}$	$\mathbf{+3x^5}$	$\mathbf{+4x^4}$	$\mathbf{-x^3}$	$\mathbf{+9x^2}$	$\mathbf{-2x}$	$\mathbf{+2}$				
	$-2x^7$	$-4x^5$		$-2x^3$							
		$\mathbf{-x^5}$	$\mathbf{+4x^4}$	$\mathbf{-3x^3}$	$\mathbf{+9x^2}$	$\mathbf{-2x}$	$\mathbf{+2}$				
		x^5		$+2x^3$		+x					
			$\mathbf{4x^4}$	$\mathbf{-x^3}$	$\mathbf{+9x^2}$	$\mathbf{-x}$	$\mathbf{+2}$				
			$-4x^4$		$-8x^2$		-4				
				$\mathbf{-x^3}$	$\mathbf{+x^2}$	$\mathbf{-x}$	$\mathbf{-2}$				

On obtient $x^9+4x^7+4x^5+4x^4-x^3+9x^2-2x+2 = (x^2+1)^2(x^5+2x^3-x+4) - x^3+x^2-x-2$, et on a

$$\frac{x^7+2x^5+4x^2-x+1}{x^2(x^2+1)^2} = x^5+2x^3+4-\frac{1}{x}+\frac{1}{x^2}-x^5-2x^3+x-4+\frac{x^3-x^2+x+2}{(x^2+1)^2}$$

$$= x-\frac{1}{x}+\frac{1}{x^2}+\frac{x^3-x^2+x+2}{(x^2+1)^2}.$$

On effectue alors la division euclidienne de x^3-x^2+x+2 par x^2+1.

$\mathbf{x^3}$	$\mathbf{-x^2}$	$\mathbf{+x}$	$\mathbf{+2}$	$\mathbf{x^2}$	$\mathbf{+1}$
$-x^3$		$-x$		$\mathbf{x}$	$\mathbf{-1}$
	$\mathbf{-x^2}$		$\mathbf{+2}$		
	x^2		$+1$		
			$\mathbf{+3}$		

On a donc $x^3-x^2+x+2=(x^2+1)(x-1)+3$, et on obtient la décomposition cherchée :

$$\frac{x^7+2x^5+4x^2-x+1}{x^2(x^2+1)^2}=x-\frac{1}{x}+\frac{1}{x^2}+\frac{x-1}{x^2+1}+\frac{3}{(x^2+1)^2}.$$

4.3 Applications au calcul intégral

La décomposition en éléments simples des fractions rationnelles réelles à des applications au **calcul intégral**. On connait en effet une primitive de $\frac{1}{(x-a)^n}$ pour $n\geq 1$ (c'est $-\frac{1}{(n-1)(x-a)^{n-1}}$ pour $n\geq 2$ et $log|x-a|$ pour $n=1$.) D'autre part si $b^2-4c<0$ en posant $s=x+\frac{b}{2}$, puis $t=\frac{s}{\sqrt{c-\frac{b^2}{4}}}$, on ramène le calcul d'une primitive d'une fonction $f:x\longmapsto\frac{cx+d}{(x^2+bx+c)^n}$ au calcul d'une primitive d'une fonction $g:t\longmapsto\frac{\alpha t+\beta}{(t^2+1)^n}$.

On trouve une primitive d'une fonction $t\longmapsto\frac{t}{(t^2+1)^n}$ en posant $r=t^2$.

Pour les fonctions du type $t\longmapsto\frac{1}{(t^2+1)^n}$, on procède par récurrence. En effet posons

$$F_n(x)=\int_0^x\frac{dt}{(t^2+1)^n}.$$

En posant $u=\frac{1}{(t^2+1)^n}, dv=dt$, on obtient $du=-\frac{2nt}{(t^2+1)^{n+1}}, v=t$. On a alors , par intégration par parties

$$F_n(x)=\int_0^x\frac{dt}{(t^2+1)^n}=\left[\frac{t}{(t^2+1)^n}\right]_0^x+2n\int_0^x\frac{t^2}{(t^2+1)^{n+1}}dt.$$

On remarque alors que

$$\frac{t^2}{(t^2+1)^{n+1}}=\frac{t^2+1}{(t^2+1)^{n+1}}-\frac{1}{(t^2+1)^n}=\frac{1}{(t^2+1)^n}-\frac{1}{(t^2+1)^{n+1}}.$$

Ceci donne $F_n(x)=\frac{x}{(x^2+1)^n}+2nF_n(x)-2nF_{n+1}(x)$ et on a

$$F_{n+1}(x)=\frac{2n-1}{2n}F_n(x)+\frac{x}{2n(x^2+1)^n}. \tag{4.1}$$

Pour les calculs d'intégrales définies,on obtient

$$\int_a^b\frac{dt}{(t^2+1)^{n+1}}=\frac{2n-1}{2n}\int_a^b\frac{dt}{(t^2+1)^n}+\frac{b}{2n(b^2+1)^n}-\frac{a}{2n(a^2+1)^n}. \tag{4.2}$$

Comme $F_1(x)=\int_0^x\frac{dt}{x^2+1}=Arctg(x)$, ceci permet de calculer par récurrence toutes les intégrales obtenues après décomposition en éléments simples d'une fraction rationnelle à intégrer.

Exemple 4.3.1 *Calculer*

$$I = \int_0^1 \frac{dx}{(x^2+2x+5)^2}.$$

En posant $s = x+1$, on obtient

$$I = \int_0^1 \frac{dx}{((x+1)^2+4)^2} = \int_1^2 \frac{ds}{(s^2+4)^2}.$$

On pose alors $t = \frac{s}{2}$, et on a

$$I = \int_{\frac{1}{2}}^1 \frac{2dt}{(4t^2+4)^2} = \frac{1}{8}\int_{\frac{1}{2}}^1 \frac{dt}{(t^2+1)^2}.$$

En appliquant la formule (4.2) avec $n=1$, $a=\frac{1}{2}$, $b=1$ on obtient

$$I = \frac{1}{8}\int_{\frac{1}{2}}^1 \frac{dt}{t^2+1} + \frac{1}{8}\left(\frac{1}{4} - \frac{1}{4(\frac{1}{4}+1)}\right) = \frac{1}{16}Arctg(1) - \frac{1}{16}Arctg(\frac{1}{2}) + \frac{1}{160}$$

$$= \frac{\pi}{64} - \frac{1}{16}Arctg(\frac{1}{2}) + \frac{1}{160}.$$

Exemple 4.3.2 *Calculer*

$$J = \int_0^{\frac{1}{2}} \frac{x^2 dx}{(x-1)(x+1)(x+2)}.$$

On a

$$\frac{x^2}{(x-1)(x+1)(x+2)} = \frac{1}{6(x-1)} - \frac{1}{2(x+1)} + \frac{4}{3(x+2)}.$$

Donc

$$J = \left[\frac{1}{6}ln(1-x) - \frac{1}{2}ln(1+x) + \frac{4}{3}ln(2+x)\right]_0^{\frac{1}{2}}$$

$$= \frac{1}{6}ln(\frac{1}{2}) - \frac{1}{2}ln(\frac{3}{2}) + \frac{4}{3}\left(ln\left(\frac{5}{2}\right) - ln(2)\right)$$

$$= \frac{4}{3}ln(\frac{5}{2}) - \frac{1}{2}ln(\frac{3}{2}) - \frac{3}{2}ln(2)$$

$$= \frac{4}{3}ln(5) - \frac{1}{2}ln(3) + \left(-\frac{3}{2} + \frac{1}{2} - \frac{4}{3}\right)ln(2).$$

On obtient

$$J = \frac{4}{3}ln(5) - \frac{1}{2}ln(3) - \frac{7}{3}ln(2).$$

Exemple 4.3.3 *Calculer*

$$K = \int_1^2 \frac{x^7 + 2x^5 + 4x^2 - x + 1}{x^2(x^2+1)^2} dx.$$

On a

$$K = \int_1^2 x dx - \int_1^2 \frac{dx}{x} + \int_1^2 \frac{dx}{x^2} + \int_1^2 \frac{x-1}{x^2+1} dx + 3\int_1^2 \frac{dx}{(x^2+1)^2}$$

$$= \left[\frac{x^2}{2}\right]_1^2 - [log(x)]_1^2 + \left[-\frac{1}{x}\right]_1^2 + \left[\frac{1}{2}log(x^2+1)\right]_1^2 - [Arctg(x)]_1^2 + 3\int_1^2 \frac{dx}{(x^2+1)^2}$$

$$= 2 - \frac{3}{2}ln(2) + \frac{1}{2}ln(5) - Arctg(2) + \frac{\pi}{4} + 3\int_1^2 \frac{dx}{(x^2+1)^2}$$

Pour calculer la dernière intégrale , on utilise la formule 4.2 avec $n = 3$, $a = 1$, $b = 2$. On obtient

$$\int_1^2 \frac{dx}{(x^2+1)^2} = \frac{1}{2}\int_1^2 \frac{dx}{x^2+1} + \frac{1}{5} - \frac{1}{2\times 2} = \frac{1}{2}Arctg(2) - \frac{\pi}{8} - \frac{1}{20}.$$

On obtient finalement

$$K = \frac{37}{20} - \frac{3}{2}ln(2) + \frac{1}{2}ln(5) + \frac{1}{2}Arctg(2) - \frac{\pi}{8}.$$

4.4 Décomposition en éléments simples et calcul intégral sous MUPAD

La décomposition des fractions rationnelles en éléments simples se réduit à des divisions euclidiennes successives et à des applications du théorème de Bezout,opérations qui peuvent se faire sous MUPAD. On va reprendre le deuxième exemple,la décomposition en éléments simples de $R = \frac{x^7+2x^5+4x^2-x+1}{x^2(x^2+1)^2}$. On commence par trouver U et V tels que $x^2U + (x^2+1)^2V = 1$.

```
gcdex(x^2, (x^2 +1)^2);
```

$$1, -x^2 - 2, 1$$

Donc $R = \frac{(x^7+2x^5+4x^2-x+1)(-x^2-2)}{(x^2+1)^2} + \frac{(x^7+2x^5+4x^2-x+1)}{x^2} = \frac{(x^7+2x^5+4x^2-x+1)(-x^2-2)}{(x^2+1)^2} + x^5 + 2x^3 + 4 - \frac{1}{x} + \frac{1}{x^2}$.

Pour décomposer le premier terme, on divise le numérateur par $(x^2+1)^2$ et on divise ensuite le quotient obtenu par x^2+1.

```
divide((x^7 +2*x^5 +4*x^2 -x +1)*(-x^2 -2),(x^2 +1)^2);
```

```
                        3    5           2    3
                  x - 2 x  - x  - 4, x - x  + x  + 2
```

```
divide(x- x^2 +x^3 +2,x^2+1);
```

```
                              x - 1, 3
```

On retrouve alors la décomposition

$$R = x - 2x^3 - x^5 - 4 + \frac{3}{(x^2+1)^2} + \frac{x-1}{x^2+1} + x^5 + 2x^3 + 4 - \frac{1}{x} + \frac{1}{x^2} = x + \frac{3}{(x^2+1)^2} + \frac{x-1}{x^2+1} - \frac{1}{x} + \frac{1}{x^2}.$$

En fait MUPAD est programmé pour décomposer les fractions rationnelles en éléments simples, avec la commande **partfrac** et aussi pour appliquer ces décompositions au calcul intégral, avec les commandes **int(f(x),x)** pour les calculs de primitives et **int(f(x),x= a..b)** pour les calculs d'intégrales définies.

On peut ainsi vérifier sous Mupad les décompositions en éléments simples et les calculs d'intégrales effectués plus haut. MUPAD peut aussi faire des calculs plus compliqués. Par exemple on peut calculer sous Mupad une primitive de $\frac{x^10+x^7-87x^3+12x+56}{(x+1)^3(x^2+x+1)^4(x-1)^8}$, avec la commande

```
int((x^10 + x^7 - 87 *x^3 +12*x + 56)/((x+1)^3 *(x^2 +x +1)^4 *(x-1)^8),x);
```

mais le résultat occupe plus de deux pages, que nous avons omis de reproduire ici. Par contre la feuille de calcul reproduite plus loin permet d'obtenir l'égalité suivante (le calcul sous Mupad prend une vingtaine de secondes), qu'il semble évidemment impossible d'obtenir "à la main"

$$\int_0^{1/2} \frac{x^{10}+x^7-87x^3+12x+56}{(x+1)^3(x^2+x+1)^4(x-1)^8}dx = \frac{2404751}{279936}ln(2) + \frac{1165}{128}ln(3/2)$$
$$-\frac{559}{2187}ln(7/4) - \frac{5365\pi\sqrt{3}}{6561} + \frac{10730\sqrt{3}arctg(\frac{2\sqrt{3}}{3})}{2187} + \frac{2228868161}{40007520}.$$

```
partfrac(x^2/((x+1)*(x-1)*(x+2)),x);
```

$$\frac{1}{6\cdot(x-1)}-\frac{1}{2\cdot(x+1)}+\frac{4}{3\cdot(x+2)}$$

```
partfrac((x^7+2*x^5+4*x^2-x+1)/(x^2*(x^2+1)^2),x);
```

$$x-\frac{1}{x}+\frac{1}{x^2}+\frac{3}{\left(x^2+1\right)^2}+\frac{x-1}{x^2+1}$$

```
int(1/((x^2+2*x+5)^2),x=0..1);
```

$$\frac{\pi}{64}-\frac{\arctan\left(\frac{1}{2}\right)}{16}+\frac{1}{160}$$

```
int(x^2/((x-1)*(x+1)*(x+2)),x=0..1/2);
```

$$\frac{4\cdot\ln\left(\frac{5}{2}\right)}{3}-\frac{\ln\left(\frac{3}{2}\right)}{2}-\frac{3\cdot\ln(2)}{2}$$

```
int((x^7+2*x^5+4*x^2-x+1)/(x^2*(x^2+1)^2),x=1..2);
```

$$\frac{\ln(5)}{2}-\frac{3\cdot\ln(2)}{2}-\frac{\pi}{8}+\frac{\arctan(2)}{2}+\frac{37}{20}$$

```
int((x^10 + x^7 - 87 *x^3 +12*x + 56)/((x+1)^3 *(x^2 +x +1)^4 *
(x-1)^8),
x=0..1/2)
```

4.5 Exercices sur le Chapitre 4

exercice 1
Décomposer en éléments simples $\frac{x}{(x+1)(x+2)(x+3)}$, et calculer $\int_0^1 \frac{x}{(x+1)(x+2)(x+3)}dx$.

exercice 2
Décomposer en éléments simples la fraction rationnelle $\frac{1}{(x+1)^2(x^2+x+1)^2}$, et calculer $\int_0^1 \frac{dx}{(x+1)^2(x^2+x+1)^2}$.

exercice 3
Décomposer en éléments simples dans $\tilde{R}[x]$, puis dans $\tilde{C}[x]$, les fractions rationnelles suivantes

$$f(x) = \frac{1}{x^2(x-1)}, f(x) = \frac{1}{(x^2-1)(x^2+1)}, f(x) = \frac{1}{x(x^2+x+1)^2},$$

$$f(x) = \frac{2x^4+1}{(x-1)^3(x^2+1)}, f(x) = \frac{2x-1}{x(x+1)^2(x^2+2x+1)^2}, f(x) = \frac{n!}{x(x+1)\dots(x+n)}.$$

exercice 4
a)Calculer la dérivée n^e de $\frac{1}{x-a}$, $a \in \mathbf{R}$.

b)En déduire la dérivée n^e de $\frac{1}{x^2+1}$.

exercice 5
Décomposer sur $\mathbf{C}$ en éléments simples la fraction

$$f(x) = \frac{1}{x^n-1}.$$

Soient $n \in N^*$ et $P \in \mathbf{C}[x]$ tel que $d^\circ(P) < n$.
b) Montrer qu'il existe n nombres complexes $(\alpha_k)_{1\leq k\leq n}$ tels que

$$\frac{P}{x^n-1} = \frac{1}{n}\sum_{k=1}^{n} \frac{\alpha_k P(\alpha_k)}{x-\alpha_k}.$$

c) En déduire que

$$\frac{P}{x^n-1} = \frac{1}{2n}\sum_{k=1}^{n} P(\alpha_k)\frac{x+\alpha_k}{x-\alpha_k} - \frac{1}{2}P(0).$$

d) Montrer que

$$\frac{sin((n-2)x)}{sin(nx)} = -\frac{1}{n}\sum_{k=1}^{n} sin(\frac{2k\pi}{n})cotg(x-\frac{k\pi}{n}).$$

exercice 6

Enoncer et démontrer un résultat du type "division selon les puissances croissantes" pour les entiers.Que donne ce résultat pour le nombre $\frac{13457490876543265}{10^9}$? Faire le lien avec vos souvenirs du CM2.

exercice 7 Soient a et b deux nombres complexes distincts.Décomposer sur $\mathbf{C}$ la fraction

$$f(x) = \frac{1}{(x-a)^n(x-b)^n}.$$

Indication : on pourra appliquer la formule de Taylor avec reste intégral au point a à la fraction rationnelle $(x-a)^n f(x)$ qui n'a pas de pôle en a.

exercice 8(sous MUPAD)

a) Décomposer en éléments simples $\frac{x^{10}+876x^4+293x+3}{(x^2+1)^8(x-1)^{12}(x+35)^9}$ et en calculer une primitive.

b) Calculer $\int_1^2 \frac{x^{10}+876x^4+293x+3}{(x^2+1)^8(x-1)^{12}(x+35)^9}dx$.

exercice 9(sous MUPAD)

Trouver une primitive de $\frac{1}{(x^2+x+1)^{13}}$ et calculer $\int_0^1 \frac{dx}{(x^2+x+1)^{13}}$.

Index