CHAPITRE 5 L'ANNEAU DES ENTIERS Z.

La théorie des nombres est une des plus belles branches des mathématiques (Zut! L'auteur s'est dévoilé comme spécialiste de la théorie des nombres). Traditionnellement l'étude des propriétés de divisibilité fait apparaître la notion de nombres premiers : les entiers naturels divisibles uniquement par 1 et par eux-mêmes (on exclut 1 par convention) dont le début de la liste peut être obtenu par le crible d'Eratosthène : on raye les multiples de 2, puis les multiples de 3,5,7 et on obtient :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, \ldots$$

ainsi que l'étude d'équations "diophantiennes comme $x^2 + y^2 = z^2$ (triangle pythagoriciens). Longtemps considérée comme une des branches les plus "pures", la théorie des nombres a trouvé des applications en informatique, cryptographie (code de cartes bancaires par exemple). Un des problèmes fondamentaux est de trouver (ou de prouver qu'il n'existe pas) un algorithme "rapide" de factorisation en produit de nombres premiers. L'arithmétique dans $\mathbf{N}$ *est souvent simplifiée par l'introduction des nombres négatifs, i.e. par l'introduction de l'anneau* $\mathbf{Z}$.

5.1 ARITHMÉTIQUE

Nous supposons connu l'ensemble

$$\mathbf{Z} := \{\ldots, -n, -n+1, \ldots, -2, -1, 0, 1, 2, \ldots, n-1, n, \ldots\}$$

qui est muni d'une loi d'addition et d'une loi de multiplication qui en font un anneau commutatif. Il est aussi muni d'une relation d'ordre qui permet de définir la *valeur absolue* d'un entier par la formule $|n| := max\{n, -n\}$.

Divisibilité : on dira que a divise b si b est un multiple de a ou encore si il existe $c \in \mathbf{Z}$ tel que $b = ac$. Un entier a est *inversible* si il existe $b \in \mathbf{Z}$ tel que $ab = 1$; on voit facilement que ceci équivaut à $a = \pm 1$. Ainsi, si a divise b et b divise a alors $a = \pm b$. Un nombre est *premier* si ses seuls diviseurs positifs sont 1 et lui-même (on exclut +1 et -1 par convention) ; on se restreint parfois aux nombres premiers positifs.

La propriété la plus fondamentale de l'anneau $\mathbf{Z}$ est l'existence de la *division euclidienne* qui est utilisée par l'étudiant depuis l'école primaire (au moins pour les nombres positifs) :

THÉORÈME: *Soit $a, b \in \mathbf{Z}$ avec $b \neq 0$ alors il existe $q, r \in \mathbf{Z}$, uniques, tels que :*
$a = bq + r \ 0 \leq r < |b|$

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

Démonstration: Supposons d'abord pour simplifier que b est positif. On regarde la suite des multiples (positifs et négatifs) de b. On constate qu'il existe $q \in \mathbf{Z}$ tel que $qb \leq a < (q+1)b$ (il suffit de prendre pour q le plus grand entier tel que $qb \leq a$) ; posons $r := a - bq$ alors il vient $0 \leq r < b$ d'où le résultat. Si b est négatif, on procède de même avec $-a$ et $-b$: on obtient $-a = q_1(-b) + r_1$ avec $0 \leq r_1 < -b = |b|$ d'où $a = q_1 b - r_1$. Si

$r_1 = 0$ on a déjà la division, sinon on écrit $a = (q_1 + 1)b + (-b - r_1)$ et on note qu'on a bien $0 \leq -b - r_1 < |b|$.

Pour prouver l'unicité, on suppose que $a = bq + r = bq' + r'$ avec $0 \leq r, r' < |b|$. On en tire $|b||q - q'| = |r - r'| < |b|$ ce qui entraîne $|q - q'| = 0$ et donc $q = q'$ puis $r = r'$. □

Remarque : la démonstration donnée est proche mais un peu différente de l'algorithme appris à l'école primaire et qui peut être décrit ainsi : on cherche $c_0 \in \{0, 1, \ldots, 9\}$ et $n \geq 0$ tel que $(c_0 10^n)b \leq a < (c_0+1)10^n b$ et on remplace a par $a_1 = a - c_0 10^n b$ et on calcule c_1 tel que $(c_1 10^{n-1})b \leq a_1 < (c_1 + 1)10^{n-1} b$ et à la fin on obtient $a = b(c_0 10^n + \ldots + c_n) + a_{n+1}$.

THÉORÈME: *Les sous-groupes de* $\mathbf{Z}$ *sont tous de la forme* $n\mathbf{Z}$ *avec* $n \in \mathbf{N}$.

Démonstration: Soit G un sous groupe de $\mathbf{Z}$. On sait que $0 \in G$, si $G = \{0\}$ alors $G = 0.\mathbf{Z}$, sinon il existe n le plus petit élément strictement positif de G. L'ensemble des multiples de n est contenu dans G ; inversement, soit $g \in G$, effectuons la division euclidienne de g par n, on obtient $g = nq + r$ avec $0 \leq r < n$. On a donc l'égalité $r = g - nq$ et donc (comme g et n sont dans G) l'ensemble G contient r mais par choix de n ceci entraîne que $r = 0$ et que g est un multiple de n. On a donc bien $G = n\mathbf{Z}$. □

Remarque : les sous-groupes de $\mathbf{Z}$ sont aussi ses *idéaux* i.e. les sous-ensembles $I \subset \mathbf{Z}$ tels que I soit un sous-groupe et tels que $a \in \mathbf{Z}$ et $b \in I$ entraîne $ab \in I$.

Définition: Le plus grand commun diviseur (PGCD) de deux nombres a et b est un nombre d qui divise a et b et tel que tout diviseur commun de a et b divise d.

Définition: Le plus petit commun multiple (PPCM) de deux nombres a et b est un nombre m qui est un multiple a et b et tel que tout multiple commun de a et b est multiple de m.

Remarque : il n'est pas évident que le PGCD ou le PPCM existe mais ceci est garanti par la proposition suivante. Quand à l'unicité, la remarque faite sur les éléments inversibles montre que le PGCD (ou le PPCM) est unique au signe près. On choisit bien sûr le signe plus.

Remarque : si $a, b \in \mathbf{Z}$ on peut définir le sous-ensemble suivant de $\mathbf{Z}$:

$$a\mathbf{Z} + b\mathbf{Z} := \{au + bv \mid u, v \in \mathbf{Z}\}$$

dont on vérifie aisément que c'est un sous-groupe. De même $a\mathbf{Z} \cap b\mathbf{Z}$ est un sous-groupe.

PROPOSITION: *Soit* a *et* b *deux entiers non nuls alors il existe deux entiers* d *et* m *tels que* $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$ *et* $a\mathbf{Z} \cap b\mathbf{Z} = m\mathbf{Z}$. *De plus l'entier* d *est un PGCD de* a *et* b, *et* m *est un PPCM de* a *et* b. *Enfin on a l'égalité* $ab = \pm md$.

Démonstration: Soit $d \in \mathbf{Z}$ tel que $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$, montrons que d est un PGCD de a et b. Tout d'abord $a = a.1 + b.0$ est un multiple de d donc d divise a (et aussi b par le même raisonnement ; on peut aussi écrire $d = au + bv$ pour certains entiers u, v, par conséquent tout entier e diviseur commun de a et b divise au, bv et donc leur somme c'est-à-dire d.

Soit $m \in \mathbf{Z}$ tel que $a\mathbf{Z} \cap b\mathbf{Z} = m\mathbf{Z}$, montrons que d est un PPCM de a et b. Tout d'abord $m \in a\mathbf{Z}$ donc m est un multiple de a (et aussi de b par le même raisonnement) ;

si m' est un multiple de a et b alors $m' \in a\mathbf{Z}$ et $m' \in b\mathbf{Z}$ et donc $m' \in m\mathbf{Z}$ c'est-à-dire que m' est un multiple de m.

On sait donc que $a = a'd$ et $b = b'd$ donc $r := a'b'd$ est un multiple de a et b et est donc divisible par m ; donc md divise $rd = ab$. Par ailleurs, d'après la première partie du théorème, il existe $u, v \in \mathbf{Z}$ tels que $d = au + bv$ donc $md = aum + bvm$; mais ab divise am et bm donc md et on peut conclure que $md = \pm ab$. □

Si $\mathrm{PGCD}(a, b) = 1$ on dit que a et b sont *premiers entre eux.* Le résultat précédent nous permet de caractériser ces nombres :

THÉORÈME: *(Bézout) Soit* $d := \mathrm{PGCD}(a, b)$ *alors il existe deux entiers* u *et* v *tels que*

$$au + bv = d$$

En particulier deux entiers a *et* b *sont premiers entre eux si et seulement si il existe* u, v *entiers tels que* $au + bv = 1$.

Démonstration: La première partie de l'énoncé est une conséquence directe de la proposition précédente. Pour la deuxième partie, notons que si $\mathrm{PGCD}(a, b) = 1$ alors il existe $u, v \in \mathbf{Z}$ tels que $au + bv = 1$; inversement si de tels u, v existent, alors un diviseur d de a et b diviserait $au + bv$ et donc 1 ce qui donne bien que a et b sont premiers entre eux. □

Une des méthodes les plus rapides pour calculer le PGCD (et par conséquent le PPCM) est la suivante :

THÉORÈME: *(Algorithme d'Euclide)*
L'algorithme suivant fournit un calcul du PGCD de a *et* b *:*
$a = bq_1 + r_1$ (division de a par b)
$b = r_1q_2 + r_2$ (division de b par r_1)
$r_1 = r_2q_3 + r_3$ (division de r_1 par r_2)
.....
$r_{n-1} = r_nq_{n+1} + r_{n+1}$ (division de r_{n-1} par r_n)
Jusqu'à ce que $r_{n+1} = 0$ *et alors* $\mathrm{PGCD}(a, b) = r_n$

Démonstration: Elle consiste à vérifier que

$$\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r_1) = \mathrm{PGCD}(r_1, r_2) = \ldots = \mathrm{PGCD}(r_{n-1}, r_n) = \mathrm{PGCD}(r_n, r_{n+1})$$

car clairement $\mathrm{PGCD}(r_n, r_{n+1}) = r_n$. Il suffit donc de montrer que pour a,b et q entier on a $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(a - bq, b)$; ceci résulte du fait que d divise a et b équivaut à d divise b et $a - bq$. □

Remarque : si on le souhaite, une variante de cet algorithme permet de trouver u, v entiers tels que $au + bv = \mathrm{PGCD}(a, b)$. En effet il suffit d'écrire $\mathrm{PGCD}(a, b) = r_n = r_{n-2} - q_nr_{n-1}$, $r_{n-1} = r_{n-3} - q_{n-1}r_{n-2}$ etc pour en tirer r_n comme combinaison de r_{n-2}, r_{n-3} et ainsi de suite jusqu'à l'exprimer comme combinaison de a et b (ceci fournit d'ailleurs une autre démonstration du théorème de Bézout).

Faisons ce calcul sur un exemple ;
1932=6.301+126
301=2.126+49
126=2.49+28
49=1.28+21
28=1.21+7
21=3.7+0 (FIN du calcul du PGCD)
et
7=28–21=2.28–49=2.126–5.49=–5.301+12.126=12.1932–77.301 (FIN du calcul)
Résultat : $\mathrm{PGCD}(1932, 301) = 7 = 12.1932 - 77.301$

THÉORÈME: *(i) (Euclide) Soit p un nombre premier, si p divise ab alors p divise a ou b.*

(ii) (Gauss) Si $\mathrm{PGCD}(a, b) = 1$ *et a divise bc alors a divise c.*

Démonstration: (i) Supposons que p ne divise pas a alors $1 = \mathrm{PGCD}(a, p) = pu + av$ donc $b = pbu + abv$ donc p divisant pbu et abv divise b.

(ii) On a de même $1 = \mathrm{PGCD}(a, b) = au + bv$ donc $c = acu + bcv$ donc a divise c. □

THÉORÈME: *(Unicité de la décomposition en facteurs premiers) Soit n un entier distinct de $0, 1, -1$ alors il existe $\varepsilon = \pm 1$, il existe des nombres premiers $p_1, \ldots, p_r$ et des entiers $m_1, \ldots, m_r \geq 1$ tels que*

$$n = \varepsilon p_1^{m_1} \ldots p_r^{m_r}$$

de plus cette décomposition est unique à l'ordre près.

Exemples : $6440 = 2^3.5.7.23$, $1932 = 2^2.3.7.23$, $301 = 7.43$ Question : Avez-vous déjà factorisé votre numéro de téléphone? Celui de la police est un nombre premier alors que celui des pompiers se décompose en 2.3^2.

Démonstration: L'existence se prouve par récurrence sur n : si n est premier alors, on est content, sinon on a $n = ab$ avec $a < n$ et $b < n$ donc a et b, d'après l'hypothèse de récurrence se décomposent en produit de nombres premiers et donc n aussi.

L'unicité découle de l'application répétée du théorème d'Euclide (ou de Gauss). □

Remarques : si l'on connait la décomposition en facteurs premiers de deux nombres on peut facilement en déduire leur PGCD, mais ce n'est pas en général une méthode efficace de calcul. Par exemple on retrouve $\mathrm{PGCD}(1932, 301) = 7$ et on peut calculer $\mathrm{PGCD}(6440, 1932) = 23$ et $\mathrm{PGCD}(6440, 301) = 1$.

APPLICATION: Soit $n \in \mathbf{N}$ qui ne soit pas le carré d'un entier naturel, alors n n'est pas non plus le carré d'un nombre rationnel ; en d'autres termes le nombre $\sqrt{n}$ n'est pas un nombre rationnel.

Démonstration: Ecrivons $n = p_1^{m_1} \ldots p_r^{m_r}$; comme n n'est pas un carré, l'un des nombres premiers p_i apparaît dans la décomposition avec un exposant m_i impair. Si l'on pouvait écrire $\sqrt{n} = a/b$ avec $a, b \in \mathbf{N}$ on aurait $b^2 = na^2$; appelons m (resp. n) l'exposant de p_i dans la décomposition de a (resp. de b), alors l'unicité de la décomposition entraîne que $2n = 2m + m_i$ ce qui est absurde puisque m_i est impair. □

APPLICATION: Il existe une infinité de nombres premiers :

Démonstration: Soient $p_1, \ldots, p_r$ un ensemble fini de nombres premiers, montrons qu'il existe un nombre premier distinct de ceux-ci, ce qui achèvera la démonstration. Pour cela considérons $N := (p_1 \ldots p_r) + 1$ et q un facteur premier de N (il en existe) ; comme les p_i ne divisent pas N on doit avoir q distinct des p_i. □

Cet énoncé peut être considérablement affiné en quantifiant "combien" il y a de nombres premiers. Appelons $\pi(x)$ le nombre de nombres premiers $\leq x$; par exemple $\pi(2) = 1$, $\pi(3) = 2$, $\pi(10) = 4$ et $\pi(100) = 25$. Il y a un siècle Hadamard et De La Vallée-Poussin ont réussi à montrer que $\pi(x)$ valait à peu près $x/\log(x)$ (présisément $\pi(x)\log(x)/x$ tend vers 1 quand x tend vers l'infini). On peut interpréter ceci en disant que la probabilité pour qu'un nombre $\leq x$ soit premier est environ $1/\log(x)$; par exemple $100/\log 100 = 21,71\ldots$ et $\pi(100)\log(100)/100 = 1,15\ldots$ est déjà proche de 1 ; en poussant un peu plus loin le calcul on obtient $\pi(1000000)\log(1000000)/1000000 = 1,084\ldots\ldots$

5.2 CONGRUENCES

L'étudiant connait depuis l'école primaire les raisonnements de parité, la "preuve" par neuf et (peut-être) la "preuve" par onze du résultat d'une multiplication. La théorie des congruences est une généralisation de ce type de raisonnement.

5.2.1 Propriétés des congruences

Soit n un entier (strictement) positif, rappelons la définition de la relation de congruence modulo n

Définition: Deux nombres entiers a et b sont *congruents modulo* n si leur différence est divisible par n. On note cela $a \equiv b \bmod n$.

C'est une relation d'équivalence : elle est réflexive, symétrique, transitive (voir chapitre 2). Enonçons quelques unes de ses propriétés :

PROPOSITION: *1) Supposons que $a \equiv b \bmod n$ et $c \equiv d \bmod n$, alors $a + c \equiv b + d \bmod n$ et $ac \equiv bd \bmod n$ et si $r \geq 0$, on a $a^r \equiv b^r \bmod n$.*

2) Si $\mathrm{PGCD}(c, n) = 1$ alors il existe $c' \in \mathbf{Z}$ tel que $cc' \equiv 1 \bmod n$ et donc la congruence $ac \equiv bc \bmod n$ entraîne $a \equiv b \bmod n$.

3) $a \equiv b \bmod mn$ entraîne $a \equiv b \bmod n$.

Démonstration: 1) L'hypothèse se traduit par $a = b + kn$ et $c = d + jn$ donc $a + c = b + d + (j + k)n$ et $ac = bd + (kd + bj + kjn)n$. L'égalité $a^r = b^r + \ell n$ s'obtient par récurrence sur r.

2) Si c et n sont premiers entre eux il existe $u, v \in \mathbf{Z}$ tels que $cu + nv = 1$ et par conséquent $cu \equiv 1 \bmod n$. Si maintenant $ac \equiv bc \bmod n$, en multipliant par u on obtient bien $a \equiv b \bmod n$.

3) C'est immédiat. □

Remarque : sans l'hypothèse $\mathrm{PGCD}(c, n) = 1$ la conclusion de l'énoncé 2) peut être fausse car par exemple $2.4 \equiv 2.1 \bmod 6$ mais $4 \not\equiv 1 \bmod 6$.

Exemples de calculs : $1995 \equiv 5 \bmod 10$ donc $1995^4 \equiv 5^4 \bmod 10$ mais $5^2 \equiv 5 \bmod 10$ donc $1995^4 \equiv 5 \bmod 10$. De même on peut calculer $1991^{1991} \equiv 1 \bmod 10$.

APPLICATION: Preuves par 9 et 11.

L'écriture d'un nombre M en base décimale $M = c_n c_{n-1} \dots c_1 c_0$ signifie :

$$M = c_n 10^n + c_{n-1} 10^{n-1} + \dots + c_1 10 + c_0$$

et par conséquent $M \equiv c_n + c_{n-1} \dots + c_1 + c_0 \bmod 9$ (puisque $10 \equiv 1 \bmod 9$) et également $M \equiv c_0 - c_1 + c_2 \dots + (-1)^{n-1} c_{n-1} + (-1)^n c_n \bmod 11$ (puisque $10 \equiv -1 \bmod 11$). Supposons qu'on veuille vérifier le résultat d'une multiplication $M \times N = L$?, on calcule les restes ℓ, m, n de la division par 9 (idem avec 11) de L, M, N et on vérifie si $mn \equiv \ell \bmod 9$. Cela ne donne qu'une vérification et non une preuve, mais on ne fait pas souvent 9 erreurs de retenue... Le choix de 9 ou 11 provient du fait qu'on a une astuce simple permettant de calculer le reste modulo 9 ou 11 sans faire de division euclidienne. Exemple : $M = 1111114444$ et $N = 1234567$ alors $M \equiv 22 \equiv 4 \bmod 9$ et $M \equiv 0 \bmod 11$, $N \equiv 28 \equiv 1 \bmod 9$ et $N \equiv 4 \bmod 11$ donc $MN \equiv 4 \bmod 9$ et $MN \equiv 0 \bmod 11$.

THÉORÈME: *(théorème des restes chinois)*

Supposons que $\mathrm{PGCD}(m, n) = 1$ *alors le système de congruence :*

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

possède une solution $x_0 \in \mathbf{Z}$ *et toutes les autres sont de la forme* $x_0 + mnk$ *avec* $k \in \mathbf{Z}$.

Démonstration: D'après le théorème de Bézout, il existe deux entiers u, v (dont on possède un algorithme de calcul) tels que $um + vn = 1$, posons donc $x_0 := a + (b - a)um$ alors $x_0 = b - (b - a)vn$ et c'est donc bien une solution du système de congruence. Soit x une autre solution, on a donc $x - x_0 \equiv 0 \bmod m$ et $x - x_0 \equiv 0 \bmod n$ donc (comme m et n sont premiers entre eux) $x - x_0 \equiv 0 \bmod mn$. □

Exemple : soit à résoudre

$$\begin{cases} x \equiv 5 \bmod 276 \\ x \equiv 2 \bmod 43 \end{cases}$$

On a vu que 276(=1932/7) et 43(=301/7) sont premiers entre eux et que $1 = 12.276 - 77.43$; on obtient donc une solution $x_0 = 5 + (2 - 5)12.276 = -9936$ et les autres solution sont donnés par $x = -9936 + 11868k$; la plus petite solution positive est 1932.

THÉORÈME: *("Petit" théorème de Fermat)*

Soit p *un nombre premier, alors pour tout entier* $a \in \mathbf{Z}$ *on a la congruence* $a^p \equiv a \bmod p$ *; si de plus* p *ne divise pas* a *alors* $a^{p-1} \equiv 1 \bmod p$.

Démonstration: Commençons par établir que $(x + y)^p \equiv x^p + y^p \bmod p$. En effet, d'après la formule du binôme de Newton, cette formule est surement vraie si tous les C_p^k pour $1 \leq k \leq p - 1$ sont divisibles par p. Mais $C_p^k k!(p - k)! = p!$ et p ne divise ni $k!$ ni $p - k$ (c'est là qu'on utilise que p est premier) car sinon, d'après le théorème d'Euclide, il diviserait un des facteurs c'est à dire un nombre $< p$; par conséquent en appliquant encore une fois Euclide on obtient que p divise C_p^k. On peut maintenant en déduire :

$$a^p - a \equiv (a - 1)^p - (a - 1) \equiv \dots \equiv 1^p - 1 \equiv 0 \bmod p$$

Si de plus p ne divise pas a alors a possède un inverse modulo p et donc $a^{p-1} \equiv 1 \bmod p$. □

COROLLAIRE: *Si $a \equiv b \not\equiv 0 \bmod p$ et si $c \equiv d \bmod (p-1)$ alors $a^c \equiv b^d \bmod p$.*

Démonstration: On sait déjà que $a^c \equiv b^c \bmod p$ et par ailleurs $c = d + k(p-1)$ donc $b^c \equiv b^d \left(b^{p-1}\right)^d \equiv b^d \bmod p$. □

Exemple : $112345^{149785} \equiv 2^5 \equiv 32 \equiv -1 \bmod 11$.

5.2.2 L'anneau $\mathbf{Z}/n\mathbf{Z}$

Notation : on désignera par $\bar{a}$ le reste de la division de a par n (c'est donc par convention un entier dans $\{0, 1, 2, \ldots, n-1\}$.

Définition: On appelle $\mathbf{Z}/n\mathbf{Z}$ l'ensemble $\{0, 1, 2, \ldots, n-1\}$ muni des lois d'addition et de multiplication suivantes : $(a, b) \mapsto \overline{(a+b)}$ et $(a, b) \mapsto \overline{ab}$.

PROPOSITION: L'ensemble $\mathbf{Z}/n\mathbf{Z}$, muni de ses lois d'addition et de multiplication est un anneau commutatif.

Démonstration: Découle immédiatement des propriétés de $\mathbf{Z}$ et des propriétés des congruences. □

On peut se demander s'il s'agit d'un corps, la réponse est la suivante :

THÉORÈME: *L'anneau $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si n est premier.*

Démonstration: Si n n'est pas premier, alors $n = ab$ avec $a, b \neq \pm 1$ et donc ni a, ni b n'est un multiple de n. Mais dans $\mathbf{Z}/n\mathbf{Z}$ on a donc $\bar{a} \neq \bar{0}$ et $\bar{b} \neq \bar{0}$ mais $\bar{a}\bar{b} = \overline{ab} = \bar{n} = 0$ donc $\mathbf{Z}/n\mathbf{Z}$ ne peut pas être un corps. Inversement si n est premier, montrons que tout élément $\bar{a} \in \mathbf{Z}/n\mathbf{Z} \setminus \{\bar{0}\}$ possède un inverse : a et n sont premier entre eux donc il existe u, v tels que $au + vn = 1$ et donc $au \equiv 1 \bmod n$ et donc (dans $\mathbf{Z}/n\mathbf{Z}$) on a $\bar{a}\bar{u} = 1$. □

On peut traduire le théorème des restes chinois ainsi :
Considérons l'application $\rho : \mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ qui a un élément $a \in \mathbf{Z}/nm\mathbf{Z}$ associe son reste modulo m et son reste modulo n ; les propriétés des congruences permettent de vérifier que c'est un morphisme d'anneaux : $\rho(a+b) = \rho(a) + \rho(b)$ et $\rho(ab) = \rho(a)\rho(b)$, le théorème des restes chinois dit que si $\mathrm{PGCD}(m, n) = 1$ alors ρ est une bijection (un isomorphisme).

Le calcul sur ordinateur s'effectue en fait modulo 2^N (avec N dépendant de la machine, du logiciel, etc). Par exemple, Turbo-Pascal recquiert, pour le type entier, des nombres compris entre -32768 et 32767 ; cela signifie qu'il travaille modulo 2^{16} (note : $2^{16} - 1 = 65535 = 32768 + 32767$.

Enfin indiquons que la cryptographie (cartes bancaires, transaction par internet, etc.) fait un usage massif, à travers le système RSA notamment, des groupes finis des éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$ et des (grands) nombres premiers. les espaces vectoriels sur le corps $\mathbf{Z}/p\mathbf{Z}$ sont eux à la base des codes correcteurs d'erreurs (compact disque, transmission d'image, etc).

CHAPITRE 6 L'ANNEAU DES POLYNÔMES

Vous avez étudié depuis la seconde jusqu'à la terminale les fonctions de variable réeelle de la forme $x \mapsto a_n x^n + \ldots + a_1 x + a_0$ *et appris à résoudre les équations du premier et du second degré. Il est commode pour approfondir cette étude de considérer les expressions formelles du type* $a_n x^n + \ldots + a_1 x + a_0$ *et de travailler directement sur elles. C'est ce point de vue qu'on adopte ici : un polynôme est défini comme la suite de ses coefficients ; cela permet notamment de développer l'analogie entre les propriétés de divisibilité dans l'anneau des polynômes et dans l'anneau* $\mathbf{Z}$. *Bien entendu la notation* $P = (a_0, \ldots, a_n)$, *même si elle présente l'avantage d'insister sur le rôle des coefficients, est impraticable et on utilisera la notation usuelle* $P = a_0 + \ldots + a_n X^n$, *celle de tout le monde, même des mathématiciens.*

6.1 POLYNÔMES

K désignera ici un sous-corps de $\mathbf{C}$ que l'on pourra prendre égal à $\mathbf{R}$ ou $\mathbf{C}$ pour simplifier.

Définition: Un *polynôme* à coefficient dans K est une suite d'éléments de K, disons $P = (a_0, a_1, \ldots, a_n, \ldots)$ telle qu'il existe n_0 avec $\forall n \geq n_0,\ a_n = 0$. Les a_i s'appellent les *coefficients* du polynôme P.

Un polynôme du type $(a_0, 0, 0, \ldots)$ s'appelle un *polynôme constant.* Le polynôme $(0, 0, \ldots)$ s'appelle le *polynôme nul.*

Le *degré* d'un polynôme non nul $P = (a_0, a_1, \ldots, a_n, \ldots)$ est l'entier

$$\deg(P) := \max\{n \in \mathbf{N} \mid a_n \neq 0\}$$

Il nous faut bien sûr définir l'addition et la multiplication :

Définition: Soit $P = (a_0, a_1, \ldots, a_n, \ldots)$ et $Q = (b_0, b_1, \ldots, b_n, \ldots)$ deux polynômes, alors leur somme et leur produit sont définis par : $P+Q := (a_0+b_0, a_1+b_1, \ldots, a_n+b_n, \ldots)$ et $PQ := (c_0, c_1, \ldots, c_n, \ldots)$ avec $c_n := \sum_{i=0}^{n} a_i b_{n-i}$.

THÉORÈME: *L'ensemble des polynômes, muni de l'addition et de la multiplication est un anneau commutatif ; l'élément neutre pour l'addition est le polynôme nul, l'élément neutre pour la multiplication est le polynôme constant* $\mathbf{1} := (1, 0, 0, \ldots)$.

On a les relations (lorsque ni P, ni Q ni $P+Q$ ne sont nuls) :

$$\deg(P+Q) \leq \max\{\deg(P), \deg(Q)\} \quad \text{et} \quad \deg(PQ) = \deg(P) + \deg(Q)$$

Démonstration: Il est immédiat de vérifier que l'addition définit une loi de groupe. Le polynôme constant dont le premier coefficient est 1 est bien l'élément neutre car si $b_0 = 1$ et $b_i = 0$ pour $i \geq 1$ on a bien $\sum_{i=0}^{n} a_i b_{n-i} = a_n$. Vérifier l'associativité est un exercice sur la notation "Sigma" que l'on laisse au lecteur.

Démontrons maintenant les formules sur les degrés : si $\deg(P) = d$ (resp. $\deg(Q) = e$) et p_d (resp. q_e) est le dernier coefficient non nul de P (resp. de Q) on voit facilement que

$p_i + q_i = 0$ dès que $i > \max(d, e)$ d'où la première inégalité. Remarquons que si $d > e$ le dernier coefficient non nul de $P + Q$ est p_d et donc dans ce cas on a $\deg(P + Q) = \max\{\deg(P), \deg(Q)\}$ (idem si $d < e$) alors que si $d = e$ tous les coefficients de $P + Q$ d'indice strictement supérieur à d sont nuls et le coefficient d'indice d vaut $p_d + q_e$ et donc peut fort bien être nul. Si $n > d + e$ alors $\sum_{i=0}^{n} p_i q_{n-i} = 0$ car chacun des termes est nul (ou bien $i > d$ ou bien $n - i > e$) ; par ailleurs le $(d+e)$-ème coefficient de PQ est $p_d q_e \neq 0$. De ces deux remarques on tire que $\deg(PQ) = d + e$. □

Voyons maintenant comment justifier et revenir à une notation plus usuelle : introduisons le polynôme $X = (0, 1, 0, 0 \ldots)$; on voit facilement que $X^2 = X.X = (0, 0, 1, 0, \ldots)$ et plus généralement que $X^n = (0, 0, \ldots, 0, 1, 0, \ldots)$ (où le 1 est le coefficient d'indice n). On en déduit une écriture plus commode (qui est celle que l'on utilisera dans toute la suite!) :

$$(a_0, a_1, \ldots, a_n, \ldots) = a_0 \mathbf{1} + a_1 X + a_2 X^2 + \ldots + a_n X^n$$

Ceci justifie la
Notation : l'ensemble des polynômes à coefficients dans K se note $K[X]$. On dit que X est une *indéterminée.*

Remarque : nous distinguons donc le polynôme $a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n$ de la fonction $x \mapsto a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$.

La propriété fondamentale de l'anneau des polynômes est, tout comme pour $\mathbf{Z}$, l'existence d'une division euclidienne :

THÉORÈME: *Soit $A \in K[X]$ et $B \in K[X] \setminus \{0\}$, il existe $Q, R \in K[X]$, uniques tels que :*

$$A = BQ + R \quad \text{et} \quad R = 0 \text{ ou } deg(R) < deg(B)$$

Démonstration: (unicité) Supposons $A = BQ + R = BQ' + R'$; alors $B(Q - Q') = R' - R$. Si R' était distinct de R alors $\deg(B) \leq \deg(B(Q - Q')) = \deg(R' - R) < \deg(B)$ amènerait une contradiction donc $R = R'$ et par conséquent $Q = Q'$.

(existence) La preuve se fait par récurrence sur $n := deg(A)$. Observons que si $\deg(A) < \deg(B)$ alors $A = 0.B + A$ fournit une division euclidienne. Supposons donc démontrée l'existence de la division euclidienne pour les polynômes de degré $\leq n - 1$ et établissons son existence pour A de degré n. On peut supposer $n \geq \deg(B) = m$ sinon on est dans un cas déjà traité ; écrivons $A = a_n X^n + \ldots$ et $B = b_m X^m + \ldots$ et considérons $A_1 := A - \frac{a_n}{b_m} X^{n-m} B$; si $A_1 = 0$ la démonstration est terminée et sinon, on voit aisément que $\deg(A_1) \leq n - 1$ car le coefficient de degré n s'annule (c'est fait pour!) donc d'après l'hypothèse de récurrence on sait que $A_1 = BQ_1 + R_1$ avec $\deg(R_1) < \deg(B)$ d'où l'on tire $A = B\left(Q_1 + \frac{a_n}{b_m} X^{n-m}\right) + R_1$ ce qui achève la démonstration de l'existence. □

Exemple : La démonstration fournit d'ailleurs un algorithme pour calculer Q et R ; illustrons cela avec $A = 2X^5 + 3X^3 + X^2 - X + 5$ et $B = X^2 + X - 1$: on peut présenter les calculs comme ceux de la division euclidienne usuelle (dans $\mathbf{Z}$) :

$$
\begin{array}{r|l}
2X^5+3X^3+X^2-X+5 & X^2+X-1 \\
\ominus\ 2X^5+2X^4-2X^3 & \hline 2X^3-2X^2+7X-8 \\
\hline -2X^4+5X^3+X^2-X+5 & \\
\ominus\ -2X^4-2X^3+2X^2 & \\
\hline 7X^3-X^2-X+5 & \\
\ominus\ 7X^3+7X^2-7X & \\
\hline -8X^2+6X+5 & \\
\ominus\ -8X^2-8X+8 & \\
\hline 14X-3 &
\end{array}
$$

ainsi $2X^5+3X3+X^2-X+5=(X^2+X-1)(2X^3-2X^2+7X-8)+(14X-3)$.

L'existence de la division euclidienne permet de développer les propriétés de divisibilité : PGCD,PPCM, théorème de Bézout, algorithme d'Euclide, théorème de Gauss, décomposition en produit de facteurs, de manière entièrement analogue à $\mathbf{Z}$. Nous donnons donc seulement les énoncés et renvoyons au chapitre précédent pour les démonstrations en signalant seulement les endroits où le vocabulaire introduit des différences. Les polynômes inversibles sont les constantes non nulles : en effet il est clair que ces polynômes sont inversibles et réciproquement si $PQ=1$ on a $\deg(P)+\deg(Q)=0$ et on conclut que P est constant. L'analogue des nombres premiers est donné par les polynômes *irréductibles*, i.e. par les polynômes P, non constants, qui ne peuvent s'écrire $P=QR$ avec Q,R deux polynômes non constants. Les polynômes inversibles sont les constantes non nulles.

Définition: Le *plus grand diviseur commun* ou PGCD de deux polynômes A et $B\in K[X]$ est un polynôme D qui divise A et B et tel que tout polynôme divisant A et B divise nécessairement D. Le *plus petit commun multiple* est un polynôme M multiple de A et B et tel que tout polynôme multiple de A et B soit divisible par M.

THÉORÈME: *Soient A,B deux polynômes, l'un d'entre eux non nul (au moins), le PGCD de A et B existe et, si l'on impose qu'il soit unitaire, il est unique. De même le PPCM existe et l'on a* $\mathrm{PPCM}(A,B)\ \mathrm{PGCD}(A,B)=AB$.

L'algorithme (d'Euclide) suivant fournit un calcul du PGCD :

$A=BQ_1+R_1$ (division de A par B)
$B=R_1Q_2+R_2$ (division de B par R_1)
$R_1=R_2Q_3+R_3$ (division de R_1 par R_2)
.....
$R_{n-1}=R_nQ_{n+1}+R_{n+1}$ (division de R_{n-1} par R_n)
Jusqu'à ce que $R_{n+1}=0$ *et alors* $\mathrm{PGCD}(A,B)=R_n$

Démonstration: La démonstration est identique au cas arithmétique : on doit seulement observer que $\deg(R_{i+1})<\deg(R_i)$ pour s'assurer que l'algorithme converge. □

Exemple de calcul : prenons $A:=X^6+X^5+X^4+X^2+X+1$ et $B=X^5+X^4+X^3+X^2+X+1$ alors
$A=BQ_1+R_1$ (avec $Q_1=X$ et $R_1=1-X^3$)
$B=R_1Q_2+R_2$ (avec $Q_2=-X^2-X-1$ et $R_2=2X^2+2X+2$)
$R_1=R_2Q_3+R_3$ (avec $Q_3=\frac{1}{2}$ et $R_3=0$)

donc $R_2 = 2(X^2+X+1)$ est le PGCD. Si l'on impose qu'ils soient unitaires $\mathrm{PGCD}(A,B) = X^2+X+1$ et $\mathrm{PPCM}(A,B) = (X^4+1)B = X^9+X^8+X^7+X^6+2X^5+2X^4+X^4+X^3+X^2+X+1$.

THÉORÈME: *(Bézout) Soit $A, B \in K[X]$ alors il existe $U, V \in K[X]$ tels que $AU+BV = \mathrm{PGCD}(A,B)$. De plus l'algorithme d'Euclide fournit également un calcul de U et V.*

Remarque : Les polynômes U et V ne sont pas uniques (en effet $U' = U+QB$ et $V' = V-QA$ font aussi l'affaire) mais on peut imposer (si A et B non constants) que $\deg(U) \leq \deg(B)-1$ et $\deg(V) \leq \deg(A)-1$.

Démonstration: On "copie" la démonstration faite pour $\mathbf{Z}$:
Considérons l'ensemble $I := \{AP+BQ \mid P,Q \in K[X]\}$; c'est un idéal de $K[X]$: la somme de deux éléments de I est dans I et le produit par un polynôme quelconque d'un élément de i est encore dans I ; l'existence de la division euclidienne entraîne, comme dans $\mathbf{Z}$, que tout idéal est engendré par un élément, c'est-à-dire que $I = DK[X] = \{DP \mid P \in K[X]\}$. Par définition de I il existe $U, V \in K[X]$ tels que $D = AU+BV$. Voyons que $D = \mathrm{PGCD}(A,B)$: tout d'abord $A \in I$ donc A est un multiple de D, idem pour B donc D divise A et B ; si maintenant C divise A et B alors C divise $D = AU+BV$ donc D est bien le PGCD. □

Exemple : reprenons le cas précédent $A := X^6+X^5+X^4+X^2+X+1$ et $B = X^5+X^4+X^3+X^2+X+1$ alors en remontant les étapes de l'algorithme d'Eclide on obtient : $R_2 = B-R_1Q_2 = B-(A-BQ_1)Q_2$ d'où $PGCD(A,B) = X^2+X+1 = (-\frac{1}{2}Q_2)A + \frac{1}{2}(1+Q_1Q_2)B$.

Définition: Un polynôme $P \in K[X]$ est dit *irréductible* s'il n'est pas constant et si les seules factorisations $P = QR$ (avec $Q, R \in K[X]$) s'obtiennent avec P ou Q constant.

Remarques : i) La notion de polynôme irréductible correspond à celle de nombre premier dans $\mathbf{Z}$.

ii) Les polynômes de degré 1 sont irréductibles car $X-a = QR$ entraîne Q ou R constant pour des raisons de degré. Néanmoins il y a beaucoup d'autres polynômes irréductibles en général ; par exemple X^2+1 est irréductible dans $\mathbf{R}[X]$, X^3-X+1 est irréductible dans $\mathbf{Q}[X]$

iii) Il est indispensable de préciser le corps K car par exemple X^2+1 n'est pas irréductible dans $\mathbf{C}[X]$ et X^3-X+1 n'est pas irréductible dans $\mathbf{R}[X]$ (ils ont chacun au moins une racine).

THÉORÈME:
(i) (Euclide) Soit P irréductible dans $K[X]$ et divisant QR alors P divise Q ou R.
(ii) (Gauss) Si $\mathrm{PGCD}(P,Q) = 1$ et P divise QR alors P divise R.

Démonstration: La démonstration est entièrement analogue à celle faite dans $\mathbf{Z}$. □

THÉORÈME: Soit $P \in K[X]$ un polynôme non constant, alors il existe $a \in K^*$ et des polynômes unitaires distincts $P_1, \ldots, P_r$ et des entiers $m_1, \ldots, m_r$ tous ≥ 1 tels que :

$$P = aP_1^{m_1} \ldots P_r^{m_r}$$

De plus les P_i, les m_i et a sont uniques.

Démonstration: La démonstration est entièrement analogue à celle faite dans $\mathbf{Z}$. Il faut seulement observer que les polynômes inversibles (i.e. les P tels qu'il existe Q avec $PQ = 1$) sont les polynômes constants non nuls. □

Exemple : reprenons les polynômes A et B dont nous avons calculé le PGCD. Dans $\mathbf{Q}[X]$ on a $A = (X^2+X+1)(X^4+1)$ et $B = (X^2+X+1)(X^2-X+1)(X+1)$ alors que sur $\mathbf{R}[X]$ on a $A = (X^2+X+1)(X^2+\sqrt{2}X+1)(X^2-\sqrt{2}+1)$ et $B = (X^2+X+1)(X^2-X+1)(X+1)$ et sur $\mathbf{C}[X]$ on a $A = (X-j)(X-\bar{j})$ et $B = (X-j)(X-\bar{j})(X+j)(X-\bar{j})(X+1)$ (où l'on note $j := -\frac{1}{2} + i\frac{\sqrt{3}}{2}$).

Remarque : on peut montrer que $K[X]$ possède une infinité de polynômes irréductibles unitaires en "copiant" la démonstration faite pour les nombres premiers.

6.2 RACINES D'UN POLYNÔME

On étudie dans ce paragraphe les premières propriétés de la fonction associée à un polynôme : si $P := a_0 + a_1X + \ldots + a_nX^n \in K[X]$ alors on peut lui associer la fonction de K dans K définie par $x \mapsto a_0 + a_1x + \ldots + a_nx^n$. En particulier on s'intéresse aux valeurs de cette fonction ; en fait il nous suffira de regarder quand la fonction s'annule, ce qui nous amène à la notion de racine d'un polynôme.

PROPOSITION: *Soit $P \in K[X]$ et soit $\alpha \in K$ alors $P(\alpha) = 0$ si et seulement si $(X - \alpha)$ divise P.*

Démonstration: *Si $P = (X-\alpha)Q$ alors visiblement $P(\alpha) = 0$. Supposons inversement que $P(\alpha) = 0$ et effectuons la division de P par $X - \alpha$. On a $P = (X - \alpha)Q + R$ avec $R = 0$ ou $\deg(R) < \deg(X - \alpha) = 1$; donc R est constant et en calculant $P(\alpha)$ on trouve que $R = P(\alpha)$ donc $R = 0$ et $X - \alpha$ divise P.* □

Définition: On dit que α est une *racine* de P si $P(\alpha) = 0$ ou si $(X - \alpha)$ divise P. On dit que α est une *racine d'ordre r* de P si $(X - \alpha)^r$ divise P mais $(X - \alpha)^{r+1}$ ne divise pas P.

THÉORÈME: *Un polynôme de degré n possède au plus n racines (comptée avec multiplicités).*

Démonstration: Supposons que $\alpha_1, \ldots, \alpha_s$ soient des éléments distincts et racines d'ordre $m_1, \ldots, m_s$ de P alors les polynômes $(X - \alpha_i)^{m_i}$ sont premiers entre eux (deux à deux) et divisent P donc leur produit divise P. Or le produit $\prod_{i=1}^{s}(X - \alpha_i)^{m_i}$ a pour degré $\sum_{i=1}^{s} m_i$ donc $\sum_{i=1}^{s} m_i \leq \deg(P) = n$. □

Par analogie avec le calcul différentiel, on peut définir la dérivée d'un polynôme et il est raisonnable de penser que l'annulation des dérivées correspond à une racine multiple. Pour démontrer cela on établit la "formule de Taylor pour les polynômes" qui servira de prototype pour la formule de Taylor générale (chapitre 14).

Définition: Soit $P = a_nX^n + a_{n-1}X^{n-1} \ldots + a_1X + a_0$ un polynôme, le *polynôme dérivé* est $P' := na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} \ldots + a_1$. On note $P^{(r)}$ la *dérivée n-ème* définit par $P^{(r+1)} = (P^{(r)})'$.

Cette opération de dérivation est donc définie sans passage à la limite mais jouit des mêmes propriétés que la dérivation des fonctions :

PROPOSITION: $(P+Q)' = P' + Q'$
$(PQ)' = P'Q + PQ'$
Plus généralement on a la formule Leibniz

$$(PQ)^{(n)} = \sum_{i=0}^{n} C_n^i P^{(i)} Q^{(n-i)}$$

Les propriétés suivantes sont équivalentes :
(i) P possède un racine d'ordre r en $X = \alpha$
(ii) $P(\alpha) = P'(\alpha) = \ldots = P^{(r-1)}(\alpha) = 0$ et $P^{(r)}(\alpha) \neq 0$

Démonstration: La démonstration de la première formule est laissée en exercice. Pour la deuxième formule on se ramène facilement au cas où $P = X^m$ et $Q = X^n$; alors $PQ' + QP' = X^n(mX^{m-1}) + X^m(nX^{n-1}) = (m+n)X^{m+n-1} = (PQ)'$. Un calcul par récurrence, à partir de la formule précédente donne la formule de Leibniz (ce calcul est fait au chapitre 14 pour la dérivation usuelle).

Si P possède une racine d'ordre r en α alors $P = (X-\alpha)^r Q$ avec $X - \alpha$ ne divisant pas Q donc $Q(\alpha) \neq 0$. En appliquant la formule de Leibniz on voit que

$$P(\alpha) = P'(\alpha) = \ldots = P^{(r-1)}(\alpha) = 0$$

et $P^{(r)}(\alpha) = r!Q(\alpha) \neq 0$. Pour établir la réciproque on va se servir de la formule suivante :

PROPOSITION: *(Formule de Taylor pour les polynômes) Soit P un polynôme de degré n et $\alpha \in K$ alors*

$$P = P(\alpha) + P^{(1)}(\alpha)(X-\alpha) + \frac{P^{(2)}(\alpha)}{2!}(X-\alpha)^2 + \ldots + \frac{P^{(n)}(\alpha)}{n!}(X-\alpha)^n$$

Démonstration: (de la formule de Taylor) Tout polynôme P de degré n peut s'écrire $P = \sum_{i=0}^{n} a_i(X-\alpha)^i$ (en effet il suffit de le vérifier pour $P = X^k$ et $X^k = (X-\alpha+\alpha)^k = \sum_{i=0}^{k} C_k^i \alpha^{k-i}(X-\alpha)^i$). La dérivation étant additive il suffit de vérifier la formule de Taylor pour le polynôme $P = (X-\alpha)^k$. Mais dans ce cas $P(\alpha) = P'(\alpha) = \ldots = P^{(k-1)}(\alpha) = 0$ et $P^{(k)}(\alpha) = k!$ donc la formule est vraie.

Terminons maintenant la preuve de la proposition :
Si $P(\alpha) = P'(\alpha) = \ldots = P^{(r-1)}(\alpha) = 0$ et $P^{(r)}(\alpha) \neq 0$ alors

$$P = \sum_{i=0}^{n} \frac{P^{(i)}(\alpha)}{i!}(X-\alpha)^i = (X-\alpha)^r \left(\frac{P^{(r)}(\alpha)}{r!} + \sum_{i=r+1}^{n} \frac{P^{(i)}(\alpha)}{i!}(X-\alpha)^{i-r} \right)$$

et on a bien $P = (X-\alpha)^r Q$ avec $Q(\alpha) = \frac{P^{(r)}(\alpha)}{r!} \neq 0$. □

Remarque : Jusqu'à présent nous aurions pu supposer le corps K commutatif quelconque, par exemple $K = \mathbf{Z}/p\mathbf{Z}$ mais la formule de Taylor n'est pas valable (telle quelle) sur $\mathbf{Z}/p\mathbf{Z}$ et de "drôles de choses" peuvent arriver en dérivant les polynômes : considérons le polynôme $P = X^{3p} + X^p + 1$ alors P n'est pas constant et pourtant $P' = 0$; par ailleurs, d'après le "petit" théorème de Fermat, le polynôme $P = X^p - X$ a pour racine tous les éléments du corps $\mathbf{Z}/p\mathbf{Z}$.

Explicitons maintenant la factorisation des polynômes à coefficients dans $\mathbf{R}$ et $\mathbf{C}$

THÉORÈME: *(Factorisation dans $\mathbf{R}[X]$ et $\mathbf{C}[X]$)*

(i) Les polynômes irréductibles dans $\mathbf{C}[X]$ sont les polynômes du premier degré ; tout polynôme de degré n se factorise sous la forme :

$$P = a_n X^n + \ldots + a_0 = a_n (X - \alpha_1)^{m_1} \ldots (X - \alpha_r)^{m_r}$$

avec les α_i distincts et $m_1 + \ldots + m_r = n$.

(ii) Les polynômes irréductibles dans $\mathbf{R}[X]$ sont les polynômes du premier degré et les polynômes du second degré de la forme $P = aX^2 + bX + c$ avec $b^2 - 4ac < 0$;

Remarque : on voit ainsi que, sur $\mathbf{R}$, tout polynôme de degré n se factorise sous la forme :

$$P = a_n X^n + \ldots + a_0 = a_n (X - \alpha_1)^{m_1} \ldots (X - \alpha_r)^{m_r} (X^2 + b_1 X + c_1)^{n_1} \ldots (X^2 + b_s X + c_s)^{n_s}$$

avec les α_i réels distincts, les couples (b_i, c_i) distincts vérifiant $b_i^2 - 4c_i < 0$ et $m_1 + \ldots + m_r + 2(n_1 + \ldots + n_s) = n$.

Démonstration: (i) Il faut démontrer que les seuls polynômes unitaires irréductibles sur $\mathbf{C}$ sont les $X - \alpha$ mais ceci est clair car tout polynôme non constant possède un facteur de ce type d'après le théorème de d'Alembert-Gauss.

(ii) Il faut démontrer que les seuls polynômes unitaires irréductibles sur $\mathbf{R}$ sont les $X - \alpha$ et les $X^2 + bX + c$ (avec $b^2 - 4c < 0$). Pour cela soit P un polynôme unitaire irréductible ; il possède une racine complexe α. Si $\alpha \in \mathbf{R}$ alors $X - \alpha$ divise P et donc $P = X - \alpha$. Sinon, observons que, comme P est à coefficient réel :

$$P(\overline{\alpha}) = \bar{P}(\overline{\alpha}) = \overline{P(\alpha)} = 0$$

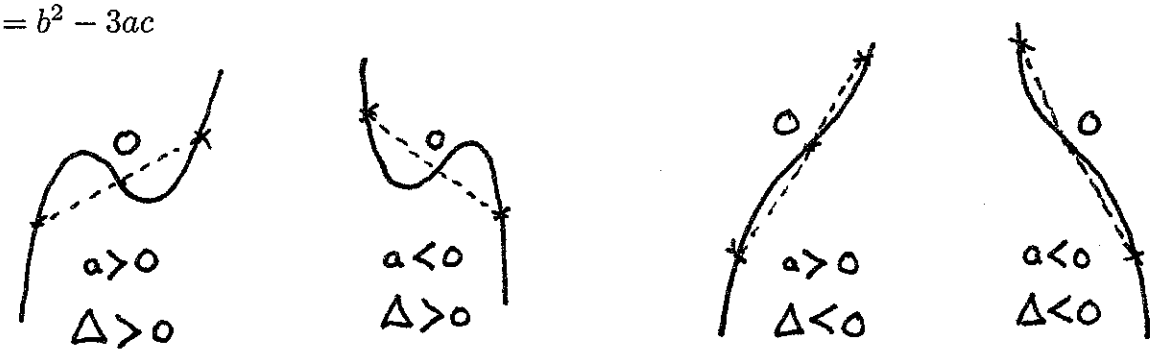
d'autre part $(X - \alpha)(X - \overline{\alpha}) = X^2 - 2Re(\alpha)X + |\alpha|^2$ est à coefficient réel et divise P donc $P = X^2 - 2Re(\alpha)X + |\alpha|^2$. □

Terminons ce paragraphe en étudiant, sur $\mathbf{R}$, le graphe des fonctions polynômes de degré ≤ 3 :

Si $P = aX + b$ on obtient une droite :

Si $P = aX^2 + bX + c$ on obtient une parabole qui a pour axe de symétrie la droite verticale $x = -\frac{b}{2a}$

Si $P = aX^3 + bX^2 + cX + d$ on obtient une cubique qui a toujours un point de symétrie ; pour étudier le signe de la dérivée $P = 3ax^2 + 2bX + c$, on a besoin du signe de $\Delta := b^2 - 3ac$



6.3 FRACTIONS RATIONNELLES

Une fraction rationnelle F à une indéterminée est une expression du type $F = \frac{P}{Q}$ avec P et Q polynômes (Q est supposé non nul et bien sûr $\frac{PR}{QR} = \frac{P}{Q}$). L'ensemble des fractions rationnelles forme un corps qu'on peut construire formellement à partir de l'anneau des polynômes de la même façon que $\mathbf{Q}$ *est construit à partir de* $\mathbf{Z}$.

Définition: Un *élément simple* de $\mathbf{C}(X)$ est une fraction rationnelle de la forme :

$$F = \frac{b}{(X-a)^n}$$

avec $a, b \in \mathbf{C}$ et $n \in \mathbf{N}^*$.

Un *élément simple* de $\mathbf{R}(X)$ est une fraction rationnelle de la forme :

$$F = \frac{b}{(X-a)^n} \quad ou \quad F = \frac{cX+d}{(X^2+aX+b)^n}$$

avec $a, b, c, d \in \mathbf{R}$ et $n \in \mathbf{N}^*$ et (dans le deuxième cas $a^2 - 4b < 0$).

L'intérêt de cette notion est illustré par le théorème suivant :

THÉORÈME: *Soit $K = \mathbf{R}$ ou $\mathbf{C}$, une fraction rationnelle de $K(X)$ peut s'écrire de manière unique comme somme d'un polynôme et d'éléments simples, cette écriture s'appelle la décomposition en éléments simples de la fraction rationnelle.*

Exemples : La décomposition en éléments simples de $F = \frac{X^3+X^2+X-1}{X^3-X}$ est $F = 1 + \frac{1}{(X-1)} - \frac{1}{(X+1)} + \frac{1}{X}$

Remarque : l'unicité de cette décomposition est très utile pour la calculer comme on le verra sur les exemples. Nous allons faire la démonstration sur $\mathbf{C}$ et laissons le lecteur adapter l'argument au corps des réels ; en fait si F est une fraction à coefficient réels, on peut la décomposer en éléments simples sur $\mathbf{R}$ et sur $\mathbf{C}$.

Démonstration: (Unicité) Il suffit de voir que si :

$$F = P + \sum_{i=1}^{r} \sum_{j=1}^{m_i} \frac{b_{ij}}{(X-a_i)^j} = 0$$

alors les coefficients b_{ij} et le polynôme P sont nuls. Pour cela multiplions F par $(X-a_i)^{m_i}$; on obtient une égalité de la forme $0 = (X-a_i)^{m_i}F = b_{im_i} + (X-a_i)G$ avec G une fraction rationnelle sans pôle en a_i. En calculant les valeurs en a_i, on obtient donc $b_{im_i} = 0$. En répétant l'opération pour chaque coefficient on obtient $b_{ij} = 0$ et donc $P = 0$.

(existence) Commençons par observer que si P et Q sont des polynômes premiers entre eux alors, d'après le théorème de Bézout, il existe deux polynômes A, B tels que $AP+BQ = 1$; donc toute fraction rationnelle de la forme $F = \frac{R}{PQ}$ peut s'écrire $F = \frac{R(AP+BQ)}{PQ} = \frac{AR}{Q} + \frac{BR}{P}$. Par ailleurs tout polynôme s'écrit à un coefficient près $D = \prod_{i=1}^{r}(X-a_i)^{m_i}$ donc toute fraction rationnelle $F = \frac{C}{D}$ va se décomposer en $\sum_{i=1}^{r} \frac{P_i}{(X-a_i)^{m_i}}$ mais si on utilise maintenant la "formule de Taylor" pour P_i au point a_i on obtient $P_i = \sum_{j=0}^{\deg(P_i)} p_{ij}(X-a_i)^j$ d'où en reportant une expression de F comme somme d'éléments simples et de polynômes. □

L'utilisation la plus fréquente de la décomposition en éléments simples est le calcul de primitives (voir chapitre 17) mais elle peut être utilisée aussi pour calculer la dérivée n-ème ; par exemple si $F = \frac{X^3+X^2+X-1}{X^3-X} = 1 + \frac{1}{X-1} - \frac{1}{X+1} + \frac{1}{X}$ alors, comme on sait que $\int \frac{dt}{(t-a)} = Log|t-a| + C'$ on en tire

$$\int F(t)dt = t + \log|\frac{t^2-t}{t+1}| + C$$

En observant que $(\frac{d}{dt})^m(\frac{1}{t-a}) = (-1)^m \frac{m!}{(t-a)^{m+1}}$ on en tire :

$$F^{(m)}(t) = (-1)^m m! \left(\frac{1}{(t-1)^{m+1}} - \frac{1}{(t+1)^{m+1}} + \frac{1}{t^{m+1}} \right)$$

Pratique de la décomposition en éléments simples : On peut appliquer la méthode suivante : on factorise le dénominateur, puis on écrit formellement le type de la décomposition en éléments simples avec des coefficients inconnus, on calcule ensuite ces coefficients à l'aide des lemmes qui suivent.

La partie polynômiale de la décomposition simple s'appelle la *partie entière* de la fraction rationnelle ; elle se calcule ainsi :

LEMME: *Soit $F = P/Q$ une fraction rationnelle et soit E le quotient de la division de P par Q, i.e. $P = EQ + R$ avec $\deg(R) < \deg Q$ alors E est la partie entière de la fraction F.*

Démonstration: En effet, en réduisant au même dénominateur la somme des éléments simples, on obtient une égalité de la forme $F = E + R/Q$ avec P, R polynômes et $\deg(R) \leq \deg(Q) - 1$. Après multiplication par Q cette égalité devient $P = EQ + R$ qui indique que E est le quotient de P par Q et R le reste puisque $\deg(R) < \deg(Q)$. □

Il est également aisé de trouver le coefficient correspondant à un pôle d'ordre maximal :

LEMME: *Soit $Q = (X-a)^m Q_1$ avec $Q_1(a) \neq 0$ et $F = P/Q$ dont la décomposition s'écrit : $F = \frac{u_m}{(X-a)^m} + \ldots$ alors $u_m = P(a)/Q_1(a) = m!P(a)/Q^{(m)}(a)$.*

Démonstration: On a $(X-a)^m F = P/Q_1 = u_m + (X-a)G$ avec G fraction rationnelle sans pôle en a ; en calculant les valeurs pour $X = a$, on en déduit $u_m = P(a)/Q_1(a)$. Par ailleur la formule de Leibniz nous donne $Q^{(m)}(a) = m!Q_1(a)$ d'où la deuxième expression. □

Ces deux lemmes sont déjà suffisants pour calculer la décomposition d'une fraction rationnelle sans pôle double.

Exemple : soit $F = \frac{X^{2n}}{X^n - 1}$ on effectue la division $X^{2n} = (X^n + 1)(X^n - 1) + 1$; on sait que les racines de $X^n - 1$ sont les racines n-èmes de l'unité et on peut factoriser $X^n - 1 = \prod_{h=0}^{n-1}(X - \alpha_h)$ avec $\alpha_h := exp(\frac{2\pi i h}{n})$ d'où une expression a priori :

$$F = E + \sum_{h=0}^{n-1} \frac{u_h}{X - \alpha_h}$$

D'après le premier lemme on a $E = X^n + 1$ et si on applique le deuxième lemme avec $P = X^{2n}$ et $Q = X^n - 1$ on obtient $u_h = \frac{(\alpha_h)^{2n}}{n(\alpha_h)^{n-1}} = \alpha_h/n$ et donc

$$F = \frac{X^{2n}}{X^n - 1} = X^n + 1 + \frac{1}{n} \sum_{h=0}^{n-1} \frac{\alpha_h}{(X - \alpha_h)}$$

Pour traiter les calculs avec des pôles multiples le plus économique est d'utiliser le lemme suivant :

LEMME: *(division aux puissances croissantes) Soit $\alpha \in K$, $P, Q \in K[X]$ avec $Q(\alpha) \neq 0$ alors pour tout $k \in \mathbf{N}$ il existe $a_i \in K$ et $R \in K[X]$ tels que :*

$$P = (a_0 + a_1(X - \alpha) + \ldots + a_{k-1}(X - \alpha)^{k-1})Q + (X - \alpha)^k R$$

En particulier si $F := P/(X-\alpha)^k Q$ alors la partie de la décomposition en éléments simples de F correspondant au pôle α s'écrit :

$$\frac{a_0}{(X - \alpha)^k} + \ldots + \frac{a_{k-1}}{(X - \alpha)}$$

Démonstration: Observons que le polynôme $P-(P(\alpha)/Q(\alpha))Q$ s'annule en α donc $P-(P(\alpha)/Q(\alpha))Q=(X-\alpha)R$; raisonnons maintenant par récurrence sur k et supposons $P=(a_0+a_1(X-\alpha)+\ldots+a_{k-1}(X-\alpha)^{k-1})Q+(X-\alpha)^kR_k$; on sait que $R_k=rQ+(X-\alpha)R_{k+1}$ (avec $r:=R_k(\alpha)/Q(\alpha)$) d'où $P=(a_0+a_1(X-\alpha)+\ldots+a_{k-1}(X-\alpha)^{k-1}+r(X-\alpha)^k)Q+(X-\alpha)^{k+1}R_{k+1}$. La deuxième affirmation est immédiate. □

Exemple : $f=\dfrac{X^{10}+X^2+1}{X^9-2X^5+X}$ Nous allons calculer la décomposition en éléments simples sur $\mathbf{C}$ et en déduire celle sur $\mathbf{R}$. Cette fraction est aussi l'occasion de faire des remarques sur l'utilisation des symétries (coefficients réels, parité).

Factorisation : le polynôme $Q:=X^9-2X^5+X$ se décompose en :
$X(X^4-1)^2=X(X-1)^2(X+1)^2(X^2+1)^2=X(X-1)^2(X+1)^2(X+i)^2(X-i)^2$
Décomposition a priori de f avec $A,B,C,D,E,F,G,H,I\in\mathbf{C}$ et $R\in\mathbf{C}[X]$:

$$R+\frac{A}{X}+\frac{B}{X+1}+\frac{C}{(X+1)^2}+\frac{D}{(X-1)}+\frac{E}{(X-1)^2}+\frac{F}{(X-i)}+\frac{G}{(X-i)^2}+\frac{H}{(X+i)}+\frac{I}{(X+i)^2}$$

Utilisation des symétries : on sait que $\tilde{f}=f$ et on observe que $f(X)=-f(-X)$; en reportant cela dans la décomposition et en utilisant l'unicité de la décomposition on obtient $R(X)=-R(-X)$, $B=D$, $E=-C$, $F=H$ et $I=-G$ d'une part et d'autre part $\bar{E}=E$, $\bar{A}=A$, $\bar{B}=B$, $\bar{C}=C$, $\bar{D}=D$, $\bar{E}=E$, $\bar{F}=H$, $\bar{G}=I$ d'où l'on tire que A, B, C, F sont réels (et $D=B$, $E=-C$) et G est imaginaire pur (et $I=-G$).

Le premier lemme permet de calculer R ; on trouve $R=X$ (qui est bien impair et à coefficients réels).

Le deuxième lemme permet de calculer A (et si on voulait C et G) : $f_0:=Xf=\frac{X^{10}+X^2+1}{(X^4-1)^2}$ donc $f_0(0)=A=1$

Le troisième lemme permet de calculer simultanément C et B :

$Q=(X+1)^2Q_1$ avec $Q_1=X^7-2X^6+3X^5-4X^4+3X^3-2X^2+X$ d'où l'on tire (par la formule de Taylor par exemple) $Q_1=-16+64(X+1)+(X+1)^2Q_2$ et de même $P=X^{10}+X^2+1=3-12(X+1)+(X+1)^2P_2$ d'où l'écriture de la division aux puissances croissantes de P par Q_1 par rapport à $(X+1)$:

$$3-12(X+1)=(a_0+a_1(X+1))(-16+64(X+1))+(X+1)^2R$$

d'où l'on tire $a_0=-3/16$ et $a_1=0$ soit $C=-3/16$ et $B=0$

On procède de même pour les coefficients G et F : On a $Q=(X-i)^2Q_i$ avec $Q_i=X(X^2-1)^2(X+i)^2$. Ceci permet de calculer $Q_i(i)=-16i$ et $Q_i'(i)=-64$ d'où $Q_i=-16i-64(X-i)+(X-i)Q_2$. De la même façon $P(i)=-1$ et $P'(i)=12i$ donc $P=-1+12(X-i)+(X-i)^2P_2$ d'où l'écriture de la division aux puissances croissantes de P par Q_i par rapport à $(X-i)$:

$$-1+12(X-i)=(b_0+b_1(X-i))(-16i-64(X-i))+(X-i)^2R$$

d'où l'on tire aisément $G = b_0 = -i/16$ et $F = b_1 = -1/2$ (on vérifie bien que G est purement imaginaire et F réel).

Conclusion : f s'écrit :

$$X + \frac{1}{X} + \frac{-3/16}{(X+1)^2} + \frac{3/16}{(X-1)^2} + \frac{-1/2}{X-i} + \frac{-i/16}{(X-i)^2} + \frac{-1/2}{X+i} + \frac{i/16}{(X+i)^2}$$

Pour obtenir la décomposition sur $\mathbf{R}$ il suffit ici de regrouper les termes complexes conjugués : $\frac{1}{(X+i)} + \frac{1}{(X-i)} = \frac{2X}{X^2+1}$ et $\frac{i}{(X+i)^2} - \frac{i}{(X-i)^2} = \frac{4X}{(X^2+1)^2}$ donc

$$f = X + \frac{1}{X} + \frac{-3}{16(X+1)^2} + \frac{3}{16(X-1)^2} - \frac{X}{X^2+1} + \frac{X}{4(X^2+1)^2}$$

Remarque. On peut souvent utiliser avantageusement un calcul de valeur particulière ou de limite pour calculer certains coefficients ou des relations entre eux. Par exemple, en gardant les notations de l'exemple précédent, une fois calculé R, on a facilement $F - R = (2X^6 + 1)/(X^9 - 2X^5 + X)$ donc

$$\lim_{x \to \infty} x(F(x) - R(x)) = 0 = A + B + D + F + H.$$

On voit qu'il n'y a pas de difficulté fondamentale pour calculer la décomposition en éléments simples sinon celle de bien ordonner les calculs.

Noether Emmy (1882–1935)