Arithmétique

Cours de L1 (S2 M-I et M-P)

2021–2022

Université de Lorraine

Version : 21 février 2022

Ce document reprend des extraits de

- Notes de cours : "Arithmétique et Algèbre", Université Henri Poincaré–Nancy 1, LMI2, 2009–2010,
- François Liret : "Arithmétique" (Dunod),
- Danchin/Hadiji/Jaffard/Löcherbach/Printems/Seuret : "Cours arithmétique et groupes, Licence première année, premier semestre", `http://perso-math.univ-mlv.fr/users/printems.jacques/L1/PolyMias1.pdf`,
- J. Rivat, "Introduction à la théorie des nombres", Polycopié / Ergodic Theory and Dynamical Systems in their Interactions with Arithmetics and Combinatorics (CIRM, Jean-Morlet Chaire, 2016),
- Exercices de G. Eguether : `http://www.iecl.univ-lorraine.fr/~Gerard.Eguether`.

Modalités :

- cours d'option L1 au S2 en M-I et M-P, sans pré-requis
- volume horaire : 26h EI + 4h TP (= 3 ECTS)
- MCC : 0.3 E1 + 0.7 E2 (E1 $\geq$ 1h, E2 = 2h)
- Compétences visées : Construire et rédiger une démonstration mathématique synthétique et rigoureuse.

Descriptif :

(I) **Arithmétique élémentaire.** Divisibilité dans $\mathbb{Z}$. PGCD de deux entiers dont un est non nul. Division euclidienne. Lemme et algorithme d'Euclide. Elements de Bézout. Lemme de Gauss. Structures usuelles. Relations d'équivalence. Congruences dans $\mathbb{Z}$. Compatibilité de la congruence avec les opérations de $\mathbb{Z}$. Entiers premiers entre eux. Nombres premiers. Valuations p-adiques. Notation $v_p(n)$. Propriétés (valuation de sommes et produits). Existence et unicité de la décomposition en facteurs premiers. PPCM. Petit théorème de Fermat.

(II) **Polynômes et leur arithmétique.** Rappels sur le degré, la divisibilité, la division euclidienne, polynôme dérivée et les racines simples. Aspects linéaires, en lien avec l'UE "Algèbre linéaire 1" : base des X^n, familles à degrés échelonnés. L'évaluation en un scalaire et la dérivation sont linéaires, noyaux. Composition des polynômes, la composition par Q est linéaire. Applications de la linéarité : formules de dérivée d'une somme, d'un produit, d'une composée. Formule de Taylor. Etude générale des racines multiples, multiplicité, caractérisation en termes de divisibilité ou d'annulation des polynômes dérivés. Ordre ou multiplicité d'annulation d'un polynôme en un scalaire a, et propriétés. Notation $mult_a(Q)$ ou $v_a(Q)$. Lien avec les valuations p-adique sur les entiers. Polynômes scindés. Théorème d'Alembert-Gauss (preuve admise, étude possible en TD). Relations coefficients-racines. Fonctions symétriques élémentaires des racines. Polynômes symétriques. PGCD de deux polynômes (dont un est non nul). Polynômes premiers entre eux. Lemme d'Euclide, algorithme d'Euclide. Elements de Bézout. Lemme de Gauss. Polynômes irréductibles, factorisation des polynômes. On n'étudiera en détail que les cas de $\mathbb{R}[X]$ et $\mathbb{C}[X]$. Exemple de la factorisation de $X^n - 1$ sur $\mathbb{R}$. PPCM. Les travaux pratiques pourront porter sur l'implémentation (itérative ou récursive) de l'algorithme d'Euclide, de divers tests de primalité, ou d'algorithmes liés à la cryptographie.

Compléments CPU :

- volume horaire : +6h EI (MCC = note de contrôle continu, coefficient = 0,5)
- renforcement des programmes de l'UE Arithmétique : "Relations de congruence, ensemble quotient, anneau $\mathbb{Z}/n\mathbb{Z}$, structure de corps si n premier, calcul modulaire."

Programme du **Concours PASS'Ingénieur** concerné par cette UE (pour les CPU) :

"*Polynômes à une indéterminée sur* $\mathbb{K}$.
Définition de l'ensemble $\mathbb{K}[X]$ des polynômes à une indéterminée sur $\mathbb{K}$, degré, valuation. Espace vectoriel $\mathbb{K}_n[X]$ des polynômes de degré inférieur ou égal à n. Multiples et diviseurs d'un polynôme, division Euclidienne. Dérivation, formule de Taylor et ordre de multiplicité d'une racine. Théorème fondamental de d'Alembert-Gauss dans $\mathbb{C}[X]$ (admis), polynômes irréductibles dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$. Décomposition d'un polynôme en produit de polynômes irréductibles. Application à la factorisation de $a + X^n$ dans $\mathbb{C}[X]$."

Ce document (rédigé par Thomas Stoll) pourra servir comme guide pour ce cours (période 2018–2023). Merci à Paul Péringuey pour la relecture attentive.

Table des matières

Chapitre 1

Arithmétique élémentaire

1.1 Divisibilité dans $\mathbb{Z}$

1.1.1 Multiple et diviseur

Soit $\mathbb{Z}$ l'ensemble des entiers relatifs (positifs ou négatifs). Il est muni de deux opérations, l'addition et la multiplication. Nous verrons ce semestre que $(\mathbb{Z}, +, \cdot)$ est un anneau commutatif. Rappelons que $\mathbb{N}$ est l'ensemble des entiers naturels (positifs ou nuls), $\mathbb{N}^*$ est l'ensemble des entiers naturels strictement positifs, et $\mathbb{Z}^*$ l'ensemble des entiers différents de zéro.

Définition 1.1. Soient $a, b \in \mathbb{Z}$. On dit que b *divise* a, ou que a est un *multiple* de b, s'il existe $q \in \mathbb{Z}$ tel que $a = bq$, on note $b|a$. Pour tout $b \in \mathbb{Z}$, l'ensemble $b\mathbb{Z} := \{nb : n \in \mathbb{Z}\}$ est dit *l'ensemble des multiples de* b. On note $D(n) = \{d \in \mathbb{N}^* : \ d \mid n\}$ l'ensemble des diviseurs positifs de n.

Notation. Si b ne divise pas a, on note $b \nmid a$.

Remarque. Dans les énoncés qui suivent, nous écarterons souvent la cas particulier de $b = 0$.

Exemple. $3 \mid 102$, $7 \nmid 102$, $0 \mid 0$, $2 \mid 0$, $0 \nmid 2$, $7\mathbb{Z} = \{\ldots, -21, -14, -7, 0, 7, 14, 21, \ldots\}$, $0\mathbb{Z} = \{0\}$; $D(12) = \{1, 2, 3, 4, 6, 12\}$.

Proposition 1.1 (Propriétés de la divisibilité)**.** *Les relations suivantes sont vraies pour des entiers a, b, c :*

(i) $a \mid a$, $a \mid -a$ *et* $a \mid 0$.

(ii) Si $a \mid b$ *et* $b \mid c$, *alors* $a \mid c$.

(iii) Si $a \mid b$ *et si* $b \neq 0$, *alors* $|a| \leq |b|$.

(iv) Si $a \mid b$ *et si* $b \mid a$, *alors* $a = \pm b$.

(v) Si $a \mid b$ *et* $a \mid c$, *alors* $a \mid (kb + \ell c)$ *quels que soient les entiers* $k, \ell \in \mathbb{Z}$.

(vi) Si $a \mid b$ *alors* $ac \mid bc$.

Démonstration. (i) Évident car $a = a \times 1 = (-a) \times (-1)$ et $0 = a \times 0$.

(ii) Si $a \mid b$ et si $b \mid c$, il existe des entiers q et r tels que $b = aq$ et $c = br$. On en déduit $c = aqr = (aq)r$, donc $a \mid c$.

(iii) Supposons que $a \mid b$, donc $b = aq$, avec $q \in \mathbb{Z}$. Si $b \neq 0$, alors $q \neq 0$, donc $|q| \geq 1$ et $|b| = |a||q| \geq |a|$.

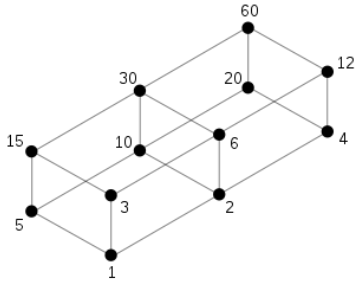
(iv) Supposons que $a \mid b$ et $b \mid a$ avec a et b non nuls. Alors il existe des entiers q et r tels que $a = bq$ et $b = ar$. On a $a = bq = (ar)q = a(rq)$, donc $1 = rq$. Puisque r et q sont des entiers, il s'ensuit $r = q = 1$ ou $r = q = -1$. Donc $a = \pm b$. Le cas $a = b = 0$ est évident.

(v) Supposons que a divise b et c. Alors il existe des entiers p et q tels que $b = ap$ et $c = aq$. Pour tous entiers k et ℓ, on a alors $kb + \ell c = k(ap) + \ell(aq) = a(kp + \ell q)$, donc $a \mid (kb + \ell c)$.

(vi) Si $a \mid b$ alors il existe q tel que $b = aq$. En multipliant par c, on trouve $bc = aqc = (ac)q$ donc $ac \mid bc$.

□

Remarque. Les *diagrammes de Hasse* permettent de visualiser l'ordre de diviseurs : les diviseurs positifs sont représentés par des points et la relation de "divisiblité" est représentée par un segment entre deux points, pointant du bas vers le haut, avec des règles "de minimalité" pour ne pas surcharger la représentation graphique (voir TD). Pour $D(60) = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$ (source Wikipedia) on trouve :



1.1.2 Division euclidienne

Proposition 1.2 (Division euclidienne)**.** *Soit b un entier non nul. Pour tout $a \in \mathbb{Z}$, il existe des entiers q et r uniques tels que*

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

L'entier q s'appelle le quotient *de a par b et l'entier r s'appelle le* reste *de la division de a par b.*

Démonstration. Nous devons montrer l'existence et l'unicité de cette écriture.

— Existence : Supposons d'abord que $b > 0$. Notons par M l'ensemble des multiples de b qui sont inférieurs ou égaux à a. C'est une partie de $\mathbb{Z}$ qui est majorée (par a), donc M a un plus grand élément bq. Le multiple $b(q+1)$ n'appartient alors pas à M, donc on a $bq \leq a < b(q+1)$. En posant $r = a - bq$, il vient $0 \leq r < b(q+1) - bq = b$ et $a = bq + r$, donc ce choix convient.

Si $b < 0$, appliquons ce qui précède à a et $-b$: il existe $q, r \in \mathbb{Z}$ tels que $a = (-b)q + r$ et $0 \leq r < -b$, et $0 \leq r < |b|$.

— Unicité : Montrons maintenant l'unicité du couple (q, r). Supposons que $a = bq + r = bq' + r'$, avec $0 \leq r < |b|$ et $0 \leq r' < |b|$. Alors en soustrayant il vient $0 = b(q - q') + (r - r')$, donc $b(q - q') = -(r - r')$ et en prenant la valeur absolue :

$$|b||q - q'| = |r - r'|.$$

Mais comme r et r' sont compris entre 0 et $|b| - 1$, on a $-|b| < r - r' < |b|$, ce qui implique $|r - r'| < |b|$ et donc $|b||q - q'| < |b|$. Puisque $|b| > 0$, on en déduit $|q - q'| < 1$ et comme $|q - q'|$ est un entier positif ou nul, il s'ensuit $|q - q'| = 0$, ou encore $q = q'$ et $r = r'$.

□

Remarque. (i) On remarque que $b \mid a$ si et seulement si le reste de la division de a par b est nul.

(ii) On écrit r, le reste de la division de a par b, aussi comme $a \mod b$, par exemple $2 \equiv 10 \mod 4$, nous développerons la théorie des congruences dans la Section 1.3.

(iii) *(Rappel de définition)* La *partie entière* d'un réel x est l'unique entier n tel que $n \leq x < n+1$, on note $n = \lfloor x \rfloor$ (parfois on note $n = E(x)$ ou $n = [x]$). Si $b > 0$, le quotient q est l'unique entier tel que $q \leq a/b < q + 1$, on a donc $q = \lfloor a/b \rfloor$.

(iv) Dans des langages de programmation, on obtient r à partir des opérations "`a % b`" (C, C++, Java, Python, SageMath), voir plus tard en TP.

1.1.3 Nombres premiers

Définition 1.2. Un entier $p \geq 2$ est *premier* si ses seuls diviseurs positifs sont 1 et p.

Remarque. L'ensemble des nombres premiers est noté $\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, \ldots\}$.

Proposition 1.3. *Tout entier $n > 1$ est produit de nombres premiers.*

Démonstration. On raisonne par récurrence. Soit un entier $n > 1$. Si n est premier, il est produit de nombres premiers (un seul terme). Sinon, il se factorise en $n = pq$, où les entiers p et q satisfont $1 < p < n$ et $1 < q < n$. Par hypothèse de récurrence, les entiers p et q sont produits de nombres premiers, donc n aussi. □

Proposition 1.4. *Soit $a \in \mathbb{Z} \setminus \{0, -1, 1\}$. Alors le plus petit diviseur supérieur ou égal à 2 de a est un nombre premier.*

Démonstration. Supposons $a > 0$. Soit $D = \{d \geq 2 : d \mid a\}$ l'ensemble des diviseurs de a strictement supérieurs à 1. Alors $D \neq \emptyset$ puisque $a \in D$ et est un sous-ensemble de $\mathbb{Z}$ minoré par 2. Il possède donc un plus petit élément p. Ainsi $p \mid a$ et vérifie $2 \leq p \leq a$. Si p n'était pas un nombre premier, alors il existerait $2 \leq q < p$ tel que $q \mid p$. Mais alors q divise aussi a ce qui contredit le fait que p soit le plus petit élément de D. Donc p est un nombre premier. □

Proposition 1.5 (Euclide)**.** *Il existe une infinité de nombres premiers.*

Démonstration. Par contraposée, supposons qu'il n'existe qu'un nombre fini de nombres premiers positifs $p_1, \ldots, p_n$. Soit $N = 1 + p_1 \cdots p_n$. Puisque $N > 1$ cet entier possède un diviseur premier positif p d'après la Proposition 1.4. Or $p \neq p_1, \ldots, p_n$ sinon il diviserait $N - p_1 \cdots p_n = 1$. On arrive à une contradiction. Donc il y a un infinité de nombres premiers. □

Démonstration alternative. Soit un entier $n \geq 2$. Rappelons la définition du factoriel : $n! = n(n-1)\cdots 2 \cdot 1$. L'entier $N = n! + 1$ n'a aucun diviseur compris entre 2 et n : en effet, un tel diviseur k diviserait $n! = n(n-1)\cdots 3 \cdot 2$ et N, donc diviserait $N - n! = 1$, ce qui n'est pas possible. Or N possède au moins un diviseur premier p. Puisque $p \geq 2$, on en déduit $p > n$. Cela montre qu'il existe des nombres premiers aussi grands qu'on veut. □

Proposition 1.6. *Soit $n \geq 2$ un nombre non premier. Il existe alors $d \leq \sqrt{n}$ tel que $d \mid n$.*

Démonstration. Soit p le plus petit diviseur supérieur à 2 de n. D'après la Proposition 1.4, p est alors un nombre premier. Soit q tel que $n = pq$. Alors $q > 1$ car n n'est pas premier, donc $q \geq p$. Donc $n = pq \geq p^2$, d'où $p \leq \sqrt{n}$. □

On en déduit que $n \geq 2$ est premier si et seulement s'il n'est divisible par aucun nombre premier inférieur ou égal à $\sqrt{n}$. C'est la base du *crible d'Ératosthène*.

Crible d'Ératosthène

Ce crible remonte à l'antiquité (3ème siècle avant J. C.). Soit $x > 2$ donné. On écrit tous les entiers de 2 à x. On commence par rayer tous les multiples de 2 sauf 2. Le plus petit entier qui reste est 3. On raye ensuite tous les multiples de 3 différents de 3, puis tous les multiples de 5 différents de 5 et ainsi de suite... On continue ce procédé jusqu'à l'étape $\lfloor \sqrt{x} \rfloor$. Les entiers qui restent sont les nombres premiers inférieurs à x.

Exemple. Exemple avec $x = 20$.

1.1.4 Idéaux de $\mathbb{Z}$

Définition 1.3. Un *idéal* de $\mathbb{Z}$ est un sous-ensemble $I \subset \mathbb{Z}$ tel que :

(i) $0 \in I$;

(ii) Si $x, y \in I$, alors $x - y \in I$.

Proposition 1.7. *Si I est un idéal de $\mathbb{Z}$, alors $ax \in I$ pour tous $a \in \mathbb{Z}$, $x \in I$.*

Remarque. L'ensemble $b\mathbb{Z}$ est un idéal de $\mathbb{Z}$. On a $b\mathbb{Z} = \{0\}$ si $b = 0$, et $b\mathbb{Z} = \mathbb{Z}$ si $b = 1$ ou $b = -1$. Nous allons montrer en fait que tous les idéaux dans $\mathbb{Z}$ sont de cette forme.

Proposition 1.8. *Soient a, b tels que $b \neq 0$. Alors $a\mathbb{Z} \subset b\mathbb{Z}$ si et seulement si $b \mid a$.*

Démonstration. Si $a\mathbb{Z} \subset b\mathbb{Z}$ alors en particulier, $a \in b\mathbb{Z}$, a est donc un multiple de b. Autrement dit, b divise a. Réciproquement, si $b \mid a$ alors $a = bc$ pour un $c \in \mathbb{Z}$. Donc pour tout $k \in \mathbb{Z}$, $ka = kcb \in b\mathbb{Z}$. □

Remarque. On peut retenir cette proposition sous la forme *"diviser signifie contenir"* (en anglais : *"to divide is to contain"*).

Proposition 1.9. *Soient I et J deux idéaux de $\mathbb{Z}$. On note $I + J = \{u + v : u \in I,\ v \in J\}$ la somme des idéaux I et J. C'est un idéal de $\mathbb{Z}$. Par ailleurs, $I \cap J$ l'intersection de I et J est aussi un idéal de $\mathbb{Z}$.*

Remarque. Si $a, b \in \mathbb{Z}$, $a\mathbb{Z} + b\mathbb{Z} = \{ax + by : x, y \in \mathbb{Z}\}$.

Proposition 1.10. *Soit I un idéal de $\mathbb{Z}$. Il existe alors $b \in \mathbb{Z}$ tel que $I = b\mathbb{Z}$.*

Démonstration. Si $I = \{0\}$ alors $b = 0$ convient. Sinon, il existe $x \in I \setminus \{0\}$. Comme $-x \in I$, on peut supposer que $x > 0$. Soit alors $b > 0$ le plus petit élément de I strictement positif. (C'est le plus petit élément de $I \cap \{1, 2, \ldots, x\}$). Montrons que $I = b\mathbb{Z}$. Comme $b \in I$, $b\mathbb{Z} \subset I$ d'après la Proposition 1.7. Soit $a \in I$. On doit montrer que a est un multiple de b. Il existe deux entiers q, r tels que $a = bq + r$ et $0 \leq r < b$. Mais $r = a - bq \in I$, donc $r = 0$ vu que $0 \leq r < b$ et b est le plus petit entier > 0 de I. □

Remarque. Nous verrons plus loin (en L2) que ce résultat dit que chaque idéal de $\mathbb{Z}$ est *principal* (engendré par un seul élément). On dit alors que b est un *générateur* de I. Si $I \neq \{0\}$ alors $-b$ est également un générateur de I.

1.1.5 pgcd

Définition 1.4. Soient $a, b \in \mathbb{Z}$ des entiers non nuls. Le plus grand entier qui divise a et b s'appelle le *pgcd (plus grand commun diviseur)* de a et b et se note $pgcd(a, b)$ ou plus simplement (a, b). On dit que a et b sont *premiers entre eux* si $(a, b) = 1$. Pour $a \neq 0$, on pose $(a, 0) = |a|$.

Dans ce qui suit, nous ne traitons que le cas (essentiel) avec $a, b \in \mathbb{Z}$ *des entiers non nuls.*

Proposition 1.11. *On a l'équivalence :*

$$d = (a, b) \iff \begin{cases} d \in \mathbb{N}^*, \\ d \mid a \text{ et } d \mid b, \\ \forall c \in \mathbb{N}, c \mid a \text{ et } c \mid b \Rightarrow c \leq d. \end{cases}$$

Remarque. (i) Pour tout $a \in \mathbb{Z}$, $(a, 1) = 1$.

(ii) Si $a \mid b$, alors $(a, b) = |a|$.

Proposition 1.12. *Soient a et b deux entiers non nuls. Soit $d = (a, b)$. On a alors*

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

Démonstration. Soit $I = a\mathbb{Z} + b\mathbb{Z}$. C'est un idéal de $\mathbb{Z}$ d'après la Proposition 1.9. Il est différent de $\{0\}$ car par exemple $a \in I$. D'après la Proposition 1.10, il existe $q \in \mathbb{Z}$ strictement positif tel que $I = q\mathbb{Z}$. Montrons que $q = (a, b)$. Comme $a, b \in I$, $q \mid a$ et $q \mid b$. Soit $c > 0$ un diviseur commun à a et b. Il existe deux entiers k et ℓ tels que $a = ck$ et $b = c\ell$. Or $q \in I$ donc il existe $m, n \in \mathbb{Z}$ tels que $q = am + bn = ckm + c\ell n = c(km + \ell n)$. Donc $c \mid q$, $c \leq q$. Donc par la Proposition 1.11, $q = (a, b) = d$. □

Corollaire 1.13 (Relation de Bézout)**.** *Soient a et b deux entiers non nuls et $d = (a, b)$. Alors :*

(i) *$\exists u, v \in \mathbb{Z}$ ("éléments de Bézout") tels que $au + bv = d$ ("relation de Bézout") ;*

(ii) *Soit $n \in \mathbb{Z}$. L'équation $ax + by = n$ possède des solutions $(x, y) \in \mathbb{Z}^2$ si et seulement si $d \mid n$;*

(iii) *Tout diviseur commun à a et b divise d :*

$$d = (a, b) \iff \begin{cases} d \in \mathbb{N}^*, \\ d \mid a \text{ et } d \mid b, \\ \forall c \in \mathbb{N}, c \mid a \text{ et } c \mid b \Rightarrow c \mid d. \end{cases}$$

Démonstration. Cela découle directement de la Proposition 1.12 et le raisonnement fait dans sa preuve. □

Remarque. Notons donc que d'après (ii) les entiers de la forme $au + bv$, $u, v \in \mathbb{Z}$ sont les multiples de (a, b).

Proposition 1.14 (Règles de calcul avec les pgcd)**.** *Soient a et b deux entiers non nuls. Alors*

(i) *$(a, b) = (-a, b) = (a, -b) = (-a, -b)$ et $(a, b) = (b, a)$;*

(ii) *$(a, b) = (a - b, b)$;*

(iii) *Si $a = bq + r$ où q et r sont des entiers alors $(a, b) = (b, r)$.*

Démonstration. Le point (i) est évident. Soit $I = a\mathbb{Z} + b\mathbb{Z}$. Alors

$$\begin{aligned} I &= \{ma + nb \ : \ m, n \in \mathbb{Z}\} = \{m(a-b) + (n+m)b \ : \ m, n \in \mathbb{Z}\} \\ &= \{k(a-b) + \ell b \ : \ k, \ell \in \mathbb{Z}\} = (a-b)\mathbb{Z} + b\mathbb{Z}. \end{aligned}$$

On en déduit que $(a, b) = (a - b, b)$ d'après la Proposition 1.12. Cela prouve (ii). Le point (iii) se déduit de (ii) par itération. □

Remarque. Cette proposition est à la base de l'algorithme d'Euclide (Section 1.1.6). Soulignons deux points : (ii) est valable pour *tous* entiers a, b (pas de condition sur les signes) ; dans (iii) nous n'imposons pas de condition sur b ni sur les autres quantités (cf. division euclidienne : $0 \leq r < |b|$).

1.1.6 Calcul du pgcd : l'algorithme d'Euclide

L'**algorithme d'Euclide** permet de calculer le pgcd de deux entiers à l'aide de divisions successives en exploitant la Proposition 1.14 (iii). Soient a et b deux entiers strictement positifs tels que $a \geq b$. On fait des divisions successives et on continue ce processus tant que les restes r_i (on admet toujours $r_i \geq 0$) des divisions euclidiennes ne sont pas nuls (on pose $r_{n+1} = 0$) :

$$\begin{aligned} a &= bq_1 + r_1, \\ b &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ r_2 &= r_3 q_4 + r_4, \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, \\ r_{n-1} &= r_n q_{n+1} + 0, \end{aligned}$$

avec

$$0 = r_{n+1} < r_n < \cdots < r_2 < r_1 < b.$$

Puisque les restes sont positifs ou nuls et diminuent strictement, le dernier (r_{n+1}) est nul. Le dernier reste non nul est un nombre $r_n > 0$ tel que $r_n \mid r_{n-1}$, donc

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = r_n.$$

Notons donc que (a, b) est le dernier reste non nul dans la suite des divisions de l'algorithme d'Euclide. Ce procédé fournit aussi u et v (*éléments de Bézout*) tels que $au + bv = (a, b)$ (*relation de Bézout*). Il suffit pour cela de *remonter* l'algorithme comme ci-dessous en utilisant à chaque étape $r_{i+1} = r_{i-1} - r_i q_{i+1}$.

Exemple. Calculer $(21, 38)$ et trouver deux entiers u et v tels que $21u + 38v = (21, 38)$.

$$\begin{aligned} 38 &= 21 \times 1 + 17 \\ 21 &= 17 \times 1 + 4 \\ 17 &= 4 \times 4 + \mathbf{1} \\ 4 &= 1 \times 4 + 0. \end{aligned}$$

On en déduit que $(21, 38) = \mathbf{1}$. Pour trouver u et v, on pourrait partir de l'avant-dernière égalité :

$$\begin{aligned} 1 &= 17 - 4 \times 4 = 17 - (21 - 17 \times 1) \times 4 = 21 \times (-4) + 17 \times 5 \\ &= 21 \times (-4) + (38 - 21 \times 1) \times 5 = 38 \times 5 + 21 \times (-9). \end{aligned}$$

Remarque. Voir Section 3.1 pour une manière structurée (facultatif). Pour des entiers de 100 chiffres (en base 10), le nombre d'étapes de l'algorithme d'Euclide n'est pas grand, il faut moins de 500 étapes, voir Corollaire 3.3.

1.2 Théorème de Bézout & Lemme de Gauss & Lemme d'Euclide

1.2.1 Théorème de Bézout

Proposition 1.15 (Théorème de Bézout)**.** *Soient a et b deux entiers non nuls. On a alors l'équivalence :*

$$(a, b) = 1 \quad \Longleftrightarrow \quad \exists u, v \in \mathbb{Z} : au + bv = 1.$$

Démonstration. Si $(a, b) = 1$ alors d'après le Corollaire 1.13, il existe u et v tels que $au + bv = 1$. Réciproquement, s'il existe deux entiers u et v tels que $au+bv = 1$, alors $1 \in a\mathbb{Z}+b\mathbb{Z}$. Donc $(a, b) \mid 1$ d'où $(a, b) = 1$. □

Proposition 1.16. *Soient a et b deux entiers non nuls. On a alors*

$$(a, b) = d \quad \Longleftrightarrow \quad \begin{cases} d \in \mathbb{N}, \\ \exists a', b' \in \mathbb{Z} \text{ tels que } (a', b') = 1 \text{ et } a = a'd,\ b = b'd. \end{cases}$$

Démonstration. Si $(a, b) = d$, alors il existe u et $v \in \mathbb{Z}$ tels que $au + bv = d$. D'autre part comme d divise a et b, il existe deux entiers a' et b' tels que $a = a'd$ et $b = b'd$. Ainsi $a'u + b'v = 1$, ce qui entraîne que $(a', b') = 1$. Réciproquement on suppose qu'il existe $d \in \mathbb{N}, a', b' \in \mathbb{Z}$ tels que $a = a'd$, $b = b'd$ et $(a', b') = 1$. D'après le théorème de Bézout, il existe deux entiers u et v tels que $a'u + b'v = 1$. En multipliant par d, on obtient $au + bv = d$. Donc $(a, b) \mid d$. Mais d divise a et b donc aussi (a, b). D'où $d = (a, b)$ (car d et (a, b) sont positifs). □

1.2.2 Lemme de Gauss

Proposition 1.17 (Lemme de Gauss)**.** *Soient a, b, c non nuls. Si $a \mid bc$ et $(a, b) = 1$ alors $a \mid c$.*

Démonstration. Comme $au + bv = 1$ pour certains u, v, on a $auc + bvc = c$. Or $a \mid auc$ et $a \mid bvc$ donc $a \mid c$. □

Proposition 1.18. *Si $(a_i, b) = 1$ pour $i = 1, \ldots, n$ alors $(a_1 \cdots a_n, b) = 1$.*

Proposition 1.19. *Si $a_1, \ldots, a_n$ sont premiers entre eux deux à deux, et si $a_i \mid b$ pour tout i alors $a_1 \cdots a_n \mid b$.*

Démonstration. Si $(a_1, a_2) = 1$, $a_1 \mid b$ et $a_2 \mid b$ alors $a_1 a_2 \mid b a_2$ et $a_1 a_2 \mid b a_1$ donc

$$a_1 a_2 \mid (b a_1, b a_2) = b(a_1, a_2) = b.$$

Si $(a_1, a_3) = (a_2, a_3) = 1$ alors par la Proposition 1.18 on a $(a_1 a_2, a_3) = 1$ etc. □

1.2.3 Lemme d'Euclide

Lemme 1.20. *Soient p un nombre premier et a un entier non nul. Alors soit $p \mid a$, soit $(a, p) = 1$.*

Démonstration. Soit $d = (a, p)$. Alors $d = 1$ ou $d = p$ car p est un nombre premier. Le premier cas correspond à $(a, p) = 1$, le second à $p \mid a$. □

Proposition 1.21 (Lemme d'Euclide)**.** *Soient p un nombre premier et a, b deux entiers non nuls. Si $p \mid ab$ alors $p \mid a$ ou $p \mid b$.*

Démonstration. Soient p un nombre premier et $a, b \in \mathbb{Z}^*$ tels que $p \mid ab$. Si p ne divise pas a alors d'après le Lemme 1.20, $(a, p) = 1$. D'après le lemme de Gauss, p divise alors b. □

Lemme 1.22. *Si p premier divise $a_1 \cdots a_n$ alors p divise au moins l'un des a_i.*

Donnons une application du lemme d'Euclide. Rappelons le coefficient binomial,

$$\binom{p}{k} = C_p^k = \frac{p!}{k!(p-k)!}$$

avec $n! = n(n-1) \cdots 2 \cdot 1$ pour $n \geq 1$ et $0! = 1$.

Proposition 1.23. *Soit p un nombre premier. Pour tout $k \in \{1, \ldots, p-1\}$, on a $p \mid \binom{p}{k}$.*

Démonstration. On a :

$$\frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{k!}.$$

Donc $p(p-1)\cdots(p-k+1) = k! \frac{p!}{k!(p-k)!}$. Comme $\frac{p!}{k!(p-k)!} \in \mathbb{N}^*$, $p \mid k! \frac{p!}{k!(p-k)!}$. Or p est premier, et $1 \leq k \leq p-1$, donc $p \nmid k!$, $(k!, p) = 1$ d'après le Lemme 1.20. Alors $p \mid \frac{p!}{k!(p-k)!}$ d'après le lemme d'Euclide. □

1.2.4 Équations diophantiennes linéaires

Le résultat suivant décrit l'ensemble des solutions dans une relation de Bézout (c'est une *équation diophantienne*).

Proposition 1.24. *Soient a et b deux entiers non nuls premiers entre eux. Soit (x_0, y_0) une solution particulière de l'équation à inconnues entières :*

$$(E): \quad ax + by = 1.$$

(Une telle solution existe d'après le théorème de Bézout). Alors les solutions de (E) sont données par

$$\begin{cases} x = x_0 + kb \\ y = y_0 - ka \end{cases} \quad \text{avec } k \in \mathbb{Z}.$$

Démonstration. On vient de voir que l'algorithme d'Euclide permet de trouver une solution particulière (x_0, y_0). Tout d'abord on vérifie facilement que pour tout $k \in \mathbb{Z}$, (x_0+kb, y_0-ka) est solution de (E) : $a(x_0 + kb) + b(y_0 - ka) = ax_0 + akb + by_0 - bka = ax_0 + by_0 = 1$. Montrons maintenant qu'il n'y en a pas d'autre. Soit (x, y) une solution de (E). On a alors $1 = ax_0 + by_0 = ax + by$. On en déduit que $a(x - x_0) = b(y_0 - y)$. Donc $a \mid b(y_0 - y)$. Or $(a, b) = 1$ donc $a \mid (y_0 - y)$ d'après le lemme de Gauss. Il existe $k \in \mathbb{Z}$ tel que $y_0 - y = ka$. On a alors $a(x - x_0) = bka$, d'où $x - x_0 = kb$ (vu que $a \neq 0$). On obtient donc $x = x_0 + kb$ et $y = y_0 - ka$, ce qui fallait montrer. □

Montrons sur un exemple comment trouver toutes les solutions d'une telle équation.

Exemple. Soit $c \in \mathbb{Z}$. Trouver tous les $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ tels que

$$931x + 513y = c.$$

Si c n'est pas un multiple de $19 = (931, 513)$ alors l'équation n'a pas de solution. Supposons donc $c = 19c'$, $c' \in \mathbb{Z}$. L'équation équivaut à $49x + 27y = c'$. Puisque $49 \times (-11) + 27 \times 20 = 1$ (voir l'exemple donné pour l'algorithme d'Euclide), les solutions sont les couples $(-11c' + 27k, 20c' - 49k)$, où $k \in \mathbb{Z}$.

1.2.5 pgcd de plusieurs entiers

Définition 1.5. Le pgcd de n entiers non nuls $a_1, \ldots, a_n$ est le plus grand entier positif qui divise $a_1, \ldots, a_n$. On le note $pgcd(a_1, \ldots, a_n)$ ou plus simplement $(a_1, \ldots, a_n)$.

Proposition 1.25. *L'ensemble $I = \{k_1a_1 + \cdots + k_na_n : k_1, \ldots, k_n \in \mathbb{Z}\} = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$ est un idéal de $\mathbb{Z}$ et engendré par $(a_1, \ldots, a_n)$.*

Démonstration. Par itération de la Proposition 1.12. □

1.2.6 Théorème fondamental de l'arithmétique

Le théorème fondamental de l'arithmétique décrit la décomposition en facteurs premiers des entiers.

Proposition 1.26 (Théorème fondamental de l'arithmétique)**.** *Soit $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Il existe $u \in \{-1, 1\}$ et k nombres premiers positifs $p_1, \ldots, p_k$ tels que*

$$n = up_1 \ldots p_k.$$

De plus cette décomposition est unique à l'ordre des nombres premiers p_i près.

Remarque. En rassemblant les nombres premiers identiques dans la décomposition de n et en réindexant, on obtient $n = up_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, où $p_1, \ldots, p_s$ sont des nombres premiers deux à deux distincts et $\alpha_1, \ldots, \alpha_s$ sont des entiers strictement positifs.

Démonstration. Montrons l'existence et l'unicité de cette écriture.

— Existence : On suppose que $n \geq 2$. Si n est premier, la décomposition en facteurs premiers est évidente, $n = n$. Si n n'est pas premier, alors il possède un diviseur premier positif p_1. On a alors $n = p_1 n_1$ avec $n_1 \geq 2$. Si n_1 n'est pas premier, il possède un diviseur premier p_2 et ainsi $n_1 = p_2 n_2$ avec $n_2 \geq 2$. D'où $n = p_1 p_2 n_2$. On construit ainsi une suite strictement décroissante d'entiers > 1 : $n_1 > n_2 > \ldots > n_i > \ldots$ (car $n/p_1 > n/(p_1 p_2) > \ldots > n/(p_1 p_2 \cdots p_i) > \ldots$). Cette suite est donc finie. C'est-à-dire qu'au bout d'un nombre fini d'étapes, le nombre $n_k = n/(p_1 p_2 \cdots p_k)$ obtenu est un nombre premier, $n_k = p$. On obtient alors $n = p_1 \cdots p_k p$.

Si $n \leq -2$, on applique ce qui précède à $-n$.

— Unicité : On suppose que n admet les deux décompositions suivantes

$$n = up_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} = vq_1^{\beta_1} \cdots q_t^{\beta_t},$$

où $u, v \in \{-1, 1\}$, $p_1, \ldots, p_s$ sont des nombres premiers deux à deux distincts, $q_1, \ldots, q_t$ sont également des nombres premiers deux à deux distincts, $\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t$ sont dans $\mathbb{N}^*$. Si $n \geq 2$ alors $u = v = 1$, si n est négatif alors $u = v = -1$. Chaque nombre premier p_i divise $q_1^{\beta_1} \cdots q_t^{\beta_t}$, donc d'après le lemme d'Euclide, p_i divise l'un des q_j. D'où $p_i = q_j$. Réciproquement on vérifie de la même façon que chaque q_j est un p_i. Donc $s = t$. En réindexant les nombres premiers dans le second membre, on arrive à l'égalité :

$$p_1^{\alpha_1} \cdots p_s^{\alpha_s} = p_1^{\beta_1} \cdots p_s^{\beta_s}.$$

Supposons que $\alpha_1 \geq \beta_1$. En divisant par p^{β_1} les deux membres, on trouve

$$p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} = p_2^{\beta_2} \cdots p_s^{\beta_s}.$$

Donc $p_1^{\alpha_1 - \beta_1}$ divise $p_2^{\beta_2} \cdots p_s^{\beta_s}$. Si $\alpha_1 - \beta_1 \geq 1$, alors d'après le lemme d'Euclide, p_1 divise p_2 ou p_3 … ou p_s ce qui est impossible car les p_i sont des nombres premiers distincts deux à deux. Donc $\alpha_1 = \beta_1$ En faisant le même raisonnement pour chaque $1 \leq i \leq s$, on montre que $\alpha_i = \beta_i$. La décomposition est donc unique à l'ordre des p_i près.

□

1.2.7 Valuation p-adique

Définition 1.6. Soient $n \in \mathbb{Z}^*$ et p un nombre premier positif. La *valuation p-adique de n* est le plus grand entier k tel que $p^k \mid n$. On la note $v_p(n)$. Si $n = 0$, on convient que $v_p(0) = +\infty$ pour tout nombre premier p.

Exemple. $v_2(23) = 0$, $v_2(24) = 3$, $v_2(32) = 5$, $v_2(2^n) = n$ pour $n \in \mathbb{N}^*$.

Proposition 1.27. *Pour $n \in \mathbb{N}^*$ on a les équivalences :*

$$v_p(n) = k \iff p^k \mid n \text{ et } p^{k+1} \nmid n,$$

$$v_p(n) = 0 \iff p \text{ ne divise pas } n.$$

Remarque. (i) Si n non nul se décompose sous la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, alors $v_{p_i}(n) = \alpha_i$ pour tout $1 \leq i \leq s$. En particulier, $v_p(n) = 0$ sauf pour un nombre fini de nombres premiers p.

(ii) Pour $n = \pm 1$, $v_p(1) = v_p(-1) = 0$.

(iii) En rappelant que $\mathcal{P}$ est l'ensemble de tous les nombres premiers positifs, on a l'écriture

$$n = u \prod_{p \in \mathcal{P}} p^{v_p(n)} \text{ avec } u = \pm 1.$$

Proposition 1.28. *Soient m et n deux entiers non nuls. Alors*

$$n \mid m \iff \forall p \in \mathcal{P},\ v_p(n) \leq v_p(m).$$

Proposition 1.29. *Soient m et n deux entiers non nuls alors*

$$(m, n) = \prod_{p \in \mathcal{P}} p^{\nu_p},$$

où pour tout $p \in \mathcal{P}$, $\nu_p = \min(v_p(m), v_p(n))$.

Proposition 1.30. *Soient m et n deux entiers. On a, pour tout nombre premier p :*

$$v_p(mn) = v_p(m) + v_p(n), \qquad v_p(m+n) \geq \min(v_p(m), v_p(n))$$

et la dernière inégalité est une égalité dès que $v_p(m) \neq v_p(n)$.

1.2.8 ppcm

Définition 1.7. Soient a et b deux entiers non nuls. Le *ppcm* (plus petit commun multiple) de a et b est le plus petit entier strictement positif multiple à la fois de a et b. On le note $ppcm(a, b)$ ou encore $[a, b]$.

Remarque. Plus généralement, le ppcm de n entiers non nuls $a_1, \ldots, a_n$ est le plus petit commun multiple de $a_1, \ldots, a_n$ noté $ppcm(a_1, \ldots, a_n)$ ou plus simplement $[a_1, \ldots, a_n]$. L'ensemble $I = a_1\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z}$ est un idéal de $\mathbb{Z}$ et engendré par $[a_1, \ldots, a_n]$.

Proposition 1.31.

$$m = [a, b] \iff \begin{cases} m \in \mathbb{N}^*, \\ a \mid m \text{ et } b \mid m, \\ \forall c \in \mathbb{N}, a \mid c \text{ et } b \mid c \Rightarrow m \leq c. \end{cases}$$

Proposition 1.32. *Soient $a, b \in \mathbb{Z}^*$. On a $a\mathbb{Z} \cap b\mathbb{Z} = [a, b]\mathbb{Z}$.*

Démonstration. Soit q le générateur positif de $a\mathbb{Z} \cap b\mathbb{Z}$. Alors q est un multiple de a et de b. Si $c \geq 0$ est un multiple commun à a et b, alors $c \in a\mathbb{Z} \cap b\mathbb{Z} = q\mathbb{Z}$. Donc $q \mid c$ et ainsi $q \leq c$. Cela prouve que $q = [a, b]$. □

Proposition 1.33. *Soient m et n deux entiers non nuls. Alors*

$$[m, n] = \prod_{p \in \mathcal{P}} p^{c_p}$$

où pour tout $p \in \mathcal{P}$, $c_p = \max(v_p(m), v_p(n))$.

Démonstration. Cela découle de la Proposition 1.28. □

Proposition 1.34. *Soient m et n deux entiers non nuls. Si m et n sont de même signe, alors*

$$[m, n](m, n) = mn.$$

Démonstration. On remarque que $\max(x, y) + \min(x, y) = x + y$ pour tous $x, y \in \mathbb{R}$, en particulier, par la Proposition 1.30,

$$\max(v_p(m), v_p(n)) + \min(v_p(m), v_p(n)) = v_p(m) + v_p(n) = v_p(mn).$$

□

1.3 Congruences

1.3.1 Relations d'équivalence, ensembles quotients

Définition 1.8. Soient E un ensemble et $\mathcal{R}$ une relation sur E (entre deux éléments de E). On dit que $\mathcal{R}$ est une *relation d'équivalence* sur E si elle vérifie les trois conditions suivantes :

(i) $\mathcal{R}$ est réflexive : $\forall x \in E,\ x\mathcal{R}x$;

(ii) $\mathcal{R}$ est symétrique : $\forall x, y \in E,\ x\mathcal{R}y \Rightarrow y\mathcal{R}x$;

(iii) $\mathcal{R}$ est transitive : $\forall x, y, z \in E,\ x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z$.

Exemple. Les relations suivantes sont des relations d'équivalence :

(i) Dans $\mathbb{R}^2 \setminus \{(0,0)\}$, $\vec{u}\ \mathcal{R}\ \vec{v} \Longleftrightarrow \exists \lambda \in \mathbb{R}^*$ tel que $\vec{u} = \lambda \vec{v}$.

(ii) Dans $\mathbb{Z} \times \mathbb{Z} \setminus \{(0,0)\}$, $(a,b)\mathcal{R}(a',b') \Longleftrightarrow ab' = a'b$.

Définition 1.9. Soient E un ensemble non vide et $(E_i)_{i\in I}$ une famille de sous-ensembles de E. On dit que $(E_i)_{i\in I}$ est une *partition* de E si et seulement si les trois conditions suivantes sont vérifiées :

(i) $\forall i \in I,\ E_i \neq \emptyset$;

(ii) $\forall i, j \in I,\ E_i \cap E_j = \emptyset$ si $i \neq j$;

(iii) $E = \cup_{i\in I} E_i$.

Définition 1.10. Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$. Soit $x \in E$. La *classe d'équivalence* de x pour la relation $\mathcal{R}$ est le sous-ensemble de E défini par

$$\overline{x} = \{y \in E\ :\ y\mathcal{R}x\}.$$

Tout élément de $\overline{x}$ est appelé un *représentant de la classe d'équivalence* $\overline{x}$.

Proposition 1.35. *Pour tous $x, y \in E$, on a les propriétés suivantes :*

(i) $x \in \overline{x}$;

(ii) $y \in \overline{x} \iff (y\mathcal{R}x \Rightarrow x \in \bar{y}) \iff \overline{x} = \overline{y}$.

De plus la famille des classes d'équivalence pour la relation $\mathcal{R}$ est une partition de E.

Démonstration. On montre que la famille des classes d'équivalence forme une partition de E. Tout d'abord, pour tout $x \in E$, $x \in \overline{x}$ donc $\overline{x} \neq \emptyset$.
Soient $x, y \in E$ tels que $\overline{x} \cap \overline{y} \neq \emptyset$. Il existe alors $z \in \overline{x} \cap \overline{y}$. Ce z vérifie $z\mathcal{R}x$ et $z\mathcal{R}y$. On en déduit par transitivité de $\mathcal{R}$ que $x\mathcal{R}y$ et ainsi $\overline{x} = \overline{y}$. Les classes d'équivalence sont bien deux à deux disjointes. Enfin E est bien la réunion de toutes les classes d'équivalence puisque $x \in \overline{x}$, $\forall x \in E$. □

Définition 1.11. Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$.

(i) On appelle *système de représentants* de la relation $\mathcal{R}$ toute famille $(x_i)_{i\in I}$ d'éléments de E vérifiant :

(a) $\forall x \in E$, $\exists i \in I$ tel que $x \in \overline{x_i}$;

(b) $\overline{x_i} \cap \overline{x_j} = \emptyset$ pour tous $i, j \in I$ tels que $i \neq j$.

(ii) On appelle *ensemble quotient* de E par $\mathcal{R}$ et on note $E/\mathcal{R}$ l'ensemble des classes d'équivalence de E : $E/\mathcal{R} = \{\overline{x},\ x \in E\}$.

Remarque. Si $(x_i)_{i\in I}$ est un système de représentants de $\mathcal{R}$, on a en fait

$$E/\mathcal{R} = \{\overline{x_i},\ i \in I\} \quad \text{et} \quad \#(E/\mathcal{R}) = \#(I).$$

Exemple. On reprend les exemples donnés après la Définition 1.8.

(i) Les classes d'équivalence sont les droites vectorielles privées de l'origine $\mathbb{R}\vec{u} \setminus \{\vec{0}\}$ pour tout $\vec{u} \neq \vec{0}$. L'ensemble quotient est noté $\mathbb{P}_1(\mathbb{R})$ et est appelé *espace projectif réel de dimension* 1.

(ii) Les classes d'équivalences sont les fractions $\frac{a}{b}$ d'entiers. L'ensemble quotient est $\mathbb{Q}$.

1.3.2 Congruences dans $\mathbb{Z}$

Définition 1.12. Soient $n \in \mathbb{Z}^*$ et $a, b \in \mathbb{Z}$. Si n divise $b - a$, alors on dit que b *est congru à a modulo n* et on note $a \equiv b \pmod{n}$. On dit aussi que a *est un résidu de b modulo n*. La relation ainsi définie est une *congruence modulo n*.

Remarque. Si $n \mid (b - a)$ alors $-n \mid (b - a)$. On peut donc se limiter à étudier des congruences modulo des entiers naturels.

Proposition 1.36. *La relation de congruence modulo n est une relation d'équivalence.*

Notation. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence.

Proposition 1.37. *$a \equiv b \pmod{n}$ si et seulement si a et b ont le même reste dans la division euclidienne par n.*

Démonstration. Si $a = qn + r$ avec $0 \leq r < n$, alors $a \equiv r \pmod{n}$. De même si $b = q'n + r'$ alors $b \equiv r' \pmod{n}$. Par transitivité de la relation d'équivalence, $a \equiv b \pmod{n} \Rightarrow r \equiv r' \pmod{n}$. Mais $n \mid r - r' \Rightarrow r = r'$ puisque $0 \leq |r - r'| < n$. Réciproquement, si $r = r'$, on vérifie que $a \equiv b \pmod{n}$ par transitivité de la congruence modulo n. □

Proposition 1.38. *Pour tout $a \in \mathbb{Z}$,*

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{a}, \overline{a+1}, \ldots, \overline{a+n-1}\}.$$

En particulier les nombres $\{0, 1, \ldots, n-1\}$ constituent un système (complet) de représentants de la congruence modulo n et $\#\mathbb{Z}/n\mathbb{Z} = n$.

Démonstration. Soit $x \in \mathbb{Z}$ et soit $r \in \{0, \ldots, n-1\}$ le reste de x par la division euclidienne par n. Alors $x \equiv r \pmod{n}$, autrement dit, $x \in \overline{r}$. De plus si $0 \leq r, r' < n$ et $r \neq r'$ alors $\overline{r} \cap \overline{r'} = \emptyset$ vu que $n \nmid r - r'$. On en déduit que $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ et que $\#(\mathbb{Z}/n\mathbb{Z}) = n$. Soit $a \in \mathbb{Z}$. Vérifions que $\overline{a}, \overline{a+1}, \ldots, \overline{a+n-1}$ sont deux à deux distincts. Soient $i, j \in \{0, \ldots, n-1\}$ tels que $\overline{a+i} = \overline{a+j}$. Alors $a + i \equiv a + j \pmod{n}$, et ainsi $n \mid i - j$, ce qui implique que $i = j$. Les ensembles $\overline{a+i}$, $0 \leq i \leq n-1$, sont deux à deux distincts. On en déduit que $\mathbb{Z}/n\mathbb{Z} = \{\overline{a}, \ldots, \overline{a+n-1}\}$ puisque $\#(\mathbb{Z}/n\mathbb{Z}) = n$. □

Exemple. $\{-7, 4, 12\}$ est un système de représentants de la congruence modulo 3 car $-7 \equiv 2 \pmod{3}$, $4 \equiv 1 \pmod{3}$, $12 \equiv 0 \pmod{3}$.

1.3.3 Compatibilité avec les opérations usuelles

Montrons maintenant que la congruence est compatible avec les opérations usuelles de $\mathbb{Z}$.

Proposition 1.39. *Soient $n \in \mathbb{N}^*$ et $a, b, a', b' \in \mathbb{Z}$. Soient $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$. Alors*

$$a + b \equiv a' + b' \pmod{n}, \qquad ab \equiv a'b' \pmod{n}.$$

Remarque. On peut exprimer cette équivalence sous la forme :

$$\overline{a} = \overline{a'} \text{ et } \overline{b} = \overline{b'} \quad \Rightarrow \quad \overline{a+b} = \overline{a'+b'} \text{ et } \overline{ab} = \overline{a'b'}.$$

Démonstration. Si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$ alors il existe deux entiers k, ℓ tels que $a = a' + kn$ et $b = b' + \ell n$. Alors $a + b = a' + b' + (k + \ell)n \equiv a' + b' \pmod{n}$ et $ab = a'b' + (a'\ell + b'k + k\ell n)n \equiv a'b' \pmod{n}$. □

Remarque. Pour effectuer une séquence d'opérations dans $\mathbb{Z}/n\mathbb{Z}$, on a intérêt à chaque étape de réduire modulo n, c'est-à-dire de travailler avec *des représentants petits* afin de réduire les calculs.

Proposition 1.40. *On peut définir une addition et une multiplication sur $\mathbb{Z}/n\mathbb{Z}$ de la façon suivante : Soient $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$. Soient $a, b \in \mathbb{Z}$ tels que $\alpha = \overline{a}$ et $\beta = \overline{b}$. On pose alors*

$$\alpha + \beta = \overline{a} + \overline{b} = \overline{a+b} \text{ et } \alpha\beta = \overline{a} \cdot \overline{b} = \overline{ab}.$$

Ces deux opérations sont bien définies et ne dépendent pas des choix des représentants a et b d'après la Proposition 1.39.

Remarque. On peut multiplier les éléments de $\mathbb{Z}/n\mathbb{Z}$ par des entiers de la manière suivante : soient $\alpha = \overline{a} \in \mathbb{Z}/n\mathbb{Z}$ et $k \in \mathbb{Z}$. Si $k \geq 0$, on a $k\alpha = k\overline{a} = \underbrace{\overline{a} + \cdots + \overline{a}}_{k \text{ fois}}$ et si $k \leq 0$, $k\overline{a} = -(-k)\overline{a}$ (avec $-\overline{u} = \overline{-u}$). On a alors $k\overline{a} = \overline{ka}$.

Exemple. Tables d'addition et de multiplication de $\mathbb{Z}/5\mathbb{Z}$ et de $\mathbb{Z}/6\mathbb{Z}$.

1.3.4 Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geq 2$ un entier.

Définition 1.13. Un élément $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est dit *inversible* s'il existe $\overline{a'} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{a}\overline{a'} = \overline{1}$. On note $(\mathbb{Z}/n\mathbb{Z})^*$ *l'ensemble des éléments inversibles* de $\mathbb{Z}/n\mathbb{Z}$. On notera $\overline{x}^{-1}$ l'inverse de $\overline{x}$.

Remarque. Attention, $(\mathbb{Z}/n\mathbb{Z})^*$ ne signifie pas $(\mathbb{Z}/n\mathbb{Z}) \setminus \{\overline{0}\}$. Le symbole"$*$" est donc à double sens ("enlever 0 de l'ensemble", "éléments inversibles" de l'ensemble), il faut tenir compte du contexte.

Proposition 1.41. *$\overline{1}$ est inversible d'inverse lui-même. Si $\overline{a}$ et $\overline{b} \in (\mathbb{Z}/n\mathbb{Z})^*$ alors $\overline{ab} \in (\mathbb{Z}/n\mathbb{Z})^*$ et a pour inverse $\overline{a}^{-1}\overline{b}^{-1}$.*

Proposition 1.42. *Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. Alors $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $(a, n) = 1$.*

Démonstration. Si $\overline{a}$ est inversible, alors il existe $b \in \mathbb{Z}$ tels que $\overline{a} \cdot \overline{b} = \overline{1}$. Donc il existe $k \in \mathbb{Z}$ tel que $ab = 1 + kn$ ou encore tel que $1 = kn - ab$. On en déduit que $(a, n) = 1$ d'après le théorème de Bézout. Réciproquement, si $(a, n) = 1$, alors encore d'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $au + vn = 1$. Donc $\overline{a} \cdot \overline{u} + \overline{vn} = \overline{1}$, *i.e.*, $\overline{a} \cdot \overline{u} = \overline{1}$. Donc $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$. □

Remarque. (i) Un ensemble de représentants des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est donc

$$\{a \ : \ 1 \leq a \leq n-1, \ (a, n) = 1\}.$$

Parfois on utilise tout simplement ces valeurs de a à la place de $\overline{a}$ et on dit $a \in \mathbb{Z}/n\mathbb{Z}$.

(ii) Si a et n sont grands, l'algorithme d'Euclide et la relation de Bézout permettent de trouver u (et v) tel que $au + nv = 1$ et nous pouvons choisir $b = u$ qui est donc l'inverse de $a \pmod n$. Reprenons l'exemple $49 \times (-11) + 27 \times 20 = 1$ étudié avant. Si $a = 49$ et $n = 27$, alors cette relation nous donne $\overline{49}^{-1} = \overline{-11} = 9$ dans $\mathbb{Z}/20\mathbb{Z}$ (vérification : $49 \times 9 = 441 \equiv 1 \pmod{20}$).

Exemple. L'ensemble des éléments inversibles de $\mathbb{Z}/5\mathbb{Z}$ est $\{1, 2, 3, 4\}$. L'ensemble des éléments inversibles de $\mathbb{Z}/6\mathbb{Z}$ est $\{1, 5\}$.

1.3.5 Le petit théorème de Fermat

Proposition 1.43 (Petit théorème de Fermat)**.** *Soient p un nombre premier et a un entier non divisible par p. On a alors*

$$a^{p-1} \equiv 1 \pmod{p}.$$

On a la formulation équivalente dans $\mathbb{Z}/p\mathbb{Z}$:

$$\overline{a} \neq \overline{0} \quad \Longrightarrow \quad \overline{a}^{p-1} = \overline{1}.$$

On commence par établir le lemme suivant.

Lemme 1.44. *Si $a, b \in \mathbb{N}^*$ sont premiers entre eux, alors*

$$\mathbb{Z}/b\mathbb{Z} \setminus \{0\} = \{\overline{a}, \overline{2a}, \ldots, \overline{(b-1)a}\}.$$

Démonstration. Pour montrer cela, il suffit de vérifier que les classes $\overline{ka}$, $1 \leq k \leq b-1$ ne sont pas nulles et sont deux à deux distinctes. Si $\overline{ka} = \overline{0}$ pour un $k \in \{1, \ldots, b-1\}$, alors $b \mid ka$ ce qui n'est possible car $(a, b) = 1$ et $b \nmid k$. Les classes sont donc différentes de la classe nulle. Soient $1 \leq k, \ell \leq b-1$ tels que $\overline{ka} = \overline{\ell a}$. Alors $b \mid a(k-\ell)$ donc $b \mid (k-\ell)$ puisque $(a, b) = 1$. Cela entraîne que $k = \ell$ puisque $|k - \ell| < b$. □

Démonstration de la Proposition 1.43. Soient p un nombre premier et $a \in \mathbb{Z}$ tel que $p \nmid a$. Donc $(a, p) = 1$. D'après le Lemme 1.44,

$$\mathbb{Z}/p\mathbb{Z} \setminus \{0\} = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}.$$

Mais on a également

$$\mathbb{Z}/p\mathbb{Z} \setminus \{0\} = \{\overline{1}, \overline{2}, \ldots, \overline{(p-1)}\}.$$

On en déduit

$$\overline{a} \cdot \overline{2a} \cdots \overline{(p-1)a} = \overline{1} \cdot \overline{2} \cdots \overline{(p-1)}, \tag{1.1}$$

c'est-à-dire

$$\overline{(p-1)!}\, \overline{a}^{p-1} = \overline{(p-1)!}.$$

Mais p ne divise pas $(p-1)!$ car il est premier. Donc $\overline{(p-1)!} \neq \overline{0}$. Il est donc inversible dans $\mathbb{Z}/p\mathbb{Z}$. En multipliant (1.1) par cet inverse, on en déduit que $\overline{a}^{p-1} = \overline{1}$. □

Remarque. Si $a^{n-1} \not\equiv 1 \pmod{n}$ alors n est composé. Exemple : $2^5 \equiv 2 \pmod{6}$.

Corollaire 1.45. *Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$, on a dans $\mathbb{Z}/p\mathbb{Z}$:*

$$\overline{a}^p = \overline{a}.$$

Démonstration. Si $\overline{a} = \overline{0}$ alors $\overline{a}^p = \overline{0} = \overline{a}$. Si $(a, p) = 1$, on applique le petit théorème de Fermat, $\overline{a}^{p-1} = \overline{1}$ puis on multiplie cette égalité par $\overline{a}$. □

1.3.6 Théorème des restes chinois

En fin, montrons un cas particulier du *théorème des restes chinois*. Le théorème général sera montré plus tard (en L2).

Proposition 1.46 (Théorème des restes chinois)**.** *Soient m et n tels que $(m,n)=1$. Alors pour tous $a,b\in\mathbb{Z}$ le système de congruences*

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

possède des solutions dans $\mathbb{Z}$. Elles sont de la forme x_0+kmn où x_0 est une solution particulière et k décrit $\mathbb{Z}$. Réciproquement, si pour tous $a,b\in\mathbb{Z}$, le système de congruences possède des solutions dans $\mathbb{Z}$, alors $(m,n)=1$.

Démonstration. Résoudre le système revient à chercher des entiers k et ℓ tels que $a+km=b+\ell n$ c'est-à-dire tels que

$$km-\ell n=b-a.$$

Or $(m,n)=1$, d'après le théorème de Bézout, il existe $u,v\in\mathbb{Z}$ tels que $um+vn=1$. Ainsi,

$$k=u(b-a), \qquad \ell=-v(b-a)$$

fournissent une solution particulière

$$x_0=a+u(b-a)m=b-v(b-a)n.$$

Soit x une autre solution du système. Alors $x\equiv x_0 \pmod{m}$ et $x\equiv x_0 \pmod{n}$. Donc m et n divisent $x-x_0$. Comme $(m,n)=1$, cela implique que $mn \mid (x-x_0)$.
Réciproquement si le système possède des solutions pour tous a,b alors il en possède en particulier pour $a=1$ et $b=0$. Il existe $x\in\mathbb{Z}$ tel que $x\equiv 1 \pmod{n}$ et $x\equiv 0 \pmod{m}$. Donc il existe $k,\ell\in\mathbb{Z}$ tels que

$$x=1+kn=\ell m.$$

Donc $\ell m-kn=1$, on en déduit que $(m,n)=1$.

□

Chapitre 2

Polynômes et leur arithmétique

2.1 Les anneaux

Avant de développer la théorie de l'arithmétique des polynômes nous avons besoin de certains prérequis d'algèbre, notamment de la notion d'un *anneau* et d'un *corps*. Un cours d'algèbre abstrait sera donné en L2. Certaines notions seront abordées en algèbre linéaire 1 ce semestre.

2.1.1 Définition

Définition 2.1. Un *anneau* est un ensemble non vide A muni de deux lois internes "+" et "$\cdot$" appelées *addition* et *multiplication*, vérifiant les conditions suivantes pour tous $x, y, z \in A$:

(i) $x + y = y + x$: l'addition est commutative ;

(ii) $(x + y) + z = x + (y + z)$: l'addition est associative ;

(iii) il existe un élément neutre pour l'addition noté 0_A : pour tout $x \in A$, $0_A + x = x + 0_A = x$;

(iv) tout $x \in A$ admet un opposé noté $-x$ appartenant à A tel que $x + (-x) = (-x) + x = 0_A$;

(v) $(xy)z = x(yz)$: la multiplication est associative ;

(vi) $(x + y)z = xz + yz$ et $z(x + y) = zx + zy$: la multiplication est distributive à gauche et à droite par rapport à l'addition ;

(vii) il existe un élément neutre pour la multiplication noté 1_A : $\forall x \in A$, $1_A \cdot x = x \cdot 1_A = x$.

Si de plus la multiplication est commutative, on dit que A est un *anneau commutatif*.

Remarque. Les conditions (ii)–(iv) disent que A est un *groupe* avec la loi "+" et la condition (i) implique que le groupe est *commutatif* (*groupe commutatif* ou *groupe abélien*).

Exemple.
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}$ sont des anneaux commutatifs.
- $\mathbb{N}$ n'est pas un anneau (par exemple l'entier naturel 2 n'a pas d'opposé dans $\mathbb{N}$).
- $\mathbb{Z}[i] := \{a + ib : a, b \in \mathbb{Z}\}$ où $i = \sqrt{-1}$ est un anneau commutatif. On l'appelle *l'anneau des entiers de Gauss*.
- $\mathbb{R}[X]$, l'ensemble des polynômes à coefficients réels est un anneau commutatif (voir plus tard), idem pour $\mathbb{Q}[X]$ et $\mathbb{C}[X]$.

— $M_n(\mathbb{R})$, l'ensemble des matrices carrées $n \times n$ à coefficients réels est un anneau qui n'est pas commutatif quand $n \geq 2$.

2.1.2 Diviseurs, éléments inversibles, anneaux intègres, corps

La notion de "divisibilité" recontrée et introduite pour $\mathbb{Z}$ dans le chapitre "Arithmétique élémentaire" se géneralise directement dans des structures des anneaux.

Définition 2.2. Soient A un anneau commutatif, $a, b \in A$. On dit que b *divise* a ou que a est un *multiple* de b s'il existe $c \in A$ tel que $a = bc$. On note alors $b \mid a$.

Définition 2.3. Soit A un anneau non nécessairement commutatif. On dit que $a \in A \setminus \{0_A\}$ est *un diviseur de* 0 *à gauche (resp. à droite)* s'il existe $b \in A \setminus \{0_A\}$ tel que $ab = 0_A$ (resp. $ba = 0_A$).

Exemple. (i) $M_n(\mathbb{R})$ possède des diviseurs de 0 :

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

(ii) De même $\mathbb{Z}/6\mathbb{Z}$ possède aussi des diviseurs de 0 comme le montre $\overline{2} \cdot \overline{3} = \overline{0}$. Plus généralement, $\mathbb{Z}/n\mathbb{Z}$ possède des diviseurs de 0 si et seulement si n n'est pas un nombre premier.

Définition 2.4. Un élément $a \in A$ est dit *inversible* dans A s'il existe $b \in A$ tel que $ab = ba = 1_A$. Cet élément b est alors unique et est appelé *inverse* de a. On le note a^{-1}. On notera A^* l'ensemble des éléments inversibles de A.

Remarque. Rappelons la remarque donnée avant pour $\mathbb{Z}/n\mathbb{Z}$: dans ce contexte A^* ne signifie pas $A \setminus \{0\}$ mais l'ensemble des éléments inversibles.

Exemple.
— $\mathbb{Z}^* = \{-1, 1\}$.
— $(\mathbb{R}[X])^*$ est l'ensemble des polynômes constants non nuls.
— $(M_n(\mathbb{R}))^*$ est l'ensemble des matrices de déterminant non nul.
— $(\mathbb{Z}[i])^* = \{1, -1, i, -i\}$ où $i = \sqrt{-1}$.
— $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a} : (a, n) = 1\}$.

Définition 2.5. Un *corps* est un anneau dont tous les éléments non nuls sont inversibles. Les éléments d'un corps $\mathbb{K}$ sont appelés *scalaires*.

Exemple. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps commutatifs ; $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.

Définition 2.6. Un anneau A est *intègre* s'il ne possède pas de diviseur de 0, c'est-à-dire

$$\forall x, y \in A, xy = 0_A \Rightarrow x = 0_A \text{ ou } y = 0_A.$$

Exemple. Tout corps est un anneau intègre, la réciproque est fausse : $\mathbb{Z}$ et $\mathbb{R}[X]$ sont des anneaux intègres mais ne sont pas des corps (par exemple l'entier 2 n'a pa d'inverse dans $\mathbb{Z}$; le polynôme X^2+1 n'a pas d'inverse dans $\mathbb{R}[X]$ etc.). $M_n(\mathbb{R})$ n'est pas intègre, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre si n n'est pas un nombre premier (si n n'est pas premier alors il existe $1 < a, b < n$ tels que $n = ab$ et nous avons $\overline{a}\overline{b} = \overline{n} = \overline{0}$).

Proposition 2.1. *Soit A un anneau intègre. On a alors :*

$$\forall x, y, z \in A, \quad xy = xz \text{ et } x \neq 0_A \quad \Rightarrow \quad y = z.$$

Démonstration. Si $xy = xz$ alors $x(y - z) = 0_A$. Or $x \neq 0_A$ et A est intègre, donc $y - z = 0_A$ et $y = z$. □

Remarque. Pour simplifier l'écriture, on note parfois plus simplement 0 à la place de 0_A.

Définition 2.7. La *caractéristique d'un anneau A* est le plus petit entier $n > 0$ tel que $n \cdot 1_A = 0_A$ si un tel entier existe. Si un tel entier n'existe pas, la caractéristique est nulle.

Exemple. $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{R}$ sont de caractéristique nulle, $\mathbb{Z}/p\mathbb{Z}$ (p premier) est de caractéristique p.

2.2 Polynômes à une indéterminée

Dans ce qui suit, nous désignons par $\mathbb{K}$ **un corps arbitraire** (caractéristique nulle ou > 0) et nous développons la théorie en toute généralité, notamment pour étudier les propriétés de divisibilité dans l'anneau de polynômes $\mathbb{K}[X]$ ou $\mathbb{K}$ est un corps arbitraire. Rappelons que des exemples des corps sont $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, les corps finis $\mathbb{Z}/p\mathbb{Z}$ (voir Section 2.1).

Définition 2.8. On appelle *polynôme* (*à une indéterminée et coefficients dans* $\mathbb{K}$), toute expression algébrique de la forme

$$P = a_p X^p + a_{p-1} X^{p-1} + \cdots + a_1 X + a_0,$$

avec $a_i \in \mathbb{K}$ pour tout $i \in \{0, \ldots, p\}$.

(i) Les scalaires a_i sont appelés *coefficients* du polynôme.

(ii) S'il existe, le plus grand indice i tel que $a_i \neq 0$ s'appelle *degré de* P et est noté $\deg P$.

(iii) Si tous les coefficients a_i sont nuls, P est appelé *polynôme nul* et est noté 0. Par convention, $\deg 0 = -\infty$.

(iv) Un polynôme de la forme $P = a_0$ avec $a_0 \in \mathbb{K}$ est appelé *polynôme constant*. Si $a_0 \neq 0$, son degré est 0.

(v) Les polynômes de la forme $P = a_p X^p$ sont appelés *monômes*.

(vi) Soit $P = a_p X^p + \cdots + a_0$ avec $a_p \neq 0$. On appelle *terme dominant* de P le monôme $a_p X^p$. Si le coefficient a_p du terme dominant est 1, on dit que P est un *polynôme unitaire*.

(vii) L'ensemble des polynômes à une indéterminée et coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$.

(viii) On note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.

Remarque. $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}$ dont la famille $1, X, \ldots, X^n$ forme une base appelée base canonique de $\mathbb{K}_n[X]$ (voir cours d'algèbre linéaire 1).

Exemple. (i) $P = X^3 - 2X + 1$ est un polynôme de degré 3.

(ii) $P = 1$ est un polynôme de degré 0.

(iii) Si $n \in \mathbb{N}^*$, $P = X^n - 1$ est un polynôme de degré n.

Si P appartient à $\mathbb{K}[X]$, on peut l'*évaluer* en tout nombre x de $\mathbb{K}$. On associe donc à P une fonction polynomiale $\tilde{P}$:

Définition 2.9. Pour $P = a_p X^p + a_{p-1} X^{p-1} + \cdots + a_1 X + a_0$ un polynôme de $\mathbb{K}[X]$, la *fonction polynomiale associée à* P est l'application $\tilde{P}$ définie par

$$\tilde{P} : \mathbb{K} \to \mathbb{K}, \quad x \mapsto a_p x^p + a_{p-1} x^{p-1} + \cdots + a_1 x + a_0.$$

Remarque. Nous **ne pouvons pas**, en général, identifier *polynôme* et *fonction polynomiale*. Si on travaille sur un corps infini (tels que $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$), on ne s'expose pas à des risques majeurs quand on identifie *polynôme* et *fonction polynomiale* mais prenons par exemple le polynôme $P = \overline{1}X + \overline{1}X^2$

de $\mathbb{Z}/2\mathbb{Z}[X]$. P est évidemment pas le polynôme 0. Pourtant si on regarde non le polynôme mais la fonction polynomiale $x \mapsto x + x^2$, sa valeur en $\overline{0}$ est $\overline{1}\,\overline{0} + \overline{1}\,\overline{0}^2 = \overline{0} + \overline{0} = \overline{0}$ et sa valeur en $\overline{1}$ est $\overline{1}\,\overline{1} + \overline{1}\,\overline{1}^2 = \overline{1} + \overline{1} = \overline{0}$ donc c'est bien la fonction polynomiale nulle. Ce n'est donc pas du tout de celle-ci que l'on parle quand on évoque le polynôme $X + X^2$.

Remarque.
- Si A est un anneau intègre (en particulier si A est un corps), alors $A[X]$ est intègre.
- Nous serons amenés par la suite à additionner des degrés de polynômes. Comme l'application deg est à valeurs dans $\mathbb{N} \cup \{-\infty\}$, il faut étendre la définition de l'addition. On adopte la convention suivante pour $n \in \mathbb{N} \cup \{-\infty\}$: $-\infty + n = -\infty$.
- Tout polynôme est une somme finie de monômes.
- On adopte la convention que l'on ne change pas un polynôme P en lui ajoutant un ou plusieurs monômes à coefficients nuls. Par exemple, on ne fera pas la distinction entre $X^3 - 2X + 1$ et $0X^4 + X^3 + 0X^2 - 2X + 1$.

Remarque. Un polynôme P à coefficients dans $\mathbb{K}$ peut donc être interpretée comme "suite $(a_n)_{n\in\mathbb{N}}$ indexée sur $\mathbb{N}$ d'éléments de $\mathbb{K}$ (les coefficients de P) tous nuls sauf un nombre fini". En effet, cette interpretation peut aussi servir de définition de la notion de "polynôme".

2.3 Opérations sur $\mathbb{K}[X]$

Nous allons munir $\mathbb{K}[X]$ de deux lois internes "+" et "$*$" (pour manipuler la somme et le produit des polynômes), et d'une loi externe "$\cdot$" (pour manipuler la multiplication des polynômes par des scalaires). On verra que la somme, la différence, le produit d'un polynôme par un élément de $\mathbb{K}$ ont un sens naturel et possèdent les propriétés requises (commutativité, associativité, distributivité etc.) pour que l'ensemble $\mathbb{K}[X]$ des polynômes soit muni d'une structure d'anneau, de $\mathbb{K}$-espace vectoriel et de $\mathbb{K}$-algèbre.

2.3.1 Addition de deux polynômes

Définition 2.10. Soient $P = a_n X^n + \cdots + a_0$ et $Q = b_n X^n + \cdots + b_0$ avec $n \in \mathbb{N}$. On définit alors le polynôme $P + Q$ par

$$P + Q = (a_n + b_n)X^n + \cdots + (a_1 + b_1)X + (a_0 + b_0).$$

Remarque. Dans la définition ci-dessus, il n'est pas restrictif de faire commencer les expressions des polynômes P et Q par un monôme de même degré n (quitte à rajouter des monômes avec des coefficients 0).

Proposition 2.2. *Soient P et Q deux polynômes de $\mathbb{K}[X]$. Alors on a*

$$\deg(P + Q) \leq \max(\deg P, \deg Q).$$

De plus, si $\deg P \neq \deg Q$ alors $\deg(P + Q) = \max(\deg P, \deg Q)$.

Démonstration. Notons $P = a_pX^p + \cdots + a_0$ et $Q = b_qX^q + \cdots + b_0$ avec $a_p \neq 0$ et $b_q \neq 0$, donc $p = \deg P$ et $q = \deg Q$.

(i) Si $p > q$, le coefficient du terme dominant de $P + Q$ est a_p donc

$$\deg(P + Q) = \deg P = p = \max(p, q).$$

(ii) Si $p < q$, le coefficient du terme dominant de $P + Q$ est b_q donc

$$\deg(P + Q) = \deg Q = q = \max(p, q).$$

(iii) Si $p = q$, le monôme de plus haut degré dans l'expression de $P + Q$ est $(a_p + b_p)X^p$. Donc $\deg(P + Q) \leq p = \max(p, q)$.

□

Remarque. Notons que si $p = q$ et $b_p = -a_p$, le monôme $(a_p + b_p)X^p$ est nul et l'on a $\deg(P+Q) < p = \max(p, q)$.

2.3.2 Multiplication des polynômes et d'un polynôme par un scalaire

Considérons deux monômes $P = a_pX^p$ et $Q = b_qX^q$. Il est naturel de définir le produit de P par Q comme étant le monôme

$$P * Q = a_pb_qX^{p+q}.$$

Définition 2.11. Etant donnés deux polynômes $P = a_pX^p + \cdots + a_0$ et $Q = b_qX^q + \cdots + b_0$, on définit le polynôme $P * Q$ par $P * Q = c_rX^r + \cdots + c_0$ avec $r = p + q$ et

$$c_k = \sum_{i=0}^{k} a_ib_{k-i} = \sum_{j=0}^{k} a_{k-j}b_j, \qquad k \in \{0, \ldots, r\},$$

où on a posé $a_{p+1} = a_{p+2} = \cdots = a_{p+q} = 0$ et $b_{q+1} = b_{q+2} = \cdots = b_{q+p} = 0$.

Dans la suite nous utiliserons l'écriture compacte

$$c_k = \sum_{i+j=k} a_ib_j.$$

Ici, la sommation porte sur tous les couples d'entiers (i, j) tels que $i, j \in \mathbb{N}$ et $i + j = k$.

Remarque. Si P ou Q est nul, on a donc $P * Q = 0$.

Proposition 2.3. *Soient P et Q deux polynômes de $\mathbb{K}[X]$. Alors on a*

$$\deg(P * Q) = \deg P + \deg Q.$$

Définition 2.12. Soit $P = a_pX^p + \cdots + a_0$ un polynôme de $\mathbb{K}[X]$, et $\lambda \in \mathbb{K}$. On définit alors le polynôme $\lambda \cdot P$ par

$$\lambda \cdot P = \sum_{i=0}^{p} \lambda a_iX^i$$

2.3.3 Composition des polynômes

Définition 2.13. Etant donnés deux polynômes $P = a_p X^p + \cdots + a_0$ et Q dans $\mathbb{K}[X]$. On définit le polynôme $P \circ Q$ par $P \circ Q = \sum_{k=0}^{p} a_k Q^k$.

Exemple. On note $P(X) = P \circ X$, $P(-X) = P \circ (-X)$, $P(X^2) = P \circ X^2$ etc.

Proposition 2.4. *Pour tout $\lambda \in \mathbb{K}$, $P, Q, R \in \mathbb{K}[X]$ on a*

(i) $(P + \lambda \cdot Q) \circ R = P \circ R + \lambda \cdot Q \circ R$

(ii) $(P * Q) \circ R = (P \circ R) * (Q \circ R)$

(ii) $(P \circ Q) \circ R = P \circ (Q \circ R)$

(iv) $X \circ P = P \circ X = P$

Remarque. Les propriétés (i) et (ii) disent que l'opération $\circ$ est distributive à droite. Elle n'est pas commutative et elle n'est pas distributive à gauche dans $\mathbb{K}[X]$.

Proposition 2.5. *Soient P et Q deux polynômes de $\mathbb{K}[X]$ non nuls. Alors on a*

$$\deg(P \circ Q) = \deg P \times \deg Q.$$

Proposition 2.6. *Soit P un polynôme et λ un scalaire non nul. Alors* $\deg(\lambda \cdot P) = \deg P$.

2.4 Propriétés algébriques de $\mathbb{K}[X]$

Proposition 2.7. $(\mathbb{K}[X], +, *)$ *est un anneau commutatif.*

Proposition 2.8. *L'anneau $(\mathbb{K}[X], +, *)$ vérifie les propriétés supplémentaires suivantes pour tout $(\lambda, \mu) \in \mathbb{K}^2$ et $(P, Q) \in \mathbb{K}[X]^2$:*

(i) $(\lambda + \mu) \cdot P = \lambda \cdot P + \mu \cdot P$,

(ii) $\lambda \cdot (P + Q) = \lambda \cdot P + \lambda \cdot Q$,

(iii) $\lambda \cdot (\mu \cdot P) = (\lambda\mu) \cdot P$,

(iv) $1 \cdot P = P$,

(v) $\lambda \cdot (P * Q) = (\lambda \cdot P) * Q = P * (\lambda \cdot Q)$.

On dit que $(\mathbb{K}[X], +, *, \cdot)$ est une algèbre.

Ainsi, multiplier un polynôme P par un scalaire λ est équivalent à le multiplier par le polynôme constant $\lambda \cdot 1$. On peut donc sans danger noter la multiplication interne $*$ et la multiplication externe $\cdot$ par le même symbole.

Proposition 2.9. *Soit (P, Q) un couple de polynômes tel que $P * Q = 0$. Alors $P = 0$ ou $Q = 0$. On dit que $(\mathbb{K}[X], +, *, \cdot)$ est une* algèbre intègre.

Démonstration. Soit (P, Q) un couple de polynômes tel que $P * Q = 0$. Alors on a $\deg P + \deg Q = \deg(P*Q) = -\infty$. Donc $\deg P$ ou $\deg Q$ vaut $-\infty$, ce qui est exactement la propriété demandée. □

Dorénavant, on omettra les symboles "$*$" et "$\cdot$". Ainsi PQ désignera $P * Q$, et λP désignera $\lambda \cdot P$.

L'anneau des polynômes $\mathbb{K}[X]$ a beaucoup de similarités avec l'ensemble $\mathbb{Z}$ des entiers relatifs : les deux ensembles sont des *anneaux principaux intègres* (voir L2) sur lesquels on peut définir la division euclidienne, le pgcd et le ppcm.

2.5 Division euclidienne

Définition 2.14. Soient $A, B \in \mathbb{K}[X]$. On dit que le polynôme A est *divisible* par le polynôme B s'il existe un polynôme Q tel que $A = BQ$. Dans ce cas, on note $B \mid A$ et l'on dit que A est *multiple* de B (ou que B est *diviseur* de A). Par convention, si B est non nul, le polynôme Q est parfois noté $\frac{A}{B}$ ou A/B. Si B ne divise pas A, on note $B \nmid A$.

Remarque. (i) Le polynôme nul est divisible par tous les polynômes.

(ii) Comme dans $\mathbb{Z}$, dans les énoncés, qui suivent nous écartons souvent la cas particulier de $B = 0$.

(iii) Dans le cas où A et B sont tous les deux non nuls, $B \mid A$ entraîne $\deg B \leq \deg A$.

Proposition 2.10. *Soient $A, B \in \mathbb{K}[X]$ et $A, B \neq 0$. Si $A \mid B$ et $B \mid A$ alors A et B sont proportionnels, c'est-à-dire qu'il existe tel $\lambda \in \mathbb{K}^*$ que $A = \lambda B$. On dit que A et B sont* associés.

Démonstration. D'après la remarque ci-dessus, on a à la fois $\deg A \leq \deg B$ et $\deg B \leq \deg A$. Donc $\deg A = \deg B$. Comme $B \mid A$, on en déduit que $A = BQ$ avec $\deg Q = 0$. Autrement dit Q est un polynôme constant (et non nul car A n'est pas nul). □

Proposition 2.11. *Soit $\mathbb{K}$ un corps. Deux polynômes unitaires associés de $\mathbb{K}[X]$ sont égaux.*

Proposition 2.12. *Soit B un polynôme non nul, et A un multiple de B de même degré que B. Alors A et B sont associés.*

Tout comme $\mathbb{Z}$, l'anneau $\mathbb{K}[X]$ est muni d'une division euclidienne.

Théorème 2.13 (Division euclidienne)**.** *Soient A et B deux polynômes avec B non nul. Alors il existe un unique couple (Q, R) de polynômes tel que $A = BQ + R$ et $\deg R < \deg B$. Le polynôme Q est appelé* quotient de la division de A par B*, R est le* reste*, B le* diviseur*, et A le* dividende*.*

Démonstration. On va d'abord prouver l'existence du couple (Q, R), puis son unicité.

— *Existence :* Fixons un polynôme $B = b_m X_m + \cdots + b_0$ de degré $m \geq 1$ (le cas B constant non nul étant évident). L'existence du couple (Q, R) vérifiant les propriétés voulues se montre par récurrence sur le degré de A. Pour $n \in \mathbb{N}$, on note $(\mathcal{P}_n)$ l'hypothèse de récurrence suivante :

$$(\mathcal{P}_n) \qquad (\forall A \in \mathbb{K}[X], \deg A \leq n) \Rightarrow (\exists Q, R \in \mathbb{K}[X] \quad : \quad A = BQ + R \text{ et } \deg R < \deg B).$$

Il est clair que $(\mathcal{P}_{m-1})$ est vraie. En effet, il suffit de choisir $Q = 0$ et $R = A$. Soit maintenant $n \geq m$. Supposons $(\mathcal{P}_{n-1})$ vraie et démontrons $(\mathcal{P}_n)$. Le polynôme A est de la forme $A = a_n X^n + \cdots + a_0$ avec $a_n \neq 0$. Comme $n \geq m$ et $b_m \neq 0$, l'expression

$$\hat{A} = A - \frac{a_n}{b_m} X^{n-m} B$$

est bien un polynôme, et son degré est au plus $n - 1$ (il suffit de comparer les coefficients des termes dominants dans la différence). D'après $(\mathcal{P}_{n-1})$, il existe donc deux polynômes $\hat{Q}$ et $\hat{R}$ tels que $\hat{A} = \hat{Q}B + \hat{R}$ et $\deg \hat{R} < \deg B$, donc

$$A = \left(\frac{a_n}{b_m} X^{n-m} + \hat{Q} \right) B + \hat{R}.$$

Le choix de

$$Q = \frac{a_n}{b_m} X^{n-m} + \hat{Q}, \qquad \hat{R} = R,$$

achève la preuve de $(\mathcal{P}_n)$.

— *Unicité :* Supposons que $A = BQ + R = BQ' + R'$ avec $\deg R < \deg B$ et $\deg R' < \deg B$. Alors on a $R - R' = B(Q' - Q)$. Donc, par la Proposition 2.3, $\deg(R - R') = \deg B + \deg(Q' - Q)$. Si $Q \neq Q'$, alors on en déduit que $\deg(R - R') \geq \deg B$. Donc d'après la Proposition 2.2, $\max(\deg R, \deg R') \geq \deg B$, ce qui contredit la définition de R ou de R'. Donc $Q = Q'$, puis $R = R'$.

□

Comme dans $\mathbb{Z}$, la démonstration donnée suggère un procédé de construction itératif permettant de calculer Q et R. En effet, au cours de la récurrence, on a vu comment ramener la division d'un polynôme de degré n à celle d'un polynôme de degré moins élevé (au plus $n - 1$). En pratique, on peut donc calculer le couple (Q, R) en "posant" la division comme dans $\mathbb{N}$, les puissances de X jouant le rôle des puissances de 10.

Exemple. Calculons la division du polynôme $A = 6X^3 - 2X^2 + X + 3$ par $B = X^2 - X + 1$:

$$\begin{array}{r} \left(\begin{array}{r} 6X^3 - 2X^2 + X + 3 \\ \underline{-\,6X^3 + 6X^2 - 6X} \\ 4X^2 - 5X + 3 \\ \underline{-\,4X^2 + 4X - 4} \\ -X - 1 \end{array}\right) \div \left(X^2 - X + 1\right) = 6X + 4 + \dfrac{-X - 1}{X^2 - X + 1} \end{array}$$

Ce calcul donne donc $Q = 6X + 4$ et $R = -X - 1$.

Définition 2.15. On dit qu'un sous-ensemble I de $\mathbb{K}[X]$ est un *idéal* de $(\mathbb{K}[X], +, *)$ si

(i) I est un sous-groupe de $(\mathbb{K}[X], +)$,

(ii) I est stable par multiplication par n'importe quel polynôme de $\mathbb{K}[X]$.

Remarque. La première condition dit que I est un sous-ensemble de $\mathbb{K}[X]$ tel que la loi "+" s'obtient par restriction à $I \times I$. La "somme" de deux éléments de I est de nouveau un élément de I.

Définition 2.16. Pour $B \in \mathbb{K}[X]$, on note $B\mathbb{K}[X]$ *l'ensemble des multiples* de B.

Remarque. $B\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$ et, en particulier, le singleton $\{0\}$ est un idéal. On peut interpreter $B\mathbb{K}[X]$ comme l'ensemble des multiples de B où les facteurs (arbitraires) proviennent de $\mathbb{K}[X]$.

Proposition 2.14. *Soient A et B deux polynômes. Alors $A \mid B$ si et seulement si $B\mathbb{K}[X] \subset A\mathbb{K}[X]$.*

Proposition 2.15. *Soit I un idéal de $(\mathbb{K}[X], +, *)$ non réduit à $\{0\}$. Alors il existe un unique polynôme P unitaire tel que $I = P\mathbb{K}[X]$. Le polynôme P est appelé* générateur unitaire *de I. On dit que I est un* idéal principal.

Démonstration. Soit I un idéal de $(\mathbb{K}[X], +, *)$ non réduit à $\{0\}$. On note

$$E = \{\deg A \ : \ A \in I \setminus \{0\}\}.$$

L'ensemble E est une partie non vide de $\mathbb{N}$, donc admet un plus petit élément. On en déduit que I admet un polynôme P non nul et de degré minimal. Comme pour tout $\lambda \in \mathbb{K}$, le polynôme λP appartient aussi à I, on peut toujours choisir P unitaire. La stabilité de I par multiplication par les éléments de $\mathbb{K}[X]$ assure que $P\mathbb{K}[X] \subset I$. Reste à montrer que $I \subset P\mathbb{K}[X]$. Soit donc $A \in I$. Écrivons la division euclidienne de A par P : $A = PQ + R$ avec $\deg R < \deg P$. Comme A et PQ appartiennent à I, on a aussi $R \in I$. Mais par ailleurs $\deg R < \deg P$. Vu la définition de P, on conclut que $R = 0$ et donc A est un multiple de P ou, autrement dit, $A \in P\mathbb{K}[X]$. □

2.6 pgcd et ppcm

Les notions de pgcd, ppcm (polynômes unitaires), le théoreme de Bézout, le lemme de Gauss sont encore valables sur $\mathbb{K}[X]$.

2.6.1 pgcd

Proposition 2.16. *Soient A et B deux polynômes non tous les deux nuls. L'ensemble*

$$A\mathbb{K}[X] + B\mathbb{K}[X] = \{AP + BQ \ : \ P \in \mathbb{K}[X],\ Q \in \mathbb{K}[X]\}$$

est un idéal de $\mathbb{K}[X]$ non réduit à $\{0\}$.

La Proposition 2.15 assure l'existence d'un unique polynôme unitaire D tel que $A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$.

Définition 2.17. Le générateur unitaire D de $A\mathbb{K}[X]+B\mathbb{K}[X]$ est appelé *plus grand commun diviseur* (ou plus simplement *pgcd*) de A et de B, et est noté $pgcd(A, B)$ ou plus simplement (A, B).

Démonstration de la Proposition 2.16. Notons $J = A\mathbb{K}[X] + B\mathbb{K}[X]$. Remarquons que J n'est pas réduit à $\{0\}$ car J contient A et B, et que l'un de ces deux polynômes n'est pas nul par hypothèse. Reste à montrer que J est un idéal.

(i) Montrons que J est un sous-groupe de $(\mathbb{K}[X], +)$:
- Il est évident que $0 \in J$.
- Soient C et $\hat{C}$ deux polynômes de J. Alors il existe quatre polynômes P, $\hat{P}$, Q et $\hat{Q}$ tels que $C = AP + BQ$ et $\hat{C} = A\hat{P} + B\hat{Q}$. Donc
$$C + \hat{C} = A(P + \hat{P}) + B(Q + \hat{Q}) \in J.$$
- Enfin, si $C = AP + BQ$, il est clair que $-C = A(-P) + B(-Q)$, donc $-C \in J$.

(ii) Stabilité de J par produit : Soit $C = AP+BQ$ un élément de J, et R un polynôme quelconque. Alors $RC = A(PR) + B(QR)$ donc $RC \in J$.

□

Remarque. On convient que $(0, 0) = 0$. Pour tous polynômes A et B on a donc $A\mathbb{K}[X] + B\mathbb{K}[X] = (A, B)\mathbb{K}[X]$.

Proposition 2.17. *Soient A, B deux polynômes pas tous les deux nuls. Alors (A, B) est l'unique polynôme unitaire vérifiant*

$$(A, B) \mid A, \quad (A, B) \mid B \quad et \quad (P \mid A \ et \ P \mid B) \Rightarrow P \mid (A, B). \tag{2.1}$$

Démonstration. Notons $D = (A, B)$ et montrons que D vérifie (2.1). Par définition, $D\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X]$. Comme A et B appartiennent tous les deux à l'ensemble de droite, A et B sont bien des multiples de D. Enfin, si P divise A et B alors, d'après la Proposition 2.14, $A\mathbb{K}[X] \subset P\mathbb{K}[X]$ et $B\mathbb{K}[X] \subset P\mathbb{K}[X]$. Donc $D\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X] \subset P\mathbb{K}[X]$. Donc P divise D. Pour montrer l'unicité, considérons un polynôme D' unitaire vérifiant (2.1). On a donc en particulier $D \mid D'$. Mais certainement $D' \mid D$ donc D et D' sont associés (voir la Proposition 2.10). Comme D et D' sont unitaires, on a $D = D'$ par la Proposition 2.11. □

Proposition 2.18. *Si A et B ne sont pas simultanément nuls et si C est unitaire alors on a*

$$(AC, BC) = C(A, B).$$

Démonstration. Notons $D = (A, B)$ et $\Delta = (AC, BC)$. Il suffit alors de remarquer que

$$\Delta\mathbb{K}[X] = AC\mathbb{K}[X] + BC\mathbb{K}[X] = C(A\mathbb{K}[X] + B\mathbb{K}[X]) = CD\mathbb{K}[X].$$

□

Définition 2.18. On dit que deux polynômes $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ sont *premiers entre eux* si leur pgcd vaut 1, donc si $(A, B) = 1$.

Proposition 2.19. *Deux polynômes A et B sont premiers entre eux si et seulement si il existe deux polynômes U et V tels que $AU + BV = 1$.*

Démonstration. "⇒" Si $(A, B) = 1$ alors par définition du pgcd, on a $A\mathbb{K}[X] + B\mathbb{K}[X] = \mathbb{K}[X]$. Donc $1 \in A\mathbb{K}[X] + B\mathbb{K}[X]$, ce qui signifie qu'il existe U et V tels que $AU + BV = 1$.
"⇐" Si $AU + BV = 1$ alors $1 \in A\mathbb{K}[X] + B\mathbb{K}[X]$. Le générateur unitaire de $A\mathbb{K}[X] + B\mathbb{K}[X]$ est donc un diviseur de 1, donc 1 lui-même. On a donc bien $1 = (A, B)$. □

Proposition 2.20. *Le polynôme unitaire D est le pgcd de A et de B si et seulement si*

$$D \mid A, \quad D \mid B, \qquad \text{et} \quad \left(\frac{A}{D}, \frac{B}{D}\right) = 1.$$

Proposition 2.21 (Théorème de Bézout)**.** *Supposons que D unitaire divise A et B avec A et B non tous les deux nuls. Alors on a*

$$D = (A, B) \quad \Longleftrightarrow \quad \exists U, V \in \mathbb{K}[X], \;\; AU + BV = D.$$

Démonstration. En appliquant la Proposition 2.18,

$$D = (A, B) \quad \Longleftrightarrow \quad 1 = \left(\frac{A}{D}, \frac{B}{D}\right).$$

Or d'après la Proposition 2.19, on a

$$\left(\frac{A}{D}, \frac{B}{D}\right) = 1 \quad \Longleftrightarrow \quad \exists U, V \in \mathbb{K}[X], \;\; \frac{A}{D}U + \frac{B}{D}V = 1,$$

ce qui achève la preuve du théorème. □

Proposition 2.22 (Lemme de Gauss)**.** *Si P divise AB et $(P, A) = 1$ alors P divise B.*

Démonstration. Soit $\hat{B}$ le polynôme unitaire associé à B. On a $(PB, AB) = \hat{B}(P, A) = \hat{B}$. Par hypothèse, P divise AB, et il est clair que P divise aussi PB. Donc P divise $\hat{B}$ et donc B. □

Proposition 2.23. *Un polynôme P est premier avec un produit AB si et seulement si P est premier avec A et avec B.*

Démonstration. "⇒" Supposons P premier avec AB. Soit $\tilde{P}$ divisant P et A. Alors $\tilde{P}$ divise aussi AB. Donc $\tilde{P} \mid (AB, P)$, i.e. $\tilde{P} \mid 1$. On en déduit que $\tilde{P}$ est un polynôme constant. Donc P est premier avec A. On établit de même que P est premier avec B.
"⇐" On prouve la réciproque par contraposition. Supposons que P ne soit pas premier avec AB. Alors il existe $\tilde{P}$ divisant P et AB, et tel que $\deg \tilde{P} \geq 1$. Si P est premier avec A alors $\tilde{P}$ également. D'après le théorème de Gauss, $\tilde{P}$ divise donc B. On a donc montré que $\tilde{P}$ divise à la fois P et B. Comme $\deg \tilde{P} \geq 1$, cela signifie que P et B ne sont pas premiers entre eux. □

Remarque. Une récurrence élémentaire permet de montrer plus généralement qu'un polynôme P est premier avec un produit de polynôme $A_1 \cdots A_k$ si et seulement si il est premier avec chacun des facteurs A_i.

2.6.2 L'algorithme d'Euclide

Lemme 2.24. *Soit B un polynôme non nul, et A un polynôme quelconque. Notons Q et R le quotient et le reste de la division euclidienne de A par B. Alors on a*

$$(A, B) = (B, R).$$

Démonstration. Soit D divisant A et B. Comme $R = A - BQ$, le polynôme D divise aussi R. Donc D divise (B, R). En choisissant $D = (A, B)$, on conclut que $(A, B) \mid (B, R)$. Soit maintenant D un polynôme divisant B et R. Comme $A = BQ + R$, on a aussi $D \mid A$. Donc $D \mid (A, B)$. On a donc finalement $(B, R) \mid (A, B)$. Les deux polynômes (B, R) et (A, B) sont unitaires et associés. Ils sont donc égaux. □

Ce lemme indique clairement la stratégie à suivre pour calculer (A, B). Quitte à permuter A et B, on peut toujours supposer que $\deg A \geq \deg B$. On procède alors comme suit :

- Si $B = 0$, il n'y a rien à faire : (A, B) est égal au polynôme unitaire associé à A.
- Si B n'est pas nul, on effectue la division euclidienne de A par B, ce qui donne deux polynômes Q_0 et R_1 tels que $A = BQ_0 + R_1$ et $\deg R_1 < \deg B$.

Le lemme montre que $(A, B) = (B, R_1)$. On reprend le calcul ci-dessus en remplaçant A par B, et B par R_1. En itérant le procédé, on construit deux suites $R_1, R_2, \ldots$ et $Q_0, Q_1, \ldots$ telles que :

$$\begin{aligned} A &= BQ_0 + R_1 \quad \text{avec} \quad \deg R_1 < \deg B, \\ B &= R_1Q_1 + R_2 \quad \text{avec} \quad \deg R_2 < \deg R_1, \\ R_1 &= R_2Q_2 + R_3 \quad \text{avec} \quad \deg R_3 < \deg R_2, \end{aligned}$$

et pour $2 \leq k < n$,

$$R_{k-1} = R_kQ_k + R_{k+1} \quad \text{avec} \quad \deg R_{k+1} < \deg R_k,$$

et en terminant avec

$$R_{n-1} = R_nQ_n + 0.$$

Le procédé s'arrête nécessairement au bout d'au plus $\deg P$ étapes car chaque itération diminue d'au moins 1 le degré du reste de la division euclidienne. On a donc finalement

$$(A, B) = (B, R_1) = \cdots = (R_{k-1}, R_k) = \cdots = (R_n, 0) = \hat{R}_n,$$

où $\hat{R}_n$ est le polynôme unitaire associé à R_n.

Exemple. Calculons $C := (X^3 - X^2 - X - 2, \quad X^5 - 2X^4 + X^2 - X - 2)$. Posons la division euclidienne de $X^5 - 2X^4 + X^2 - X - 2$ par $X^3 - X^2 - X - 2$:

$$\begin{array}{rl} X^5 - 2X^4 \qquad + X^2 \ - X - 2 & = \left(X^3 - X^2 - X - 2\right)\left(X^2 - X\right) + 2X^2 - 3X - 2 \\ \underline{- X^5 \ + X^4 + X^3 + 2X^2} & \\ - X^4 + X^3 + 3X^2 \ - X & \\ \underline{X^4 - X^3 \ - X^2 - 2X} & \\ 2X^2 - 3X & \end{array}$$

Donc $C = (X^3 - X^2 - X - 2, \ \ 2X^2 - 3X - 2)$. On continuant de la même manière, on calcule

$$\begin{array}{rl} X^3 \ - X^2 \ - X \ - 2 & = \left(2X^2 - 3X - 2\right)\left(\frac{1}{2}X + \frac{1}{4}\right) + \frac{3}{4}X - \frac{3}{2} \\ \underline{- X^3 + \frac{3}{2}X^2 \ + X} & \\ \frac{1}{2}X^2 \qquad - 2 & \\ \underline{- \frac{1}{2}X^2 + \frac{3}{4}X + \frac{1}{2}} & \\ \frac{3}{4}X - \frac{3}{2} & \end{array}$$

puis

$$\begin{array}{rl} 2X^2 - 3X - 2 & = \left(\frac{3}{4}X - \frac{3}{2}\right)\left(\frac{8}{3}X + \frac{4}{3}\right) \\ \underline{- 2X^2 + 4X} & \\ X - 2 & \\ \underline{- X + 2} & \\ 0 & \end{array}$$

Le pgcd est le dernier reste non nul, divisé par son coefficient dominant : $C = X - 2$.

2.6.3 ppcm

Proposition 2.25. *Considérons deux polynômes non nuls A et B. Alors l'ensemble $A\mathbb{K}[X] \cap B\mathbb{K}[X]$ est un idéal non réduit à $\{0\}$.*

Démonstration. On vérifie facilement les deux conditions dans la défintion d'un idéal (Définition 2.15). □

Définition 2.19. Le générateur unitaire D de $A\mathbb{K}[X] \cap B\mathbb{K}[X]$ est appelé *plus petit commun multiple* (ou plus simplement *ppcm*) de A et B. On le note ppcm(A,B) ou plus simplement $[A, B]$.

Remarque. Si A ou B est nul, on a $A\mathbb{K}[X] \cap B\mathbb{K}[X] = \{0\}$. On adopte alors la convention que $[A, B] = 0$. Ainsi, on aura toujours $A\mathbb{K}[X] \cap B\mathbb{K}[X] = [A, B]\mathbb{K}[X]$.

Proposition 2.26. *Soient A et B deux polynômes non nuls. Le ppcm de A et de B est l'unique polynôme unitaire vérifiant la propriété suivante :*

$$A \mid [A, B], \quad B \mid [A, B] \text{ et } (A \mid M \text{ et } B \mid M) \Rightarrow [A, B] \mid M.$$

Démonstration. La preuve se fait de manière analogue comme dans $\mathbb{Z}$. □

Proposition 2.27. *Soit C un polynôme unitaire et A, B deux polynômes. Alors on a*

$$[AC, BC] = C[A, B].$$

Démonstration. Il suffit de remarquer que $AC\mathbb{K}[X] \cap BC\mathbb{K}[X] = C(A\mathbb{K}[X] \cap B\mathbb{K}[X])$. □

Proposition 2.28. *Soient A et B deux polynômes non nuls. Le polynôme unitaire M est le ppcm de A et de B si et seulement si*

$$A \mid M, \quad B \mid M \quad \text{et} \quad \left(\frac{M}{A}, \frac{M}{B}\right) = 1.$$

Proposition 2.29. *Soient A et B deux polynômes. Il existe une constante λ non nulle telle que*

$$\lambda AB = (A, B)[A, B].$$

- *Si de plus A et B sont unitaires, alors $\lambda = 1$.*
- *Si A et B sont premiers entre eux alors AB et $[A, B]$ sont associés.*

Démonstration. Écartons le cas évident où l'un des deux polynômes A et B est nul. On peut alors appliquer la Proposition 2.28. On en déduit que

$$\left(\frac{[A, B]}{A}, \frac{[A, B]}{B}\right) = 1. \tag{2.2}$$

Notons λ l'inverse du coefficient du terme dominant de AB. Alors λAB est unitaire, et la Proposition 2.27 combinée avec (2.2) montre que

$$\left(\lambda AB\frac{[A,B]}{A}, \lambda AB\frac{[A,B]}{B}\right) = \lambda AB.$$

En appliquant la Proposition 2.18, on constate que le membre de gauche de cette égalité vaut $[A,B](A,B)$. □

Exemple. $\text{ppcm}(X(X-2)^2(X^2+1)^4, (X+1)(X-2)^3(X^2+1)^3) = X(X+1)(X-2)^3(X^2+1)^4$.

2.7 Polynômes irréductibles

Dans cette section, nous allons introduire une classe de polynômes qui jouent dans $\mathbb{K}[X]$ le même rôle que les nombres premiers dans $\mathbb{Z}$: les polynômes irréductibles.

Définition 2.20. Soit $P \in \mathbb{K}[X]$ non nul. On dit que P est *irréductible* s'il vérifie les conditions suivantes :

(i) P est non constant ;

(ii) $\forall Q, R \in \mathbb{K}[X]$, $P = QR \Rightarrow Q$ ou R est constant.

Remarque. (i) À la différence des nombres premiers, les polynômes irréductibles ont une infinité de diviseurs, mais on notera bien que ces diviseurs sont triviaux.

(ii) Tout polynôme de degré 1 est irréductible. En effet, soit P de degré 1, et Q un diviseur de P. Alors $\deg Q \in \{0,1\}$. Si $\deg Q = 0$ alors Q est une constante, si $\deg Q = 1$ alors $\deg Q = \deg P$ donc P et Q sont associés. Par conséquent il y a une infinité de polynômes irréductibles.

(iii) Il est important de bien tenir compte du corps $\mathbb{K}$ en question. Un polynôme peut être irréductible sur un corps mais réductible sur un autre corps (voir exemple ci-dessous).

Exemple. Le polynôme $X^2 - 1 = (X-1)(X+1)$ est réductible dans $\mathbb{R}[X]$. Le polynôme $X^2+1 = (X-i)(X+i)$ est réductible dans $\mathbb{C}[X]$ mais est irréductible dans $\mathbb{R}[X]$. Le polynôme $X^2 - 2 = (X-\sqrt{2})(X+\sqrt{2})$ est réductible dans $\mathbb{R}[X]$ mais est irréductible dans $\mathbb{Q}[X]$.

Proposition 2.30. *Soit A un polynôme et P un polynôme irréductible ne divisant pas A. Alors $(A,P) = 1$.*

Démonstration. Soit B un diviseur commun de A et de P. Comme P est irréductible, B doit être constant, ou associé à P. Le deuxième cas est exclus car on a supposé que P ne divisait pas A. Donc B est constant. On a donc bien $(A,P) = 1$. □

De même que tout entier possède une décomposition en facteurs premiers, tout polynôme a une décomposition en facteurs irréductibles.

Théorème 2.31 (Décomposition en facteurs irréductibles)**.** *Soit P un polynôme non constant. Alors il existe un entier $k \geq 1$, k entiers $\alpha_1, \ldots, \alpha_k$ non nuls, k polynômes irréductibles unitaires $P_1, \ldots, P_k$ deux à deux distincts, et $\lambda \in \mathbb{K} \setminus \{0\}$ tels que*

$$P = \lambda \prod_{i=1}^{k} P_i^{\alpha_i}.$$

Cette décomposition, appelée décomposition en facteurs irréductibles*, est unique à ordre des facteurs près.*

Démonstration. La preuve est analogue à celle dans $\mathbb{Z}$ et est laissée au lecteur. □

2.7.1 Polynômes dérivés

Définition 2.21. Soit $P = a_n X^n + \cdots + a_1 X + a_0$ un polynôme de $\mathbb{K}[X]$. On appelle *polynôme dérivé* noté P' le polynôme suivant :

$$P' = \sum_{j=1}^{n} j a_j X^{j-1} = n a_n X^{n-1} + \cdots + a_1.$$

La proposition suivante dit que la dérivation est linéaire (voir aussi le cours d'algèbre linéaire 1).

Proposition 2.32. *Soient P et Q deux polynômes, et $\lambda \in \mathbb{K}$.*

(i) *Si* $\deg P > 0$ *alors* $\deg P' = \deg P - 1$,
(ii) *Si P est constant alors* $P' = 0$,
(iii) $(P+Q)' = P' + Q'$,
(iv) $(\lambda P)' = \lambda P'$,
(v) $(PQ)' = P'Q + PQ'$.
(vi) $(P \circ Q)' = (P' \circ Q)\ P'$

Définition 2.22. Soit P un polynôme dans $\mathbb{K}[X]$. On définit par récurrence

$$P^{(0)} = P \quad \text{et} \quad P^{(n+1)} = \left(P^{(n)}\right)', n \geq 0.$$

Remarque. En appliquant la Proposition 2.32 on obtient que la dérivation n-ième est une application linéaire.

Proposition 2.33 (Formule de Leibniz)**.** *Soient P et Q deux polynômes. On a la formule suivante pour la dérivée n-ième du polynôme produit :*

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

Démonstration. La démonstration est identique à la démonstration de la formule de Liebniz dans le cas de la dérivée n-ième d'un produit de fonctions de classe $\mathcal{C}^n$ (voir cours d'Analyse 1). □

2.8 Fonctions polynomiales et racines

Jusqu'à présent, nous avons traité les polynômes comme des objets algébriques abstraits. Dans ce qui suit, nous allons aussi remplacer la variable muette X par des éléments du corps $\mathbb{K}$ (toujours arbitraire). Voici la definition donnée au début du chapitre (Définition 2.9) : pour $P = a_p X^p + a_{p-1} X^{p-1} + \cdots + a_1 X + a_0$ un polynôme de $\mathbb{K}[X]$, la *fonction polynomiale associée à P* est l'application $\tilde{P}$ définie par

$$\tilde{P} : \mathbb{K} \to \mathbb{K}, \quad x \mapsto a_p x^p + a_{p-1} x^{p-1} + \cdots + a_1 x + a_0.$$

La confusion entre un polynôme et sa fonction polynomiale associée n'a, dans le cas où le corps $\mathbb{K}$ est infini (et donc en particulier lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$) pas de conséquence fâcheuse. Dans la pratique, on confondra donc souvent P et $\tilde{P}$. Rappelons que c'est par contre tout autre chose lorsque $\mathbb{K}$ est un corps fini.

La proposition suivante dit que l'évaluation d'un polynôme en un scalaire est linéaire.

Proposition 2.34. *Soit $x \in \mathbb{K}$ un scalaire fixé. Alors on a pour tous polynômes P et Q, et pour tout scalaire λ :*

(i) $\tilde{P}(x) + \tilde{Q}(x) = (\tilde{P} + \tilde{Q})(x)$,

(ii) $\lambda \tilde{P}(x) = (\lambda \tilde{P})(x)$,

(iii) $\tilde{P}(x)\tilde{Q}(x) = (\tilde{P}\tilde{Q})(x)$,

Dans ce qui suit pour un polynôme P appartenant à $\mathbb{K}$ nous utiliserons toujours $\tilde{P}$ pour sa fonction polynomiale associée.

Définition 2.23. Soient $\gamma \in \mathbb{K}$ et $P \in \mathbb{K}[X]$. On dit que γ est *racine* ou *zéro* de P si $\tilde{P}(\gamma) = 0$.

Proposition 2.35. *Soit $\gamma \in \mathbb{K}$ et $P \in \mathbb{K}[X]$. Alors γ est une racine de P si et seulement si $X - \gamma$ divise P.*

Démonstration. "⇒" Supposons que $\tilde{P}(\gamma) = 0$. La division euclidienne de P par $X - \gamma$ donne $P = Q(X - \gamma) + R$ avec $\deg R = 0$. En substituant γ à X dans la relation ci-dessus, on trouve $\tilde{R}(\gamma) = 0$. Comme R est constante, on conclut que $R = 0$. "⇐" Si $(X - \gamma) \mid P$ alors il existe Q tel que $P = Q(X - \gamma)$, ce qui donne $\tilde{P}(\gamma) = \tilde{Q}(\gamma)(\gamma - \gamma) = 0$. □

Exemple. Il existe Q tel que $X^4 - 2X^3 + X^2 - X - 2 = (X - 2)Q$ car 2 est racine de $X^4 - 2X^3 + X^2 - X - 2$. On trouve $X^4 - 2X^3 + X^2 - X - 2 = (X - 2)(X^3 + X + 1)$.

Définition 2.24. Soit $P \in \mathbb{K}[X]$, $\gamma \in \mathbb{K}$ et $k \in \mathbb{N}^*$. On dit que γ est *racine de P de multiplicité k* si $(X - \gamma)^k \mid P$ et $(X - \gamma)^{k+1} \nmid P$. L'entier k est appelé *ordre de multiplicité* ou simplement *ordre* de la racine. On note $k = mult_\gamma(P)$ ou $k = v_\gamma(P)$.

Remarque. On parle de racine simple ($k = 1$), racine double ($k = 2$), racine triple ($k = 3$) etc.

Exemple. Soit $P = X^5 - 9X^4 + 25X^3 - 9X^2 - 54X + 54$ un polynôme sur $\mathbb{R}[X]$ et $\gamma = 3$. On a $\tilde{P}(3) = 0$ et

$$\begin{aligned} P &= (X - 3)(X^4 - 6X^3 + 7X^2 + 12X - 18) \\ &= (X - 3)^2(X^3 - 3X^2 - 2X + 6) \\ &= (X - 3)^3(X^2 - 2). \end{aligned}$$

3 est donc racine d'ordre 3 du polynôme P et $mult_3(P) = 3$.

Remarque. Pour $a \in \mathbb{K}$, on peut définir "l'ordre d'annulation en a" par

$$v_a : \mathbb{K}[X] \to \mathbb{Z} \cup \{\infty\}, \qquad P \mapsto \sup\{k \in \mathbb{N} \mid \exists Q \in \mathbb{K}[X], P = (X - a)^k Q\}.$$

Cette fonction associe à un polynôme P non nul l'ordre de multiplicité de la racine a dans P (ordre qui vaut 0 si a n'est pas racine, et l'infini si P est nul). Notons aussi que si P est non nul, $v_a(P)$ est égal au degré du plus petit monôme non nul de $P(a + X)$. L'application v_a est comme ν_p (la valuation p-adique dans $\mathbb{Z}$) une *valuation*.

Proposition 2.36. *Soit P un polynôme non nul, et γ une racine de P. Alors γ est une racine simple si et seulement si $\tilde{P}'(\gamma) \neq 0$.*

Démonstration. Nous allons prouver la négation de l'équivalence : i.e. γ est une racine au moins double de P si et seulement si $\tilde{P}(\gamma) = \tilde{P}'(\gamma) = 0$. Supposons donc que γ est une racine au moins double de P. Alors $(X - \gamma)^2 \mid P$. Donc P s'écrit $P = Q(X - \gamma)^2$ pour un certain polynôme Q. Il est donc immédiat que $\tilde{P}(\gamma) = 0$. En dérivant, on trouve $P' = Q'(X - \gamma)^2 + 2(X - \gamma)Q$, donc $\tilde{P}'(\gamma) = 0$. Réciproquement, supposons que $\tilde{P}(\gamma) = \tilde{P}'(\gamma) = 0$. La division euclidienne de P par $(X - \gamma)^2$ s'écrit $P = Q(X - \gamma)^2 + R$ avec $\deg R \leq 1$. Comme $P(\gamma) = 0$, on a $R(\gamma) = 0$. En dérivant la relation $P = Q(X - \gamma)^2 + R$, on obtient $\tilde{R}'(\gamma) = 0$. Comme R' est un polynôme constant, on a $R' = 0$, puis, comme $\tilde{R}(\gamma) = 0$, R est nul aussi. □

Proposition 2.37. *Soient $P \in \mathbb{K}[X]$, $\gamma \in \mathbb{K}$. Alors γ est une racine multiple d'ordre $k = mult_\gamma(P)$ de P (avec $k \in \mathbb{N}^*$) si l'une des conditions équivalentes suivantes est vérifiée :*

(i) $(X-\gamma)^k$ divise P et $(X-\gamma)^{k+1}$ ne divise pas P ;

(ii) Il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-\gamma)^k Q$ et $\tilde{Q}(\gamma) \neq 0$;

(iii) $\tilde{P}(\gamma) = \tilde{P}'(\gamma) = \cdots = \tilde{P}^{(k-1)}(\gamma) = 0$ et $\tilde{P}^{(k)}(\gamma) \neq 0$.

Démonstration.
— (i) $\Rightarrow$ (ii) est clair : $P = (X-\gamma)^k Q$ avec $\tilde{Q}(\gamma) \neq 0$.
— (ii) $\Rightarrow$ (i) Si $P = (X-\gamma)^k Q$ alors il est clair que $(X-\gamma)^k$ divise P. Mais si $(X-\gamma)^{k+1}$ divise P alors il existe $Q_1 \in \mathbb{K}[X]$ tel que $P = (X-\gamma)^{k+1} Q_1$. Ainsi $Q = (X-\gamma)Q_1$ ce qui contredit le fait que $\tilde{Q}(\gamma) \neq 0$.
— (ii) $\Rightarrow$ (iii), par récurrence sur k. Soit $k = 1$. On suppose que $P = (X-\gamma)Q$ avec $\tilde{Q}(\gamma) \neq 0$. Alors $P' = (X-\gamma)Q' + Q$. Ainsi $\tilde{P}'(\gamma) = \tilde{Q}(\gamma) \neq 0$. On suppose la propriété vérifiée jusqu'au rang k. Soit P un polynôme de la forme $P = (X-\gamma)^{k+1}Q$ avec $\tilde{Q}(\gamma) \neq 0$. Alors on peut appliquer l'hypothèse de récurrence à $P' = (X-\gamma)^k((k+1)Q + (X-\gamma)Q')$. Alors $\tilde{P}'(\gamma) = \cdots = (\tilde{P}')^{(k-1)}(\gamma) = 0$ et $(\tilde{P}')^{(k)}(\gamma) \neq 0$. On obtient donc $\tilde{P}(\gamma) = 0 = \cdots = \tilde{P}^{(k)}(\gamma)$ et $\tilde{P}^{(k+1)}(\gamma) \neq 0$.
— (iii) $\Rightarrow$ (ii). On suppose que $\tilde{P}(\gamma) = \cdots = \tilde{P}^{(k)}(\gamma) = 0$ et $\tilde{P}^{(k+1)}(\gamma) \neq 0$. Alors γ est une racine de multiplicité $m \geq 1$; $P = (X-\gamma)^m Q$ avec $Q(\gamma) \neq 0$. Si $k > m$ alors d'après le sens (i)$\Rightarrow$ (iii), $\tilde{P}(\gamma) = 0 = \cdots = \tilde{P}^{(m)}(\gamma)$ et $\tilde{P}^{(m+1)}(\gamma) \neq 0$. Ce qui est impossible donc $k \leq m$. On vérifie de la même manière que $k = m$.

□

Exemple. On considère le polynôme de l'exemple précédent. On a $\tilde{P}(3) = 0$, puis

$$\begin{aligned} P' &= 5X^4 - 36X^3 + 75X^2 - 18X - 54, \qquad \tilde{P}'(3) = 0, \\ P'' &= 20X^3 - 108X^2 + 150X - 18, \qquad \tilde{P}''(3) = 0, \\ P''' &= 60X^2 - 216X + 150, \qquad \tilde{P}'''(3) = 42 \neq 0. \end{aligned}$$

Proposition 2.38. *Soit P un polynôme non nul admettant les racines $\gamma_1, \ldots, \gamma_k$ avec multiplicité $\alpha_1, \ldots, \alpha_k$. Alors $\prod_{i=1}^k (X-\gamma_i)^{\alpha_i}$ divise P.*

Démonstration. On sait déjà que $(X-\gamma_1)^{\alpha_1}$ divise P. Supposons que $\prod_{i=1}^{j-1}(X-\gamma_i)^{\alpha_i}$ divise P (avec $j \leq k$). Comme les γ_i sont deux à deux distincts, les polynômes $(X-\gamma_i)^{\alpha_i}$ sont premiers entre eux deux à deux. Cela permet donc d'affirmer que $(X-\gamma_j)^{\alpha_j}$ est premier avec $\prod_{i=1}^{j-1}(X-\gamma_i)^{\alpha_i}$. Comme P est multiple de $(X-\gamma_j)^{\alpha_j}$ par hypothèse, et de $\prod_{i=1}^{j-1}(X-\gamma_i)^{\alpha_i}$, P est également multiple du ppcm de ces deux polynômes qui, d'après la Proposition 2.29, vaut $\prod_{i=1}^{j}(X-\gamma_i)^{\alpha_i}$. Nous venons donc de montrer par récurrence sur j que $\prod_{i=1}^k (X-\gamma_i)^{\alpha_i}$ divise P. □

Proposition 2.39. *Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \in \mathbb{N}$. Alors P admet au plus n racines comptées avec leur ordre de multiplicité : si $\{\gamma_1, \ldots, \gamma_k\}$ est l'ensemble des racines de P, et α_i est la multiplicité de γ_i, alors on a $\alpha_1 + \cdots + \alpha_k \leq n$.*

Démonstration. D'après la Proposition 2.38, on a $\prod_{i=1}^{k}(X-\gamma_i)^{\alpha_i} \mid P$. Donc

$$\sum_{i=1}^{k} \deg\left((X-\gamma_i)^{\alpha_i}\right) \leq \deg P.$$

Le membre de gauche vaut $\sum_{i=1}^{k} \alpha_i$, d'où le résultat. □

Remarque. En particulier, si $P \neq 0$, toutes les racines de P sont de multiplicité inférieure ou égale à $\deg P$. Le seul polynôme ayant une infinité de racines est le polynôme nul.

Remarque. La Proposition 2.39 est vraie sur $A[X]$ où A est un anneau intègre, mais il est faux si l'anneau n'est pas intègre. Par exemple, dans $\mathbb{Z}/8\mathbb{Z}$, l'équation $\overline{1}\,X^2 - \overline{1} = \overline{0}$ a 4 solutions $(\overline{1}, \overline{3}, \overline{5}, \overline{7})$.

2.8.1 Formule de Taylor

Proposition 2.40 (Formule de Taylor)**.** *Soit $\mathbb{K}$ un corps de caractéristique nulle (donc infini) et soient $P \in \mathbb{K}[X]$ de degré n et $a \in \mathbb{K}$. On a la formule de Taylor :*

$$P(X) = P(a) + P'(a)(X-a) + \cdots + \frac{P^{(k)}(a)}{k!}(X-a)^k + \cdots + \frac{P^{(n)}(a)}{n!}(X-a)^n.$$

Démonstration. Écrivons $P(X) = \sum_{k=0}^{n} a_k(X-a+a)^k$. Si on développe chaque terme $(X-a+a)^k$ par la formule du binôme $(X-a+a)^k = \sum_{i=0}^{k} \binom{k}{i} a^{k-i}(X-a)^i$ on obtient, en réordonnant suivant les puissances de $X-a$, $P(X) = \sum_{k=0}^{n} b_k(X-a)^k$ avec des coefficients b_k que l'on va expliciter maintenant. On a $P^{(0)}(a) = P(a) = b_0$ et, pour $1 \leq \ell \leq n$, par linéarité de la dérivation à l'ordre ℓ,

$$\begin{aligned}
P^{(\ell)}(X) &= \sum_{k=0}^{n} b_k \left((X-a)^k\right)^{(\ell)} \\
&= \sum_{k=\ell}^{n} b_k \left((X-a)^k\right)^{(\ell)} \\
&= \sum_{k=\ell}^{n} b_k k(k-1)\cdots(k-\ell+1)(X-a)^{k-\ell} \\
&= b_\ell \ell! + \sum_{k=\ell+1}^{n} b_k k(k-1)\cdots(k-\ell+1)(X-a)^{k-\ell}.
\end{aligned}$$

En évaluant cette quantité en a, nous obtenons $P^{(\ell)}(a) = b_\ell \ell!$, c'est à dire $b_\ell = P^{(\ell)}(a)/\ell!$. □

Remarque. La spécificité de cette formule de Taylor dans le cas polynomial est qu'il n'y a pas de reste. Travailler sur un corps de caractéristique nulle permet de diviser par $\ell!$.

Exemple. Pour $P = X^3 + X$ et $a = 1$ on obtient :

$$X^3 + X = 2 + 4(X-1) + 3(X-1)^2 + (X-1)^3.$$

2.9 Polynômes scindés

2.9.1 Définitions et théorème fondamental de l'algèbre

Définition 2.25. Un polynôme *scindé* sur $\mathbb{K}$ est un polynôme $P \in \mathbb{K}[X]$ constant ou admettant des racines $\gamma_1, \ldots, \gamma_r$ dans $\mathbb{K}$ de multiplicités respectives $\alpha_1, \ldots, \alpha_r$ telles que $\alpha_1 + \cdots + \alpha_r = \deg P$.

Remarque. Un polynôme scindé non constant est donc de la forme $P = \lambda \prod_{i=1}^{r} (X - \gamma_i)^{\alpha_i}$. Notons aussi qu'un polynôme constant de $\mathbb{K}[X]$ ne peut pas être scindé.

Le très important résultat suivant est connu sous le nom de *théorème fondamental de l'algèbre* ou *théorème de d'Alembert-Gauss*. Il en existe de nombreuses preuves, mais toutes dépassent le cadre du programme. Il est à la base de la principale différence entre les corps $\mathbb{R}$ et $\mathbb{C}$ concernant les polynômes et leur factorisation.

Théorème 2.41 (Théorème de d'Alembert-Gauss / Théorème fondamental d'algèbre)**.** *Soit $P \in \mathbb{C}[X]$ non constant. Alors P possède au moins une racine complexe.*

2.9.2 Polynômes irréductibles de $\mathbb{C}[X]$

Théorème 2.42. *Un polynôme P est irréductible dans $\mathbb{C}$ si et seulement si* $\deg P = 1$.

Démonstration. On a déjà vu que tout polynôme de degré 1 était irréductible (que ce soit dans $\mathbb{C}$ ou dans $\mathbb{R}$). Pour montrer la réciproque, donnons-nous un polynôme P de degré au moins 2. Le théorème fondamental nous dit que P admet au moins une racine γ_1. Donc P est divisible par $X - \gamma_1$. Clairement $X - \gamma_1$ n'est pas constant et n'est pas associé à P car de degré strictement inférieur à 2. Donc P n'est pas irréductible. □

Théorème 2.43. *Tout polynôme de $\mathbb{C}[X]$ est scindé. Un polynôme de $\mathbb{C}[X]$ de degré n a donc exactement n racines complexes (comptées avec multiplicité).*

Démonstration. La preuve découle par récurrence en utilisant le Théorème 2.41. □

Remarque. Le résultat est faux pour $\mathbb{R}[X]$ comme le montre l'exemple $P = X^2 + 1$. Ce polynôme n'est pas scindé sur $\mathbb{R}$.

Exemple. Soit $P(X) = 3X^3 - 2X^2 + 6X - 4$. Considéré comme un polynôme à coefficients dans $\mathbb{Q}$ ou $\mathbb{R}$, P n'a qu'une seule racine (qui est simple) $\alpha = 2/3$ et il se décompose en $P(X) = 3(X - \frac{2}{3})(X^2 + 2)$. P n'est donc pas scindé ni sur $\mathbb{R}$ ni sur $\mathbb{Q}$. Si on considère maintenant P comme un polynôme à coefficients dans $\mathbb{C}$ alors $P(X) = 3(X - \frac{2}{3})(X - i\sqrt{2})(X + i\sqrt{2})$ et admet 3 racines simples. P est bien scindé sur $\mathbb{C}$ (comme tout polynôme sur $\mathbb{C}$).

Remarque. Toutes les équations de degré 2 ont deux solutions (éventuellement confondues) dans $\mathbb{C}$. Le théorème fondamental exprime que toute équation de degré n admet n solutions (éventuellement confondues) dans $\mathbb{C}$. Dans le cas $n = 3$ ou 4, il existe des formules (assez compliquées) donnant les solutions en fonction des coefficients. Pour une équation de degré supérieur ou égal à 5, il a été prouvé par E. Galois, que de telles formules n'existent pas.

Corollaire 2.44 (Factorisation sur $\mathbb{C}$)**.** *Tout polynôme P non nul de $\mathbb{C}[X]$ admet une décomposition en facteurs irréductibles du type suivant :*

$$P = \lambda \prod_{i=1}^{k} (X - \gamma_i)^{\alpha_i},$$

où $\{\gamma_1, \ldots, \gamma_k\}$ est l'ensemble des racines de P, α_i est la multiplicité de γ_i, et λ est le coefficient du terme dominant de P.

2.9.3 Polynômes irréductibles de $\mathbb{R}[X]$

Dans $\mathbb{R}[X]$, la situation est un peu plus compliquée. On sait d'ores et déjà que pas tous les polynômes irréductibles sont de degré 1 : par exemple, $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$ car n'a pas de racine réelle (la fonction polynomiale associée est minorée par 1, donc ne s'annule jamais).

Proposition 2.45. *Soient $P \in \mathbb{R}[X]$ et $\gamma \in \mathbb{C}$. γ est racine de P (vu comme polynôme de $\mathbb{C}[X]$) si et seulement si $\overline{\gamma}$ est racine de P. En particulier, les racines complexes non réelles de P sont deux à deux conjuguées.*

Démonstration. On a $\tilde{P}(\gamma) = 0$ si et seulement si $\overline{\tilde{P}(\gamma)} = 0$. Or P a des coefficients réels, la dernière égalité est égale à $\tilde{P}(\overline{\gamma}) = 0$. □

Lemme 2.46. *Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de $\mathbb{C}[X]$. Notons $\overline{P} = \sum_{k=0}^{n} \overline{a_k} X^k$ le polynôme conjugué. Alors γ est racine de P de multiplicité α si et seulement si $\overline{\gamma}$ est racine de $\overline{P}$ de multiplicité α.*

Démonstration. Soit γ une racine de P de multiplicité α. Alors il existe un polynôme Q tel que $P = Q(X - \gamma)^\alpha$. En prenant le conjugué de cette expression, on obtient $\overline{P} = \overline{Q}(X - \overline{\gamma})^\alpha$. Donc $\overline{\gamma}$ est racine de $\overline{P}$ de multiplicité $\geq \alpha$. En échangeant les rôles de P et $\overline{P}$, λ et $\overline{\lambda}$, on obtient le résultat. □

Théorème 2.47. *Les polynômes irréductibles de $\mathbb{R}[X]$ sont :*

- *Les polynômes de degré 1 ;*
- *Les polynômes de degré 2 à discriminant strictement négatif : $P = aX^2 + bX + c$ avec $a \neq 0$ et $\triangle = b^2 - 4ac < 0$.*

Démonstration. On sait déjà que les polynômes de degré 1 sont irréductibles. Soit maintenant $P = aX^2 + bX + c$ à discriminant strictement négatif. La fonction $t \mapsto P(t)$ associée ne s'annule pas sur $\mathbb{R}$, et donc aucun polynôme de degré 1 ne saurait diviser P. Par ailleurs, on sait que toute équation de degré 2 à coefficients réels et discriminant positif ou nul admet au moins une solution réelle. Donc les polynômes de degré 2 à discriminant positif ne sont pas irréductibles dans $\mathbb{R}[X]$. Soit maintenant $P \in \mathbb{R}[X]$ un polynôme de degré au moins 3. Supposons que P n'ait pas de racine réelle (sinon P n'est pas irréductible dans $\mathbb{R}[X]$). D'après le Lemme 2.46, les racines complexes non réelles de P sont deux à deux conjuguées (avec ordres de multiplicité égaux deux à deux). Le Corollaire 2.44 assure donc l'existence de nombres complexes (non réels) $\gamma_1, \ldots, \gamma_p$, d'entiers $\beta_1, \ldots, \beta_p$, et d'un réel λ, tels que

$$P = \lambda \prod_{i=1}^{p} \left((X - \gamma_i)^{\beta_i} (X - \overline{\gamma_i})^{\beta_i} \right).$$

Mais un calcul facile montre que

$$(X - \gamma_i)^{\beta_i} (X - \overline{\gamma_i})^{\beta_i} = (X^2 - 2\Re(\gamma_i)X + |\gamma_i|^2)^{\beta_i},$$

où $\Re(\gamma_i)$ désigne la partie réelle de γ_i. Donc P est divisible par le polynôme réel $X^2 - 2\Re(\gamma_i)X + |\gamma_i|^2$ (de degré 2) et n'est donc pas irréductible.

□

En reprenant la preuve ci-dessus, on déduit facilement le résultat suivant.

Corollaire 2.48 (Factorisation sur $\mathbb{R}$)**.** *Soit P un polynôme à coefficients réels. Soient $\gamma_1, \gamma_2, \ldots, \gamma_p$ ses racines réelles de multiplicités respectives $\alpha_1, \ldots, \alpha_p$, et $\delta_1, \bar{\delta}_1, \delta_2, \bar{\delta}_2, \ldots, \delta_q, \bar{\delta}_q$ ses paires de racines complexes conjuguées de multiplicités respectives $\beta_1, \beta_2, \ldots, \beta_q$. Alors*

$$P = \lambda (X - \gamma_1)^{\alpha_1} \cdots (X - \gamma_p)^{\alpha_p} (X^2 - b_1 X + c_1)^{\beta_1} \cdots (X^2 - b_q X + c_q)^{\beta_q},$$

où λ est le coefficient du terme de plus haut degré de P et où on a posé pour $1 \leq j \leq q$:

$$b_j = \delta_j + \bar{\delta}_j, \quad c_j = \delta_j \bar{\delta}_j.$$

Exemple (Factorisation de $X^n - 1$ sur $\mathbb{R}$). Cherchons de factoriser $P = X^n - 1$ sur $\mathbb{R}$. Les racines de ce polynôme sont des racines d'unité de la forme $e^{2i\pi j/n}$ pour $0 \leq j < n$. Nous distinguons les cas $n = 2k$ et $n = 2k + 1$. Pour $n = 2k$, les racines réelles de P sont $1 = e^{2i\pi 0/(2k)}$ et $-1 = e^{2i\pi k/(2k)}$, pour le cas $n = 2k + 1$ uniquement $1 = e^{2i\pi 0/(2k+1)}$ est une racine réelle. Or $e^{2i\pi j/n} + e^{-2i\pi j/n} = 2\cos(2\pi j/n)$, nous trouvons donc les factorisations

$$X^{2k} = (X - 1)(X + 1) \prod_{j=1}^{k-1} \left(X^2 - 2\cos\left(\frac{\pi j}{k}\right) X + 1 \right),$$

$$X^{2k+1} = (X - 1) \prod_{j=1}^{k} \left(X^2 - 2\cos\left(\frac{2\pi j}{2k+1}\right) X + 1 \right).$$

Exemple. $P(X) = 2X^4(X-1)^3(X^2+1)^2(X^2+X+1)$ est déjà décomposé en facteurs irréductibles dans $\mathbb{R}[X]$ alors que sa décomposition dans $\mathbb{C}[X]$ est $P(X) = 2X^4(X-1)^3(X-i)^2(X+i)^2(X-j)(X-j^2)$ où $j = e^{2i\pi/3} = \frac{-1+i\sqrt{3}}{2}$.

2.10 Relations entre coefficients et racines

Commençons par un exemple concret. Soit P un polynôme scindé de degré 3. On a $P = a_3(X-\gamma_1)(X-\gamma_2)(X-\gamma_3) = a_3X^3 + a_2X^2 + a_1X + a_0$. En identifiant les coefficients des puissances de X on trouve

$$a_2 = -a_3(\gamma_1+\gamma_2+\gamma_3), \qquad a_1 = a_3(\gamma_1\gamma_2+\gamma_1\gamma_3+\gamma_2\gamma_3), \qquad a_0 = -a_3(\gamma_1\gamma_2\gamma_3).$$

Définition 2.26. Soit $(\gamma_i)_{1\le i\le n}$ une famille de n éléments de $\mathbb{K}$. La *kème fonction symétrique élémentaire* de la famille $(\gamma_i)_{1\le i\le n}$ est l'élément σ_k de $\mathbb{K}$ défini par

$$\sigma_k = \sum_{1\le i_1<i_2<\cdots<i_k\le n} \gamma_{i_1}\gamma_{i_2}\cdots\gamma_{i_k}.$$

Ainsi

$$\sigma_1 = \gamma_1+\cdots+\gamma_n, \qquad \sigma_2 = \sum_{1\le i<j\le n}\gamma_i\gamma_j, \qquad \ldots, \quad \sigma_n = \gamma_1\cdots\gamma_n,$$

et on définit $\sigma_0 = 1$.

Proposition 2.49. *Soit $P \in \mathbb{K}[X]$ scindé de degré n et soient $\gamma_1,\ldots,\gamma_n$ les racines de P comptées sans multiplicités. Alors si $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ (avec $a_n \neq 0$) on a pour tout $1 \le k \le n$,*

$$\sigma_k = (-1)^k\frac{a_{n-k}}{a_n}.$$

En particulier, a_{n-1} est l'opposé de la somme des racines et $(-1)^n a_0$ est le produit des racines.

Démonstration. On a $P = a_nX^n + \cdots + a_1X + a_0 = a_n(X-\gamma_1)\cdots(X-\gamma_n)$. Pour obtenir la formule, il suffit de développer $a_n(X-\gamma_1)\cdots(X-\gamma_n)$ et d'identifier les coefficients des termes de plus haut degré. □

Remarque. Toute quantité qui dépend de manière symétrique des racines $\gamma_1,\ldots,\gamma_n$ peut s'exprimer en fonction des coefficients du polynôme P.

Chapitre 3

Compléments (CPU)

3.1 Compléments (CPU) : Calcul de pgcd et des éléments de Bézout

Exemple. On peut utiliser le *calcul matriciel* pour trouver de manière *plus efficace* (a, b), u et v dans $au + bv = (a, b)$. Prenons l'exemple de $a = 931$ et $b = 513$. Nous itérons la relation

$$a = b \times q + r \quad \Longleftrightarrow \quad \begin{cases} b = 0 \times a + 1 \times b \\ r = 1 \times a - q \times b \end{cases} \quad \Longleftrightarrow \quad \begin{pmatrix} b \\ r \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

On calcule

$$\begin{aligned} 931 = 513 \times 1 + 418 \quad &\Longleftrightarrow \quad \begin{pmatrix} 513 \\ 418 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 931 \\ 513 \end{pmatrix} \\ 513 = 418 \times 1 + 95 \quad &\Longleftrightarrow \quad \begin{pmatrix} 418 \\ 95 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 513 \\ 418 \end{pmatrix} \\ 418 = 95 \times 4 + 38 \quad &\Longleftrightarrow \quad \begin{pmatrix} 95 \\ 38 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 418 \\ 95 \end{pmatrix} \\ 95 = 38 \times 2 + 19 \quad &\Longleftrightarrow \quad \begin{pmatrix} 38 \\ 19 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 95 \\ 38 \end{pmatrix} \end{aligned}$$

et $38 = 19 \times 2 + 0$. Il vient donc $(931, 513) = 19$ et

$$\begin{pmatrix} 38 \\ 19 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 931 \\ 513 \end{pmatrix} = \begin{pmatrix} 5 & -9 \\ -11 & 20 \end{pmatrix} \begin{pmatrix} 931 \\ 513 \end{pmatrix}.$$

La seconde ligne dans le produit matriciel de droite donne la relation de Bézout : $19 = -11 \times 931 + 20 \times 513$.

3.2 Compléments (CPU) : Analyse d'algorithme d'Euclide

Proposition 3.1 (Suite de Fibonacci)**.** *La suite*

$$F_0 = 0, \quad F_1 = 1, \quad F_2 = 1, \quad F_3 = 2, \quad F_4 = 3, \quad F_5 = 5, \quad F_6 = 8, \quad F_7 = 13 \dots$$

définie par la relation de récurrence $F_{n+2} = F_{n+1} + F_n$*, vérifie*

$$F_n = \frac{1}{\sqrt{5}}(\varphi^n - \hat{\varphi}^n),$$

où φ *est le nombre d'or :*

$$\varphi = \frac{1+\sqrt{5}}{2}, \qquad \hat{\varphi} = \frac{1-\sqrt{5}}{2} = -\frac{1}{\varphi}, \qquad \varphi^2 = \varphi + 1,$$

et comme $|\hat{\varphi}| \leq 1$*, on a*

$$\forall n \geq 0, \quad \left| F_n - \frac{1}{\sqrt{5}}\varphi^n \right| \leq 1.$$

Démonstration. Une preuve possible serait de vérifier que l'expression donnée satisfait à la relation de récurrence et les valeurs initiales. □

Étudions maintenant la vitesse de convergence de l'algorithme d'Euclide (Lamé, 1845).

Proposition 3.2. *Soit* $n \geq 4$ *et* $1 \leq b \leq a < F_n$*. Le nombre* $N(a, b)$ *d'étapes dans l'algorithme d'Euclide (pour calculer* (a, b)*) est* $\leq n - 3$*. De plus* $N(F_n, F_{n-1}) = n - 2$*.*

Démonstration. Si $b \mid a$ alors $N(a, b) = 1$. On a aussi $N(1, a) = N(a, a) = 1$. Raisonnons par récurrence. Pour $n = 4$, $1 \leq b \leq a < 3$ donc $b = 1$ ou $b = 2 = a$. D'où $N(a, b) = 1$. Pour $n = 5$, $1 \leq b \leq a \leq 4 = F_5 - 1$.

— Si $b = 1$ ou $b = a$ alors $N(a, b) = 1$,
— Si $b = 2$ ou $a = 3$ alors $N(a, b) = 2$,
— Si $b = 2$ ou $a = 4$ alors $N(a, b) = 1$,
— Si $b = 3$ ou $a = 4$ alors $N(a, b) = 2$.

Supposons la propriété vraie pour n. Soit $1 \leq b \leq a < F_{n+1}$.

— Si $b < F_n$ alors $a = bq + r$ avec $r < b < F_n$, donc

$$N(a, b) = 1 + N(b, r) \leq 1 + n - 3 = n - 2.$$

— Si $b \geq F_n$ alors $a = q_1 b + r_1$ avec $q_1 = 1$ et $r_1 < b$. Comme $a < F_{n+1}$,

$$r_1 = a - b < F_{n+1} - F_n = F_{n-1}.$$

On recommence : $b = q_2 r_1 + r_2$ avec $r_2 < r_1 < F_{n-1}$ et

$$N(a, b) = 2 + N(r_1, r_2) \leq 2 + n - 4 = n - 2.$$

Conclusion :

$$n \geq 4 \quad \text{et} \quad 1 \leq b \leq a < F_n \quad \Longrightarrow \quad N(a,b) \leq n-3.$$

Pour calculer $N(F_n, F_{n-1})$, on compte les signes "=" :

$$(F_n, F_{n-1}) = (F_{n-1}, F_{n-2}) = \cdots = (F_2, F_1).$$

□

Corollaire 3.3. *Si $1 \leq a, b < x$ entier, alors*

$$N(a,b) \leq \frac{\log x}{\log \varphi} + 1 \leq 4.785 \log_{10} x + 1.$$

Démonstration. Soit n tel que $F_{n-1} < x \leq F_n$. On a $N(a,b) \leq n-3+1$ (si $a < b$) et

$$\frac{1}{\sqrt{5}} \varphi^{n-1} \leq F_{n-1} + 1 \leq x \quad (x \text{ entier}),$$

d'où

$$n - 1 \leq \frac{\log x\sqrt{5}}{\log \varphi} = \frac{\log x}{\log \varphi} + \frac{\log \sqrt{5}}{\log \varphi}$$
$$N(a,b) \leq n - 2 \leq \frac{\log x}{\log \varphi} + 1.672276 - 1.$$

□

Question : Quel est le plus petit entier a tel qu'il existe un entier $b < a$ tel que l'algorithme d'Euclide pour la recherche de (a,b) nécessite au moins n divisions ?

3.3 Compléments (CPU) : Structure de $\mathbb{Z}/n\mathbb{Z}$, indicatrice d'Euler

Définition 3.1. On appelle *indicatrice d'Euler* (ou *indicateur d'Euler*) le nombre $\varphi(n)$ d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Exemple. L'ensemble des éléments inversibles de $\mathbb{Z}/12\mathbb{Z}$ sont les entiers $1 \leq a \leq 12$ tels que $(a, 12) = 1$. Cet ensemble est $\{1, 5, 7, 11\}$, donc $\varphi(12) = 4$.

Proposition 3.4 (Théorème d'Euler)**.** *Si $(a,n) = 1$, alors $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Remarque. La preuve classique de ce théorème utilise la structure du groupe de $(\mathbb{Z}/n\mathbb{Z})^*$ et le théorème de Lagrange que nous ne traitons pas ici. On peut également généraliser la preuve directe donnée pour le petit théorème de Fermat pour obtenir le théorème d'Euler en remplaçant $\{1, 2, \ldots, p-1\}$ par $\{b_1, b_2, \ldots, b_{\varphi(n)}\}$ avec $(b_i, n) = 1$ pour tout i.

Remarque. Si p est premier alors $\varphi(p) = p-1$ et donc le petit théorème de Fermat est un corollaire du théorème d'Euler.

Proposition 3.5. *On a*

$$\sum_{d|n} \varphi(d) = n.$$

Démonstration. En simplifiant les n fractions suivantes :

$$\frac{1}{n}, \frac{2}{n}, \dots, \frac{n-1}{n}, \frac{n}{n},$$

on obtient des dénominateurs d qui divisent n. On a ainsi

$$n = \sum_{d|n} \sum_{\substack{1 \le a \le d \\ (a,d)=1}} 1 = \sum_{d|n} \varphi(d)$$

où la somme intérieure précédente compte le nombre de fractions de dénominateurs d. □

Remarque. $(\mathbb{Z}/p\mathbb{Z})^*$ est un *groupe commutatif* par rapport à la multiplication mod p (commutativité, associativité, élément neutre, éléments inverses).

Proposition 3.6. *Le groupe $(\mathbb{Z}/p\mathbb{Z})^*$, pour p premier, est cyclique : il existe g tel que*

$$\{\overline{1}, \overline{2}, \dots, \overline{p-1}\} = \{\overline{g}, \overline{g^2}, \dots, \overline{g^{p-1}} = \overline{1}\}.$$

On dit que g est un générateur*, ou une* racine primitive.

Remarque. Si g est un générateur alors les autres générateurs sont les g^a avec $1 \le a \le p-1$ et $(a, p-1) = 1$. Par conséquent il y a $\varphi(p-1)$ générateurs, c'est-à-dire beaucoup. En pratique, en essayant $g = 2, 3, 5, 6, 7, 8, 10, 11, \dots$ on trouve vite un générateur. On ne sait pas démontrer que cette méthode est rapide "en théorie".

Exemple. 2 n'est pas générateur de $(\mathbb{Z}/7\mathbb{Z})^*$ car $\{\overline{2}, \overline{2^2}, \dots, \overline{2^6}\} = \{\overline{1}, \overline{2}, \overline{4}\}$. 3 est générateur de $(\mathbb{Z}/7\mathbb{Z})^*$ car $\{\overline{3}, \overline{3^2}, \dots, \overline{3^6} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$.

Définition 3.2. Étant donné p premier, g générateur de $(\mathbb{Z}/p\mathbb{Z})^*$, pour chaque a, $1 \le a \le p-1$, il existe un unique b, $1 \le b \le p-1$ tel que $g^b \equiv a \pmod{p}$. On dit que b est le *logarithme discret* de a relativement à g.

Remarque. Si p est grand, g connu, le calcul de b connaissant a est considéré comme un problème difficile (*problème du logarithme discret*).

Proposition 3.7. *[Théorème de Wilson] Soit $n \ge 2$ un entier. Alors*

$$n \text{ est un nombre premier} \iff (n-1)! \equiv -1 \pmod{n}.$$

Démonstration. Si $n = 2$, alors $(n-1)! \equiv -1 \pmod 2$. Soit maintenant n un nombre premier ≥ 3. Tout élément $\overline{1}, \overline{2}, \ldots, \overline{n-1}$ a un inverse dans $\mathbb{Z}/n\mathbb{Z}$ et ces inverses sont dans $\mathbb{Z}/n\mathbb{Z} \setminus \{0\}$. On peut donc former des paires constituées d'un élément et de son inverse sauf quand l'élément est égal à son propre inverse. Mais pour $(x, n) = 1$, on a

$$\overline{x} = \overline{x}^{-1} \Longleftrightarrow \overline{x}^2 = \overline{1} \Longleftrightarrow (\overline{x} - \overline{1})(\overline{x} + \overline{1}) = \overline{0} \Longleftrightarrow \overline{x} = \overline{1} \text{ ou } \overline{x} = \overline{-1} = \overline{n-1},$$

car n est un nombre premier. On en déduit que

$$\overline{1} \cdot \overline{2} \cdots \overline{n-1} = \overline{1} \cdot (\overline{2} \cdot (\overline{2})^{-1}) \cdot (\overline{3} \cdot (\overline{3})^{-1}) \cdots (\overline{m} \cdot (\overline{m})^{-1}) \cdot \overline{n-1},$$

où $m = \frac{n-3}{2}$ donc

$$\overline{1} \cdot \overline{2} \cdots \overline{n-1} = \overline{n-1} = \overline{-1}.$$

Donc $(n-1)! \equiv -1 \pmod n$.
Réciproquement, si $(n-1)! \equiv -1 \pmod n$, alors il existe $k \in \mathbb{Z}$ tel que $(n-1)! = -1 + kn$, ou encore $kn - (n-1)! = 1$. Ainsi on a une relation de Bézout entre n et tout entier $1 \leq j < n$. Donc $1, 2, \ldots, n-1$ sont premiers avec n. Cela prouve que n est un nombre premier. □

Proposition 3.8. *Soit p un nombre premier, $k \in \mathbb{Z}$ tel que $0 \leq k \leq p-1$. Alors*

$$k!(p-1-k)! \equiv (-1)^{k+1} \pmod p.$$

Démonstration. Si $p = 2$, on vérifie directement l'énoncé. Supposons p impair. On a $\pmod p$

$$\begin{aligned}
(p-1)! &\equiv k!(k+1)\cdots(p-1) \\
&\equiv k!(p-(k+1))(-1)\cdot(p-(k+2))(-1)\cdots(p-(p-1))(-1) \\
&\equiv k!(p-(k+1))!(-1)^{(p-1)-(k+1)+1} \\
&\equiv k!(p-1-k)!(-1)^{-k} \equiv -1.
\end{aligned}$$

□

Corollaire 3.9. *Soit p un nombre premier impair. Alors*

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv \begin{cases} 1 \pmod p, & p \equiv 3 \pmod 4 \\ -1 \pmod p, & p \equiv 1 \pmod 4. \end{cases}$$

Corollaire 3.10. *Si $p \equiv 1 \pmod 4$ alors $x^2 \equiv -1 \pmod p$ possède une solution :*

$$x \equiv \pm\left(\frac{p-1}{2}\right)! \pmod p.$$

Théorème 3.11 (Théorème des deux carrés de Fermat)**.** *Si $p \equiv 1 \pmod 4$ alors il existe des entiers $x, y \in \mathbb{Z}$ tels que $p = x^2 + y^2$.*

Démonstration. Si $p \equiv 1 \pmod 4$ alors, par le Corollaire 3.10 il existe $a \in \mathbb{Z}$ tel que $a^2 \equiv -1 \pmod p$. Considérons $\mathcal{A} = \{x - ay : \quad 0 \leq x \leq \sqrt{p}, \quad 0 \leq y \leq \sqrt{p},\}$. On a $\#\mathcal{A} = (\lfloor \sqrt{p} \rfloor + 1)^2 > p$ donc par le principe de tiroirs (de Dirichlet) il existe $z_1 = x_1 - ay_1 \in \mathcal{A}$ et $z_2 = x_2 - ay_2 \in \mathcal{A}$ tels que $z_1 \neq z_2$ et $z_1 \equiv z_2 \pmod p$. Cela implique que $x_1 - x_2 \equiv a(y_1 - y_2) \pmod p$. Posons $x = x_1 - x_2$ et $y = y_1 - y_2$, donc $x^2 + y^2 = a^2y^2 + y^2 \equiv 0 \pmod p$. Or $0 \leq x, y < \sqrt{p}$ on a $x^2 + y^2 < 2p$ et donc $x^2 + y^2 = p$ car $x^2 + y^2 = 0$ implique $z_1 = z_2$ qui est une contradiction à la construction de z_1 et z_2. □

3.4 Compléments (CPU) : Polynôme d'interpolation de Lagrange

Proposition 3.12. *Soit $n \in \mathbb{N}^*$. Soient $a_1, \dots a_n$ des éléments deux à deux distincts de $\mathbb{K}$, et $b_1, \dots b_n$ des éléments de $\mathbb{K}$. Alors il existe un unique polynôme P de degré inférieur ou égal à $n-1$ vérifiant $P(a_j) = b_j$ pour tout $1 \leq j \leq n$. Ce polynôme est donné par la formule suivante :*

$$P = \sum_{k=1}^{n} b_k \prod_{i \neq k} \frac{X - a_i}{a_k - a_i}.$$

Démonstration. Il est immédiat que le polynôme P proposé convient bien. Supposons que Q soit un autre polynôme solution. On a alors $P(a_j) - Q(a_j) = 0$ pour tout j avec $1 \leq j \leq n$. Le polynôme $P - Q$ qui est de degré inférieur ou égal à $n - 1$ (comme différence de tels polynômes), a alors au moins n racines (les a_j sont distincts). C'est donc le polynôme nul et $P = Q$. □

Remarque. La formule ci-dessus est due au mathématicien Joseph Louis Lagrange (1736-1813) ; on parle du "polynôme d'interpolation de Lagrange associé aux couples $(a_1, b_1), \dots, (a_n, b_n)$".

Exemple. Le polynôme d'interpolation de Lagrange P tel que $P(-1) = 2$, $P(0) = 1$ et $P(1) = -1$ est

$$P = 2\frac{X(X-1)}{(-1)\cdot(-2)} + \frac{(X+1)(X-1)}{1\cdot(-1)} - \frac{(X+1)X}{2\cdot 1} = -\frac{1}{2}X^2 - \frac{3}{2}X + 1.$$

Dans le plan muni d'un repère orthonormé, on a ainsi trouvé une parabole passant par les trois points de coordonnées $(-1, 2)$, $(0, 1)$ et $(1, -1)$.

Remarque. Dès que d est supérieur ou égal à n, il existe une infinité de polynômes P de degré d tels $P(a_j) = b_j$ pour $1 \leq j \leq n$.

3.5 Compléments (CPU) : Sommes de Newton

Proposition 3.13. *Soit*

$$P = \prod_{i=1}^{n}(X - \gamma_i) = \sum_{i=0}^{n}(-1)^i \sigma_i X^{n-i}$$

et notons

$$S_k = \gamma_1^k + \cdots + \gamma_n^k, \qquad k \geq 1,$$

les sommes de Newton. *Nous avons les identités suivantes :*

(i) Si $p \geq n$ alors

$$S_p - \sigma_1 S_{p-1} + \sigma_2 S_{p-2} - \cdots + (-1)^n \sigma_n S_{p-n} = 0.$$

(ii) Si $1 \leq p < n$ alors

$$S_p - \sigma_1 S_{p-1} + \sigma_2 S_{p-2} - \cdots + (-1)^{n-1} \sigma_{p-1} S_1 + (-1)^p \sigma_p p = 0.$$

Démonstration. (i) Soit $p \geq n$. Pour un i fixé on a

$$\begin{aligned}\gamma_i^p - \sigma_1 \gamma_i^{p-1} + \sigma_2 \gamma_i^{p-2} - \cdots + (-1)^n \sigma_n \gamma_i^{p-n} &= \gamma_i^{p-n}(\gamma_i^n - \sigma_1 \gamma_i^{n-1} + \cdots + (-1)^n \sigma_n) \\ &= \gamma_i^{p-n} P(\gamma_i) = 0,\end{aligned}$$

d'où le résultat en sommant sur $1 \leq i \leq n$.

(ii) Soit $1 \leq p < n$. Toujours à i fixé, une division euclidienne de P par $X - \gamma_i$ donne

$$\begin{aligned}\frac{P}{X - \gamma_i} = X^{n-1} + (\gamma_i - \sigma_1) X^{n-2} + \left(\gamma_i^2 - \gamma_i \sigma_1 + \sigma_2\right) X^{n-3} + \cdots \\ + \left(\gamma_i^{n-1} - \gamma_i^{n-2} \sigma_1 + \cdots + (-1)^{n-1} \sigma_{n-1}\right)\end{aligned}$$

d'où en sommant sur $1 \leq i \leq n$

$$\begin{aligned}\sum_{i=1}^{n} \frac{P}{X - \gamma_i} = X^{n-1} + (S_1 - n\sigma_1) X^{n-2} + (S_2 - S_1 \sigma_1 + n\sigma_2) X^{n-3} + \cdots \\ + (S_{n-1} - S_{n-2} \sigma_1 + \cdots + (-1)^{n-1} n \sigma_{n-1}).\end{aligned}$$

On observe que nous avons deux écritures différentes pour la derivée de P :

$$\begin{aligned}P' &= (X - \gamma_2) \cdots (X - \gamma_n) + \cdots + (X - \gamma_1) \cdots (X - \gamma_{n-1}) \\ &= \sum_{i=1}^{n} \frac{P}{X - \gamma_i} = \sum_{i=0}^{n-1} (-1)^i (n - i) \sigma_i X^{n-i-1}.\end{aligned}$$

Pour $1 \leq p < n$, on compare le coefficient en X^{n-p-1} dans ces deux écritures et on trouve :

$$S_p - \sigma_1 S_{p-1} + \sigma_2 S_{p-2} - \cdots + (-1)^{p-1} \sigma_{p-1} S_1 + (-1)^p n \sigma_p = (n - p)(-1)^p \sigma_p,$$

d'où

$$S_p - \sigma_1 S_{p-1} + \sigma_2 S_{p-2} - \cdots + (-1)^{p-1}\sigma_{p-1}S_1 + (-1)^p p\sigma_p = 0.$$

□

Remarque. On ne peux pas harmoniser les deux cas en écrivant

$$S_p - \sigma_1 S_{p-1} + \sigma_2 S_{p-2} - \ldots + (-1)^{n-1}\sigma_{p-1}S_1 + (-1)^n \sigma_p S_0 = 0$$

car cela est faux vu que $S_0 = \sum_{i=1}^n \gamma_i^0 = \sum_{i=1}^n 1 = n \neq p$.

Terminons avec deux exemples de calculs.

Exemple. Notons $\gamma_1, \gamma_2, \gamma_3$ les trois racines complexes du polynôme $P = X^3 - X + 1$. Calculer $\gamma_1^7 + \gamma_2^7 + \gamma_3^7$.

Réponse : Les relations entre coefficients et racines s'écrivent $\sigma_1 = 0$, $\sigma_2 = -1$ et $\sigma_3 = -1$. On effectue la division euclidienne de X^7 par P :

$$X^7 = P \cdot (X^4 + X^2 - X + 1) - 2X^2 + 2X - 1.$$

Si γ_i est une racine de P on a donc $\gamma_i^7 = -2\gamma_i^2 + 2\gamma_i - 1$ (puisque $\tilde{P}(\gamma_i) = 0$). On en déduit

$$\begin{aligned}\gamma_1^7 + \gamma_2^7 + \gamma_3^7 &= -2(\gamma_1^2 + \gamma_2^2 + \gamma_3^2) + 2(\gamma_1 + \gamma_2 + \gamma_3) - 3 \\ &= -2(\sigma_1^2 - 2\sigma_2) + 2\sigma_1 - 3 = -7.\end{aligned}$$

Exemple. Notons $\gamma_1, \gamma_2, \gamma_3$ les trois racines complexes du polynôme $P = X^3 + 3X^2 + 4X - 8$. Calculer $S_2 = \gamma_1^2 + \gamma_2^2 + \gamma_3^2$ et $S_4 = \gamma_1^4 + \gamma_2^4 + \gamma_3^4$.

Réponse : Les relations entre coefficients et racines s'écrivent $\sigma_1 = -3$, $\sigma_2 = 4$ et $\sigma_3 = 8$. Nous allons utiliser les identités de la proposition (nous pouvons aussi utiliser la démarche dans l'exemple précédent). Pour $n = 3$ cela donne

$$\begin{aligned} S_1 + 3 &= 0 \quad (p = 1), \\ S_2 + 3S_1 + 8 &= 0 \quad (p = 2), \\ S_3 + 3S_2 + 4S_1 - 24 &= 0 \quad (p = 3), \\ S_4 + 3S_3 + 4S_2 - 8S_1 &= 0 \quad (p = 4). \end{aligned}$$

Donc, on trouve $S_1 = -3$, $S_2 = 1$, $S_3 = 33, S_4 = -127$.