64

et par définition de la somme de 2 classes, ceci s'écrit encore :

$$(\overline{a+b})+\overline{c} = \overline{a}+(\overline{b+c})$$

et encore $(\overline{a}+\overline{b})+\overline{c} = \overline{a}+(\overline{b}+\overline{c})$

Le lecteur achèvera la démonstration.

Exemples : Nous construisons ci-dessous les tables d'addition et de multiplication de $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.

$\mathbb{Z}/5\mathbb{Z}$:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

algèbre

$\mathbb{Z}/6\mathbb{Z}$:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Dans les calculs sur les congruences modulo n, plutôt que d'utiliser le système de classes $\bar{0},\bar{1},\ldots,\overline{n-1}$ on pourra remplacer $\overline{n-1}$ par $-\bar{1}$, $\overline{n-2}$ par $-\bar{2}$ ... . Ainsi pour calculer, dans $\mathbb{Z}/23\mathbb{Z}$, $(\overline{20})^2$ on peut remplacer $\overline{20}$ par $-\bar{3}$ et il est un peu plus facile de calculer $(-\bar{3})^2$ que $\overline{20^2}$.

Exercice 29 : Montrer que $n(n+1)(2n+1)$ est multiple de 6.

Montrer que si p est un nombre premier ≥ 5, p^2-1 est multiple de 24.

Indiquons une solution pour le second exercice : comme p est premier, il n'est pas multiple de 3. Dans $\mathbb{Z}/3\mathbb{Z}$ on a $\overline{p} = \bar{1}$ ou $\bar{2}$ c'est-à-dire $\overline{p} = \pm\bar{1}$ [illegible]

la maquette de la couverture a été réalisée par le LEP Cyfflé - NANCY

B.P. 239 - 54506 VANDOEUVRE-les-NANCY CEDEX
Dépôt légal : 2e trimestre 1986
n° de la publication : 2-85406-094-6
Le Responsable de la collection : Philippe LOMBARD

Réf. N 530

MPISE

MODULE AA

ARITHMÉTIQUE ET ALGÈBRE

ARITHMETIQUE — Pages

I - RAPPELS SUR LES NOMBRES ENTIERS 1

II - DIVISIBILITE - NOMBRES PREMIERS 5

1.- Définitions 5

2.- PGCD Théorème fondamental 9

3.- Applications du théorème fondamental 17

4.- Sur la répartition des nombres premiers 21

III - CONGRUENCES 23

1.- Définitions. L'anneau $\mathbb{Z}/n\mathbb{Z}$ 23

2.- Le corps $\mathbb{Z}/p\mathbb{Z}$ 28

3.- Solutions d'une congruence 32

IV - VERS UNE GENERALISATION 37

LES NOMBRES COMPLEXES

1.- Construction 45

2.- Représentation géométrique 48

3.- Formule de De Moivre - Applications trigonométriques 52

4.- L'équation du second degré dans C 56

5.- Racines $n^{\text{ièmes}}$ d'un nombre complexe 58

POLYNOMES, FONCTIONS POLYNOMIALES

I - INTRODUCTION 61

1.- Fonctions polynomiales sur $\mathbb{R}$ 64

2.- Polynômes et fonctions polynomiales 65

3.- Formule du binôme 68

II - PROPRIETES ARITHMETIQUES DE K[X] 72

1.- Division euclidienne 72

2.- L'arithmétique de K[X] 74

III - RACINES D'UN POLYNOME 80

IV - CAS DES POLYNOMES SUR $\mathbb{R}$ ou $\mathbb{C}$ 84

FRACTIONS RATIONNELLES

1.- Définition 88

2.- Pôles - Eléments simples 90

3.- Pratique de la décomposition en éléments simples 93

APPENDICE - PETIT VOCABULAIRE ALGEBRIQUE 103

PARTIE 1 : ARITHMÉTIQUE

I - RAPPELS SUR LES NOMBRES ENTIERS

Les entiers naturels sont les nombres 0,1,2,3,... Leur ensemble est désigné par $\mathbb{N}$. Les entiers relatifs (ou entiers rationnels) sont les nombres ...-4,-3,-2,-1,0,1,2,3,... Leur ensemble est désigné par $\mathbb{Z}$. Dans la suite le mot "entier" signifiera "entier relatif".

On sait que $\mathbb{Z}$ est muni d'une addition et d'une multiplication qui font de cet ensemble un anneau commutatif unitaire et que cet anneau est ordonné.

Il existe par ailleurs sur $\mathbb{Z}$ une division euclidienne :

• Tout d'abord si a et b sont deux entiers naturels et si b est non nul, la suite $0,b,2b,3b,\ldots$ tend vers l'infini. Il existe donc un entier unique q tel que $qb \leq a < (q+1)b$. On pose $r = a-qb$. On a donc $0 \leq r < b$. On voit facilement que les relations $a = bq+r$ et $0 \leq r < b$ définissent parfaitement le couple (q,r). En effet si l'on a $a = bq'+r'$ et si par exemple $q' \geq q$ (donc $r' \leq r$), par différence on trouve $b(q'-q) = r-r'$. Les inégalités vérifiées par r et r' impliquent que $0 \leq r-r' < b$ et b qui divise $b(q'-q)$ ne peut diviser $r-r'$ que si $r = r'$. Par suite $q = q'$.

• Cette division s'étend aux éléments de $\mathbb{Z}$. Par exemple si $a \geq 0$ et $b < 0$, on pose $a = (-q)(-b)+r$ et on a : $0 \leq r < -b = |b|$. On peut énoncer la :

Proposition 1 : *Soient a et b deux entiers relatifs $(b \neq 0)$. Il existe un entier relatif q et un entier naturel r déterminés de manière unique, tels que :*

$$a = qb+r \quad et \quad 0 \leq r < |b|.$$

Remarque : De $a = qb+r$ on tire $\frac{a}{b} = q + \frac{r}{b}$. Comme $0 \leq \frac{r}{b} < 1$, q n'est autre que la partie entière de $\frac{a}{b}$ (on peut donc faire des divisions euclidiennes avec toute calculette pourvue d'une touche "partie entière").

Exercice 1 : Montrer que le reste de la division de $(a^2+(a-1)^2)^2$ par $4a^2$ est $(2a-1)^2$.

Rappelons enfin que les propriétés de l'ensemble ordonné $\mathbb{N}$ sont à la base du principe de récurrence:

Soit P une proposition dépendant d'un entier naturel n.

Si P(0) est vraie et si P(n) implique P(n+1), P est vraie pour tout entier naturel.

Ce principe est parfois utilisé sous la forme suivante :

Si P(0) est vraie et si P(0),P(1),...,P(n) impliquent P(n+1), P est vraie pour tout entier naturel.

Bref aperçu d'analyse combinatoire

Comme on le sait, les nombres entiers servent à compter. On va s'en servir ici pour recenser certaines parties d'ensembles finis.

a - Permutations : Soit $E = \{x_1,x_2,\ldots,x_n\}$ un ensemble à n éléments. Une permutation de E est une application f bijective de E dans E. C'est-à-dire que f est injective (si $x_i \neq x_j$, $f(x_i) \neq f(x_j)$) et surjective ($\forall i, \exists j, f(x_j) = x_i$).

Une permutation de E est donc une manière d'ordonner les éléments de E : on choisit le 1er élément (on a n choix possibles), puis le 2ème (il reste (n-1) choix), puis le 3ème (il reste (n-2) choix)... Finalement on trouve que le nombre de permutations est $n\times(n-1)\times(n-2)\times\ldots\times2\times1$ c'est-à-dire n!.

Le nombre de permutations d'un ensemble à n éléments est n!.

Exercice 2 : Ecrire toutes les permutations de {a,b,c} et de {a,b,c,d}.

b - Arrangements : Soient $E = \{x_1,x_2,\ldots,x_n\}$ un ensemble à n éléments et k un entier inférieur ou égal à n. On appelle arrangement de k objets de E la donnée d'une suite ordonnée $(y_1,y_2,\ldots,y_k)$ d'éléments de E. Dire que la suite est ordonnée signifie que l'on distinque par exemple (a,b,c) et (a,c,b).

En raisonnant comme ci-dessus on constate que le nombre d'arrangements de k objets de E est égal à $n(n-1)\ldots(n-k+1)$. Ce nombre est noté en général A_n^k

$$A_n^k = n(n-1)\ldots(n-k+1).$$

Exercice 3 : Ecrire tous les arrangements de 2 objets parmi {a,b,c,d}.

Si $k = n$ on retrouve la notion précédente : $A_n^n = n!$.

c - Combinaisons : Considérons à nouveau un ensemble $E = \{x_1,\ldots,x_n\}$ et un entier $k \leq n$. On appelle combinaison de k objets de E une partie de E à k éléments.

Cette fois on n'ordonne plus la partie, c'est-à-dire qu'on ne distingue pas entre {a,b,c} et {a,c,b}. Cette remarque permet de calculer le nombre C_n^k de combinaisons de k objets parmi n :

A chaque partie à k éléments de E on fait correspondre, en ordonnant ces éléments de toutes les manières possibles, un nombre de k! suites ordonnées de k éléments. Le nombre A_n^k d'arrangements est donc égal à $k! \times C_n^k$ d'où :

$$C_n^k = \frac{n(n-1)\ldots(n-k+1)}{k!}$$

ce que l'on écrit aussi

$$C_n^k = \frac{n!}{k!(n-k)!}$$

en multipliant haut et bas par $(n-k)!$.

Propriétés : a) $C_n^k = C_n^{n-k}$

b) $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$

La relation a) est évidente avec $C_n^k = \frac{n!}{k!(n-k)!}$.

On peut aussi revenir à la définition et remarquer qu'à toute partie à k éléments de E est associée (par complémentarité) une partie à n-k éléments.

b) Soit $E = \{x_1,\ldots,x_n\}$. Le nombre de parties à k éléments de E est égal au nombre de parties à k éléments qui contiennent x_n ajouté au nombre de parties à k éléments qui ne contiennent pas x_n.

Si une partie à k éléments contient x_n, elle est de la forme $\{y_1,\ldots,y_{k-1},x_n\}$ où $\{y_1,\ldots,y_{k-1}\}$ est une partie de $E' = \{x_1,\ldots,x_{n-1}\}$. Le nombre de ces parties est donc C_{n-1}^{k-1}.

Si une partie à k éléments ne contient pas x_n elle est une partie à k éléments de E'. Le nombre de ces parties est donc C_{n-1}^{k}. En réunissant toutes ces remarques on trouve la formule b.

Exercice 4 : Montrer par récurrence sur n que le nombre de parties d'un ensemble E à n éléments (y compris E et l'ensemble vide) est égal à 2^n.

Exercice 5 : Montrer que $\sum_{k=o}^{n} C_n^k = 2^n$ (utiliser l'exercice précédent).

Exercice 6 : Montrer que $\sum_{k=o}^{n} (-1)^k C_n^k = 0$ (traiter d'abord le cas où n est impair).

Exercice 7 : Soit p_n le nombre des permutations u d'un ensemble à n éléments qui vérifient $u(x) \neq x\ \forall x$. Montrer que $n! = p_n + C_n^1 p_{n-1} + \ldots + C_n^{n-2} p_2 + 1$. ($p_1 = 0$ n'apparaît pas dans la formule).

Remarque :

- On convient que $0! = 1$. On remarque que $C_n^0 = 1$, que $C_n^n = 1$.
- C_n^k est un nombre entier. Donc $k!$ divise $n(n-1)\ldots(n-k+1)$.

Comme n est quelconque, cela signifie que le produit de k nombres consécutifs est multiple de $k!$.

Triangle de Pascal

La formule b) ci-dessus permet de calculer de proche en proche les C_n^k : on fait figurer ces nombres dans un tableau triangulaire. Les lignes correspondent à $n = 0,1,2,\ldots$ et les colonnes à $k = 0,1,2,\ldots$ Les formules $C_n^0 = C_n^n = 1$, permettent de remplir le bord vertical et le bord oblique du triangle. Un élément d'une ligne est obtenu en ajoutant l'élément qui est au dessus de lui et l'élément qui est au-dessus et à gauche.

C_0^0	1
C_1^0 C_1^1	1 1
C_2^0 C_2^1 C_2^2	1 2 1
C_3^0 C_3^1 C_3^2 C_3^3	1 3 3 1
C_4^0 C_4^1 C_4^2 C_4^3 C_4^4	1 4 6 4 1
	1 5 10 10 5 1
	1 6 15 20 15 6 1

Dans le chapitre sur les polynômes on retrouvera les nombres C_n^k dans la formule dite du binôme, qui permettra de démontrer certaines propriétés de ces nombres. Le simple examen du triangle de Pascal (donc essentiellement les formules $C_n^0 = C_n^n = 1$ et $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$), nous donne déjà des résultats. A titre d'exercice le lecteur peut montrer :

• Dans chaque ligne horizontale du triangle, la somme des termes est le double de la somme des termes de l'horizontale précédente.

• La somme des termes de la ligne n est 2^n.

• Un élément du triangle est égal à la somme des termes placés au-dessus de lui dans la colonne verticale précédente.

II - DIVISIBILITÉ, NOMBRES PREMIERS

1.- Définitions

Un entier b non nul <u>divise</u> l'entier a s'il existe un entier c tel que $a = bc$. On dit aussi que a est un <u>multiple</u> de b, que b est un <u>diviseur</u> de a. La relation "b divise a" se notera $b|a$ et sa négation $b \nmid a$: ainsi $24|72$ et $3 \nmid 11$.

Les relations suivantes sont vraies pour des entiers a,b,c :

$a\|a$, $a\|-a$, $a\|0$	$(a \neq 0)$
$1\|a$	
$a\|b$ et $b\|c \Rightarrow a\|c$	$(a,b \neq 0)$
$a\|b \Rightarrow ac\|bc$	$(c \neq 0)$
$a\|b$ et $a\|c \Rightarrow a\|mb+nc$	$(m,n \in \mathbb{Z})$.

On remarquera aussi que $a|b$ si et seulement si le reste de la division euclidienne de b par a est 0. Une bonne partie de l'arithmétique

consiste en l'étude de cette relation de divisibilité. Des entiers vont jouer un rôle primordial par rapport à cette relation : ce sont les nombres premiers.

Définition :

Un entier naturel p est dit premier si ses seuls diviseurs positifs sont 1 et p. Par convention, 1 n'est pas premier.

Remarque :

La relation $a|b$ étant équivalente à chacune des relations $-a|b$, $a|-b$, $-a|-b$, les propriétés des entiers relativement à la divisibilité peuvent être considérées sur $\mathbb{N}$ seulement. D'où le fait qu'on considère seulement des nombres premiers positifs, cela simplifiera en général les énoncés de résultats.

La liste des nombres premiers commence par $2,3,5,7,11,13,17,\ldots$ Un nombre entier a tel que $|a| \neq 1$ et $|a|$ non premier est dit composé.

Exercice 8 : Vérifier que tout nombre pair inférieur ou égal à 200 est somme de 2 nombres premiers. (On conjecture que tout nombre pair est somme de deux nombres premiers. C'est l' "hypothèse de Goldbach").

Proposition 2 : Tout entier naturel n, sauf 1, est produit de nombres premiers.

Si n est premier, il n'y a rien à démontrer. Sinon soit n non premier et soit p_1 son plus petit diviseur différent de 1. p_1 est premier sinon

$$\exists \ell,\ 1 < \ell < p_1 \quad \text{et} \quad \ell | p_1,$$

mais comme $p_1|n$ on a $\ell|n$ et cela contredit le choix de p_1. On a donc $n = p_1 n_1$. Si n_1 est premier on a fini, sinon soit p_2 le plus petit diviseur différent de 1 de n_1. Comme ci-dessus p_2 est premier, $n_1 = p_2 n_2$ et $n = p_1 p_2 n_2$. On a clairement $n > n_1 > n_2$ et si on répète le raisonne-

ment on fait apparaître une suite $n_1 > n_2 > n_3 > n_4 > \ldots$ de nombres entiers naturels strictement décroissante. Cette suite est donc finie c'est-à-dire que pour un indice k, n_k est premier et par suite $n = p_1 p_2 \ldots p_k n_k$ est un produit de nombres premiers.

On verra plus bas que cette décomposition de n en produit de nombres premiers est unique.

Remarque :

Si n est négatif on a un résultat analogue : $n = -p_1 p_2 \ldots p_k$.

Exercice 9 : Montrer que si $a < n^2$ et si a n'est divisible par aucun des nombres premiers plus petit que n, a est premier.

Proposition 3 : Il y a une infinité de nombres premiers.

Soit p un nombre premier. On va montrer qu'il existe un nombre premier plus grand que p ce qui entraînera le résultat. Soit $2,3,5,\ldots,p$ l'ensemble de tous les premiers inférieurs ou égaux à p. Le nombre $n = 2.3.5. \ldots .p+1$ n'est divisible par aucun des nombres $2,3,5,\ldots,p$. Comme n admet un diviseur premier, celui-ci est strictement plus grand que p ce qu'il fallait prouver.

La distribution des nombres premiers est assez régulière. Ainsi dans les 5 premiers paquets de 1000 nombres (de 1 à 1000, de 1001 à 2000...) le nombre d'entiers premiers est respectivement égal à 168, 135, 127, 120, 119 et dans les 5 derniers paquets de 1000 précédant 10 000 000 on en trouve 62, 58, 67, 64, 53 : on constate une lente décroissance avec quelques "soubresauts".

Exercice 10 : Décomposer en facteurs premiers le nombre $10! = 1.2.3 \ldots 9.10$.

Exercice 11 : Montrer que n^2-n+41 est premier pour $0 \leq n \leq 40$ et ne l'est pas pour $n = 41$.

Exercice 12 : Quelle est la plus petite valeur de n (entier naturel) telle que $2.3. \ldots .n+1$ n'est pas premier ?

Quelle est la plus petite valeur de p, nombre premier, telle que $2.3.5. \ldots p+1$ n'est pas premier ?

Quelle est la plus petite valeur de p premier telle que 2^p-1 n'est pas premier ?

Comment déterminer qu'un nombre est premier ?

Pour reconnaître si n est premier, on le divise successivement par $2,3,5,7,\ldots$ Si aucune de ces divisions ne "tombe juste" c'est que n est premier. Il faut savoir s'arrêter : soient p_k et p_{k+1} deux nombres premiers successifs ; supposons que $n = qp_k+r$ avec $q < p_{k+1}$ il est inutile d'aller plus loin.

Exercice 13 : Justifier cette dernière assertion.

Le procédé ci-dessus indiqué suppose que l'on a une table des nombres premiers (ou qu'on les connaît par coeur). Si ce n'est pas le cas - si n est très grand - on divise n par $2,3,4,5,6,\ldots$ (en négligeant d'ailleurs les divisions par des nombres dont on sait qu'ils sont composés) et on s'arrêt dès qu'on a écrit $n = qm$ avec $q < m$.

Exercice 14 : On rappelle que $x^k-1 = (x-1)(x^{k-1}+x^{k-2}+\ldots+x+1)$ et que, si k est impair, $x^k+1 = (x+1)(x^{k-1}-x^{k-2}+\ldots -x+1)$.

Montrer que si a^k-1 est premier, $a = 2$ et k premier.

Montrer que si a^k+1 est premier, k est une puissance de 2.

Exercice 15 : Montrer qu'il existe des suites d'entiers consécutifs arbitrairement longues ne contenant aucun nombre premier.

Exercice 16 : Montrer, par récurrence sur n, que le $n^{\text{ième}}$ nombre premier est majoré par $2^{2^{n-1}}$ (cette majoration est considérablement trop forte).

Le crible d'Eratosthène

Il s'agit d'écrire tous les nombres premiers entre 2 et un certain entier n. On écrit ces $(n-1)$ nombres, puis on supprime les multiples stricts de 2, c'est-à-dire $4,6,8,\ldots$ et on conserve 2 qui est premier. Le premier nombre non supprimé est 3 qui est premier. On supprime alors les multiples

stricts de 3. Reste 5 qui est premier. On supprime les multiples stricts de 5 et ainsi de suite : quand on a fait apparaître $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \ldots, p_k$ et qu'on a supprimé leurs multiples stricts, le 1^{er} nombre qui reste est p_{k+1}, le $k+1^{ième}$ nombre premier. Dès qu'on est arrivé à $p_k > \sqrt{n}$ le processus est terminé (cf. exercice 9) c'est-à-dire que tous les nombres restant dans la liste sont premiers.

(2)	(3)	~~4~~	(5)	~~6~~	(7)	~~8~~	~~9~~	~~10~~
(11)	~~12~~	(13)	~~14~~	~~15~~	~~16~~	(17)	~~18~~	(19)	~~20~~
~~21~~	~~22~~	(23)	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	(29)	~~30~~
(31)	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	(37)	~~38~~	~~39~~	~~40~~
(41)	~~42~~	(43)	~~44~~	~~45~~	~~46~~	(47)	~~48~~	~~49~~	~~50~~

Dans cet exemple on a pris $n = 50$. On a fait apparaître successivement 2,3,5,7 et on a barré leurs multiples. Le 1^{er} nombre non barré est 11 qui est premier et $11 > \sqrt{50}$. Les autres nombres non barrés (13,17,..., 43,47) sont premiers.

2.- PGCD. Théorème fondamental de l'arithmétique

Proposition 4 : *Tout idéal de $\mathbb{Z}$ est formé par l'ensemble des multiples d'un entier n (que l'on peut choisir positif). On dit que n engendre I ou que n est un générateur de I.*

Soit en effet I un idéal de $\mathbb{Z}$. Si $I = \{0\}$, I est l'ensemble des multiples de 0. Sinon soit $x \neq 0$ dans I. Si $x < 0$ le nombre $-x$ est positif. Il y a donc des nombres strictement positifs dans I. Soit n le plus petit d'entre eux et soit $a \in I$. La division euclidienne de a par n donne $a = nq+r$ avec $0 \leq r < n$. Comme $n \in I$, $nq \in I$ donc $a-nq \in I$. Par suite $r \in I$. Le choix de n et la relation $0 \leq r < n$ implique que $r = 0$ donc a est multiple de n.

Définition : Le plus grand commun diviseur de deux entiers a et b (PGCD de a et b) non nuls tous les deux, est le plus grand entier positif qui divise à la fois a et b.

On le note PGCD(a,b) ou encore (a,b) (on trouve parfois la notation $a \wedge b$).

On définit de la même manière le PGCD de plusieurs entiers $(a_1, a_2, \ldots, a_r)$: c'est le plus grand entier positif qui divise à la fois chacun des a_i.

Considérons alors l'ensemble I de tous les entiers qui peuvent s'écrire ma+nb (m et n prenant des valeurs entières). Il est immédiat que cet ensemble est un idéal. Par exemple si $x = ma+nb \in I$ et $x' = m'a+n'b \in I$, $x-x' = (m-m')a+(n-n')b$ est aussi élément de I. Il résulte de la proposition 4 que I est l'ensemble des multiples d'un entier naturel d :

- a et b sont éléments de I donc d|a et d|b.
- soit c un nombre divisant a et b : c|ma+nb pour tout couple (m,n) d'entiers. Comme $d \in I$ il est de la forme $d = ua+vb$ pour un couple (u,v) d'entiers. Donc c|d. En particulier le PGCD de a et b divise d. Comme le PGCD est le plus grand diviseur il résulte de ceci que d = PGCD(a,b). On a donc prouvé :

Proposition 5 : *Le PGCD de a et b est le générateur positif de l'idéal formé par les nombres ma+nb* $(m,n \in \mathbb{Z})$.

Ce qui entraîne le résultat suivant :

Théorème 1 :

- *Si d = PGCD(a,b) il existe* $u,v \in \mathbb{Z}$ *tels que* $d = ua+vb$.
- *L'équation* $ax+by = n$ *admet une solution* (x,y) *si et seulement si PGCD(a,b)|n.*
- *Tout diviseur commun à a et b divise PGCD(a,b).*

Cela est évident par la proposition 5.

Proposition 6 : *PGCD(a,b) = PGCD(a-b,b). Si* $a = bq+r$, *PGCD(a,b) = PGCD(r,b).*

La 2ème assertion est une conséquence de la 1ère (par itération).

Pour la 1ère on applique la proposition 5 : l'ensemble des nombres de la forme $ma+nb$ est égal à l'ensemble des nombres de la forme $ma-mb+(n+m)b = m(a-b)+(n+m)b$.

Exercice 17 : Déterminer les entiers n tels que $PGCD(2n+18,n+3) = 1$.

Définition : Deux entiers sont dits premiers entre eux si leur PGCD est égal à 1.

Ce qui signifie que $+1$ et -1 sont les seuls entiers qui divisent à la fois a et b.

Remarque :

"Soient a et b deux nombres premiers" et "soient a et b deux nombres premiers entre eux" sont deux phases qui se ressemblent beaucoup... mais qu'il faut distinguer !(Certains auteurs parlent de nombres étrangers plutôt que de nombres premiers entre eux).

Proposition 7 : *$PGCD(a,b) = d$ si et seulement s'il existe deux entiers a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.*

Si $PGCD(a,b) = d$, $d|a$ et $d|b$ donc $a = da'$ et $b = db'$.

Si a' et b' n'étaient pas premiers entre eux, ils auraient un diviseur commun c et $a = dca''$, $b = dcb''$ impliquerait que $dc|a$ et b ce qui contredit la définition de d. La démonstration de la réciproque est laissée au lecteur.

Théorème 2 : *(de Bezout)*

Deux nombres a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v tels que $ua+vb = 1$.

La condition nécessaire est le 1er point du théorème 1. Pour la condition suffisante il suffit de remarquer que si $d|a$ et $d|b$, $d|ua+vb$ donc $d = \pm 1$.

Lemme d'Euclide :

1) Si p est premier et $p|ab$ alors $p|a$ ou $p|b$.

2) Si $a|bc$ et $PGCD(a,b) = 1$ alors $a|c$.

3) Si $PGCD(a,b) = 1$, si $a|n$ et $b|n$ alors $ab|n$.

Prouvons d'abord le point 2 : comme PGCD(a,b) = 1 il existe u et v tels que au+bv = 1 (Bezout). En multipliant par c cette relation on trouve acu+bcv = c. Comme a|acu et a|bcv, a divise la somme de ces nombres donc a|c.

Le point 1 est une conséquence de 2 à cause du :

Lemme 1 : *Si p est premier, si a est entier on a $p|a$ ou $PGCD(a,p) = 1$.*

Cela est clair car PGCD(a,p)|p et comme p est premier, PGCD(a,p) = 1 ou p.

Ainsi avec les hypothèses du lemme d'Euclide si p ne divise pas a c'est que PGCD(a,p) = 1 et par le point 2, p|b.

Pour le 3 : a|n donc n = am. Comme b|am et que PGCD(a,b) = 1, c'est que b|m. Donc m = bk et ainsi n = abk.

Le 2 du lemme d'Euclide peut aussi se démontrer à partir du lemme suivant :

Lemme 2 : *$PGCD(ac,bc) = c\ PGCD(a,b)$.*

Si d = PGCD(a,b) on a a = da' et b = db' avec PGCD(a',b') = 1. Donc ac = dca' et bc = dcb' et par suite PGCD(ac,bc) = dc (Proposition 7).

Exercice 18 : Montrer le point 2 du lemme d'Euclide à partir de ce résultat.

Corollaire : *Si p est premier, p divise C_p^k (nombre de combinaisons de k dans p) pour $1 \leq k \leq p-1$.*

Car $C_p^k = \frac{p(p-1)\ldots(p-k+1)}{k!}$. On sait que $k!$ divise $p(p-1)\ldots(p-k+1)$ et $k!$ est premier avec p (car $k < p$) d'où le résultat.

L'algorithme d'Euclide

Il s'agit d'un procédé permettant de déterminer le PGCD de deux nombres.

Soient a et b deux entiers. Supposons $a \geq b > 0$. En divisant a par b on obtient $a = q_1 b + r_1$ avec $0 \leq r_1 < b$. Si $r_1 \neq 0$ on divise b par r_1 : $b = q_2 r_1 + r_2$ et $0 \leq r_2 < r_1$. Puis, si $r_2 \neq 0$ on divise r_1 par r_2 et ainsi de suite. On obtient ainsi une suite $b, r_1, r_2, \ldots$ de nombres positifs, strictement décroissante. Il existe donc un entier n tel que $r_{n+1} = 0$. Les deux dernières étapes du processus sont :

$$r_{n-2} = q_n r_{n-1} + r_n \quad (0 < r_n < r_{n-1})$$

$$r_{n-1} = q_{n+1} r_n .$$

Proposition 8 : *Avec les notations ci-dessus,* $r_n = PGCD(a,b)$.

Soit $d = PGCD(a,b)$. On a successivement :

$$d|a,\ d|b \Rightarrow d|r_1 = a - q_1 b$$

$$d|b,\ d|r_1 \Rightarrow d|r_2$$

et par une récurrence immédiate $d|r_n$.

Par ailleurs comme $r_{n-1} = q_{n+1} r_n$, $r_n | r_{n-1}$ et comme $r_{n-2} = q_n r_{n-1} + r_n$, $r_n | r_{n-2}$. On remonte ainsi jusqu'aux deux premières relations : $b = q_2 r_1 + r_2$, $r_n | r_2$ et r_1 donc $r_n | b$ et $a = q_1 b + r_1$, $r_n | r_1$ et b donc $r_n | a$. Ainsi $r_n | a$ et b donc $r_n | d$. Ceci ajouté à $d | r_n$ montre que $r_n = d$.

Cet algorithme est aisément programmable sur calculettes, surtout si l'on remarque que la division euclidienne de a par b consiste en une succession de soustractions : $a-b$, $a-2b, \ldots, a-qb$ que l'on arrête dès que $0 \leq a-qb < b$.

Les résultats qui précèdent s'appliquent, en modifiant ce qui doit l'être, au PGCD de n entiers. Par exemple si d est le PGCD de $a_1, a_2, \ldots, a_n$, il existe des entiers $u_1, u_2, \ldots, u_n$ tels que $d = a_1 u_1 + \ldots + a_n u_n$.

Ou encore : l'équation $a_1x_1+\ldots+a_nx_n = k$ admet une solution $(x_1,\ldots,x_n)$ si et seulement si k est un multiple du PGCD de $(a_1,\ldots,a_n)$. Les démonstrations de ces résultats se font comme ci-dessus, le point de départ étant de considérer l'idéal I engendré par $(a_1,\ldots,a_n)$ c'est-à-dire l'ensemble des nombres entiers de la forme $a_1u_1+a_2u_2+\ldots+a_nu_n$ quand $u_1,u_2,\ldots,u_n$ parcourent $\mathbb{Z}$. On peut aussi se ramener au cas du PGCD de deux nombres en utilisant la :

Proposition 9 : *(Associativité du PGCD)*
Si a,b,c sont 3 entiers, $PGCD(a,b,c) = PGCD(PGCD(a,b),c)$.

La démonstration est immédiate (on montre que chacun des deux nombres de cette relation divise l'autre).

Proposition 10 : *Soient a et b deux entiers naturels premiers entre eux. L'équation $ax+by = 1$ admet une seule solution (x_0,y_0) telle que $|x_0| < b$ et $|y_0| < a$. L'ensemble des solutions de cette équation est donné par $x = x_0+kb$ et $y = y_0-ka$ où k prend toutes les valeurs entières.*

Remarquons d'abord que si x et y sont deux solutions de l'équation :

$$ax+by = 1$$

$$ax'+by' = 1$$

on a, par différence $a(x-x')+b(y-y') = 0$. Comme a et b sont premiers entre eux et que $a|b(y-y')$, on a $a|(y-y')$ soit $y-y' = ka$. Il vient alors $x'-x = kb$.

Réciproquement si (x,y) est une solution, $(x+kb,y-ka)$ est aussi solution. Parmi toutes ces solutions il en est une telle que $|x+kb| < b$ puisque dans chaque intervalle entier de longueur b, on peut trouver un nombre de la forme $x+kb$. Si $x_0 = x+kb$ est choisi pour que $|x_0| < b$, il est immédiat que $|y_0| < a$.

Théorème fondamental de l'arithmétique :

La décomposition en facteurs premiers d'un entier est définie de manière unique (à l'ordre près des facteurs).

Soit n un entier (que l'on suppose positif) admettant deux décompositions en facteurs premiers :

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$$

Dans chacune de ces décompositions nous regroupons les facteurs égaux d'où :

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_\ell^{b_\ell}.$$

Comme p_i est premier $(1 \leq i \leq k)$ et divise n, le lemme d'Euclide implique que p_i doit diviser l'un des q_j donc, comme q_j est premier, lui être égal. Ainsi, chaque p_i est un q_j et de même chaque q_j est un p_i. Par suite $k = \ell$ et les deux décompositions de n s'écrivent :

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}.$$

Supposons $a_1 = b_1 + c$ avec $c \geq 0$. On trouve :

$$n = p_1^{b_1} p_1^{c} p_2^{a_2} \cdots p_k^{a_k} = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

et en divisant les deux premiers membres par $p_1^{b_1}$, il vient :

$$p_1^{c} p_2^{a_c} \cdots p_k^{a_k} = p_2^{b_2} \cdots p_k^{b_k}.$$

p^c doit donc diviser le membre de droite donc être égal à l'un des p_i $(2 \leq i \leq k)$ ce qui est exclus. Donc $c = 0$ d'où $a_1 = b_1$ et de même $a_i = b_i$ pour tout i.

Pratique de la décomposition en facteurs premiers

Elle suit la méthode exposée dans la proposition 2. Il s'agit d'abord de trouver le plus petit diviseur premier de l'entier considéré n. Pour ceci on divise n par $2,3,5,\ldots$ successivement jusqu'à obtenir un reste nul. On trouve $n = p_1 n_1$ et on recommence le même processus avec n_1.

Par exemple soit à décomposer 630 : 630 est multiple de 2 et $630 = 2.315$; 315 est multiple de 3 et $315 = 3.105$; $105 = 3.35$; $35 = 5.7$ et on arrive ainsi à $630 = 2.3 .5.7$.

Dès que les nombres sont assez grands, ce processus est long (et fastidieux). Il est très simplifié si l'entier initial est décomposé en produit de facteurs : il n'est par exemple pas très difficile de trouver la décomposition en facteurs premiers de 50!.

Notation

Soient n un nombre entier, p un nombre premier. On pose $r_p(n)$ = exposant de p dans la décomposition en facteurs premiers de n si $p|n$, $r_p(n) = 0$ sinon.

Alors : $n = \prod_{p \text{ premier}} p^{r_p(n)}$: c'est-à-dire que n est le produit pour tous les p premiers de $p^{r_p(n)}$. Le produit est bien entendu fini puisque les $r_p(n)$ sont nuls sauf pour les facteurs premiers de n. L'avantage de cette notation, c'est qu'elle est homogène pour tous les nombres entiers.

A titre d'exercice nous montrons le résultat suivant : $r_p(n!) = r_p(n!) = \sum_{k \geq 1} \left[\frac{n}{p^k}\right]$ où $[x]$ désigne la partie entière de x.

La somme écrite à droite est finie car pour k assez grand, $p^k > n$ et $\left[\frac{n}{p^k}\right] = 0$ (puisque $\frac{n}{p^k} < 1$). On a $n! = 1.2... n$. Parmi les entiers $1,2,...,n$ il y en a $\left[\frac{n}{p}\right]$ qui sont multiples de p, à savoir p, $2p$,.. .., $\left[\frac{n}{p}\right]p$.

Les entiers entre 1 et n qui sont multiples de p^2 sont en nombre égal à $\left[\frac{n}{p^2}\right]$ .. et ainsi de suite.

Ainsi le nombre d'entiers entre 1 et n qui sont multiples de p sans l'être de p^2 est $\left[\frac{n}{p}\right]-\left[\frac{n}{p^2}\right]$ et chacun de ces nombres interviennent avec l'exposant 1 dans le terme en p de la décomposition en facteur premiers de n.

Le nombre d'entiers entre 1 et n qui sont multiples de p^2 sans l'être de p^3 est $\left[\frac{n}{p^2}\right] - \left[\frac{n}{p^3}\right]$ et ils interviennent avec l'exposant 2 dans le terme en p de la décomposition de n. On a donc, en itérant :

$$r_p(n!) = \left(\left[\frac{n}{p}\right]-\left[\frac{n}{p^2}\right]\right)+2\left(\left[\frac{n}{p^2}\right]-\left[\frac{n}{p^3}\right]\right)+3\left(\left[\frac{n}{p^3}\right]-\left[\frac{n}{p^4}\right]\right)+\ldots$$

ce qui donne le résultat cherché.

Par exemple pour $n = 10$ on a à considérer :

1,2,3,4,5,6,7,8,9,10.

2,6 et 10 sont multiples de 2 sans l'être de 4.
4 est multiple de 2^2 sans l'être de 2^3.
8 est multiple de 2^3 sans l'être de 2^4.

Donc $r_2(10!) = 3+2+3 = 8$.

Exercice 19 : Montrer que le nombre de zéros qui terminent l'écriture de n! (écrit dans le système décimal) est égal à $r_5(n!)$). (remarquer que $r_5(n!) < r_2(n!)$ et en déduire que la plus grande puissance de 10 qui divise n! est égale à la plus grande puissance de 5 qui divise n!). Déterminer le nombre de zéros terminant 100!.

3.- Applications du théorème fondamental

Dans ce paragraphe p désigne toujours un nombre premier.

Diviseurs d'un entier

Soit n un entier, $n = p_1^{a_1} \ldots p_r^{a_r}$ sa décomposition en facteurs premiers. Si $d = q_1^{b_1} \ldots q_s^{b_s}$ divise n, chaque q_i doit diviser un p_j et on voit de suite que $d = p_1^{b_1} \ldots p_r^{b_r}$ avec $0 \leq b_1 \leq a_i$. Réciproquement tout nombre de cette forme est un diviseur de n.

Proposition 11 : *Les diviseurs de* $p_1^{a_1} \ldots p_r^{a_r}$ *sont les nombres de la forme* $p_1^{b_1} \ldots p_r^{b_r}$ *avec* $0 \leq b_i \leq a_i$, $1 \leq i \leq r$.

Détermination du PGCD

Proposition 12 : $PGCD(a,b) = \prod_p p^{r_p}$ où $r_p = Min(r_p(a), r_p(b))$.

Cela résulte immédiatement de la proposition 11.

Par exemple le PGCD de $2^3.3^5.7.11^4.13$ et de $2^4.3^2.11^3.13.23$ est $2^3.3^2.11^3.13$.

Nombre de diviseurs d'un entier

Si $n = p_1^{a_1} \dots p_r^{a_r}$, ses diviseurs sont de la forme $p_1^{b_1} \dots p_r^{b_r}$ avec $0 \leq b_i \leq a_r$ pour $1 \leq i \leq r$.

Pour chaque i on a donc le choix entre a_i+1 valeurs de b_i (tous les entiers entre 0 et a_r, bornes comprises).

Proposition 13 : Le nombre de diviseurs de l'entier $n = p_1^{a_1} \dots p_r^{a_r}$ est égal à $(a_1+1)(a_2+1)\dots(a_r+1)$.

Somme des diviseurs d'un entier

On désigne par $\sigma(n)$ la somme des diviseurs de l'entier n.

Lemme : Si $PGCD(a,b) = 1$, $\sigma(ab) = \sigma(a)\sigma(b)$.

Soient $a = p_1^{a_1} \dots p_r^{a_r}$ et $b = q_1^{b_1} \dots q_s^{b_s}$. Comme a et b sont premiers entre eux, aucun des p_i n'est un q_j. Les diviseurs de a sont de la forme $p_1^{a'_1} \dots p_r^{a'_r}$ avec $0 \leq a'_i \leq a_i$ et leur somme est :

$$\sigma(a) = \sum_{\substack{0 \leq a'_i \leq a_i \\ 1 \leq i \leq r}} p_1^{a'_1} \dots p_r^{a'_r}$$

De même $$\sigma(b) = \sum_{\substack{0 \leq b'_i \leq b_i \\ 1 \leq i \leq s}} q_1^{b'_1} \dots q_r^{b'_r}$$

et $$\sigma(ab) = \sum_{\substack{0 \leq a'_i \leq a_i, 0 \leq b'_j \leq b_j \\ 1 \leq i \leq r \ , 1 \leq j \leq s}} p_1^{a'_1} \dots p_r^{a'_r} q_1^{b'_1} \dots q_r^{b'_r}$$

et on se convainc que ce nombre n'est autre que $\sigma(a)\sigma(b)$.

Proposition 14 : Si $n = p_1^{a_1} \dots p_r^{a_r}$, $\sigma(n) = \frac{p_1^{a_1+1}-1}{p_1-1} \cdot \frac{p_2^{a_2+1}-1}{p_2-1} \dots \frac{p_r^{a_r+1}-1}{p_r-1}$.

On a d'abord $\sigma(p^a) = 1+p+p^2+\dots+p^a = \frac{p^{a+1}-1}{p-1}$.

Comme les nombres $p_1^{a_1} \dots p_r^{a_r}$ sont premiers entre eux 2 à 2, une application itérée du lemme ci-dessus donne le résultat.

Remarque :

Cette démonstration est donnée à titre d'exemple. De très nombreuses fonctions définies sur $\mathbb{N}$ vérifient un résultat analogue au lemme. Pour calculer la valeur en un entier n quelconque d'une telle fonction il suffira de connaître sa valeur pour les entiers particuliers p^a (où p est premier).

Exercice 20 :

- Quels sont les nombres à 2 chiffres qui admettent le plus grand nombre de diviseurs ?
- Quel est le plus petit entier positif qui a 4 diviseurs ? 30 diviseurs ?

Exercice 21 : Soit k le nombre de diviseurs d'un entier n. Montrer que si n n'est pas un carré k est pair et que le produit des diviseurs de n est $n^{k/2}$. Montrer que si $n = m^2$, le produit des diviseurs de n est m^k.

Exercice 22 : On appelle nombre parfait un nombre qui est égal à la moitié de la somme de ses diviseurs. Essayer de trouver des nombres parfaits (on sait démontrer qu'un nombre pair est parfait si et seulement si il est de la forme $2^{p-1}(2^p-1)$ où 2^p-1 est un nombre premier. On ne connaît aucun nombre parfait impair).

PPCM, détermination du PPCM

Définition : On appelle PPCM de deux entiers a et b et on note PPCM(a,b) le plus petit entier positif qui est à la fois multiple de a et de b.

La proposition 11 nous donne aussitôt :

Proposition 15 : $PPCM(a,b) = \prod_p p^{q_p}$ *avec* $q_p = Max(r_p(a), r_p(b))$.

Comme la somme $Max(r_p(a),r_p(b))+Min(r_p(a),r_p(a))$ est égale à $r_p(a)+r_p(b)$ on a :

Proposition 16 : $PPCM(a,b)PGCD(a,b) = ab$.

Donnons une autre démonstration de ce résultat. Il est clair que $PGCD(a,b) \mid ab$. Posons $k = \frac{ab}{PGCD(a,b)}$.

$k = a \times \frac{b}{PGCD(a,b)} = b \times \frac{a}{PGCD(a,b)}$ donc k est un multiple commun à a et b. Soit ℓ un multiple commun à a et b. Considérons $\frac{\ell}{k} = \frac{\ell\ PGCD(a,b)}{ab}$. On sait qu'il existe (x,y) tel que $ax+by = PGCD(a,b)$, donc $\frac{\ell}{k} = \frac{\ell\ ax+\ell\ by}{ab} = \frac{\ell x}{b} + \frac{\ell y}{a}$. Comme ℓ est multiple de a et b, on a $\frac{\ell x}{b}$ et $\frac{\ell y}{a}$ entiers donc $\ell \geq k$ ce qui prouve que k est le PPCM de a et b.

En cours de route on a même montré que ℓ est multiple de k donc :

Proposition 17 : *Le PPCM de a et b divise tout multiple commun à a et b.*

On notera le caractère symétrique du PPCM par rapport au PGCD. Ces deux notions jouant des rôles analogues on peut dire que l'un des deux est superflu. Dans la pratique l'usage du PGCD est plus commode que celui du PPCM.

Exercice 23 : Soit I l'idéal des multiples d'un entier a et J l'idéal des multiples de b. Montrer que le générateur de $I \cap J$ est le PPCM de a et b.

Remarque :

On peut généraliser le PPCM à plusieurs nombres (avec une propriété d'associativité analogue à celle du PGCD). Il faut prendre garde au fait que

la proposition 16 ne se généralise pas. Ainsi

$$PPCM(10,6,15)PGCD(10,6,15) = 30 \neq 900$$

Exercice 24 : Montrer que $PPCM(a^2,ab,b^2) = (PPCM(a,b))^2$ (utiliser $PPCM(a^2,ab,b^2) = PPCM(a^2,ab,ab,b^2)$ et l'associativité du PPCM).

Exercice 25 : Déterminer x et y tels que $x+y-1 = PPCM(x,y)$

4.- Sur la répartition des nombres premiers

(Le contenu de ce paragraphe est hors programme).

Soit $(p_1,p_2,\ldots,p_n,\ldots)$ la suite des nombres premiers rangés par ordre croissant. C'est une partie très ardue mais très fascinante des mathématiques que d'avoir des informations sur la répartition de cette suite. Nous citons ici quelques résultats dans ce sens.

1) Le n^{e} nombre premier p_n est à peu près égal à $n \log n$. Plus correctement : $p_n \sim n \log n$ quand n tend vers l'infini.

2) Pour un réel positif x, soit $\pi(x)$ le nombre d'entiers premiers inférieurs ou égaux à x. $\pi(x)$ est une fonction à valeurs entières. On a par exemple : $\pi(2) = 1$, $\pi(10) = 4$, $\pi(20) = 8$, $\pi(20,5) = 8$. On a :

$$\pi(x) \sim \frac{x}{\log x} \quad \text{quand} \quad x \quad \text{tend vers l'infini.}$$

C'est le célèbre "théorème des nombres premiers" démontré simultanément et indépendamment par Hadamard et de la Vallée Poussin en 1896.

Sous la forme du résultat 1 (qui est d'ailleurs équivalent à 2), on voit que les nombres premiers ont tendance à s'écarter de plus en plus les uns des autres. Mais cela n'est vrai qu'en "moyenne". Les comportements ponctuels sont plus irréguliers. On a par exemple conjecturé qu'il existait une infinité de nombres premiers p tels que p+2 soit lui-même premier. Comme exemple de ces "premiers jumeaux" on a bien sûr 3 et 5, 5 et 7, 41 et 43 et, pour aller plus loin, $1159142985 \times 2^{2304} \pm 1$.

Ce n'est là qu'une conjecture. On sait toutefois que la suite $p_{n+1} - p_n$ n'est pas croissante alors que la suite $(n+1)\log(n+1) - n \log n$ l'est. (Vérifier cette dernière assertion).

3) On peut se poser le problème de trouver une formule permettant de construire tous les nombres premiers. (Par exemple $p_{n+1} = p_n^2 - p_n + 3$ serait une formule-fausse!- donnant p_{n+1} à partir de p_n). Il n'existe rien de tel.

On pourrait être moins ambitieux et chercher une fonction f telle que $f(n)$ soit un nombre premier pour tout entier n. On n'en connaît pas (en tout cas construite à partir de fonctions élémentaires. Car l'application qui à n associe p_n est une telle fonction !). Par exemple :

Exercice 26 : Si $P(x) = a_0 + a_1 x + \ldots + a_n x^n$ est un polynôme à coefficients entiers, il existe des entiers n tel que $P(n)$ ne soit pas premier. (Montrer que $P(n) \mid P(n+P(n))$ quel que soit l'entier n.

Exercice 27 : Montrer que $x^2 - x + 41$ est premier pour $0 \leq x \leq 40$ et que $x^2 - 79x + 1601 = (x-40)^2 + (x-40) + 41$ est premier pour $0 \leq x \leq 79$.

4) Existe-t-il une fonction f simple telle que $f(n)$ soit premier pour une infinité de n ? La situation ici est moins désespérée.

- Fermat avait conjecturé que $2^{2^n}+1$ était toujours un nombre premier. Euler a montré que $641 \mid 2^{2^5}+1$.

- Mersenne a considéré les nombres $2^n - 1$. Si $2^n - 1$ est premier c'est que n est premier (exercice 13, § 1). (la réciproque est fausse : $2^{11}-1$ n'est pas premier). On ne sait s'il existe une infinité de nombres premiers p tels que $2^p - 1$ soit premier. Mais il existe une procédure relativement simple pour déterminer si $2^p - 1$ est premier. C'est ainsi que l'on construit de très grands nombres premiers. Les plus grands connus à ce jour sont :

$$2^{44497}-1,\ 2^{86243}-1,\ 2^{132049}-1,\ 2^{216091}-1.$$

Il existe quand même des résultats positifs tel le célèbre théorème de Dirichlet:

Si a et b sont premiers entre eux, il existe une infinité de nombres premiers de la forme $a+kb$. Contentons-nous de démontrer un cas très particulier de ce théorème :

Il existe une infinité de nombres premiers de la forme $4n-1$ (c'est-à-dire congrus à -1 modulo 4).

Supposons que ces nombres premiers forment un ensemble fini $\{q_1, q_2, \ldots, q_r\}$. Remarquons que si un nombre premier est différent de 2 il est congru à ± 1 modulo 4.

Considérons $n = 4q_1 q_2 \ldots q_r - 1$: aucun des nombres q_i ne divise n, n est impair. Donc si $n = p_1 p_2 \ldots p_k$, les p_i sont tous de la forme $4m+1$ (puisqu'aucun p_i n'est un q_j). Donc $p_i \equiv 1 \pmod 4$ d'où $n \equiv 1 \pmod 4$ ce qui est absurde.

5) Pour en revenir à la distribution des nombres premiers parmi les nombres entiers, citons 2 résultats :

- Entre n et 2n, il existe un nombre premier.
- Si n est assez grand, il existe un nombre premier entre n^3 et $(n+1)^3$.

Et on conjecture que :

- Si n est assez grand, il existe un nombre premier entre n^2 et $(n+1)^2$.

III - CONGRUENCES

1.- Définitions. L'anneau $\mathbb{Z}/n\mathbb{Z}$

Définition :

Si n est un entier relatif, si a et b sont deux entiers relatifs tels que n divise b-a, on dit que b est congru à a modulo n et on note $b \equiv a \pmod n$. On dit aussi que a est un résidu de b modulo n, ou un reste de b modulo n. La relation ainsi définie est une congruence modulo n.

Remarque : Si $n|b-a$, $-n|b-a$. On peut donc se limiter à étudier des congruences modulo des entiers naturels.

Proposition 18 : *La relation de congruence est une relation d'équivalence c'est-à-dire que :*

$b \equiv a \pmod n \Rightarrow a \equiv b \pmod n$

$a \equiv a \pmod n$

$b \equiv a \pmod n$ *et* $c \equiv b \pmod n \Rightarrow c \equiv a \pmod n$.

La classe d'équivalence de a pour cette relation, c'est-à-dire l'ensemble des entiers b congrus à a modulo n est la classe de congruence de a modulo n.

Comme on le sait, l'ensemble des classes de congruence forme une partition de $\mathbb{Z}$: tout élément de $\mathbb{Z}$ est dans une classe et deux classes distinctes n'ont aucun nombre en commun.

Proposition 19 : *a et b sont congrus entre eux modulo n si et seulement s'ils ont même reste dans la division euclidienne par n.*

Si $a = qn+r$ $(0 \leq r < n)$ on a $a-r = qn$ donc $a \equiv r \pmod{n}$ d'où le résultat.

Un élément d'une classe de congruence modulo n est un <u>représentant</u> de cette classe. Une famille d'entiers $a_1, a_2, \ldots, a_k$ telle que tout entier b est congru modulo n à l'un des a_j et telle que si $i \neq j$, x_i est non congru à a_j et un <u>système de représentants</u> de la congruence.

Proposition 20 : *Les nombres $(0,1,\ldots,n-1)$ constituent un système de représentants de la congruence modulo n.*

En effet tout entier est congru à son reste dans la division par n donc à un élément de l'ensemble $(0,1,\ldots,n-1)$. Deux éléments de cet ensemble ne sont pas congrus entre eux : car si $0 \leq i < j \leq n-1$, $j-i$ ne peut être multiple de n.
(On considère parfois comme système de représentants l'ensemble $(1,2,\ldots,n)$).

Proposition 21 : *Si $a \equiv b$ et $a' \equiv b' \pmod{n}$, alors :*
$a+a' \equiv b+b' \pmod{n}$,
$aa' \equiv bb' \pmod{n}$.

(on dit que la congruence est "compatible" avec les opérations de $\mathbb{Z}$).

On a : $b-a = kn$ et $b'-a' = k'n$ pour deux entiers k et k'.

En faisant la somme de ces relations :

$$(b+b')-(a+a') = (k+k')n \quad \text{donc} \quad a+a' \equiv b+b' \pmod{n}$$

Par ailleurs $bb'-aa' = b(b'-a')+(b-a)a'$

$$= (bk'+a'k)n \quad \text{donc} \quad aa' \equiv bb' \pmod{n}.$$

(Remarquer qu'en faisant $a' = b' = -1$ dans la $2^{\text{ème}}$ relation on trouve que $a \equiv b \pmod{n} \Rightarrow -a \equiv -b \pmod{n}$. On en déduit, avec les hypothèses de la proposition que $a-a' \equiv b-b' \pmod{n}$).

Ces propriétés vont nous permettre de faire des calculs sur l'ensemble des classes de congruence.

Soit par exemple un nombre premier p différent de 3. Montrons que $8p^2+1$ n'est pas premier : comme p est premier et $p \neq 3$, 3 n'est pas un diviseur de p. Donc la classe de p modulo 3 est soit la classe de 1, soit la classe de 2. Dans le 1^{er} cas, $p \equiv 1 \pmod{3}$ donc, en élevant au carré : $p^2 \equiv 1 \pmod{3}$. Comme $8 \equiv 2 \pmod{3}$, on arrive à $8p^2 \equiv 2 \pmod{3}$ donc $8p^2+1 \equiv 3 \equiv 0 \pmod{3}$, donc $3 \mid 8p^2+1$. De la même manière on traite le cas $p \equiv 2 \pmod{3}$. (On peut aussi remarquer que $2 \equiv -1 \pmod{3}$, donc $p \equiv 2 \pmod{3} \Leftrightarrow p \equiv -1 \pmod{3}$ donc $p^2 \equiv 1 \pmod{3}$ et c'est le cas précédent).

Exercice 28 : Montrer que si p et $8p^2+1$ sont premiers, alors $8p^2-1$ est premier.

On désigne par $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes de congruence modulo n ($\mathbb{Z}/n\mathbb{Z}$ se lit : $\mathbb{Z}$ sur $\mathbb{Z}$ N$\mathbb{Z}$).

La classe d'un entier a sera notée $\bar{a}$. Ainsi l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ est, par exemple : $\bar{0},\bar{1},\ldots,\overline{n-1}$. Ecrire que $a \equiv b \pmod{n}$ c'est écrire que $\bar{a} = \bar{b}$. Il faut noter que cette dernière relation n'a de sens que si l'on sait que les classes sont considérées modulo n. On évitera de l'utiliser sans plus de précision dans les cas où il faut considérer à la fois les classes modulo n et modulo m.

Soient maintenant deux classes α et β dans $\mathbb{Z}/n\mathbb{Z}$.

Il existe donc deux éléments a et b de $\mathbb{Z}$ tels que $\alpha = \bar{a}$ et $\beta = \bar{b}$.

Posons : $\alpha+\beta = \overline{a+b}$ et $\alpha\beta = \overline{ab}$

c'est-à-dire $\bar{a}+\bar{b} = \overline{a+b}$ et $\bar{a}\bar{b} = \overline{ab}$.

Proposition 22 : *Les formules ci-dessus définissent deux opérations dans* $\mathbb{Z}/n\mathbb{Z}$. *Muni de ces opérations,* $\mathbb{Z}/n\mathbb{Z}$ *est un anneau commutatif unitaire.*

Il faut remarquer que la définition de $\alpha+\beta$ semble dépendre du choix de a et b. On s'assure d'abord qu'il n'en est rien. Supposons que $\alpha = \bar{a}'$ et $\beta = \bar{b}'$. Cela signifie que a et a' sont dans la même classe, et de même pour b et b'.

Donc

$$a \equiv a' \pmod{n}$$
$$b \equiv b' \pmod{n}$$

La proposition 21 indique donc que $a+b \equiv a'+b' \pmod{n}$ et que $ab \equiv a'b' \pmod{n}$ ou encore que $\overline{a+b} = \overline{a'+b'}$ et $\overline{ab} = \overline{a'b'}$.

Cela signifie que partant de (a',b') au lieu de (a,b) pour représenter α et β on arrive au même résultat pour la somme et le produit de ces deux classes.

Il est à la fois simple et fastidieux de s'assurer que $\mathbb{Z}/n\mathbb{Z}$ est un anneau. Remarquons d'abord que $\bar{0}$ est élément neutre pour l'addition et $\bar{1}$ pour la multiplication :

$$\bar{a} = \overline{a+0} = \bar{a}+\bar{0}$$

$$\bar{a} = \overline{a\times 1} = \bar{a}\times\bar{1}$$

L'associativité de l'addition se montre comme suit : on sait que dans $\mathbb{Z}$,

$$(a+b)+c = a+(b+c).$$

Donc :

$$\overline{(a+b)+c} = \overline{a+(b+c)}$$

et par définition de la somme de 2 classes, ceci s'écrit encore :

$$(\overline{a+b})+\overline{c} = \overline{a}+(\overline{b+c})$$

et encore $(\overline{a}+\overline{b})+\overline{c} = \overline{a}+(\overline{b}+\overline{c})$

Le lecteur achèvera la démonstration.

Exemples : Nous construisons ci-dessous les tables d'addition et de multiplication de $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.

$\mathbb{Z}/5\mathbb{Z}$:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\mathbb{Z}/6\mathbb{Z}$:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Dans les calculs sur les congruences modulo n, plutôt que d'utiliser le système de classes $\bar{0},\bar{1},\ldots,\overline{n-1}$ on pourra remplacer $\overline{n-1}$ par $-\bar{1}$, $\overline{n-2}$ par $-\bar{2}$ ... . Ainsi pour calculer, dans $\mathbb{Z}/23\mathbb{Z}$, $(\overline{20})^2$ on peut remplacer $\overline{20}$ par $-\bar{3}$ et il est un peu plus facile de calculer $(-\bar{3})^2$ que $\overline{20^2}$.

Exercice 29 : Montrer que $n(n+1)(2n+1)$ est multiple de 6.

Montrer que si p est un nombre premier ≥ 5, p^2-1 est multiple de 24.

Indiquons une solution pour le second exercice : comme p est premier, il n'est pas multiple de 3. Dans $\mathbb{Z}/3\mathbb{Z}$ on a $\bar{p} = \bar{1}$ ou $\bar{2}$ c'est-à-dire $\bar{p} = \pm\bar{1}$ donc $\bar{p}^2-\bar{1} = \bar{0}$, p^2-1 est multiple de 3.

Maintenant dans $\mathbb{Z}/8\mathbb{Z}$, comme p est impair, on a $\bar{p} = \bar{1}, \bar{3}, \bar{5}$ ou $\bar{7}$ c'est-à-dire $\bar{p} = \pm\bar{1}$ ou $\pm\bar{3}$ et alors $\bar{p}^2 = \bar{1}$ ou $\bar{3}^2 = \bar{1}$ donc $\bar{p}^2 - \bar{1} = \bar{0}$. Ce qui signifie que p^2-1 est multiple de 8. Il l'est aussi de 3 et comme $PGCD(3,8) = 1$, $24 = 3\times 8 \mid p^2-1$.

Exercice 30 : Montrer que n^3+n^2+1 n'est pas divisible par 5. Quels sont les entiers n tels que n^4+n^3+1 est divisible par 5 ? (On examine successivement toutes les valeurs de $\bar{n}$ dans $\mathbb{Z}/5\mathbb{Z}$).

Exercice 31 : Montrer que quel que soit n, les nombres n, $n+2$ et $n+10$ forment un système de représentants de $\mathbb{Z}/3\mathbb{Z}$. En déduire qu'on ne peut trouver p tel que p, $p+2$ et $p+10$ soient trois nombres premiers.

Exercice 32 : Soient a et b deux nombres premiers entre eux. Montrer que les restes des diviseurs de $a, 2a, \ldots, (b-1)a$ par b sont distincts 2 à 2 (c'est-à-dire que $a, 2a, \ldots, (b-1)a$ est un système de représentants de $\mathbb{Z}/b\mathbb{Z}$).

2.- Le corps $\mathbb{Z}/p\mathbb{Z}$

En examinant les tables de multiplication de $\mathbb{Z}/5\mathbb{Z}$ on constate : que dans $\mathbb{Z}/5\mathbb{Z}$, pour tout $\bar{a} \neq \bar{0}$, il existe $\bar{b}$ avec $\bar{a}\bar{b} = \bar{1}$. Cela est faux dans $\mathbb{Z}/6\mathbb{Z}$: ainsi les multiples de $\bar{2}$ sont $\bar{0}.\bar{2} = \bar{0}$, $\bar{1}.\bar{2} = \bar{2}$, $\bar{2}.\bar{2} = \bar{4}$, $\bar{3}.\bar{2} = \bar{0}$, $\bar{4}.\bar{2} = \bar{2}$, $\bar{5}.\bar{2} = \bar{4}$, aucun n'est égal à $\bar{1}$.

Proposition 23 : Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, un élément $\bar{a}$ est inversible si et seulement si $PGCD(a,n) = 1$.

Si $PGCD(a,n) = 1$, par Bezout on sait qu'il existe u et v tels que $au+nv = 1$. Donc $au = 1-nv$ et, dans $\mathbb{Z}/n\mathbb{Z}$, $\bar{a}\bar{u} = \bar{1}$: $\bar{u}$ est l'inverse de $\bar{a}$.

Si l'on suppose que $\bar{a}$ est inversible, il existe $\bar{b}$ tel que $\bar{a}\bar{b} = \bar{1}$ ou encore $n \mid ab-1$, c'est-à-dire que $ab-1 = kn$. On a donc $ab-nk = 1$ et par Bezout ceci donne $PGCD(a,b) = 1$.

Exercice 33 : Dans $\mathbb{Z}/n\mathbb{Z}$, on a $\bar{2} = \bar{1}+\bar{1}$, $\bar{3} = \bar{1}+\bar{1}+\bar{1}$ ... : on dit que $\bar{1}$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$. On voit que $\bar{3}$ engendre le groupe additif de $\mathbb{Z}/8\mathbb{Z}$ (calculer $\bar{3}+\bar{3}$, $\bar{3}+\bar{3}+\bar{3}$ ...). Montrer que $\bar{a}$ engendre le groupe additif de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si a est premier avec n (remarquer que $\bar{a}+\bar{a}+\ldots+\bar{a}$ (k fois) est la classe de ka).

Proposition 24 : Si p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps. Réciproquement $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Si p est un nombre premier, il est premier avec $1,2,\ldots,p-1$. Or $\bar{1},\bar{2},\ldots,\overline{p-1}$ sont les classes non nulles de $\mathbb{Z}/p\mathbb{Z}$, la proposition précédente entraîne qu'elles sont toutes inversibles donc que $\mathbb{Z}/p\mathbb{Z}$ est un corps.

Réciproquement si tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est inversible c'est que n est premier avec $1,2,\ldots,n-1$. Donc n est premier (sinon il aurait un diviseur m avec $1 < m \leq n-1$).

Le (petit) théorème de Fermat

Théorème 3 : Si p est premier et si a n'est pas multiple de p, $a^{p-1} \equiv 1 \pmod{p}$.

Lemme : Si a et b sont deux entiers premiers entre eux, les nombres $a,2a,\ldots,(b-1)a$ forment un système de représentants des classes modulo b.

Il suffit de montrer que les restes de ces nombres dans la division euclidienne par b sont (à l'ordre près) $1,2,\ldots,b-1$. Ou encore que ces restes sont différents de 0 et différents 2 à 2. Si l'un des restes est nul, c'est que ka est multiple de b. Comme $\mathrm{PGCD}(a,b) = 1$ c'est que $b|k$ ce qui est impossible puisque $1 \leq k \leq b-1$.

Par ailleurs pour $k \neq \ell$ soit :

$$ka = qb+r \quad (0 < r < b)$$
$$\ell a = q'b+r' \quad (0 < r' < b).$$

Par différence, si $r = r'$:

$$(k-\ell)a = (q-q')b$$

donc $b|(k-\ell)a$ et comme $PGCD(a,b) = 1$, $b|(k-\ell)$ ce qui est impossible car $1 \leq |k-\ell| \leq b-1$.

On peut alors démontrer le théorème de Fermat :

Soit a un entier non multiple de p, c'est-à-dire que $PGCD(a,p) = 1$. Les nombres $a,2a,\ldots,(p-1)a$ forment un système de représentants des classes modulo p. Donc le produit de ces nombres est congru modulo p au produit $1.2\ldots(p-1)$ (puisque $1,2,\ldots,p-1$ est aussi un système de représentants).

$a.2a\ldots(p-1)a \equiv 1.2\ldots(p-1) \pmod p$ ou encore

$$a^{p-1}(1.2\ldots(p-1)) \equiv 1.2\ldots(p-1) \pmod p \qquad (1)$$

Comme p est premier, il est premier avec $1,2,\ldots,(p-1)$ donc avec leur produit (à cause du lemme d'Euclide) et par suite $(p-1)!$ est inversible modulo p. On peut donc simplifier la relation (1) par $\overline{(p-1)!}$ ce qui donne $a^{p-1} \equiv 1 \pmod p$.

Corollaire : *Si p est premier, $a^p \equiv a \pmod p$ pour tout entier a.*

Si $a \not\equiv 0 \pmod p$ c'est le théorème de Fermat en multipliant a^{p-1} et 1 par a. Si $a \equiv 0 \pmod p$ c'est évident.

Exercice 34 : Soit a un entier non multiple de 7. Déterminer les entiers x tels que a^x-1 soit multiple de 7 (montrer que x est déterminé par sa classe modulo 6).

Déterminer les entiers y tels que y^y-1 soit multiple de 7.

Exercice 35 : Montrer que 10^n+9 est multiple de 7 si et seulement si il est multiple de 13.

Exercice 36 : Montrer que a^7-a $(a \in \mathbb{N})$ est multiple de 42.

Trouver un diviseur commun supérieur à 200 aux nombres $a^{13}-a$.

Le théorème de Fermat a un correspondant dans les anneaux $\mathbb{Z}/n\mathbb{Z}$. Nous en donnons une version édulcorée.

Proposition 25 : Si a est premier avec n, il existe k tel que $a^k \equiv 1 \pmod{n}$.

Comme les classes $\bar{a}$, $\bar{a}^2$, $\bar{a}^3$,... sont des éléments de l'ensemble fini $\mathbb{Z}/n\mathbb{Z}$, elles ne peuvent être distinctes deux à deux. Il existe donc r et s tels que $\bar{a}^r = \bar{a}^s$.

Comme $\bar{a}$ est inversible, $\bar{a}^s$ est inversible et ainsi $\bar{a}^{-s}$ admet $\bar{a}^{--s}$ comme inverse.

La relation $\bar{a}^r = \bar{a}^s$ donne $\bar{a}^r\bar{a}^{-s} = \bar{a}^s\bar{a}^{-s} = \bar{1}$ c'est-à-dire $\bar{a}^{r-s} = \bar{1}$ et on prend $k = r-s$.

Exercice 37 : Soit a un entier. Montrer qu'il existe un multiple de a s'écrivant 999...9000...0. (Ecrire $a = 2^\alpha 5^\beta b$ avec PGCD(10,b) = 1, montrer qu'il existe k tel que $10^k \equiv 1 \pmod{b}$).

Si a est un entier premier avec 30, montrer qu'il existe un multiple de a qui s'écrit 111...11 (Utiliser le nombre 99...900...0 trouvé ci-dessus et le diviser de manière convenable).

Exercice 38 : Trouver les entiers n tels que n^4-1 soit multiple de 15.

Théorème de Wilson : Le nombre p est premier si et seulement si $(p-1)! \equiv -1 \pmod{p}$.

L'équation $x^2-1 \equiv 0 \pmod{p}$ n'admet que 2 solutions $\bar{1}$ et $\overline{p-1}$ dans $\mathbb{Z}/p\mathbb{Z}$. (cf. le paragraphe suivant en cas de doute). Donc les classes $\bar{2}$, $\bar{3}$,...,$\overline{p-2}$ de $\mathbb{Z}/p\mathbb{Z}$ sont groupées 2 par 2 dans le passage de $\bar{x}$ à $\bar{x}^{-1}$.

Par suite : $\bar{1}.\bar{2}. \ldots (\overline{p-1}) = ((\bar{2}.\bar{2}^{-1})(\bar{3}.\bar{3}^{-1})\ldots)(\overline{p-1}) = (\overline{p-1}) = -\bar{1}$

d'où le résultat. (Il existe un premier p pour lequel la relation de la ligne ci-dessus n'est pas légitime. Quel est ce nombre ?).

La réciproque est facile : si $1.2\ldots(p-1) \equiv -1 \pmod{p}$, tout nombre plus petit que p est premier avec p (car inversible dans $\mathbb{Z}/p\mathbb{Z}$, l'inverse de $\bar{a}$ étant $\overline{-1.2\ldots(a-1)(a+1)..(p-1)}$) donc p est premier.

3.- Solutions d'une congruence

De nombreux problèmes se traduisent par des équations du type $f(x,y,z) \equiv 0 \pmod{n}$, f étant souvent un polynôme à coefficients entiers. Nous donnons ici quelques exemples de telles équations.

a) L'équation $a^2-10b^2 = 2$ n'admet pas de solution (a,b).

Si a et b vérifient cette équation, on doit avoir $a^2 \equiv 2 \pmod{5}$ puisque $10 \equiv 0 \pmod{5}$. Les classes modulo 5 sont $\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}$ et leurs carrés sont $\bar{0},\bar{1},\bar{4},\bar{4},\bar{1}$: aucun de ces carrés n'est $\bar{2}$ d'où le résultat.

b) L'équation $a_0+a_1x+\ldots+a_nx^n \equiv 0 \pmod{p}$ (1) où p est premier et les x_i sont entiers (et $a_n \not\equiv 0 \pmod{p}$) a au plus n solutions modulo p.

On verra plus loin que c'est là un résultat général dans la théorie des polynômes sur un corps. On le démontre ici par récurrence sur n.

Si $n = 1$ c'est clair, $a_0+a_1x \equiv 0 \pmod{p}$ admet l'unique solution $\bar{x}=-\bar{a}_0\bar{a}_1^{-1}$ ($a_1 \not\equiv 0 \pmod{p}$ donc $\bar{a}_1$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$).

Supposons le théorème vrai pour $(n-1)$ et considérons l'équation (1). Si elle n'a pas de solution, c'est gagné. Sinon, soit u une solution de (1) :

$$a_0+a_1u+\ldots+a_nu_n \equiv 0 \pmod{p}. \quad (2)$$

L'équation (1) est donc équivalente à :

$$a_0+a_1x+\ldots+a_nx^n-(a_0+a_1u+\ldots+a_nu^n) \equiv 0 \pmod{p}$$

ou encore à $$a_1(x-u)+a_2(x^2-u^2)+\ldots+a_n(x^n-u^n) \equiv 0 \pmod{p} \quad (3)$$

On vérifie facilement que :

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

On peut donc mettre $(x-u)$ en facteur dans l'équation (3) et on arrive à :

$$(x-u)(a_1+b_1x+\ldots+b_kx^k+\ldots+b_{n-1}x^{n-1}) \equiv 0 \pmod{p} \quad (4)$$

(on a regroupé les puissances de x de même exposant), avec des b_i entiers (qui dépendent de u).

Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, le produit de 2 éléments ne peut être nul que si l'un des deux est nul. Donc on a comme solution de (4) : $x-u \equiv 0 \pmod p$ (et on retrouve que $x = u$ est solution) ou bien $a_1+b_1x+..+b_{n-1}x^{n-1} \equiv 0 \pmod p$ qui par hypothèse de récurrence a au plus $n-1$ solutions.

c) Le théorème chinois

Théorème 4 : *Soient m et n deux entiers premiers entre eux et a et b deux entiers quelconques. Il existe un entier x tel que :*

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

Soient u et v tels que $um+vn = 1$ (Bezout)

Donc $vn \equiv 1 \pmod m$ et $um \equiv 0 \pmod m$

$vn \equiv 0 \pmod n$ et $um \equiv 1 \pmod n$.

On a donc :

$avn \equiv a \pmod m$ et $bum \equiv 0 \pmod m$

$avn \equiv 0 \pmod n$ $bum \equiv b \pmod n$.

En ajoutant ces relations on arrive ainsi à :

$avn+bum \equiv a \pmod m$

$avn+bum \equiv b \pmod n$,

c'est le résultat cherché avec $x = avn+bum$.

Remarque : Soient x et y deux solutions de ce système.

Par différence :

$x-y \equiv 0 \pmod m$

$x-y \equiv 0 \pmod n$.

Donc m et n divisent $x-y$ et comme $PGCD(m,n) = 1$, $mn \mid (x-y)$. On en déduit aisément que si x est une solution du système, les autres solutions sont les nombres $x+kmn$ où k parcourt $\mathbb{Z}$.

Généralisation : Si $m_1,\ldots,m_k$ sont des entiers deux à deux premiers entre eux, si $a_1,\ldots,a_n$ sont des entiers quelconques, il existe x tel que

$$x \equiv a_i \pmod{m_i} \quad \forall i = 1,2,\ldots,n.$$

On remarque que m_i est premier avec $m_1m_2\ldots m_{i-1}m_{i+1}\ldots m_n$.
En appliquant le résultat précédent, il existe y_i tel que :

$$y_i \equiv 1 \pmod{m_i}$$
$$y_i \equiv 0 \pmod{m_1\ldots m_{i-1}m_{i+1}\ldots m_n}$$

Ceci pour tout $i = 1,\ldots,n$.
On vérifie alors facilement que $x = a_1y_1+a_2y_2+\ldots+a_ny_n$ convient.

Exemple : Si un train circule tous les 4 jours entre deux villes à partir du 2 janvier et si un autre train circule tous les 7 jours à partir du 3 janvier, quels sont les jours où les trains circulent simultanément ? En numérotant 1,2,3,...,365 (366) les jours de l'année on est en fait conduit à résoudre :

$$x \equiv 2 \pmod 4$$
$$x \equiv 3 \pmod 7$$

En suivant la méthode du théorème (à partir de $2.4-7 = 1$) on trouve $x = 10,\ 10+28,\ 10+56,\ldots$

Remarque : Si m et n ne sont pas premiers entre eux, l'existence ou non de solutions dépend de a et b.

Par exemple : $\begin{cases} x \equiv 3 \pmod 6 \\ x \equiv 2 \pmod 4 \end{cases}$

n'a pas de solutions alors que

$$\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 2 \pmod 4 \end{cases}$$

a des solutions.

Exercice 39 : Montrer que pour tout entier naturel n, on peut trouver n entiers consécutifs tous divisibles par un cube (autre que ± 1).

On cherche $m+1, m+2, \ldots, m+n$ et des nombres $a_1, \ldots, a_n$ tels que $a_1^3 | m+1$, $a_2^3 | m+2, \ldots$

Ou encore
$$m \equiv -1 \pmod{a_1^3}$$
$$m \equiv -2 \pmod{a_2^3}$$
$$\vdots$$
$$m \equiv -n \pmod{a_n^3}.$$

On est donc dans la situation du théorème choinois généralisé. Il suffit de prendre les a_i^3 premiers entre eux deux à deux. Par exemple $a_1 = 2$, $a_2 = 3$, $a_3 = 5, \ldots$ c'est-à-dire la suite des nombres premiers.

d) Un cas du (grand) théorème de Fermat

Le grand théorème de Fermat affirme que si n est supérieur ou égal à 3, on ne peut pas trouver d'entiers x,y,z tels que $x^n+y^n = z^n$. Ce théorème, non démontré à ce jour malgrè de très nombreux travaux (et quelques avancées récentes très importantes) a été résolu pour certaines valeurs de n. Nous indiquons seulement :

L'équation $x^3+y^3 = z^3$ n'admet pas de solution (x,y,z) où x, y et z sont des entiers non multiples de 3.

Supposons en effet $x^3+y^3 = z^3$ (1)

On en déduit : $x^3+y^3 \equiv z^3 \pmod 9$ (2)

et aussi : $x^3+y^3 \equiv z^3 \pmod 3$ (3)

Par le petit théorème de Fermat, la relation (3) implique

$$x+y \equiv z \pmod 3$$

donc $z = x+y+3u$. En reportant cette valeur dans l'équation (1) on trouve :

$$x^3+y^3 \equiv (x+y+3u)^3 \pmod 9$$

soit
$$x^3+y^3 \equiv x^3+y^3+3x^2y+3xy^2 \pmod 9 \qquad (4)$$

(les autres termes sont multiples de 9).

La relation (4) donne :

$$3x^2y+3xy^2 \equiv 0 \pmod 9$$

ou encore
$$x^2y+xy^2 \equiv 0 \pmod 3$$

c'est-à-dire
$$xy(x+y) \equiv 0 \pmod 3.$$

Comme $x+y \equiv z \pmod 3$, la dernière relation s'écrit : $xyz \equiv 0 \pmod 3$ donc $3|x$ ou $3|y$ ou $3|z$. C'est ce qu'il fallait démontrer.

e) Caractères de divisibilité

Soit n un nombre entier. Ecrit en base 10 on a

$$n = a_q 10^q + a_{q-1} 10^{q-1} + \ldots + a_1 10 + a_0$$ (où les a_i sont des chiffres c'est-à-dire $0 \leq a_i \leq 9$).

On a $10 \equiv 1 \pmod 9$ donc $10^r \equiv 1 \pmod 9$. La classe de n modulo 10 est donc $\bar{a}_q + \bar{a}_{q-1} + \ldots + a_0 = \overline{a_q + a_{q-1} + \ldots + a_0}$. Ainsi un nombre est multiple 9 si et seulement si la somme de ses chiffres est multiple de 9.

On a un résultat analogue avec 3.

Exercice 40 : Quelle est la signification de la preuve par 9 d'une multiplication ?

Exercice 41 : En remarquant que $10 \equiv -1 \pmod{11}$, indiquer un caractère de divisibilité par 11. Comment reconnaître qu'un nombre est multiple de 99 ?

On a des caractères de divisibilité par 2,5,4 que le lecteur connaît. On peut assez facilement énoncer des caractères de divisibilité par : 99 ou 101 (en utilisant $100 \equiv 1 \pmod{99}$ ou $100 \equiv -1 \pmod{101}$).

Par rapport à un nombre tel que 7, le caractère de divisibilité n'est pas très commode mais on peut l'établir comme suit (les congruences sont calculées modulo 7).

On a $10 \equiv 3$, $10^2 \equiv 2$, $10^3 \equiv 6$, $10^4 \equiv 4$, $10^5 \equiv 5$, $10^6 \equiv 1$

et on retrouve la suite 3,2,... à partir de 10^7.

Donc $a_q 10^q + \ldots + a_1 . 10 + a_0$ est multiple de 7 si et seulement si

$$a_0 + 3a_1 + 2a_2 + 6a_3 + 4a_4 + 5a_5 + a_6 + 3a_7 + 2a_8 + 6a_9 + \ldots$$

est multiple de 7.

IV - VERS UNE GÉNÉRALISATION

Il est d'un grand intérêt d'étudier les nombres complexes qui annulent des polynômes de la forme $x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a$ où $a_0,a_1,\ldots,a_{n-1}$ sont des nombres entiers.

Avant de considérer le cas où $n = 2$, citons d'abord la :

Proposition 26 : Soit u vérifiant : $u^n+a_{n-1}u^{n-1}+\ldots+a\,u+a_0 = 0$ où $a_{n-1},\ldots,a_0$ sont des entiers. Si $u \in \mathbb{Q}$, alors $u \in \mathbb{Z}$.

En effet supposons $u = \frac{r}{s}$ où $\frac{r}{s}$ est une fonction irréductible et portons cette valeur dans l'équation :

$$\left(\frac{r}{s}\right)^n+a_{n-1}\left(\frac{r}{s}\right)^{n-1}+\ldots+a_1\frac{r}{s}+a_0 = 0.$$

En multipliant par s^n on trouve :

$$r^n+a_{n-1}r^{n-1}s+\ldots+a_1rs^{n-1}+a_0s^n = 0.$$

Comme $s \mid a_{n-1}r^{n-1}s+\ldots+a_0s^n$, s divise aussi r^n.

Comme $PGCD(r,s) = 1$ (puisque la fraction $\frac{r}{s}$ est supposée irréductible) on a donc $s = 1$ donc $u \in \mathbb{Z}$.

Dans les cas les plus simples on est conduit à étudier des ensembles de la forme $\mathbb{Z}(\sqrt{d}) = \{a+b\sqrt{d},\ a,b \in \mathbb{Z}\}$ où d est un nombre entier que l'on suppose "sans facteurs carrés" c'est-à-dire que la décomposition de d en facteurs premiers est $d = p_1p_2\ldots p_k$ avec des p_i distincts deux à deux. On voit facilement que $\mathbb{Z}(\sqrt{d})$ est un anneau. On peut donc y définir une notion de multiple. Par exemple dans $\mathbb{Z}(\sqrt{6})$, $-24+14\sqrt{6}$ est multiple de $2+3\sqrt{6}$ car $(2+3\sqrt{6})(6-2\sqrt{6}) = -24+14\sqrt{6}$.

La notion de multiple ou de diviseur débouche sur une notion de nombre premier : un nombre est premier s'il n'a que des diviseurs "élémentaires". Précisons ce que l'on entend par là : dans $\mathbb{Z}$, 3 admet comme diviseurs : $+3,-3,+1,-1$. Ce sont les diviseurs élémentaires de 3.

Le nombre de diviseurs élémentaires d'un entier est donc très réduit.

Il n'en est pas toujours de même dans les anneaux quadratiques, c'est-à-dire les anneaux $\mathbb{Z}(\sqrt{d})$. Par exemple dans $\mathbb{Z}(\sqrt{2})$, on a $(\sqrt{2}-1)(\sqrt{2}+1) = 1$. On peut donc diviser tout élément de $\mathbb{Z}(\sqrt{2})$ par $(\sqrt{2}+1)$, puisque cela revient à multiplier par $(\sqrt{2}-1)$:

$$(3+5\sqrt{2})/(\sqrt{2}+1) = (3+5\sqrt{2})(\sqrt{2}-1)$$

$(\sqrt{2}+1)$ divise tous les éléments de $\mathbb{Z}(\sqrt{2})$. Mais on a aussi $(\sqrt{2}-1)^n(\sqrt{2}+1)^n = 1$ donc, pour la même raison que ci-dessus $(\sqrt{2}+1)^n$ divise tous les éléments de $\mathbb{Z}(\sqrt{2})$. Comme $(\sqrt{2}+1) > 1$, la suite $(\sqrt{2}+1)^n$ est une suite strictement croissante, ses termes forment une infinité de diviseurs élémentaires de n'importe quel élément de $\mathbb{Z}(\sqrt{2})$. Ainsi $(a+b\sqrt{2})$ est multiple de $(1+\sqrt{2})^n$.

Il l'est aussi de $(a+b\sqrt{2})$, de $-(a+b\sqrt{2})$.

Plus généralement : Si $x \in \mathbb{Z}(\sqrt{2})$, x est multiple de $\pm(\sqrt{2}+1)^n$, de $\pm(\sqrt{2}-1)^n$, de $\pm(\sqrt{2}+1)^n x$, de $\pm(\sqrt{2}-1)^n x$ pour $n \in \mathbb{N}$. On sait montrer qu'il n'y a pas d'autres diviseurs élémentaires de x.

La situation générale est la suivante : si $u \in \mathbb{Z}(\sqrt{d})$, on dit que u est une unité s'il existe $u' \in \mathbb{Z}(\sqrt{d})$ tel que $uu' = 1$. (c'est-à-dire si u est inversible dans $\mathbb{Z}(\sqrt{d})$). Il est alors clair que tout x de $\mathbb{Z}(\sqrt{d})$ est divisible par u quelle que soit l'unité u ainsi que par ux. Ce sont ces nombres u et ux qui sont les diviseurs élémentaires de x.

On dira alors que x est premier s'il n'admet que des diviseurs élémentaires.

Remarquons enfin que si $a+b\sqrt{d}$ est une unité de $\mathbb{Z}(\sqrt{d})$, son inverse est $+(a-b\sqrt{d})$ ou $-(a-b\sqrt{d})$:

Soit $a'+b'\sqrt{d}$ l'inverse de $a+b\sqrt{d}$. On a donc

$$(a+b\sqrt{d})(a'+b'\sqrt{d}) = 1 \qquad (1)$$

ou encore, en effectuant :

$$\begin{cases} aa'+bb'd = 1 \\ ab'+ba' = 0 \end{cases} \qquad (2)$$

Si maintenant nous multiplions $(a-b\sqrt{d})$ par $(a'-b'\sqrt{d})$ on trouve :

$$(a-b\sqrt{d})(a'-b'\sqrt{d}) = aa'+bb'd-(ab'+ba')\sqrt{d}$$

et compte tenu du système (2) :

$$(a-b\sqrt{d})(a'-b'\sqrt{d}) = 1 \qquad (3)$$

Multiplions alors (1) par (3) en remarquant que $(a+b\sqrt{d})(a-b\sqrt{d}) = a^2-db^2$:

$$(a^2-db^2)(a'^2-db'^2) = 1.$$

Mais c'est le produit de 2 nombres entiers donc $a^2-db^2 = \pm 1$ c'est-à-dire que $(a+b\sqrt{d})(a-b\sqrt{d}) = \pm 1$. Ainsi $a-b\sqrt{d}$ est, au sign e près, l'inverse de $a+b\sqrt{d}$.

Regardons maintenant sur 2 exemples en quoi des anneaux quadratiques peuvent ressembler ou non à $\mathbb{Z}$.

Exercice 42 : On a utilisé (ou ?) $a+b\sqrt{d} = 0 \Rightarrow a = 0$ et $b = 0$. Justifier cette implication.

$\mathbb{Z}(\sqrt{10})$

Montrons que $2, 3, 2+\sqrt{10}, -2+\sqrt{10}$ sont des éléments premiers de $\mathbb{Z}(\sqrt{10})$.

Supposons par exemple que :

$$2+\sqrt{10} = (a+b\sqrt{10})(a'+b'\sqrt{10}).$$

On tire facilement de ceci par une méthode que l'on vient de développer que :

$$2-\sqrt{10} = (a-b\sqrt{10})(a'-b'\sqrt{10})$$

et en multipliant membre à membre ces égalités :

$$-6 = (2+\sqrt{10})(2-\sqrt{10}) = (a^2-10b^2)(a'^2-10b'^2)$$

On doit donc avoir

$$a^2-10b^2 = \pm 6 \quad (\text{donc} \quad a'^2-10b'^2 = \pm 1)$$

$$a^2-10b^2 = \pm 2 \quad (\text{donc} \quad a'^2-10b'^2 = \pm 3)$$

$$a^2-10b^2 = \pm 3 \quad (\text{donc} \quad a'^2-10b'^2 = \pm 2)$$

$$a^2-10b^2 = \pm 1 \quad (\text{donc} \quad a'^2-10b'^2 = \pm 6).$$

Les 1^{er} et $4^{ème}$ cas sont interchangeables, de même le $2^{ème}$ et le $3^{ème}$. Or si $a^2-10b^2 = \pm 1$, c'est que $a+b\sqrt{10}$ est une unité, on a mis en évidence un diviseur élémentaire de $2+\sqrt{10}$ c'est sans intérêt pour montrer que $2+\sqrt{10}$ est premier.

Et $a^2-10b^2 = \pm 2$ est impossible (cf. le paragraphe III 3,a)

Donc $2+\sqrt{10}$ est premier (ce n'est pas une unité, sinon son inverse serait $\pm(2-\sqrt{10})$ et $(2+\sqrt{10})(2-\sqrt{10}) = -6$.

On a de même que 2,3 sont premiers (la démonstration, analogue, est laissée au lecteur).

Or : $6 = 2.3 = (2+\sqrt{10})(-2+\sqrt{10})$: on a là deux décompositions en facteurs premiers de 6 et elles sont distinctes : il faut s'assurer que $2+\sqrt{10}$ n'est pas de la forme $2.u$ ou $3u$ (u étant une unité) mais c'est élémentaire (pourquoi ?).

Le théorème fondamental de l'arithmétique n'est pas vrai dans $\mathbb{Z}(\sqrt{10})$.

Exercice 43 : En utilisant $6 = 2.3 = (1+i\sqrt{5})(1-i\sqrt{5})$ où $i = \sqrt{-1}$, montrer que le théorème fondamental est faux dans $\mathbb{Z}(\sqrt{-5}) = \mathbb{Z}(i\sqrt{5})$.

$\mathbb{Z}(i)$

C'est l'ensemble des entiers de Gauss c'est-à-dire de tous les nombres de la forme $a+bi$ avec $a,b \in \mathbb{Z}$ et i racine de $x^2+1 = 0$ (le lecteur peu familier avec les nombres complexes peut remettre à un peu plus tard la lecture de ce paragraphe).

On a, en utilisant un résultat vu ci-dessus, que $a+bi$ est une unité si $(a+bi)(a-bi) = \pm 1$ donc si $a^2+b^2 = \pm 1$. Comme $a,b \in \mathbb{Z}$, ceci n'est possible que si $a = \pm 1$ et $b = 0$ ou $a = 0$, $b = \pm 1$. Les unités de $\mathbb{Z}(i)$ sont $1,-1,i,-i$.

Dans $\mathbb{Z}(i)$ le théorème fondamental de l'arithmétique est vrai. On a en fait une division euclidienne.

Proposition 27 : *Si* a *et* b *sont deux entiers de Gauss et* $b \neq 0$, *il existe deux entiers de Gauss* q *et* r *tels que* $a = bq+r$ *et* $|r| < |b|$. ($|r|$ *est le module de* r, *ie si* $r = u+ir$, $|r| = \sqrt{u^2+r^2}$).

Considérons $\frac{a}{b}$. C'est un nombre complexe. On peut l'écrire $\alpha+i\beta$ et il est facile de voir que $\alpha,\beta \in \mathbb{Q}$. Il existe donc deux entiers m et n tels que $|\alpha-m| \leq \frac{1}{2}$ et $|\beta-n| \leq \frac{1}{2}$ (pourquoi ?).

Alors :

$$\begin{aligned} \left|\frac{a}{b} -(m+in)\right|^2 &= |(\alpha+i\beta)-(m+in)|^2 \\ &= |(\alpha-m)+i(\beta-n)|^2 \\ &= (\alpha-m)^2+(\beta-n)^2 \\ &\leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1. \end{aligned}$$

Si on pose $q = m+in$ et $r = a-bq$ on trouve donc le résultat cherché puisque $|a-bq| < |b|$.

De ceci on tire le théorème fondamental de l'arithmétique en suivant le même processus que dans $\mathbb{Z}$ (la proposition 1 du chapitre I a pour conséquence la proposition 4 du paragraphe II.2 dont découle toute la suite. On notera que l'unicité de q et de r n'est pas exigée dans la proposition 27 mais qu'elle n'avait pas servi dans $\mathbb{Z}$ pour arriver au théorème fondamental.

EXERCICES COMPLEMENTAIRES

1) Soit q un entier supérieur ou égal à 2.

a) Soit n un entier naturel. Montrer qu'il existe un entier naturel k tel que $q^k \leq n < q^{k+1}$ puis qu'il existe un entier a_k, $0 \leq a_k \leq q-1$, tel que $a_k q^k \leq n < a_{k+1} q^{k+1}$. Donner une majoration de $n-a_k q^k$.

b) Montrer par récurrence que tout entier naturel n peut s'écrire $n = a_k q^k + a_{k-1} q^{k-1} + \ldots + a_1 q + a_0$ $(0 \leq a_i \leq q-1)$. Montrer que cette décomposition est unique : c'est la décomposition de n en base q. Les a_i sont les chiffres de n en base q.

c) Soit $\varphi(n)$ le nombre de chiffres en base 2. Soient deux entiers a et b $(b \neq 0)$. Montrer qu'il existe $q \in \mathbb{N}$ et un entier $r \in \mathbb{Z}$ tels que $a = bq+r$ et $\varphi(r) < \varphi(b)$. (Montrer d'abord que si $0 \leq u < b$, on a soit $\varphi(u) < \varphi(b)$ soit $\varphi(b-u) < \varphi(b)$). Déterminer q et r pour $a = 24$ et $b = 5$ et pour $a = 23$, $b = 5$ (le couple (q,r) n'est pas unique).

d) Montrer que le nombre de chiffres de n en base q est $[\log_q n]+1$ où $\log_q$ est le logarithme dans la base q et $[x]$ est la partie entière de x. Soit $A = 4444^{4444}$. Soit $S(x)$ la somme des chiffres de n en base 10. On pose $S(A) = B$, $S(B) = C$, $S(C) = D$. Calculer D (considérer la classe de A modulo 9).

e) On écrit, à la suite l'un de l'autre, tous les nombres entiers (en base 10) : 12345678910111213 ... Combien de chiffres a-t-on écrit quand on arrive à 636 (inclus). Quel est le 10000 chiffre de la liste ? Combien de fois a-t-on écrit le chiffre 5 quand on arrive à 646 ? et le chiffre 0 ?

2) a) Si $(a,b) = 1$, $\mathrm{PGCD}(a+b,a-b) = 1$ ou 2.

b) Si $\mathrm{PGCD}(a,b) = 1$, $\mathrm{PGCD}(a^2-ab+b^2,a+b) \mid 3$.

c) Si $PGCD(a,b) = PGCD(x,b) = PGCD(a,y) = 1$, $PGCD(ax+by,ab) = 1$.

d) Si a,b,c sont premiers entre eux deux à deux la condition nécessaire et suffisante pour que $bcx+acy+abz$ soit premier avec abc et que x,y,z soient respectivement premiers à a,b,c.

3) a) Si p premier est la différence entre les carrés de deux nombres, ces nombres ne peuvent être que $\frac{p-1}{2}$ et $\frac{p+1}{2}$.

b) Soit p un entier naturel impair. On calcule $a_1 = p+1^2$, $a_2 = p+2^2$, $a_3 = p+3^2$,... $a_{\frac{p-1}{2}} = p+\left(\frac{p-1}{2}\right)^2$. Si le premier des a_k qui est un carré est $a_{\frac{p-1}{2}}$, c'est que p est premier.

c) Un nombre premier ne peut être la somme de plusieurs nombres impairs consécutifs.

d) Vérifier que $x^4+4y^4 = (x^2-2xy+2y^2)(x^2+2xy+2y^2)$.

En déduire que : p premier et $p = x^4+4y^4$ (pour un couple d'entiers x et y) n'est possible que si $p = 5$.

4) On définit les entiers a_n et b_n par :

$$(1+\sqrt{2})^n = a_n+b_n\sqrt{2}.$$

Montrer que a_n et b_n sont premiers entre eux (on pourra s'intéresser si $(1-\sqrt{2})^n$).

5) Soit $F_n = 2^{2^n}+1$. Montrer que F_n divise $F_{n+k}-2$ (revoir l'exercice 14, § II.1). En déduire que $PGCD(F_n,F_m) = 1$ si $m \neq n$.

Exercices : Indications et résultats

Exercice 1 : Considérer $(a^2+(a-1)^2)^2-(2a-1)^2$.

Exercice 5 : Remarquer que l'ensemble des parties de E est la réunion des ensembles de parties à k éléments $(0 \leq k \leq n)$.

Exercice 6 : Pour k impair on utilise $C_n^k = C_n^{n-k}$.

Pour k pair utiliser $C_n^k = C_{n-1}^k+C_{n-1}^{k-1}$.

Exercice 7 : Pour une permutation u, considérer les x tels que $u(x) = x$. Si k est le nombre de ces éléments, u apparaît comme une permutation d'un ensemble de k objets.

Exercice 9 : Si $a = rs$ on a soit $r \leq \sqrt{a}$, soit $s \leq \sqrt{a}$.

Exercice 10 : $10! = 2^8 3^4 5^2 7$.

Exercice 12 : 4, 13, 11.

Exercice 13 : Voir l'exercice 9.

Exercice 14 : $a^k-1 = (a-1)(a^{k-1}+a^{k-2}+\ldots+1)$ donc $a-1 \mid a^k-1$.
Si $k = rs$, $a^k-1 = a^{rs}-1 = (a^r)^s-1$ et $(a^r-1) \mid a^{rs}-1$.
On raisonne de manière analogue pour a^k+1 en utilisant la formule $x^k+1 = (x+1)(x^{k-1} \ldots +1)$.

Exercice 15 : $n!+2, n!+3, n!+4, \ldots, n!+n$ sont tous composés.

Exercice 17 : On trouve les nombres pairs non multiples de 3 $(2n+18 = 2(n+3)+12)$.

Exercice 20 : Si un nombre à 4 diviseurs, il est de la forme $p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ avec $(a_1+1)(a_2+1) \ldots (a_r+1) = 4$ donc ou bien $r = 1$ et $a_1 = 3$, ou bien $r = 2$ et $a_1 = a_2 = 1$. Donc on trouve p^3 ou pq. En donnant à p et q les plus petites valeurs possibles on trouve que 6 est le plus petit nombre avec 4 diviseurs.

Exercice 22 : 6, 28,...

Exercice 25 : Ecrire que $x \mid x+y-1$ donc que $x \mid y-1$ et de même $y \mid x-1$.

Exercice 28 : p et $8p^2+1$ ne sont simultanément premiers que si $p = 3$ (à cause de ce qui précède) et $8.3^2-1 = 71$ est premier.

Exercices 34,35,36 : Ce sont des applications du théorème de Fermat. Pour 36 par exemple : $a^7-a \equiv 0 \pmod 7$ et $a^2-1 \equiv 0 \pmod 3$ donc $a^6-1 \equiv 0 \pmod 3$ et $a^7-a \equiv 0 \pmod 3$. De même $a^7-a \equiv 0 \pmod 2$. Donc a^7-a est multiple de 7,3,2 donc de 42. Le nombre $a^{13}-a$ est toujours multiple de 2730.

PARTIE 2 : NOMBRES COMPLEXES

1.- Construction du corps des nombres complexes

On se propose de construire un corps $\mathbb{C}$ commutatif, contenant $\mathbb{R}$ et dans lequel -1 est un carré. Il existe donc dans $\mathbb{C}$ un élément i tel que $i^2 = -1$. Comme $\mathbb{C}$ contient x et y pour tout $x,y \in \mathbb{R}$, $\mathbb{C}$ doit contenir iy et $x+iy$. Si $z = x+iy$ et $z' = x'+iy'$ sont deux éléments de cette forme, les règles de calcul dans un corps donnent :

$$z+z' = x+x'+i(y+y')$$
$$zz' = (x+iy)(x'+iy') = xx'+iyx'+ixy'+i^2yy'$$
$$= xx'-yy'+i(xy'+yx').$$

Ainsi zz' et $z+z'$ ont aussi la forme $X+iY$ avec X et Y réels. Si nous assimilons le nombre $x+iy$ au couple (x,y) nous sommes conduits au résultat suivant :

Théorème 1 : *Sur l'ensemble $\mathbb{R}^2$ on définit une addition et une multiplication par les formules :*

$$(x,y)+(x',y') = (x+x',y+y')$$
$$(x,y).(x',y') = (xx'-yy',xy'+yx').$$

Ces 2 lois font de $\mathbb{R}^2$ un corps commutatif appelé corps des nombres complexes et noté $\mathbb{C}$. La partie de $\mathbb{C}$ formée par les éléments de la forme $(x,0)$ est un sous-corps qui est isomorphe à $\mathbb{R}$. Le carré de l'élément $(0,1)$ est $(-1,0)$.

La vérification des axiomes de corps est élémentaire. Tout d'abord l'addition définie dans le théorème n'est autre que l'addition de l'espace vectoriel $\mathbb{R}^2$, c'est donc une loi de groupe dont l'élément neutre est $(0,0)$. Nous nous limitons à vérifier l'associativité de la multiplication et à déterminer l'inverse d'un élément.

$$(x,y)((x',y')(x'',y'')) = (x,y)(x'x''-y'y'',x'y''+y'x'')$$

$$= (xx'x''-xy'y''-yx'y''-yy'x'',xx'y''+xy'x''+yx'x''-yy'y'')$$

$$= (xx'x''-yy'x''-xy'y''-yx'y'',xx'y''-yy'y''+xy'x''+yx'x'')$$

$$= (xx'-yy',xy'+yx')(x'',y'')$$

$$= ((x,y)(x',y'))(x'',y'').$$

Soit $z = (x,y)$ un élément non nul. Si $t' = (x',y')$ est l'inverse de z on a $tz' = (1,0)$ donc $xx'=yy' = 1$ et $xy'+x'y = 0$. C'est un système de 2 équations linéaires à 2 inconnues dont la solution est :

$$x' = \frac{x}{x^2+y^2}\ ,\ y' = -\frac{y}{x^2+y^2}\ .\ \text{(Comme } (x,y) \neq (0,0),\ x^2+y^2 \neq 0).$$

Les autres assertions du théorème sont de vérifications immédiates.

Conséquences, notations

- On note i le nombre complexe $(0,1)$.
- Le nombre complexe $(x,0)$ est identifié au réel x.
- La loi de multiplication sur $\mathbb{C}$ donne : $(0,1)(y,0) = (0,y)$. Compte tenu de ce qui précède $(0,y)$ est iy.
- Le nombre (x,y) est égal à $(x,0)+(0,y)$ donc est noté $x+iy$.

Ainsi : Tout nombre complexe z s'écrit, de manière unique, sous la forme $x+iy$ où x et y sont réels. C'est la représentation cartésienne (ou algébrique) de z. On dit que x est la partie réelle de z et y sa partie imaginaire et on note $x = \mathrm{Re}\ z$, $y = \mathrm{Im}\ z$.

On retrouve donc les résultats énoncés de manière heuristique au début de ce paragraphe.

Définition : On appelle conjugué du nombre complexe $z = x+iy$ le nombre noté $\bar{z}$ égal à $x-iy$. On appelle module de z et on note $|z|$ le nombre réel $\sqrt{x^2+y^2} = \sqrt{z\bar{z}}$.

On vérifie facilement que :

$$\overline{z'+z''} = \bar{z}'+\bar{z}''$$

$$\overline{z'z''} = \bar{z}'\bar{z}''$$

$|zz'| = |z|\,|z'|$ (résulte de $|z| = \sqrt{z\bar{z}}$).

Et aussi que :

$$\text{Re } z = \frac{1}{2}(z+\bar{z})$$

$$\text{Im } z = \frac{1}{2i}(z-\bar{z}) = \frac{i}{2}(\bar{z}-z)$$

(comme $i^2 = -1$ on a $\frac{1}{i} = -i$).

On a exprimé ci-dessus les parties réelles et imaginaires de l'inverse z^{-1} d'un nombre complexe z. Avec ces notations on a :

$$\frac{1}{z} = \frac{\bar{z}}{|z|^2} .$$

Exercice 1 : Ecrire sous forme cartésienne les nombres complexes $(1-i)^4$,

$$(3+2i)^2,\ \frac{1+2i}{1-i},\ \frac{1-i}{10+2i},\ \frac{i+\sqrt{5}}{(1-i)^2},\ (3+i)^4+(3-i)^4,\ \frac{1+\sqrt{2}+i(1-\sqrt{2})}{1+i\sqrt{2}} .$$

Exercice 2 : Calculer $1+j+j^2$ où $j = \frac{-1+i\sqrt{3}}{2}$. a,b,c désignant trois nombres réels, calculer $(a+b+c)(a+bj+cj^2)(a+bj^2+cj)$.

Exercice 3 : Quels sont les nombres complexes z tels que z et z^{-1} aient le même module ? Quels sont les nombres z tels que z, z^{-1} et $z-1$ aient le même module ?

Exercice 4 : Déterminer les nombres complexes z tels que $3z^2+2|z|^2-1 = 0$.

Exercice 5 : Si a et b sont deux entiers relatifs et n un entier naturel, montrer qu'il existe deux entiers relatifs c et d tels que $(a^2+b^2)^n = c^2+d^2$.

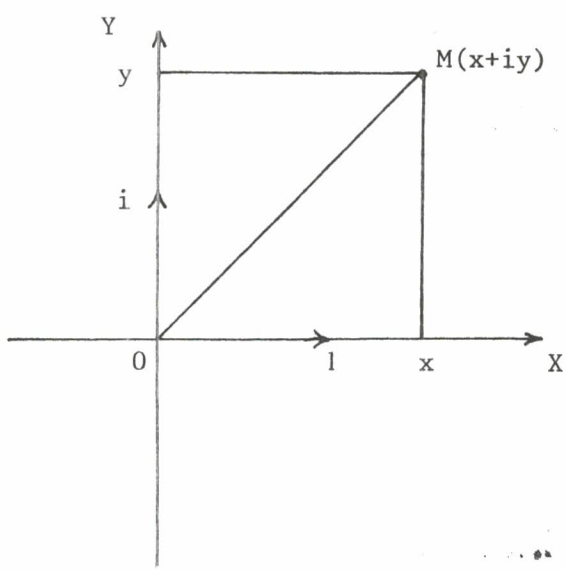
La structure de corps de l'ensemble des nombres complexes permet d'y calculer comme on le fait dans $\mathbb{R}$ et par exemple de résoudre des systèmes d'équations linéaires par les méthodes usuelles :

Exercice 6 : Résoudre dans $\mathbb{C}$: $\begin{cases} ix-3y = 2-3i \\ (1+i)x+2iy = 5-i \end{cases}$

$\begin{cases} (2+i)x+7y = 1+2i \\ (1-i)\bar{x}-i\bar{y} = 4-i \end{cases}$

2.- Représentation géométrique des nombres complexes

Les nombres complexes ont été construits en munissant le groupe additif sous-jacent à l'espace vectoriel $\mathbb{R}^2$ d'une structure multiplicative. Un nombre complexe $z = x+iy$ peut ainsi être assimilé au vecteur de composantes (x,y) dans l'espace $\mathbb{R}^2$.



Cette assimilation se fait en considérant $\mathbb{R}^2$ muni de sa structure auclidienne et d'une base orthonormée portée par les axes OX et OY. Si le point M de coordonnée (x,y) est associé au complexe $z = x+iy$, on dit que M est l'image de z et que z est l'affixe de M. Le premier vecteur de la base orthonormée est associé à 1 et le second à i.

Comme conséquences immédiates de cette représentation signalons :

- Si M est l'image de z et M' l'image de z' l'image de z+z' est N tel que $\overrightarrow{ON} = \overrightarrow{OM}+\overrightarrow{OM'}$.
- Le module de z n'est autre que la longueur du segment OM. L'inégalité du triangle donne :

Proposition 1 : $|z+z'| \leq |z|+|z'|$.

Par ailleurs, si z est différent de 0 et si r est son module on a $z = rz'$ où z' est de module 1 donc est l'affixe d'un point du cercle trigonométrique. Par suite il existe θ tel que $z = r(\cos\theta + i\sin\theta)$. On appelle <u>argument</u> de z l'ensemble des nombres $\theta+2k\pi$ ($k \in \mathbb{Z}$) et on note $\arg z = \theta \pmod{2\pi}$. L'un de ces nombres est dans l'intervalle $[0,2\pi[$. C'est la <u>détermination principale</u> de l'argument et on le note $\operatorname{Arg} z$.

Par exemple :

- Si z est réel positif, $\operatorname{Arg} z = 0$,
- Si z est réel négatif, $\operatorname{Arg} z = \pi$,
- Si z est imaginaire pur (c'est-à-dire de la forme ia avec $a \in \mathbb{R}$), $\operatorname{Arg} z = \frac{\pi}{2}$ si $a > 0$ et $\operatorname{Arg} z = \frac{3\pi}{2}$ si $a < 0$.

Tout nombre complexe s'écrit $z = r(\cos\theta + i\sin\theta)$ avec $|z| = r$ et $\arg z = \theta \pmod{2\pi}$. Cette écriture est la <u>représentation trigonométrique</u> du nombre complexe z. Elle est parfaitement définie par z (si ce n'est que θ est déterminé modulo 2π).

On a vu que $\operatorname{Re}(z+z') = \operatorname{Re} z + \operatorname{Re} z'$ et $\operatorname{Im}(z+z') = \operatorname{Im} z + \operatorname{Im} z'$. Par contre $\operatorname{Re}(zz')$ et $\operatorname{Im}(zz')$ sont de formes assez compliquées. Le produit de z par z' se décrit mieux par la représentation trigonométrique:

<u>Proposition 2</u> : $|zz'| = |z|\,|z'|$.
$\arg(zz') = \arg z + \arg z' \ (\text{modulo } 2\pi)$.

Le premier point a déjà été vu. Pour le second soient $z = r(\cos\theta + i\sin\theta)$ et $z' = r'(\cos\theta' + i\sin\theta')$ ($r = |z|$, $z' = |z'|$, $\theta = \arg z$, $\theta' = \arg z'$). Effectuons zz' :

$$\begin{aligned} zz' &= rr'(\cos\theta + i\sin\theta)(\cos\theta' + i\sin\theta') \\ &= rr'[(\cos\theta\cos\theta' - \sin\theta\sin\theta') + i(\cos\theta\sin\theta' + \\ &\qquad\qquad \sin\theta\cos\theta')] \\ &= rr'(\cos(\theta+\theta') + i\sin(\theta+\theta')). \end{aligned}$$

On a donc bien $\arg(z+z') = \theta+\theta'$ (et on retrouve $|zz'| = rr'$).

Il est d'usage de noter $e^{i\theta}$ (et de lire "exponentielle $i\theta$") le nombre complexe $\cos\theta + i\sin\theta$. Le lecteur verra plus tard une justification

analytique de cette notation. La proposition ci-dessus nous donne une justification formelle car le résultat : arg zz' = arg z + arg z' se traduit par $e^{i\theta}e^{i\theta'} = e^{i(\theta+\theta')}$ qui est la formule espérée pour la fonction exponentielle. La représentation trigonométrique d'un nombre complexe est donc de la forme $re^{i\theta}$. Les nombres complexes de module 1 sont les nombres $e^{i\theta}$. Par exemple : $e^{i\frac{\pi}{2}} = i$, $e^{i\pi} = -1$, $e^{3i\frac{\pi}{2}} = -i$, $e^{2i\pi} = e^0 = 1$.

Le conjugué de $re^{i\theta}$ est $re^{-i\theta}$. En utilisant les formules : $\mathrm{Re}\ z = \frac{1}{2}(z+\bar{z})$, $\mathrm{Im}\ z = \frac{i}{2}(\bar{z}-z)$ pour $z = e^{i\theta} = \cos\theta + i\sin\theta$ on arrive à :

Proposition 3 :

$$\sin\theta = \frac{e^{i\theta}-e^{-i\theta}}{2i} \quad et \quad \cos\theta = \frac{e^{i\theta}+e^{-i\theta}}{2} \quad (Formules\ d'Euler)$$

(En l'abscence d'une définition analytique pour e^z quand z est complexe, ces formules ne traduisent qu'un changement de notation).

Remarque : Dans les calculs les formules d'Euler interviendront souvent dans la situation suivante : soit $z = e^{i\theta}+1$. On a donc

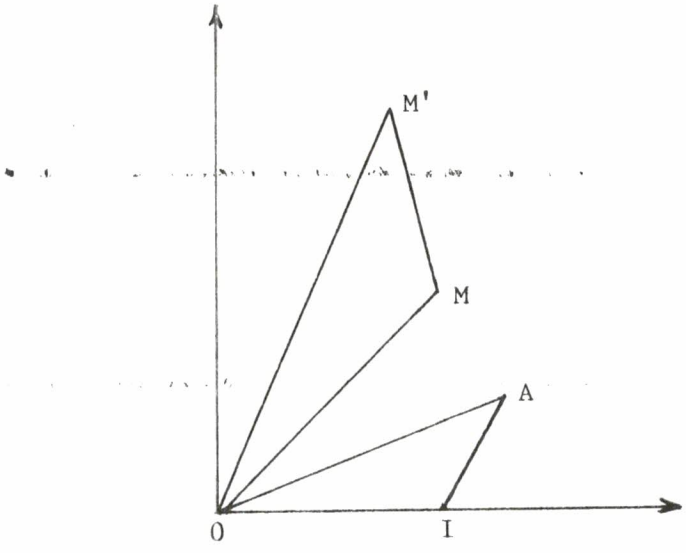
$$z = e^{i\frac{\theta}{2}}\left(e^{i\frac{\theta}{2}}+e^{-i\frac{\theta}{2}}\right) = 2e^{i\frac{\theta}{2}}\cos\frac{\theta}{2}.$$

Interprétation géométrique des opérations dans $\mathbb{C}$

Soient a un nombre complexe d'image A, z un nombre complexe d'image M.

Addition : le nombre complexe z+a a pour image M' tel que $\vec{OM'} = \vec{OM}+\vec{OA}$, c'est-à-dire que M' est l'image de M par la translation de vecteur OA.

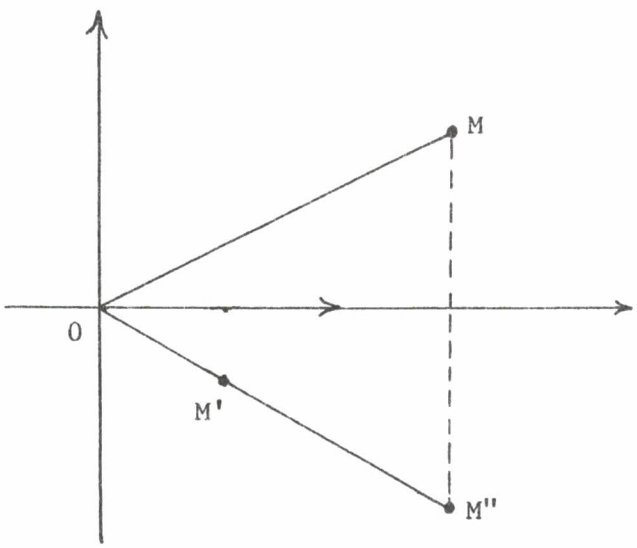
Sur la figure ci-contre le nombre z' d'image M' est le produit de z d'image M par a d'image A.



Multiplication : Soit I l'image de 1. Si M' est l'image de az, on a Arg z' = Arg a + Arg z (mod 2π). Donc $(\vec{OM},\vec{OM'})$ = Arg a. D'autre part $|z'| = |a|\,|z|$ donc $\frac{OM'}{OM} = |a| = \frac{OA}{OI}$. Les deux triangles OIA et OMM' sont donc semblables : le point M' est l'image de M par la similitude de rapport $|a|$ et d'angle Arg a.

Conjugaison : Il est clair que l'image de $\bar{z}$ est déduite de celle de z par la symétrie orthogonale d'axe OX.

Passage à l'inverse : Soit M l'image de z.
On désigne par M'' l'image de $\bar{z}$ et par M' l'image de z^{-1}. On a $z = re^{i\theta}$, $\bar{z} = re^{-i\theta}$ et $z^{-1} = \frac{1}{r}e^{-i\theta}$. Donc O,M',M'' sont alignés et OM'.OM'' = 1. Ainsi M' se déduit de M par $\mathcal{S}\circ J$ où $\mathcal{S}$ est la symétrie orthogonale d'axe OX et J est l'inversion de centre O de rapport 1.



Exercice 7 : Soient z et z' deux complexes de module 1. Montrer que $\frac{z+z'}{1+zz'}$ est réel.

Trouver les nombres complexes z tels que z^2 et z^6 soient conjugués.

Ecrire sous forme cartésienne le nombre complexe $(1+i)^{28}$.

Dans un autre module de ce cours seront étudiées de manière plus complète les liaisons entre la géométrie euclidienne plane et les nombres complexes. Nous indiquons ici, à titre d'exemples, quelques résultats dans ce sens.

Soient A, B, C trois points du plan et a, b, b leurs affixes. Le triangle ABC est équilatéral si et seulement si $\vec{BA}$ est l'image de $\vec{BC}$ par une rotation d'angle $\frac{\pi}{3}$ (ou $-\frac{\pi}{3}$). Une rotation d'angle $\frac{\pi}{3}$ correspond à la multiplication par le nombre complexe $e^{i\frac{\pi}{3}}$. Donc ABC est équilatéral si et seulement si $(a-b) = e^{i\frac{\pi}{3}}(c-b)$ (ou $(a-b) = e^{-i\frac{\pi}{3}}(c-b)$). En remarquant que $1-e^{i\frac{\pi}{3}} = -e^{\frac{2i\pi}{3}}$ on arrive à :

Le triangle ABC est équilatéral si et seulement si $j = e^{\frac{2i\pi}{3}}$ où j^2 est solution de l'équation $a+bz+cz^2 = 0$ (où j est le nombre $e^{\frac{2i\pi}{3}}$).

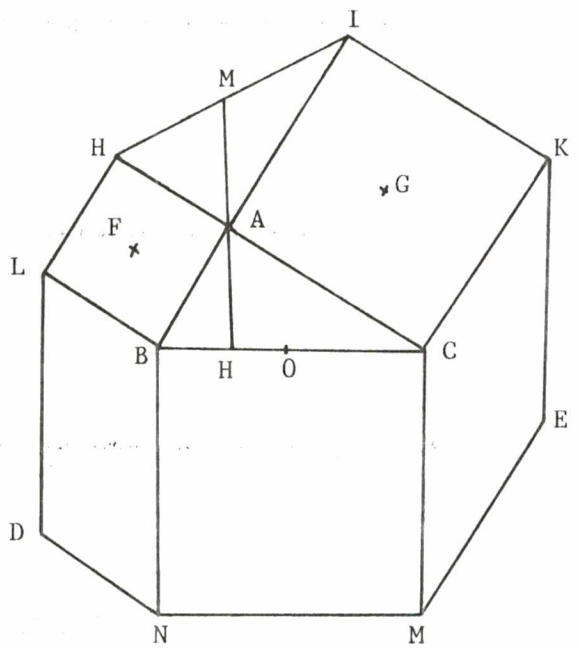
Exercice 8 : Avec les mêmes notations, montrer que ABC est équilatéral si et seulement si $a^2+b^2+c^2 = ab+bc+ca$ (on pourra montrer d'abord que l'on peut supposer $a = 0$).

ABC est équilatéral si et seulement si $\frac{1}{a-b} + \frac{1}{b-c} + \frac{1}{c-a} = 0$.

Exercice 9 : On construit 3 carrés sur les côtés d'un triangle et on complète la figure par 2 parallélogrammes (voir ci-contre).
Montrer que ADE est un triangle isocèle-rectangle.

F et G désignant les centres de 2 carrés et O le milieu de BC, montrer que FOG est isocèle-rectangle.

Montrer que la hauteur AH de ABC est alignée avec la médiane AM de AHI.



Exercice 10 : Montrer que si $|z| = 1$ on a $|1+z| \geq 1$ ou $|1+z^2| \geq 1$ (déterminer la partie A du cercle unité telle que $z \in A \Leftrightarrow |1+z| < 1$ et montrer que si $z \in A$, $z^2 \notin A$).

Montrer que si $z \in \mathbb{C}$ on a $|1+z| \geq \frac{1}{2}$ ou $|1+z^2| \geq 1$.

Exercice 11 : Montrer que 3 points du plan sont alignés si et seulement si leurs affixes vérifient :

$$z_1\bar{z}_2+z_2\bar{z}_3+z_3\bar{z}_1 = \bar{z}_1z_2+\bar{z}_2z_3+\bar{z}_3z_1.$$

3.- Formule de De Moivre. Applications trigonométriques

La formule donnée dans la proposition s'étend bien entendu au produit de n nombres complexes :

$$\arg(z_1 z_2 \ldots z_n) = \arg z_1 + \ldots + \arg z_n \pmod{2\pi}$$

qui entraîne :

$$\prod_{k=1}^{n} (\cos\theta_k + i \sin\theta_k) = \cos\theta + i \sin, \text{ où } \theta = \sum_{k=1}^{n} \theta_k .$$

Un cas important de cette formule est celui où les arguments θ_k sont égaux entre eux :

$$\boxed{(\cos\theta + i \sin\theta)^n = \cos n\theta + i \sin n\theta} \quad \text{(Formule de De Moivre)}$$

Applications

1) Rappelons la formule du binôme : $(X+Y)^n = \sum_{k=0}^{n} C_n^k X^k Y^{n-k}$ (voir le paragraphe 1.3 de la 3ème partie de ce cours).

En faisant $X = \cos\theta$ et $Y = i \sin\theta$ dans cette formule et en utilisant :

$$\begin{aligned} i^k &= 1 \quad \text{si} \quad k \equiv 0 \pmod 4 \\ &= i \quad \text{si} \quad k \equiv 1 \pmod 4 \\ &= -1 \quad \text{si} \quad k \equiv 2 \pmod 4 \\ &= -i \quad \text{si} \quad k \equiv 3 \pmod 4, \end{aligned}$$

on trouve :

$$(\cos\theta + i \sin\theta)^n = (\cos^n\theta - C_n^2 \cos^{n-2}\theta \sin^2\theta + C_n^4 \cos^{n-4}\theta \sin^4\theta \ldots)$$

$$+ i(C_n^1 \cos^{n-1}\theta \sin\theta - C_n^3 \cos^{n-3}\theta \sin^3\theta + \ldots)$$

(les derniers termes de chaque parenthèse s'écrivent quand on connait la classe de n modulo 4. Par exemple si $n \equiv 1 \pmod 4$, les expressions du second membre se terminent respectivement par $C_n^{n-1} \cos\theta \sin^{n-1}\theta$ et $\sin^n\theta$).

La formule de De Moivre donne ainsi :

$$\cos n\theta = \cos^n\theta - C_n^2 \cos^{n-2}\theta \sin^2\theta + C_n^4 \cos^{n-4}\theta \sin^4\theta + \ldots$$

$$\sin n\theta = C_n^1 \cos^{n-1}\theta \sin\theta - C_n^3 \cos^{n-3}\theta \sin^3\theta + \ldots$$

On remarquera que dans l'expression de $\cos^n\theta$ apparaissent des puissances de $\cos\theta$ et des puissances <u>paires</u> de $\sin\theta$.

En utilisant $\sin^2\theta = 1-\cos^2\theta$ on voit que $\cos n\theta = P(\cos\theta)$ où P est un polynôme de degré n à coefficients entiers. Quel résultat de même nature peut-on énoncer pour $\sin n\theta$?

<u>Exercice 12</u> : Calculer $\cos 5\theta$ en fonction de $\cos\theta$ et $\sin 5\theta$ en fonction de $\sin\theta$.

On a aussi, facilement :

$$\operatorname{tg} n\theta = \frac{\sin n\theta}{\cos n\theta} = \frac{C_n^1\cos^{n-1}\theta\sin\theta - C_n^3\cos^{n-3}\theta\,\sin^3\theta+\ldots}{\cos^n\theta - C_n^2\cos^{n-2}\theta\,\sin^2\theta+\ldots}$$

et en divisant numérateur et dénominateur par $\cos^n\theta$:

$$\operatorname{tg} n\theta = \frac{C_n^1\operatorname{tg}\theta - C_n^3\operatorname{tg}^3\theta+\ldots}{1-C_n^2\operatorname{tg}^2\theta-C_n^4\operatorname{tg}^2\theta+\ldots} \quad .$$

2) On peut aussi exprimer $\cos^n\theta$ et $\sin^n\theta$ à l'aide des nombres $\cos k\theta$ et $\sin k\theta$ (pour $0 \leq k \leq n$). Pour cela on utilise les formules d'Euler qui nous donnent :

$$2^n\cos^n\theta = (e^{i\theta}+e^{-i\theta})^n \quad \text{et} \quad 2^n i^n \sin^n\theta = (e^{i\theta}-e^{-i\theta})^n.$$

On développe les seconds membres de ces 2 relations en regroupant les termes équidistants des extrêmes :

$$2^n\cos^n\theta = (e^{ni\theta}+e^{-ni\theta})+C_n^1(e^{(n-2)i\theta}+e^{-(n-2)i\theta})$$

$$+C_n^2(e^{(n-4)i\theta}+e^{-(n-4)i\theta})+\ldots$$

ce qui donne finalement (en distinguant selon la parité de n) :

$$2^{2p-1}\cos^{2p}\theta = \cos 2p\theta + C_{2p}^1\cos(2p-2)\theta+\ldots+C_{2p}^{p-1}\cos 2\theta+\frac{1}{2}C_{2p}^p$$

$$2^{2p}\cos^{2p+1}\theta = \cos(2p+1)\theta+C_{2p+1}^1\cos(2p-1)\theta+\ldots+C_{2p+1}^p\cos\theta.$$

Exercice 13 : Calculer de même $\sin^n\theta$.

3) On sait que $1+q+\ldots+q^{n-1} = \frac{q^n-1}{q-1}$ (si $q \neq 1$).

En particulier, si $q = e^{i\theta}$ on a :

$$S = 1+e^{i\theta}+\ldots+e^{i(n-1)\theta} = \frac{e^{in\theta}-1}{e^{i\theta}-1} .$$

En factorisant $e^{\frac{in\theta}{2}}$ au numérateur et $e^{i\frac{\theta}{2}}$ au dénominateur du second membre, il vient :

$$S = e^{i(n-1)\frac{\theta}{2}} \frac{e^{in\frac{\theta}{2}} - e^{-in\frac{\theta}{2}}}{e^{i\frac{\theta}{2}} - e^{-i\frac{\theta}{2}}} = e^{i(n-1)\frac{\theta}{2}} \frac{\sin n\frac{\theta}{2}}{\sin\frac{\theta}{2}} .$$

En séparant parties réelles et imaginaires des deux membres de cette égalité, on arrive finalement à :

$$1+\cos\theta+\ldots+\cos(n-1)\theta = \frac{\sin n\frac{\theta}{2}}{\sin\frac{\theta}{2}} \cos(n-1)\frac{\theta}{2} ,$$

$$\sin\theta+\ldots+\sin(n-1)\theta = \frac{\sin n\frac{\theta}{2}}{\sin\frac{\theta}{2}} \sin(n-1)\frac{\theta}{2} .$$

Exercice 14 : Montrer que $\cos\frac{\pi}{11} + \cos\frac{3\pi}{11} + \cos\frac{5\pi}{11} + \cos\frac{7\pi}{11} + \cos\frac{9\pi}{11} = \frac{1}{2}$.

Calculer $\cos\theta+\cos 3\theta+\ldots+\cos(2n-1)\theta$.

Exercice 15 : Calculer $\sum_{k=o}^{n} C_n^k \cos k\theta$ et $\sum_{k=o}^{n} C_n^k \sin k\theta$.

Exercice 16 : Calculer $\sum_{k=1}^{n} \cos^k\theta \cos k\theta$ (on utilise, comme d'habitude, $\cos k\theta = \mathrm{Re}(e^{ik\theta})$ et aussi $e^{i\theta}\cos\theta-1 = e^{i\theta}(\cos\theta-e^{-i\theta}) = ie^{i\theta}\sin\theta$).

Calculer

$$\sum_{k=o}^{n} \frac{\cos kx}{\cos^k x} , \quad \sum_{k=o}^{n} \frac{\sin kx}{\cos^k x} , \quad \sum_{k=o}^{n} \frac{\cos kx}{\sin^k x} .$$

Exercice 17 : Montrer que $\Sigma\cos(\pm a_1 \pm a_2 \ldots \pm a_n) = 2^n \cos a_1 \ldots \cos a_n$ (la somme est étendue à toutes les combinaisons possibles de + et -). Calculer $\Sigma\sin(\pm a_1 \pm a_2 \ldots \pm a_n)$.

4.- L'équation du second degré dans $\mathbb{C}$

Racines carrées d'un nombre complexe

Soit a un nombre complexe non nul de module r et d'Argument α : $a = re^{i\alpha}$. On se propose de chercher $z \in \mathbb{C}$ tel que $z^2 = a$. Supposons $z = ue^{i\theta}$. On a donc $u^2e^{2i\theta} = re^{i\theta}$ soit $u^2 = r$ et $2\theta = \alpha \pmod{2\pi}$. On a donc $u = \sqrt{r}$ et $\theta = \frac{\alpha}{2}$ ou $\frac{\alpha}{2} + \pi$. L'équation $z^2 = a$ a donc deux solutions z_1 et z_2 où $z_2 = -z_1$.

Proposition 4 : Si a est un nombre complexe non nul, l'équation $z^2 = a$ a deux solutions z_1 et $-z_1$ avec $|z_1| = \sqrt{|a|}$ et $\text{Arg } z_1 = \frac{1}{2} \text{Arg } a$.

Ce résultat peut être retrouvé en utilisant la représentation cartésienne de a et z :

Soit $a = s+it$ et $z = x+iy$. La relation $z^2 = a$ est équivalente au système (I)

$$(I) \begin{cases} x^2-y^2 = s \\ 2xy = t. \end{cases}$$

Remarquons que si (x,y) est une solution de (I), $(-x,-y)$ est aussi solution.

Le système (I) est équivalent à (II)

$$(II) \begin{cases} x^2-y^2 = s \\ 4x^2y^2 = t^2 \\ \text{signe}(x).\text{signe } y = \text{signe}(t). \end{cases}$$

Donc x^2 et $-y^2$ sont solutions de $X^2-sX-\frac{t^2}{4}$ ce qui donne :

$$x^2 = \frac{1}{2}(s+\sqrt{s^2+t^2}) \quad \text{et} \quad -y^2 = \frac{1}{2}(s-\sqrt{s^2+t^2}).$$

(remarquer que $x^2 \geq 0$ et $-y^2 \leq 0$!).

On retrouve donc 2 solutions (x,y) et $(-x,-y)$.

Exercice 18 : Montrer que $z^2 = a$ admet une racine et une seule dans le domaine $\{z|\text{Re}z > 0\} \cup \{z|\text{Re}z = 0 \text{ et } \text{Im } z > 0\}$. Décrire d'autres domaines du plan complexe dans lesquels $z^2 = a$ possède une racine et une seule.

Si a est réel positif, ses racines carrées sont $\sqrt{a}$ et $-\sqrt{a}$. Si a est réel négatif, ses racines carrées sont $i\sqrt{-a}$ et $-i\sqrt{-a}$.

La notation $\sqrt{a}$ n'est utilisée que si a est réel positif. Il n'est pas possible d'étendre cette notation pour a complexe : il y a d'abord un problème d'unicité (quelle est celle des racines que l'on désignera par ce symbole ?) : il peut être réglé en prenant celle des racines se trouvant par exemple dans le domaine décrit dans l'exercice précédent. Mais il y a aussi un problème de relation fonctionnelle : $\sqrt{ab} = \sqrt{a}\sqrt{b}$ ne pourrait être toujours vraie (pourquoi ?). Cela rend le symbole $\sqrt{a}$ non seulement inopérant mais dangereux.

Exercice 19 : Calculer le module, l'argument, la partie réelle, la partie imaginaire des racines carrées de i, de $-i$ et des racines quatrièmes de i et $-i$.

Equation du second degré

L'équation $az^2+bz+c = 0$ $(a,b,c \in \mathbb{C},\ a \neq 0)$ se ramène à la forme :

$$a\left[\left(z+\frac{b}{2a}\right)^2 - \frac{b^2-4ac}{4a^2}\right] = 0$$

Donc z vérifie : $\left(z+\frac{b}{2a}\right)^2 = \frac{b^2-4ac}{4a^2}$.

Si l'on désigne par α le nombre b^2-4ac et par u et $-u$ les racines de α on arrive donc à :

$$z_1 = \frac{-b+u}{2a} \quad \text{et} \quad z_2 = \frac{-b-u}{2a}.$$

Ce sont les deux racines de $az^2+bz+c = 0$. Elles sont confondues si $u = 0$ c'est-à-dire si $b^2 = 4ac$.

Exercice 20 : Déterminer z tel que $az+b\bar{z}+c = 0$ $(a,b,c) \in \mathbb{C}$.

Exercice 21 : Déterminer z tel que $\frac{n+\frac{1}{2}+z}{n+\frac{1}{2}-\bar{z}}$ soit réel quel que soit l'entier rationnel n.

5.- Racines $n^{\text{ièmes}}$ d'un nombre complexe

Soit $z = re^{i\theta}$ un nombre complexe $(z \neq 0)$. Cherchons les nombres complexes u tels que $u^n = z$ où n désigne un entier supérieur ou égal à 1. Posons $u = \rho e^{i\alpha}$.

De $u^n = z$ on tire $\rho^n = r$ et $n\alpha = \theta \pmod{2\pi}$. Donc ρ est la racine $n^{\text{ième}}$ de r et α peut prendre n valeurs :

$$\frac{\theta}{n}\ ,\ \frac{\theta}{n} + \frac{2\pi}{n}\ ,\ \ldots,\ \frac{\theta}{n} + \frac{2(n-1)\pi}{n}$$

c'est-à-dire $\alpha = \frac{\theta}{n} + \frac{2k\pi}{n}$ $(0 \leq k \leq n-1)$.

Proposition 5 : *Si z est un nombre complexe non nul, il existe n nombres complexes u tels que $u^n = z$. Ces nombres sont les racines $n^{\text{ièmes}}$ de z.*

En particulier si $z = 1$ on obtient :

Proposition 6 : *Il existe n nombres complexes u tels que $u^n = 1$. Ce sont les nombres $e^{\frac{2ik\pi}{n}}$ $(0 \leq k \leq n-1)$.*

Exemples : Les racines $2^{\text{ièmes}}$ de 1 sont ± 1. Les racines 3^{e} de 1 sont 1, $e^{\frac{2i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ et $e^{-\frac{2i\pi}{3}}$; le premier de ces deux derniers nombres est usuellement noté j, le second est $j^2 = \bar{j}$. Les racines 4^{e} de 1 sont ± 1, $\pm i$.

Les racines $n^{\text{ièmes}}$ de 1 vérifient $z^n - 1 = 0$. On sait que $z^n - 1 = (z-1)(z^{n-1} + z^{n-2} + \ldots + z + 1)$. Les racines $n^{\text{ièmes}}$ de 1 autres que 1 vérifient donc $z^{n-1} + z^{n-2} + \ldots + z + 1 = 0$. De plus si $n = 2m$ est un nombre pair, on a $z^{2m} - 1 = (z^2-1)(z^{2m-2} + z^{2m-4} + \ldots + z^2 + 1)$; $z^2 - 1$ s'annule en ± 1, donc les racines $n^{\text{ièmes}}$ de 1 non réelles vérifient $z^{n-2} + z^{n-4} + \ldots + z^2 + 1 = 0$ lorsque n est pair.

Si u et v sont des racines $n^{\text{ièmes}}$ d'un nombre complexe z on a : $u^n = z$ et $v^n = z$ donc $(\frac{u}{v})^n = 1$. Ainsi $\frac{u}{v}$ est une racine $n^{\text{ième}}$ de 1, c'est-à-dire que $u = \rho v$ où ρ est une racine $n^{\text{ième}}$ de 1. Réciproquement si v est une racine $n^{\text{ième}}$ de z et ρ une racine $n^{\text{ième}}$ de 1, ρv est une racine $n^{\text{ième}}$ de z. Donc :

Proposition 7 : Si v est une racine $n^{ième}$ de z, l'ensemble des racines $n^{ièmes}$ de z est l'ensemble des ρv où ρ parcourt l'ensemble des racines $n^{ièmes}$ de 1.

Posons $\xi = e^{\frac{2i\pi}{n}}$. L'ensemble des racines $n^{ièmes}$ de 1 est l'ensemble $\xi, \xi^2, \xi^3, \ldots, \xi^n = 1$. Donc si v est une racine $n^{ième}$ de z, les racines $n^{ièmes}$ de z sont $\xi v, \xi^2 v, \ldots, \xi^n v$.

Si M_0 est l'image de v dans le plan complexe, les points $M_1, M_2, \ldots, M_{n-1}$ images des racines $n^{ièmes}$ de z sont déduits de M par des rotations d'angles $\frac{2\pi}{n}$, $\frac{4\pi}{n}$, ..., $\frac{2(n-1)\pi}{n}$ (qui sont les arguments des nombres ξ^k). Donc l'ensemble des racines $n^{ièmes}$ de z forme dans le plan complexe un polygone régulier à n côtés, inscrit dans le cercle de rayon ρ où $\rho = \sqrt[n]{|z|}$. En particulier les racines $n^{ièmes}$ de 1 forment les sommets du polygone régulier à n côtés, inscrit dans le cercle unité, l'un des sommets étant le point d'affixe 1.

Exercice 22 : Déterminer les nombres réels θ tels que $\prod_{k=1}^{n} (\cos k\theta + i \sin k\theta) = 1$.

Exercice 23 :

- A quels moments de la journée les 2 aiguilles d'une horloge sont-elles superposées ? opposées l'une à l'autre ? perpendiculaires l'une à l'autre ?

- A quels moments de la journée la permutation des 2 aiguilles d'une horloge donne une position possible pour ces aiguilles ?

Indication : Pour cet exercice on peut imaginer qu'un cercle de rayon unité a été tracé sur le cadran de l'horloge. La position de chaque aiguille est donc repérée par un point de ce cercle. Supposons que la position "midi" corresponde au point d'affixe 1 : si la position de la grande aiguille au temps t est z, celle de la petite aiguille est z^{12}. La superposition des 2 aiguilles sera donnée par $z = z^{12}$ ... .

Exercice 24 : Soient $M_0, M_1, \ldots, M_{n-1}$ les sommets d'un polygone régulier inscrit dans le cercle unité. Calculer le produit $M_0M_1 \times M_0M_2 \times \ldots \times M_0M_{n-1}$. (On peut supposer que M_0 est d'affixe 1. Si $z_1, z_2, \ldots, z_{n-1}$ sont les affixes de $M_1, M_2, \ldots, M_{n-1}$ on doit évaluer $\left| \prod_{i=1}^{n-1} (1-t_i) \right|$.

Vérifier que les nombres $(1-z_i)$ sont racines du polynôme $(1-z)^{n-1} + \ldots + (1-z) + 1$ et conclure).

Exercice 25 : Soit $n = 2m$ un entier pair. Les racines $n^{\text{ièmes}}$ de l'unité différentes de ± 1 sont donc $e^{\frac{2i\pi}{n}}, e^{\frac{4i\pi}{n}}, \ldots$. En remarquant que ces racines annulent le polynôme $x^{n-2}+x^{n-4}+\ldots+x^2+1 = P(x)$ et en les regroupant 2 à 2, montrer que $P(x) = \prod_{k=1}^{m-1} (x^2-2x\cos\frac{k\pi}{m}+1)$. En déduire que

$$\prod_{k=1}^{m-1} \sin\frac{k\pi}{m} = \frac{\sqrt{m}}{2^{m-1}} .$$

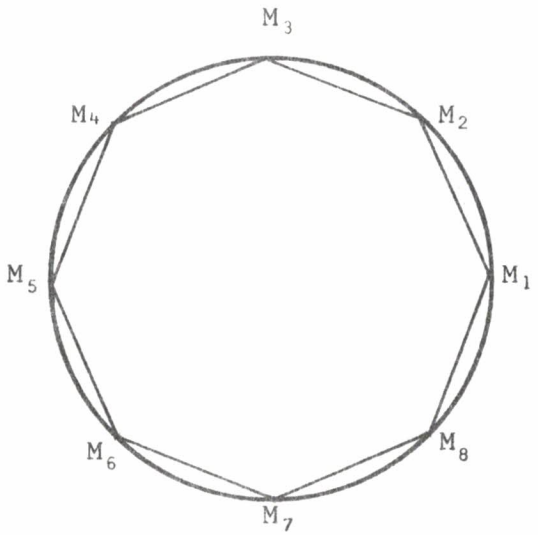
Remarques complémentaires sur les racines $n^{\text{ièmes}}$ de l'unité

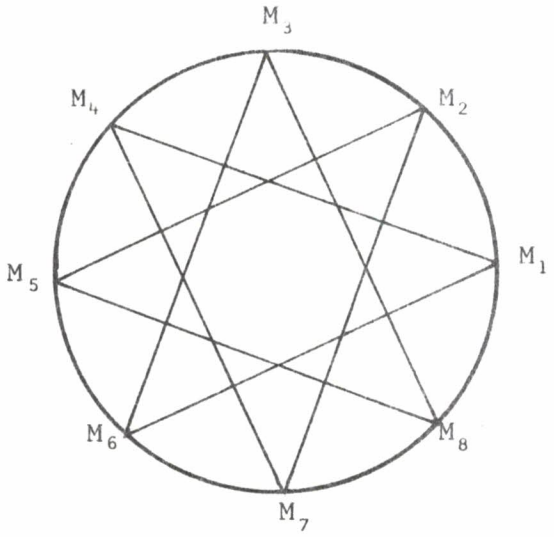
Soit U_n l'ensemble des racines $n^{\text{ièmes}}$ de l'unité. Il est clair que si u et $v \in U_n$, $uv \in U_n$ et $u^{-1} \in U_n$. Les racines $n^{\text{ièmes}}$ de 1 forment donc un sous-groupe à n éléments du groupe multiplicatif de $\mathbb{C}$. De plus si $\xi = e^{\frac{2i\pi}{n}}$, $U_n = \{\xi,\xi^2,\ldots,\xi^{n-1},\xi^n\}$: U_n est cyclique, engendré par ξ.

Soit $\alpha \in \mathbb{Z}/n\mathbb{Z}$. Désignons par k un élément de $\mathbb{Z}$ tel que la classe de k modulo n soit égale à α. Si à α on associe ξ^k il est aisé de vérifier que cela définit une application de $\mathbb{Z}/n\mathbb{Z}$ dans U_n et que cette application est un isomorphisme de groupes.

Soit $\zeta \in U_n$. Quelle est la condition sur ζ pour que $U_n = \{\zeta,\zeta^2,\ldots,\zeta^{n-1},\zeta^n\}$? On a $\zeta = \xi^k$ pour un certain k. Il est facile de voir (en utilisant si l'on veut la remarque précédente) que ζ répond à la question (c'est-à-dire que ζ "engendre" U_n) si et seulement si k et n sont premiers entre eux.

On a vu plus haut que les racines $n^{\text{ièmes}}$ de l'unité étaient les sommets d'un polygone régulier à n côtés. Plus précisément (en conservant $\xi = e^{\frac{2i\pi}{n}}$), les nombres $\xi,\xi^2,\ldots,\xi^{n-1},\xi^n$ sont les affixes des sommets consécutifs $M_1,M_2,\ldots,M_n = 1$ du polygone régulier convexe à n côtés. Si l'on choisit un générateur $\zeta = e^{\frac{2ik\pi}{n}}$, en prenant $\zeta,\zeta^2,\ldots,\zeta^n$ on obtient les sommets consécutifs d'un polygone étoilé régulier à n côtés. Par exemple au polygone $M_1M_2M_3\ldots M_8M_1$ on peut associer l'étoile à 8 branches $M_1M_4M_7M_2M_5M_8M_3M_6M_1$ en prenant comme générateur $\xi^3 = e^{6i\pi/8}$ (ou, aussi bien $\xi^5 = e^{10i\pi/8}$ qui donne la même étoile, parcourue dans l'autre sens).





Exercice 26 : Pour les valeurs de n comprises entre 3 et 20 combien y-a-t'il d'étoiles à n branches ?

Exercices. Résultats et indications

2) $1+j+j^2 = 0$. Le produit proposé est égal à $a^3+b^3+c^3$.

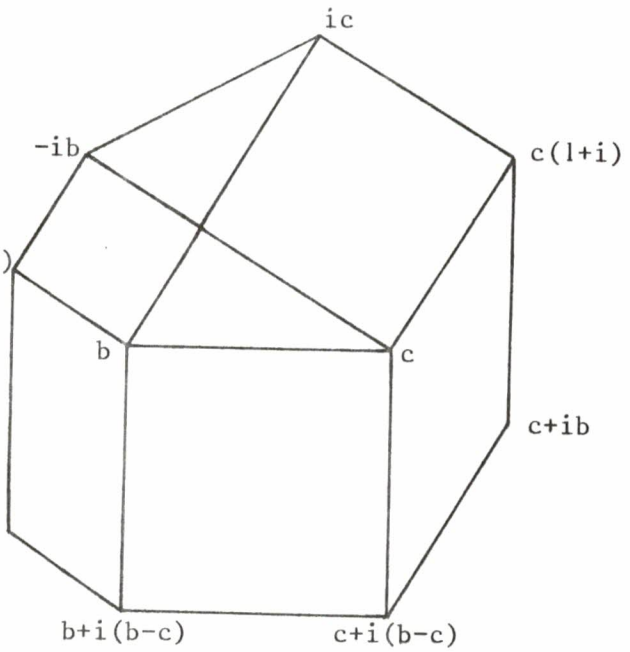
3) $|z| = |z^{-1}| \Leftrightarrow |z| = 1$.
$|z| = |z^{-1}| = |z-1| \Leftrightarrow z = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$

5) $a^2+b^2 = |a+bi|$ donc $(a^2+b^2)^n = |(a+bi)^n|$.

7) Utiliser : $z \in \mathbb{R} \Leftrightarrow z = \bar{z}$
Ecrire z sous forme trigonométrique.
Ecrire $1+i = \sqrt{2}\, e^{i\pi/4}$.

8) Si u est complexe, le triangle $A(a),B(b),C(c)$ est équilatéral si et seulement si $A'(a-u),B'(b-u),C'(c-u)$ l'est. De plus l'égalité $a^2+b^2+c^2 = ab+bc+ca$ est invariante par la transformation $z \to z-u$. En faisant $u = a$ on peut donc supposer $a = 0$ et on utilise le résultat qui précède.

9) Les affixes des différents points de la figure sont indiqués ci-contre. (On a supposé que A est d'affixe 0). Pour montrer que ADE est isocèle rectangle, il suffit de remarquer que AE est l'image de AD par une rotation d'angle $\frac{\pi}{2}$ donc que $c+ib = i\,(b-ic)$.



10) A est l'arc du cercle unité contenant -1 et limité par $-\frac{1}{2}+i\frac{\sqrt{3}}{2}$ et $-\frac{1}{2}-i\frac{\sqrt{3}}{2}$.

11) Ajouter $z_2\bar{z}_2$ aux deux membres de la relation et montrer que celle-ci n'est autre que : $(z_1-z_2)(\bar{z}_3-\bar{z}_2) = (\bar{z}_1-\bar{z}_2)(z_3-z_2)$.

14) La somme proposée est $\mathrm{Re}\left(e^{\frac{i\pi}{11}} + e^{\frac{3i\pi}{11}} + \ldots + e^{\frac{9i\pi}{11}}\right) = \mathrm{Re}\left(e^{\frac{i}{11}}\right)\left(1+e^{\frac{2i\pi}{11}} + e^{\frac{4i\pi}{11}} + \ldots + e^{\frac{8i\pi}{11}}\right)$ qui se calcule facilement.

15) $\sum_{k=0}^{n} C_n^k \cos k\theta = \mathrm{Re}\left(\sum_{k=0}^{n} C_n^k e^{ik\theta}\right) = \mathrm{Re}(1+e^{i\theta})^n = \cos n\frac{\theta}{2}\cos^n\frac{\theta}{2}$.

16) $\sum_{k=1}^{n} \cos^k\theta \cos k\theta = \mathrm{Re}\sum_{k=1}^{n}(\cos\theta\, e^{i\theta})^k$. C'est à nouveau la somme d'une progression géométrique. On trouve par exemple $\Sigma\cos^k\theta\cos k\theta = \frac{\cos^{n+1}\theta \sin n\theta}{\sin\theta}$.

17) Pour la somme des cosinus on fait une récurrence sur n (en la considérant comme partie réelle d'une somme d'exponentielle). La somme des sinus est nulle : à chaque terme de la forme sin u correspond un terme sin(-u).

18) Les nombres z tels que Arg z = 0 ont une racine carrée et une seule dans $\mathbb{R}^+$. Ceux tels que $0 < \mathrm{Arg}\ z < \pi$ (resp. $\pi < \mathrm{Arg}\ z < 2\pi$) ont une racine et une seule dans $0 < \mathrm{Arg}\ z < \frac{\pi}{2}$ (resp. $\frac{3\pi}{2} < \mathrm{Arg}\ z < 2\pi$).

Enfin si $\mathrm{Arg}\ z = \pi$, z a une racine carrée (et une seule) d'argument $\frac{\pi}{2}$.

Des domaines possèdant la même propriété sont obtenus en prenant un demi-plan ouvert quelconque dont le bord contient 0 auxquel on adjoint une des demi-droites d'origine 0 constituant le bord.

22) $\prod_{k=1}^{n} (\cos k\theta + i \sin k\theta) = e^{i\theta \sum_{k=1}^{n} k} = e^{i\frac{n(n+1)}{2}\theta}$.

23) La permutation des aiguilles donne une position possible si $z^{143} = 1$ (c'est-à-dire $z^{144} = z$).

24) Comme $z^n - 1 = (z-1)(z^{n-1}+\ldots+1)$, les nombres $z_1,\ldots,z_{n-1}$ sont racines de $z^{n-1}+\ldots+z+1 = 0$ donc les nombres $(1-z_i)$ sont racines de $(1-z)^{n-1}+\ldots+(1-z)+1 = 0$. Le produit des racines de ce polynôme est égal au terme constant soit n. Donc $M_0M_1\times\ldots\times M_0M_{n-1} = n$.

PARTIE 3 : POLYNÔMES, FONCTIONS POLYNOMIALES

Dans toute cette partie, K désigne un corps commutatif. Le lecteur peut supposer que $K = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

I - INTRODUCTION

1.- Fonctions polynomiales sur $\mathbb{R}$

Si $a_0, a_1, \ldots, a_n$ sont des nombres réels, la fonction de $\mathbb{R}$ dans $\mathbb{R}$ qui à x associe $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \sum_{k=o}^{n} a_k x^k$ est une fonction polynomiale. On dit qu'elle est de degré n si $a_n \neq 0$. Les nombres $a_0, a_1, \ldots, a_n$ sont les coefficients de cette fonction. Le terme $a_r x^r$ est un monôme.

On sait ajouter et multiplier entre elles de telles fonctions :

Soient $f(x) = a_n x^n + \ldots + a_0$

$g(x) = b_r x^r + \ldots + b_0$

et supposons $n \geq r$.

Les fonctions $f+g$ et fg sont définies par :

$$(f+g)(x) = f(x) + g(x)$$

et

$$fg(x) = f(x)g(x).$$

Ce qui donne :

$$(f+g)(x) = a_n x^n + \ldots + a_{r+1} x^{r+1} + (a_r + b_r) x^r + \ldots + (a_1 + b_1) x + (a_0 + b_0).$$

Remarquons que l'on peut supposer $g(x) = b_n x^n + \ldots + b_0$ (en posant $b_n = b_{n-1} = \ldots = b_{r+1} = 0$) ce qui permet d'écrire

$$(f+g)(x) = \sum_{k=o}^{n} (a_r + b_r) x^r.$$

La valeur en x du produit fg est définie par :

$$fg(x) = \left(\sum_{k=o}^{n} a_k x^k\right)\left(\sum_{=o}^{r} b_\ell x^\ell\right)$$

Pour calculer ce produit on doit multiplier entre eux tous les monômes $a_k x^k$ avec tous les monômes $b_\ell x^\ell$ ce qui donne des monômes $a_k x^k b_\ell x^\ell = a_k b_\ell x^{k+\ell}$. On regroupe ensuite les termes de cette forme pour lesquels $k+\ell$ est le même et on trouve :

$$fg(x) = \sum_{s=o}^{n+r} c_s x^s \quad \text{avec} \quad c_s = \sum_{k+\ell=s} a_k b_\ell x^s,$$

la notation $\sum_{k+\ell=s}$ signifiant que l'on fait la somme de toutes les quantités correspondant à k et ℓ vérifiant $k+\ell = s$. On peut aussi écrire $c_s = \sum_k a_k b_{s-k}$ (puisque $\ell = s-k$), la somme étant étendue à tous les indices k pour lesquels elle a un sens : il faut $0 \leq k \leq n$, $0 \leq s-k \leq r$.

On remarque que la somme et le produit de f et g sont déterminés par les coefficients de f et g.

D'autre part la fonction f détermine ses coefficients : c'est-à-dire que si $f(x) = a_n x^n + \ldots + a_1 x + a_0$ et $f(x) = b_r x^r + \ldots + b_1 x + b_0$, on a $n = r$ et $a_0 = b_0$, $a_1 = b_1, \ldots, a_n = b_n$. Si l'on suppose par exemple $r < n$ on a : $\lim_{x\to\infty} \frac{f(x)}{x^n} = a_n$ et $\lim_{x\to\infty} \frac{f(x)}{x^n} = 0$ selon que l'on prend l'une ou l'autre des écritures de f et cela n'est pas possible (si l'on a supposé $a_n \neq 0$). Il faut donc $r = n$ et $b_n = a_n$. On étudie ensuite le comportement à l'infini de $f(x) - a_n x^n$ pour montrer que $a_{n-1} = b_{n-1}$ ... . (Cela signifie que les fonctions $x \to x^n$ forment une famille libre dans l'espace vectoriel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$).

2.- Fonctions polynomiales et polynômes

Il y a donc correspondance biunivoque entre les fonctions polynomiales réelles et leurs coefficients. Cela cesse d'être vrai sur des corps autres que $\mathbb{R}$. Par exemple sur $\mathbb{Z}/p\mathbb{Z}$ on peut définir des fonctions polynomiales par des formules du type : $x \to a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ ($a_i \in \mathbb{Z}/p\mathbb{Z}$). On a vu plus haut que pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, $x^p = x$. Donc les deux fonctions polynomiales de $\mathbb{Z}/p\mathbb{Z}$ définies par x^p et x respectivement sont égales.

Pour des raisons diverses on souhaite distinguer dans certaines situations les expressions x^p et x. On est donc conduit à définie :

- D'une part les fonctions polynomiales à coefficients dans un corps K.
- D'autre part des expressions formelles nommées polynômes : un polynôme est une suite $(a_0,a_1,\ldots,a_n)$ de coefficients qui sont éléments d'un corps K. Somme et produit de deux polynômes sont définis à l'aide des coefficients par des formules analogues à celles que l'on a données ci-dessus pour les fonctions polynomiales. On note usuellement le polynôme $(0,1)$ par X et il est aisé de voir que tout polynôme peut s'écrire $a_0+a_1X+\ldots+a_nX^n$: on retrouve la notation usuelle mais ici X n'est pas une "variable" mais un polynôme particulier. On dit que X est une "indéterminée".

On remarquera que tout polynôme $P = a_0+a_1X+\ldots+a_nX$ définit sans ambiguïté une fonction polynomiale $\widetilde{P}$ définie par la formule :

$$x \to a_0+a_1x+\ldots+a_nx^n = \widetilde{P}(x).$$

(Bien entendu une telle fonction peut être définie par plusieurs polynômes si le corps est par exemple $\mathbb{Z}/p\mathbb{Z}$).

Si P est un polynôme à coefficients dans K, si $a \in K$ l'élément $\widetilde{P}(a)$ du corps K est appelé <u>valeur prise par le polynôme P au point a</u>. On n'hésitera pas à noter cette valeur par $P(a)$.

Dans ce qui suit un grand nombre de résultats sont énoncés pour des polynômes à coefficients dans K : ils sont bien entendu vrais pour de tels polynômes. Mais comme nous n'avons pas défini les polynômes, le lecteur peut se limiter aux polynômes à coefficients dans $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ (ou en général dans tout corps contenant $\mathbb{Q}$) et considérer que "polynôme" est un abus de langage pour "fonctions polynomiales".

<u>Exercice 1</u> : Montrer que toute fonction polynomiale à coefficients dans $\mathbb{C}$ ou $\mathbb{Q}$ définit parfaitement ses coefficients.

<u>Remarque</u> : Une autre façon d'exprimer qu'une fonction polynomiale définit ses coefficients est de remarquer :

- D'abord que l'ensemble des fonctions polynomiales est un espace vectoriel sur le corps de définition.
- Et ensuite que les fonctions $1,x,x^2,\ldots$ sont une base de cet espace vectoriel.

Cette remarque est valable d'ailleurs pour un corps quelconque K à condition de remplacer "fonction polynomiale" par "polynôme".

Proposition 1 : Si K est un corps commutatif l'ensemble des polynômes à coefficients dans K est un anneau commutatif unitaire noté $K[X]$.

(Dans tout ce qui suit nous distinguerons, de manière un peu naïve les polynômes en les désignant par $a_0+a_1X+\ldots+a_nX^n$ des fonctions polynomiales désignées par $a_0+a_1x+\ldots+a_nx^n$). La démonstration de la proposition est simple et fastidieuse si l'on raisonne en terme de polynômes. Si on se limite aux fonctions polynomiales sur $\mathbb{R}$ par exemple elle est par contre à peu près évidente. Ainsi l'associativité de la multiplication n'est autre que la formule :

$$\forall x,\ (PQ)R(x) = PQ(x)R(x) = P(x)Q(x)R(x)$$

$$= P(x)(QR)(x) = P(QR)(x),$$

qui utilise la définition du produit de 2 fonctions et l'associativité de la multiplication dans $\mathbb{R}$.

Exercice 2 : La multiplication des polynômes étant définie à l'aide de leurs coefficients, montrer qu'elle est associative.
(Remarquer que le produit $(PQ)R$ des 3 polynômes $P(x) = \sum_{k=o}^{n} a_kX^k$, $Q(x) = \sum_{\ell=o}^{r} b_\ell X^\ell$, $R(x) = \sum_{m=o}^{s} c_mX^m$ a comme coefficient du terme de degré t la somme de tous les produits $(a_kb_\ell)c_m$ pour tous les triplets (k,ℓ,m) tels que $(k+\ell)+m = t$).

Les éléments inversibles dans l'anneau $K[X]$ sont les constantes non nulles.

Le degré d'un polynôme

On appelle degré du polynôme $a_nX^n+a_{n-1}X^{n-1}+\ldots+a_1X+a_0$ le plus grand des indices k tels que $a_k \neq 0$. On le note $d°(P)$.

On a clairement :

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

$d^\circ(P+Q) \leq \mathrm{Max}(d^\circ(P), d^\circ(Q))$.

Il y a égalité dans cette formule si $d^\circ(P) \neq d^\circ Q$.

(Mais $d^\circ((X^3+X)+(-X^3+2)) = 1$).

Les constantes non nulles, c'est-à-dire les polynômes $P(X) = a_0$, $a_0 \neq 0$, sont les polynômes de degré 0. On convient que le degré du polynôme 0 est $-\infty$. Ce qui permet à la formule $d^\circ(PQ) = d^\circ(P)+d^\circ(Q)$ d'être toujours vraie.

Exercice 3 : On appelle valuation du polynôme $a_nX^n+\ldots a_1X+a_0$ le plus petit des indices k tel que $a_k \neq 0$. On la note $\omega(P)$ (et on convient que $\omega(0) = +\infty$). Déterminer $\omega(PQ)$ et $\omega(P+Q)$.

Si $P(X) = a_nX^n+a_{n-1}X^{n-1}+\ldots+a_0$ est un polynôme de degré n (c'est-à-dire si a_n est non nul) on dit parfois que a_n est le coefficient dominant de P. Si $a_n = 1$, on dit que P est un polynôme unitaire. On a $P(X) = a_n\left(X^n+\frac{a_{n-1}}{a_n}X^{n-1}+\ldots+\frac{a_0}{a_1}\right)$, donc tout polynôme P est le produit d'un polynôme unitaire par une constante.

Exercice 4 : a) Combien y-a-t-il d'applications de $\mathbb{Z}/p\mathbb{Z}$ dans lui-même ?

b) Montrer que toute application polynomiale de $\mathbb{Z}/p\mathbb{Z}$ dans lui-même peut se mettre sous la forme $f(x) = a_{p-1}x^{p-1}+a_{p-2}x^{p-2}+\ldots+a_0$ $(a_i \in \mathbb{Z}/p\mathbb{Z})$.

c) Montrer que toute application de $\mathbb{Z}/p\mathbb{Z}$ dans lui-même est polynomiale.

3.- La formule du binôme

On se propose d'écrire le polynôme $P(X) = (1+X)^n$ sous la forme $a_0+a_1X+\ldots+a_nX^n$. Or $P(X)$ est le produit de n facteurs tous égaux à $(1+X)$. Le terme général du produit est obtenu en prenant un terme dans le 1^{er} facteur, un terme dans le $2^{ème}$,..., un terme dans le $n^{ième}$ et en multipliant ces n termes entre eux. Comme chacun de ces termes vaut soit 1, soit X, leur produit sera de la forme $1^{n-k}X^k$ pour un k compris entre 0 et n.

Or le terme X^k se rencontrera chaque fois que l'on a choisi X dans k facteurs, quelconques par ailleurs, et 1 dans les autres. Donc le nombre de fois où on rencontre X^k n'est autre que le nombre de parties à k éléments d'un ensemble à n éléments c'est-à-dire C_n^k. D'où :

Proposition 2 (*Formule du binôme*)

$$(1+X)^n = \sum_{k=0}^{n} C_n^k X^k.$$

On a, de manière analogue :

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$$

et, en remplaçant b par $-b$ dans la formule ci-dessus :

$$(a-b)^n = \sum_{k=0}^{n} (-1)^k C_n^k a^{n-k} b^k.$$

Les deux dernières formules sont valables pour a et b dans un corps commutatif quelconque (et même un anneau commutatif).

Exercice 5 : Montrer la formule du binôme par récurrence sur n.

C'est à cause de cette formule que les nombres C_n^k sont souvent appelés coefficients du binôme ou coefficients binomiaux.

Comme cas particulier de ces formules on a les résultats classiques :

$$(a+b)^2 = a^2+2ab+b^2$$

$$(a+b)^3 = a^3+3ab^2+3a^2b+b^3.$$

La formule du binôme permet d'établir de nombreuses formules avec les C_n^k. Nous en donnons quelques exemples.

a) En faisant $X = 1$ dans la formule du binôme :

$$2^n = \sum_{k=0}^{n} C_n^k$$

b) En faisant $X = -1$:

$$0 = \sum_{k=o}^{n} (-1)^k C_n^k$$

c) En dérivant $f(x) = (1+x)^n$ on trouve :

$$f'(x) = n(1+x)^{n-1} = \sum_{k=1}^{n} k\, C_n^k x^{k-1},$$

et en faisant $x = 1$:

$$n\, 2^{n-1} = \sum_{k=1}^{n} k\, C_n^k.$$

On peut aussi faire $x = -1$ dans $f'(x)$ ou intégrer $f(x)$ et faire dans la formule obtenue $x = 1$ ou $x = -1$ ...

Exercice 6 : Calculer $\sum_{k=o}^{n} k^2 C_n^k$.

Exercice 7 : En intégrant $(1+x)^n$, calculer $1 - \frac{1}{2} C_n^1 + \frac{1}{3} C_n^2 + \ldots + \frac{(-1)^n}{n+1} C_n^n$.

Exercice 8 : En utilisant $(1+x)^{m+k} = (1+x)^m (1+x)^k$, montrer que

$$\sum_{p+q=n} C_k^p\, C_m^q = C_{k+m}^n.$$

Exercice 9 : Montrer que pour tout k et tout n $(k \leq n)$:

$$C_k^k + C_{k+1}^k + \ldots + C_n^k = C_{n+1}^{k+1}.$$

En déduire la valeur de $1+2+\ldots+n$, $1.2+2.3+\ldots+(n-1)n$, $1.2.3+2.3.4+\ldots+(n-2)(n-1)n$.

d) Calcul des sommes $S_k = 1^k + 2^k + \ldots + n^k$.

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

En écrivant cette relation pour $x = 1,2,\ldots,n$ et en ajoutant :

$$\sum_{k=1}^{n} (1+k)^2 = \sum_{k=1}^{n} (1+2k+k^2)$$

$$= \sum_{k=1}^{n} 1 + 2 \sum_{k=1}^{n} k + \sum_{k=1}^{n} k^2.$$

En posant $1+k = \ell$, la somme de gauche est :

$$\sum_{k=1}^{n} (1+k)^2 = \sum_{\ell=2}^{n+1} \ell^2 = \sum_{\ell=1}^{n} \ell^2 - 1 + (n+1)^2.$$

Par suite on trouve :

$$(n+1)^2 - 1 = \sum_{k=1}^{n} 1 + 2S_1 = n + 2S_1$$

et finalement on retrouve la formule $S_1 = \frac{n(n+1)}{2}$.

Pour calculer S_2 , on va utiliser S_1 et la formule donnant $(1+k)^3$. Par un processus analogue, on trouve :

$$\sum_{k=1}^{n} (1+k)^3 = n + 3S_2 + 3S_1 + \sum_{k=1}^{n} k^3,$$

ou encore :

$$(1+n)^3 = n + 3S_2 + 3S_1 + 1.$$

On aurait de même :

$$(1+n)^4 = n + 4S_3 + 6S_2 + 4S_1 + 1.$$

Les quantités S_k se calculent donc de proche en proche.

Exercice 10 : Calculer S_2, S_3, S_4 en fonction de n.

Exercice 11 : Soient a et r deux entiers. On pose $a_0 = a$, $a_1 = a+r$, ..., $a_n = a+nr$.

Calculer $a_0+a_1+\ldots+a_n$, $a_0^2+a_1^2+\ldots+a_n^2$.

II - PROPRIÉTÉS ARITHMÉTIQUES DE K[X]

1.- Division euclidienne dans K[X]

A beaucoup de points de vue, la structure de l'anneau des polynômes à coefficients dans un corps évoque celle des nombres entiers. Le point essentiel à cet égard est la possibilité de définir une division euclidienne dans K[X].

Théorème 1 : *Soient A et B deux polynômes à coefficients dans K avec $B \neq 0$. Il existe un couple (Q,R) de polynômes à coefficients dans K, définis de manière unique, tels que $A = BQ+R$ et $d^\circ R < d^\circ B$ ou $R = 0$.*
On dit que Q est le quotient et R le reste dans la division euclidienne de A par B.

Posons $A = a_n X^n+\ldots+a_0$

$B = b_m X^m+\ldots+b_0$ et supposons $b_m \neq 0$.

Si $d^\circ A = d^\circ B = 0$, on pose $Q = a_0 b_0^{-1}$ (dans ce cas $b_0 = b_m$, $a_0 = a_n$) et $R = 0$.

Si $d^\circ A < d^\circ B$, on pose $Q = 0$ et $R = A$. Cela est vrai en particulier si $d^\circ A = 0$ et $d^\circ B \neq 0$.

On peut donc, si $d^\circ A = 0$ trouver Q et R répondant à la question. On va démontrer le théorème en faisant une récurrence sur le degré de A. On a le résultat si $d^\circ A = 0$ et supposons que le résultat est vrai si le degré de A est strictement plus petit que n. Considérons alors A et B comme ci-dessus. On peut supposer $d^\circ B \leq d^\circ A$ sinon on a le résultat. Comme $b_m \neq 0$, considérons le polynôme $B' = a_n b_m^{-1} X^{n-m}\ B = a_n X^n+a'_n X^{n-1}+\ldots+a'_0$ (les valeurs des coefficients $a'_{n-1},\ldots,a'_0$ sont sans intérêt ici).

Alors :

$$A-B' = (a_n X^n+a_{n-1}X^{n-1}+\ldots+a_0)-(a_n X^n+a'_{n-1}X^{n-1}+\ldots+a'_0)$$

$$= a''_{n-1}X^{n-1}+a''_{n-2}X^{n-2}+\ldots+a''_0.$$

Par hypothèse de récurrence on a :

$$A-B' = BQ'+R' \quad \text{pour} \quad Q',R' \in K[X] \quad \text{et} \quad d^\circ R' < d^\circ B.$$

En portant dans cette dernière relation la valeur de B on trouve :

$$A = (a_n b_m^{-1} X^{n-m}+Q')B+R'.$$

On a donc montré le résultat pour A avec $Q = a_n b_m^{-1} X^{n-m}+Q'$ et $R = R'$.
Il nous reste à montrer l'unité du couple (Q,R).
Supposons donc que :

$$A = BQ_1+R_1 \quad (d^\circ R_1 < d^\circ B \quad \text{où} \quad R_1 = 0)$$
$$A = BQ_2+R_2 \quad (d^\circ R_2 < d^\circ B \quad \text{où} \quad R_2 = 0).$$

Par différence on trouve : $B(Q_1-Q_2) = R_2-R_1$. Donc $d^\circ B+d^\circ(Q_1-Q_2) = d^\circ(R_2-R_1)$. Comme $d^\circ(R_2-R_1) \leq \text{Min}(d^\circ R_1, d^\circ R_2) < d^\circ B$, on arrive à une contradiction sauf si $Q_1-Q_2 = 0$ et $R_2-R_1 = 0$.

Pratique de la division

Pour diviser un polynôme A par un polynôme B, on suit fidèlement la méthode utilisée dans la démonstration du théorème : on construit d'abord $B' = a_n b_m^{-1} X^{n-m} B$ puis on recommence en remplaçant A par $A-B'$ ... . Il sera plus simple de montrer cela sur un exemple : supposons $A = 2X^5+X^4+2X^3+3X^2+X+4$ et $B = 2X^3+X^2+1$. On dispose les polynômes comme on le fait dans la division des nombres entiers. On s'arrête lorsque le dernier reste (le dernier polynôme de la forme $A-B'$) est de degré strictement plus petit que celui de B.

$$\begin{array}{l|l} 2X^5+X^4+2X^3+3X^2+X+4 & 2X^3+X^2+1 \\ \underline{-(2X^5+X^4\quad\quad+X^2)} & \\ 2X^3+2X^2+X+4 & X^2+1 \\ \underline{-(2X^3+X^2\quad\quad+1)} & \\ X^2+X+3 & \end{array}$$

On a ici $a_n = a_5 = 2$, $b_m = b_3 = 2$. Le polynôme $a_n b_m^{-1} X^{n-m} B$ est donc $X^2B = 2X^5+X^4+X^2$. On a placé ce polynôme en dessous de A et on a fait la soustraction. Le polynôme A-B' est $2X^3+2X^2+X+4$ et pour ce nouveau polynôme $a_3 = 2$ et en multipliant B par 1, puis en faisant la différence apparaît X^2+X+3 dont le degré est $2 < 3 = d°B$. Le quotient de A par B est donc X^2+1, le reste est X^2+X+3. Si on est un peu familier avec ces calculs, on ne porte pas le polynôme B' en dessous de A mais on fait directement le calcul de A-B'.

Exercice 12 : Déterminer le quotient et le reste dans la division de $3X^5+X^4-6X^2+5X-1$ par $2X^3-X+1$, $5X^5-2X^3+X^2+7X-3$ par $X+2$, de $2X^4+5X^2-10X+1$ par $2X^2-5X+5$.

Exercice 13 :

a) Montrer que le reste de la division d'un polynôme P par X-a est P(a) et que le reste dans la division de $(X^p)^q$ par (X^p-a) est a^q.

b) Soit k un entier naturel. Posons $k = qp+r$ $(0 \leq r < p)$. Montrer que le reste de la division de X^k par (X^p-a) est $a^q X^r$ et en déduire le reste de la division d'un polynôme P par le polynôme X^p-a.

Exercice 14 : Calculer P(a) pour $P = 2X^4+5X^2-10X+1$ et $a = \frac{5+i\sqrt{15}}{4}$ (cf. exercice 13. Trouver le lien entre a et $2X^2-5X+5$).

Exercice 15 : Quel est le reste de la division de X^n-1 par X^m-1 ?

Exercice 16 : Les restes de la division d'un polynôme P par (X-1), (X-2), (X-3) sont respectivement a,b,c. Quel est le reste de la division de P par (X-1)(X-2)(X-3) ?

2.- L'arithmétique de K[X]

Comme dans tout anneau, on peut définir la notion de multiple dans K[X] : le polynôme A est multiple du polynôme B s'il existe un polynôme C tel que A = BC. On dit aussi que B est un diviseur de A, que B divise A. On notera là encore : $B|A$.

Remarque 1 : Si le polynôme A divise B et si B divise A on a : B = AC et A = BD donc A = ACD et par suite CD = 1. Le polynôme C est donc inversible dans K[X], C est une constante non nulle (et de même pour D). Donc B = aA avec $a \in K$. Si on choisit a égal à l'inverse du coefficient dominant de A, on voit que B est unitaire et qu'il est le seul polynôme unitaire multiple de A. De même que dans $\mathbb{Z}$ on avait, du point de vue des propriétés multiplicatives, un caractère d'unicité en se limitant aux entiers naturels, dans K[X], ce sont les polynômes unitaires qui nous permettront d'établir certaines propriétés d'unicité.

D'autre part K[X] est pourvu d'une division euclidienne. Si on se reporte au chapitre II de la partie "Arithmétique" de ce cours on constate que la division euclidienne est à la base de toute la théorie qui y est développée. On va donc pouvoir, sans efforts, calquer dans K[X] les résultats obtenus dans $\mathbb{Z}$.

Le rôle des entiers premiers sera tenu par les polynômes irréductibles. Remarquons que si P est un polynôme, si $x \in K$ $(a \neq 0)$, P est divisible par a et par aP : ce sont les diviseurs "triviaux" de P.

Définition : Un polynôme P est dit irréductible s'il n'a pas d'autres diviseurs que les diviseurs triviaux. Ou encore : les seuls diviseurs de P sont des polynômes de degré égal à celui de P ou de degré 0.

On remarquera que tout polynôme de degré 1 est irréductible.

Remarque 2 : La notion de polynôme irréductible dépend du corps dans lequel il est étudié. Ainsi X^2-2 est un polynôme de $\mathbb{Q}[X]$ et de $\mathbb{R}[X]$. Dans $\mathbb{Q}[X]$ il est irréductible, dans $\mathbb{R}[X]$ il est réductible $(X^2-2 = (X-\sqrt{2})(X+\sqrt{2}))$.

Proposition 3 : Tout idéal I de K[X] est formé par l'ensemble des multiples d'un polynôme unitaire P, déterminé de manière unique : on dit que P engendre I ou que P est un générateur de I.

Si $I = \{0\}$, I est l'ensemble des multiples de 0.

Sinon, il existe dans I des polynômes de degré positif.

Soit P le polynôme de plus petit degré dans I. On peut supposer P unitaire (quitte à le multiplier par une constante).

Soit A un élément de I. La division euclidienne de A par P donne $A = PQ+R$ avec $R = 0$ où $d°R < d°P$. Comme I est un idéal, $PQ \in I$, $A-PQ \in I$ et donc, compte tenu du choix de P, on a $R = 0$: A est un multiple de P.

Remarque 3 : Cette démonstration est à comparer à celle de la proposition 4 d'"Arithmétique". Elle lui est en tout point analogue sauf qu'on y remplace une propriété telle que $0 \leq r < n$ par $d°R < d°P$. Sous réserve de ce changement la plupart des démonstrations de la partie Arithmétique vont s'appliquer ici : on se dispensera donc de les réécrire.

Définition : On appelle plus grand commun diviseur de deux polynômes A et B et on note $PGCD(A,B)$ le polynôme unitaire divisant A et B et qui est de degré maximum parmi tous les polynômes divisant A et B.

(Si l'on supprime le qualificatif "unitaire", on obtient un PGCD de A et B).

Proposition 4 : *Le PGCD de A et B est le générateur unitaire de l'idéal engendré par A et B, c'est-à-dire de tous les polynômes de $K[X]$ de la forme $UA+VB$, où U et V parcourent $K[X]$.*

Théorème 2 : *Si $D = PGCD(A,B)$, il existe $U,V \in K[X]$ tels que $D = UA+VB$. Tout diviseur commun à A et B divise $PGCD(A,B)$.*

Proposition 5 : *$PGCD(A,B) = PGCD(A-B,B)$. Si $A = BQ+R$, $PGCD(A,B) = PGCD(B,R)$.*

On ne peut plus ici comme dans la proposition 6 d'Arithmétique dire que la deuxième assertion résulte de la première par itération. Mais il est clair que si $D|A$ et B, alors $D|B$ et R et réciproquement.

Définition : Deux polynômes A et B sont dit premiers entre eux si leur PGCD est égal à 1 : seules les constantes non nulles divisent simultanément A et B.

On a encore le théorème de Bezout :

Théorème 3 (de Bezout) :

Deux polynômes A et B de K[X] sont premiers entre eux si et seulement si il existe U et V ∈ K[X] tels que UA+VB = 1.

Lemme d'Euclide pour les polynômes :

Si P est un polynôme irréductible, si P|BC alors P|B ou P|C.
Si A divise BC et si A est premier avec B, alors A divise C.
Si A|P, B|P et PGCD(A,B) = 1, alors AB|P.

Algorithme d'Euclide :

Pour les polynômes comme pour les nombres entiers, la méthode pratique pour déterminer le PGCD de A et B est l'algorithme d'Euclide :

On écrit : $A = Q_1B+R_1$ ($R_1 = 0$ ou $d°R_1 < d°B$). Si $R_1 \neq 0$:

$B = Q_2R_1+R_2$ ($R_2 = 0$ ou $d°R_2 < d°R_1$)

et ainsi de suite. On obtient des restes $R_1, R_2, R_3 \ldots$ dont les degrés forment une suite strictement décroissante. Il existe donc un entier n tel que $R_{n+1} = 0$. Les deux dernières étapes du processus sont :

$$R_{n-2} = Q_nR_{n-1}+R_n$$

$$R_{n-1} = Q_{n+1}R_n$$

et $PGCD(A,B) = R_n$: ce qui se démontre comme pour les nombres entiers.

Exemple : Déterminer le PGCD de $A = X^4-X^3+4X^2-X+3$ et de $B = X^3+2X+3$.

$X^4-X^3+4X^2-X+3$	$X-1$	$X+1$
$-(X^4 \quad +2X^2+3X)$	$X^3 \quad +2X+3$	X^2-X+3
$-X^3+2X^2-4X+3$	$-(X^3-X^2+3X$	
$-(-X^3 \quad -2X-3)$	X^2-X+3	
$2X^2-2X+6$	$-(X^2-X+3)$	
	0	

La disposition des calculs (écriture du quotient au dessus du diviseur) facilite la tâche.

On a ici : $Q_1 = X-1$, $R_1 = 2X^2-2X+6$.

On notera que dans la division de B par R_1, on a remplacé R_1 par X^2-X+3 qui est $\frac{R_1}{2}$: du point de vue de la divisibilité il n'y a aucun inconvénient à remplacer un polynôme par son produit par une constante. Le changement opéré ici - qui revient à remplacer R_1 par un polynôme unitaire - facilite les calculs en évitant les coefficients fractionnaires. R_1 étant ainsi modifié on a $Q_2 = X+1$ et $R_2 = 0$. Donc R_1 est le PGCD de A et B :

$$PGCD(A,B) = X^2-X+3.$$

Exercice 17 : Déterminer le PGCD de $X^5+X^4+2X^3-2X+3$ et $X^4+3X^3+7X^2+8X+6$.
" $X^4+X^3-3X^2-4X-1$ et X^3+X^2-X-1.

Exercice 18 : Montrer que X^3+1 et X^2+1 sont premiers entre eux.
Déterminer U et V tels que $U(X^3+1)+V(X^2+1) = 1$.
Mêmes questions pour X^7-X-1 et X^5+1.

Exercice 19 : Déterminer le PGCD de (X^n-1) et (X^m-1). (cf. exercice 15 où on a montré que le reste de la division de X^n-1 par X^m-1 était X^r-1 où r est le reste de la division de n par m).

Remarque : Si A et B sont deux éléments de K[X], si L est un corps contenant K, la division euclidienne de A par B donne un quotient Q et un reste R qui sont dans K[X] donc la condition d'unicité du théorème 1 implique que Q et R sont le quotient et le reste de la division de A par B dans L[X]. Donc quotient et reste d'une division eucli-

dienne ne dépendent pas du corps dans lequel on se place. En particulier le PGCD de deux polynômes A et B de K[X] est le même que si on considère A et B dans L[X] (à cause de l'algorithme d'Euclide).

On remarquera par contre que la division de X^2+1 par $2X-1$ a comme quotient $\frac{X}{2}+\frac{1}{4}$ et comme reste $\frac{5}{4}$, qui ne sont pas des polynômes à coefficients dans $\mathbb{Z}$.

Exercice 20 : Trouver un polynôme $P \in \mathbb{Q}[X]$ tel que $(P+1)$ soit multiple de $(X-1)^2$ et $(P-1)$ soit multiple de X^3 (suivre une démarche analogue à celle de la démonstration du théorème chinois).

L'analogie entre K[X] et $\mathbb{Z}$ développée dans ce paragraphe se poursuit jusqu'à l'équivalent du théorème fondamental :

Théorème 4 : *Tout polynôme à coefficients dans K[X] s'écrit, de manière unique, sous la forme :*

$$A = uP_1P_2\dots P_n$$

où $u \in K$ et $P_1, P_2, \dots, P_n$ sont des polynômes unitaires irréductibles de K[X].

Pour la partie unicité du théorème, la démonstration est la même que dans $\mathbb{Z}$ grâce à l'emploi du lemme d'Euclide.

Pour l'existence, on considère - si A n'est pas irréductible - le polynôme P_1 non constant, de plus petit degré, qui divise A. Alors P_1 est irréductible (sinon il admet un diviseur non trivial qui diviserait A). Donc $A = P_1B_1$ et, si B_1 est non irréductible, soit P_2 le polynôme de plus petit degré qui divise B_1. P_2 est irréductible et $A = P_1P_2B_2$. La suite $B_1, B_2, \dots$ est formée des polynômes dont les degrés décroissent strictement donc il existe k tel que B_k est irréductible.

Exercice 21 : Un polynôme de $\mathbb{R}[X]$ est divisible par X^2+X+1 si et seulement si il est divisible (dans $\mathbb{C}[X]$) par $(X-j)$ et $(X-j^2)$ où $j = e^{\frac{2i\pi}{3}}$.

En déduire quels sont les entiers m tels que $(X+1)^m-X^m-1$ est divisible par X^2+X+1.

Exercice 22 : Décomposer en facteurs irréductibles sur $\mathbb{R}$ le polynôme X^8+X^4+1. (Remarquer que $X^8+X^4+1 = (X^4+1)^2-X^4\dots$).

III - RACINES D'UN POLYNÔME

Définition : Un élément α de K est appelé racine de $P \in K[X]$ si $P(\alpha) = 0$.

On dit aussi que α est un zéro de P.

Théorème 5 : *α est une racine de P si et seulement si le polynôme $(X-\alpha)$ divise le polynôme P.*

La division euclidienne de P par $X-\alpha$ donne :

$$P = (X-\alpha)Q+R$$

où $R = 0$ ou bien de degré 0 : R est donc une constante. Si l'on considère la valeur en α de la relation ci-dessus on trouve que $R = P(\alpha)$. Donc $P(\alpha) = 0$ si et seulement si R est nul, donc si et seulement si $(X-\alpha)$ divise P.

Théorème 6 : Un polynôme de degré n admet au plus n racines distinctes.

Soient en effet $\alpha_1, \alpha_2, \ldots, \alpha_m$ des racines distinctes d'un polynôme P de degré n.

On a : $P = (X-\alpha_1)Q_1$

Comme $P(\alpha_2) = 0$, que $\alpha_2-\alpha_1 \neq 0$, $Q_1(\alpha_2) = 0$. Donc $Q_1 = (X-\alpha_2)Q_2$ et par suite : $P = (X-\alpha_1)(X-\alpha_2)Q_2$.

En itérant ce procédé on trouve :

$$P = (X-\alpha_1)(X-\alpha_2) \ldots (X-\alpha_m)Q_m$$

ce qui implique que $d^\circ P \geq m$.

Corollaire : *Si $P \in K[X]$ est de degré inférieur ou égal à n et a au moins $n+1$ racines, $P = 0$.*

Remarque : Une conséquence du théorème est de justifier l'identification entre polynômes et fonctions polynomiales si K est un corps infini : car si P et Q sont deux polynômes et si $\tilde{P} = \tilde{Q}$, cela signifie que $P-Q$ a une infinité de racines (à savoir les éléments de K) donc $P-Q = 0$.

La démonstration du théorème précédent donne aussi le résultat suivant :

Proposition 6 : *Si le polynôme P admet $\alpha_1,\ldots,\alpha_m$ comme racines ($\alpha_i \neq \alpha_j$ si $i \neq j$), il est multiple de $(X-\alpha_1)\ldots(X-\alpha_m)$.*

On notera que cette proposition résulte aussi du lemme d'Euclide pour les polynômes car si $\alpha_i \neq \alpha_j$, $(X-\alpha_i)$ et $(X-\alpha_j)$ sont premiers entre eux.

Exercice 23 : Quelles sont les racines de $X^{p-1}-1$ dans $\mathbb{Z}/p\mathbb{Z}[X]$?

En déduire une autre démonstration du théorème de Wilson (Arithmétique, III,2).

Multiplicité d'une racine

Définition : On appelle multiplicité de la racine α du polynôme P l'entier r tel que $(X-\alpha)^r$ divise P et $(X-\alpha)^{r+1}$ ne divise pas P.

Proposition 7 : *Soient $\alpha_1,\alpha_2,\ldots,\alpha_m$ des racines distinctes d'un polynôme P de degré n. La somme des multiplicités de ces racines est inférieure ou égale à n. Plus précisément, le polynôme P est divisible par $(X-\alpha_1)^{r_1}\ldots(X-\alpha_m)^{r_m}$ où r_i désigne la multiplicité de α_i.*

En effet, par définition $(X-\alpha_1)^{r_1}$ divise P. Donc $P = (X-\alpha_1)^{r_1}P_2$. On sait que P s'annule en α_2 et comme $\alpha_2 \neq \alpha_1$, $P_1(\alpha_1) = 0$ donc $(X-\alpha_2)$ divise P_2.

Supposons que nous ayons montré que $(X-\alpha_2)^k$ divise P_2 pour un entier $k < r_2$. On a donc :

$$P = (X-\alpha_2)^{r_2}Q_1$$

et $$P = (X-\alpha_1)^{r_1}(X-\alpha_2)^k P_2.$$

Comme $k < r_2$, en simplifiant par $(X-\alpha_2)^k$ ces deux relations on trouve :

$(X-\alpha_2)^{r_2-k} Q_1 = (X-\alpha_1)^{r_1} P_2$: le polynôme $(X-\alpha_2)$ divise le membre de gauche, α_2 est différent de α_1 donc $(X-\alpha_2)$ divise P_2 ou encore $(X-\alpha_2)^{k+1}$ divise P_1. Par une récurrence immédiate, on a le résultat.

Remarque : On peut aussi conclure en remarquant que $(X-\alpha_1)^{r_1}, \ldots (X-\alpha_m)^{r_m}$ sont des diviseurs de P premiers entre eux deux à deux : leur produit doit donc diviser P.

Remarque : Si un polynôme de degré 2 ou 3 est réductible il admet nécessairement une racine : un polynôme de degré 2 ne peut être décomposé qu'en produit de 2 polynômes de degré 1, un polynôme de degré 3 peut être décomposé en produit de 3 polynômes de degré 1 ou d'un polynôme de degré 1 par un polynôme de degré 2. Par suite un polynôme de degré 2 ou 3 est irréductible si et seulement s'il n'admets pas de racines. Le résultat est faux dès que le degré du polynôme est supérieur ou égal à 4 : $(X^2+1)(X^2+X+1)$ est réductible sur $\mathbb{R}$ et n'admet pas de racines.

Relations entre coefficients et racines

Si P est un polynôme de degré 2 dont les racines sont α et β on a :

$$aX^2+bX+c = a(X-\alpha)(X-\beta)$$

et en effectuant le membre de droite on trouve

$$\frac{b}{a} = -(\alpha+\beta) \quad \text{et} \quad \frac{c}{a} = \alpha\beta.$$

De même si P est de degré 3 ayant 3 racines α,β,γ :

$$aX^3+bX^2+cX+d = a(X-\alpha)(X-\beta)(X-\gamma).$$

En effectuant :

$$\frac{b}{a} = -(\alpha+\beta+\gamma), \ \frac{c}{a} = \alpha\beta+\alpha\gamma+\beta\gamma, \ \frac{d}{a} = -\alpha\beta\gamma.$$

Ces formules se généralisent aisément :

Si $P = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 = a_n (X-\alpha_1)\ldots(X-\alpha_n)$, on a :

$$\frac{a_{n-1}}{a_n} = -(\alpha_1+\alpha_2+\ldots+\alpha_n)$$

$$\frac{a_{n-2}}{a_n} = \sum_{1\leq i<j\leq n} \alpha_i \alpha_j$$

$$\vdots$$

$$\frac{a_{n-k}}{a_n} = (-1)^k \sum_{1\leq i_1<\ldots<i_k\leq n} \alpha_{i_1}\ldots\alpha_{i_k}$$

$$\vdots$$

$$\frac{a_0}{a_n} = (-1)^n \alpha_1\alpha_2\ldots\alpha_n$$

En particulier la connaissance des n racines d'un polynôme unitaire de degré n détermine les coefficients de ce polynôme. La réciproque est fausse, en tout cas si l'on veut des formules de nature algébrique.

Les seconds membres des relations entre coefficients et racines sont "symétriques" par rapport aux racines (c'est-à-dire que si l'on permute les α_i les quantités $\Sigma\alpha_i, \Sigma\alpha_i\alpha_j$ ... ne changent pas. En fait on sait montrer que toute relation symétrique par rapport aux racines d'un polynôme peut s'exprimer à l'aide de ces quantités.

Par exemple si $\alpha_1, \alpha_2 \ldots \alpha_n$ sont les racines de $X^n + a_{n-1}X^{n-1} + \ldots + a_0$:

$$(\alpha_1^2+\alpha_2^2+\ldots+\alpha_n^2) = (\alpha_1+\alpha_2+\ldots+\alpha_n)^2 - 2(\alpha_1\alpha_2+\alpha_1\alpha_3+\ldots+\alpha_{n-1}\alpha_n)$$

Posons $\sigma_1 = \alpha_1+\alpha_2+\ldots+\alpha_n$, $\sigma_2 = \sum_{1\leq i<j\leq n} \alpha_i\alpha_j, \ldots, \sigma_n = \alpha_1\alpha_2\ldots\alpha_n$.

Alors $\sum_{i=1}^{n} \alpha_i^2 = \sigma_1^2 - 2\sigma_2 = a_{n-1}^2 - 2a_{n-2}$.

Exercice 24 : Montrer que $\sum_{i=1}^{n} \alpha_i^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$.

Calculer de même $\sum_{i=1}^{n} \alpha_i^4$.

Exercice 25 : Soient $\alpha_1, \alpha_2, \alpha_3$ les racines de X^3+pX+q.

En remarquant que $\alpha_i^3 = -p\alpha_i - q$, montrer que l'on peut écrire : $\alpha_i^k = a\alpha_i^2 + b\alpha_i + c$ (a,b,c dépendant de k). Déduire de ce résultat et des formules précédentes l'expression de $\alpha_1^7+\alpha_2^7+\alpha_3^7$ en fonction de p et q.

IV - CAS DES POLYNÔMES SUR IR OU $\mathbb{C}$

En ce qui concerne les polynômes à coefficients dans $\mathbb{C}$, le résultat de base est le théorème suivant (que nous ne démontrerons pas).

Théorème 7 : *(d'Alembert-Gauss) (Théorème fondamental de l'algèbre)*

Tout polynôme de degré n à coefficients complexes admet n racines dans $\mathbb{C}$ (comptées avec leur multiplicité).
C'est-à-dire encore :
Tout polynôme de $\mathbb{C}[X]$ se décompose en produit de polynômes de degré 1.
Ou encore :
Les seuls polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Soit $P = a_n X^n + \ldots + a_1 X + a_0$ un polynôme à coefficients complexes et désignons par α une racine de P. Le polynôme P peut donc s'écrire :

$$P = (X-\alpha)(b_{n-1}X^{n-1} + \ldots + b_0)$$

Si on désigne par $\bar{P}$ le polynôme $\bar{a}_n X^n + \ldots + \bar{a}_1 X + \bar{a}_0$ on a (par application immédiate des formules $\overline{zz'} = \bar{z}\bar{z}'$ et $\overline{z+z'} = \bar{z}+\bar{z}'$) :

$$\bar{P} = (X-\bar{\alpha})(\bar{b}_{n-1}X^{n-1} + \ldots + \bar{b}_0).$$

Donc si α est une racine de P, $\bar{\alpha}$ est une racine de $\bar{P}$.

En particulier si $P \in \mathbb{R}[X]$ le raisonnement ci-dessus s'applique à toute racine complexe α de P. Mais dans ce cas $\bar{P} = P$ donc :

Proposition 8 : *Si α est une racine complexe de multiplicité r d'un polynôme P à coefficients réels, $\bar{\alpha}$ est racine de P avec la multiplicité r.*

Le complément sur la multiplicité se déduit de l'écriture de P sous la forme $(X-\alpha)^r(c_{n-r}X^{n-r}+\ldots+c_0)$.

Ce résultat joint au théorème de d'Alembert Gauss donne :

Théorème 8 : *Tout polynôme de $\mathbb{R}[X]$ se décompose en produit de polynômes de degré 1 et de polynômes de degré 2 dont le discriminant est négatif.*
Ou encore :
Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant négatif.

Soit P un polynôme de degré n à coefficients réels. Le théorème de d'Alembert-Gauss entraîne que P peut s'écrire :

$$P = a(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n)$$

où $\alpha_1,\alpha_2,\ldots,\alpha_n$ sont des nombres complexes. La proposition 8 entraîne qu'il existe r avec $\alpha_1,\alpha_2,\ldots,\alpha_r \in \mathbb{R}$ et $\alpha_{r+1},\alpha_{r+2},\ldots,\alpha_n$ sont complexes non réels et vérifiant : $\alpha_{r+1} = \bar{\alpha}_{r+2}, \alpha_{r+3} = \bar{\alpha}_{r+4},\ldots,\alpha_{n-1} = \bar{\alpha}_n$.
Donc

$$P = a(X-\alpha_1)\ldots(X-\alpha_r)(X-\alpha_{r+1})(X-\bar{\alpha}_{r+1})\ldots(X-\alpha_{n-1})(X-\bar{\alpha}_{n-1}).$$

Or $(X-\alpha_k)(X-\bar{\alpha}_k) = X^2-(2\ \mathrm{Re}\ \alpha_k)X+|\alpha_k|^2$ est un polynôme de degré 2, à coefficients réels, admettant deux racines non réelles donc à discriminant négatif ce qui prouve le résultat.

Remarque : Ces racines non réelles d'un polynôme à coefficients réels sont groupées 2 par 2, elles sont donc en nombre pair. Ce qui impose qu'un polynôme de $\mathbb{R}[X]$ de degré impair admet au moins une racine réelle. Cela est clair pour des raisons analytiques car un tel polynôme varie de $-\infty$ à $+\infty$ (si on suppose son coefficient dominant positif) et passe donc par la valeur 0. Ce résultat est d'ailleurs indispensable pour prouver le théorème de d'Alembert-Gauss.

Exercice 26 : On considère le polynôme $P = (X+1)^n - e^{2ina}$ de $\mathbb{C}[X]$ (n entier naturel, a réel). Montrer que les racines de P sont

$2ie^{i(\frac{k\pi}{n}+a)} \sin(\frac{k\pi}{n}+a) = x_k \quad (0 \leq k \leq n-1)$.

Calculer de deux manières différentes $x_0.x_1. \ldots .x_{n-1}$ et en déduire que $\prod_{k=0}^{n-1} \sin(\frac{k\pi}{n}+a) = \frac{\sin n a}{2^{n-1}}$.

Polynômes à coefficients dans $\mathbb{Q}$

Une démarche analogue à celle du théorème 8 peut être effectuée pour les polynômes de $\mathbb{Q}[X]$: on commence par décomposer ces polynômes en facteurs de degré 1 sur $\mathbb{C}$ puis on regroupe (si possible), certains des facteurs pour obtenir une décomposition sur $\mathbb{Q}$. Ce procédé est surtout utilisé pour démontrer qu'un polynôme est irréductible sur $\mathbb{Q}$ et ne peut de toute manière fonctionner que si l'on connaît les racines complexes du polynôme ce qui n'est pas le cas le plus usuel.

Exemple 1 : $P = 1+X+X^2+X^3+X^4$ est irréductible sur $\mathbb{Q}$. On a $X^5-1 = (X-1)P$ donc les racines de P sont les racines $5^{\text{ème}}$ de l'unité différentes de 1. Aucune de ces racines n'est réelle dans P est irréductible sur $\mathbb{Q}$ ou est produit de deux polynômes de degré 2 de $\mathbb{Q}[X]$. Si l'on est dans ce cas l'un de ces polynômes ne peut être que $(X-e^{\frac{2i\pi}{5}})(X-e^{\frac{8i\pi}{5}}) = X^2-2\cos\frac{2\pi}{5}X+1$ et $\cos\frac{2\pi}{5}$ n'est pas dans $\mathbb{Q}$ (ce que le lecteur pourra vérifier).

Exemple 2 : Pour tout entier n il existe un polynôme de degré n irréductible sur $\mathbb{Q}[X]$, par exemple le polynôme X^n-2.

Soient $\alpha = \sqrt[n]{2}$ et $u = e^{\frac{2i\pi}{n}}$

Les racines complexes de P sont $u\alpha, u^2\alpha, \ldots, u^n\alpha$. Donc dans $\mathbb{C}[X]$, $P = (X-u\alpha)(X-u^2\alpha)\ldots(X-u^n\alpha)$. Si P se décompose en facteurs irréductibles dans $\mathbb{Q}[X]$, il admet un facteur R de degré $k < n$ qui est nécessairement de la forme $(X-u^{i_1}\alpha)\ldots(X-u^{i_k}\alpha)$. Le terme constant de ce polynôme est de la forme $u^r\alpha^k$. Ce nombre doit être dans $\mathbb{Q}$, donc dans $\mathbb{R}$ ce qui implique $r = 0$. Il reste donc que $\alpha^k \in \mathbb{Q}$ c'est-à-dire $2^{k/n} = \frac{a}{b}$ (où $\frac{a}{b}$ désigne une fraction irréductible). Par suite $b^n 2^k = a^n$: a est donc un

nombre pair, $a = 2a'$ et il vient $b^n 2^k = 2^n a'^n$. Comme $k < n$, on voit que b doit aussi être pair ce qui contredit le fait que $\frac{a}{b}$ est irréductible. Le polynôme X^n-2 est donc irréductible sur $\mathbb{Q}$.

Exercices - Indications et résultats

4) Le nombre d'applications de $\mathbb{Z}/p\mathbb{Z}$ dans lui-même est p^p qui est aussi le nombre d'applications polynomiales à cause de b) (qui résulte du théorème de Fermat).

10) $S_2 = \frac{n(n+1)(2n+1)}{6}$, $S_3 = \frac{n^2(n+1)^2}{4} = S_1^2$,

11) Méthode analogue à celle qui a permis de calculer les sommes S_k.

12) Quotients et restes sont : $\frac{3}{2}X^2+\frac{1}{2}X+\frac{3}{4}$ et $-7X^2+\frac{21}{4}X-\frac{7}{4}$, $5X^4-10X^3+18X^2-35X+77$ et -157, $X^2+\frac{5}{2}X+\frac{25}{4}$ et $\frac{35}{4}X-\frac{121}{4}$.

14) a est une racine de $2X^2-5X+5$. En divisant P par ce dernier polynôme on trouve un reste $R = \frac{35}{4}X-\frac{121}{4}$ et $P(a) = R(a) = \frac{-309+35i\sqrt{15}}{16}$.

15) Le reste est X^r-1 où r est le reste de la division de n par m.

18) Les polynômes U et V sont respectivement $\frac{1}{2}(X+1)$ et $\frac{1}{2}(-X^2-X+1)$, $-X^6+X^4-X^3+X+1$ et X^4-X^2+X.

19) $PGCD(X^n-1, X^m-1) = X^d-1$ où $d = PGCD(m,n)$.

21) $m \equiv \pm 1 \pmod 6$.

22) $X^8+X^4+1 = (X^2-X\sqrt{3}+1)(X^2+X\sqrt{3}+1)(X^2-X+1)(X^2+X+1)$.

23) $X^{p-1}-1 = (X-\bar{1})(X-\bar{2})\ldots(X-\overline{p-1})$ et le terme constant de ce polynôme est $(\overline{p-1})!$ (si p impair).

24) $\sum_{i=1}^{n} \alpha_i^4 = \sigma_1^4-4\sigma_1^2\sigma_2+4\sigma_3\sigma_1+2\sigma_2^2-4\sigma_4$.

25) $\alpha_1^7+\alpha_2^7+\alpha_3^7 = -7p^2q$.

PARTIE 4 : FRACTIONS RATIONNELLES

1.- Définition

Si P et Q désignent deux fonctions polynomiales de $\mathbb{R}$ dans $\mathbb{R}$ et A l'ensemble des zéros de Q, on peut définir la fonction rationnelle $f(x) = \frac{P(x)}{Q(x)}$: c'est une fonction définie sur le complémentaire de A dans $\mathbb{R}$ et à valeurs dans $\mathbb{R}$.

Si $f = \frac{P}{Q}$ et $g = \frac{R}{S}$ désignent deux fonctions de cette forme, A étant l'ensemble des zéros de Q et B l'ensemble des zéros de S, on définit de manière naturelle les fonctions rationnelles f+g et fg. Ce sont deux fonctions définies sur le complémentaire de AUB dans $\mathbb{R}$ par les formules :

$$(f+g)(x) = \frac{P(x)S(x)-Q(x)R(x)}{Q(x)S(x)} ,$$

$$(fg)(x) = \frac{P(x)R(x)}{Q(x)S(x)} .$$

Les raisons invoquées dans la partie précédente et qui justifiaient de distinguer les fonctions polynomiales des polynômes sont encore vraies ici. Une nouvelle raison vient s'ajouter aux autres : si l'on veut considérer l'ensemble des fonctions rationnelles on aboutit à un phénomène que R. Godement dans son "Cours d'Algèbre" avait déjà épinglé :

> *"On trouve, dans un manuel d'Algèbre destiné aux élèves des Lycées et Collèges, la phrase suivante : "Sous réserve de ne pas donner aux variables des valeurs qui annulent le numérateur ou le dénominateur, l'ensemble des fractions rationnelles muni des lois d'addition et de multiplication présente une structure de corps". Que pensez-vous de cet énoncé ? "*

C'est-à-dire que si l'on veut considérer l'ensemble des fractions rationnelles (en particulier toutes les fractions rationnelles de la forme $\frac{1}{x-a}$) on doit enlever tous les zéros des dénominateurs, c'est-à-dire tous les nombres réels.

Si l'on se place sur un corps fini le phénomène s'aggrave : ainsi $\frac{1}{(x-\bar{2})(x-\bar{1})x}$ n'est nulle part définie sur $\mathbb{Z}/3\mathbb{Z}$.

On est donc conduit à considérer des fractions rationnelles : une fraction rationnelle à coefficients dans un corps K est le quotient de deux polynômes. On munit cet ensemble d'une addition et d'une multiplication par les formules :

$$\frac{P}{Q} + \frac{R}{S} = \frac{PS+QR}{RS}$$

$$\frac{P}{Q} \times \frac{R}{S} = \frac{PR}{QS} .$$

On doit faire un effort supplémentaire pour dégager correctement cette notion : si A est un polynôme, on confond la fraction rationnelle $\frac{P}{Q}$ et la fraction $\frac{AP}{AQ}$ (en terme de fonctions rationnelles, si l'on se place sur l'ensemble des x qui ne sont pas zéros du polynôme AQ, les deux fractions rationnelles $\frac{P}{Q}$ et $\frac{AP}{AQ}$ sont égales. Ce qui les distingue c'est que le domaine de définition de $\frac{P}{Q}$ est en général plus grand que celui de $\frac{AP}{AQ}$).

L'identification de $\frac{P}{Q}$ et $\frac{AP}{AQ}$ se fait via une relation d'équivalence ($\frac{P}{Q}$ équivalent à $\frac{R}{S}$ si et seulement si $PS = QR$) de la même manière que les fractions $\frac{3}{5}$ et $\frac{6}{10}$ sont deux représentants d'une classe d'équivalence dans l'ensemble des fractions, cette classe étant un nombre rationnel. Nous n'insisterons pas sur la construction correcte de l'ensemble des fractions rationnelles : le problème est essentiellement de montrer que si f et g sont deux fractions, représentées par $\frac{P}{Q}$ et $\frac{R}{S}$, la somme $f+g$ étant la classe de $\frac{PS+QR}{QS}$, cette définition de l'addition ne dépend pas des représentants $\frac{P}{Q}$ et $\frac{R}{S}$ choisis pour f et g. Et ce même bien sûr pour le produit fg.

Si $\frac{P}{Q}$ est une fraction rationnelle, si $A|P$ et $A|Q$ posons $P = AP'$ et $Q = AQ'$. On a alors $\frac{P}{Q} = \frac{P'}{Q'}$. On dit qu'on a simplifié la fraction rationnelle $\frac{P}{Q}$.

En particulier si $A = PGCD(P,Q)$, la fraction rationnelle $\frac{P'}{Q'}$ à laquelle on aboutit ne peut plus être simplifiée. On dit que c'est une fraction rationnelle irréductible. Deux écritures irréductibles de $\frac{P}{Q}$ ne diffèrent que par multiplication d'une constante.

Théorème 1 : *L'ensemble des fractions rationnelles à coefficients dans un corps K est un corps noté $K(X)$.*

Le lecteur est invité à vérifier tout seul ce théorème.

2.- Pôles - Eléments simples

Définition : Soit $f = \frac{P}{Q}$ une fraction rationnelle irréductible à coefficients dans K. On appelle pôle de f (dans K) les zéros du polynôme Q. Si α est un pôle de f on dit qu'il est de multiplicité r si α est un zéro de multiplicité r de Q.

- Les pôles sont relatifs à l'écriture irréductible de f. Ainsi $\frac{X-1}{(X-1)(X-2)}$ n'admet que le pôle 2.

- Les pôles sont relatifs au corps considérés. Ainsi $\frac{1}{X^2+1}$ n'a pas de pôles sur $\mathbb{R}$ et a $\pm i$ comme pôles sur $\mathbb{C}$.

Soit $f = \frac{P}{Q}$ une fraction rationnelle irréductible. On peut supposer que Q est unitaire (sinon on multiplie numérateur et dénominateur de f par une constante convenable). La décomposition en facteurs irréductibles de Q est $Q_1^{\alpha_1} \ldots Q_r^{\alpha_r}$. La décomposition en éléments simples de f consiste à écrire f comme somme d'un polynôme et de fractions rationnelles de la forme $\frac{R}{Q_i^{\beta_i}}$ (les éléments simples) où $1 \leq \beta_i \leq \alpha_i$ et $d^\circ R < d^\circ Q_i$.

Cela est toujours possible, et de manière unique.

Par exemple :

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

Ce résultat est surtout important en analyse et plus précisément pour l'étude des problèmes suivants :

1) Calcul des dérivées successives d'une fraction rationnelle.

2) Développement en série entière d'une fraction rationnelle. Et surtout

3) Recherche des primitives d'une fraction rationnelle.

C'est donc lorsque $K = \mathbb{R}$ (c'est-à-dire que les Q_i sont de degré 1 ou 2) et éventuellement $K = \mathbb{C}$ (c'est-à-dire que les Q_i sont de degré 1) que la décomposition en éléments simples est utile.

Nous allons nous contenter d'indiquer les grandes lignes de la démonstration du théorème, nous réservant au paragraphe suivant d'insister sur les méthodes pratiques de décomposition en éléments simples.

Théorème 2 : *Soit $f = \frac{P}{Q}$ une fraction rationnelle irréductible dans $K(X)$.*
Supposons $Q = Q_1^{\alpha_1} \dots Q_k^{\alpha_k}$ où les Q_i sont distincts 2 à 2 et irréductibles. Alors f s'écrit de manière unique comme somme d'un polynôme A de $K[X]$ et d'une fraction rationnelle $\sum_{i=1}^{k} S_i$ où les S_i sont de la forme $\sum_{j=1}^{\alpha_i} \frac{B_j}{Q_i^j}$, les B_j étant des polynômes de $K[X]$ tels que $d^\circ B_j < d^\circ Q_i$.

En particulier

Si $K = C$, les Q_i sont de degré 1 donc les B_j sont des nombres complexes.

Si $K = \mathbb{R}$, les Q_i sont de degré 1 (et alors les B_j sont des nombres réels) ou de degré 2 (et alors les B_j sont des polynômes à coefficients réels de degré inférieur ou égal à 1).

Avec les notations du théorème, A est la partie entière de la fraction f et les S_i sont les parties polaires de f relatives alors $Q_i^{\alpha_i}$.
La démonstration du théorème se fait en 3 étapes.

a) Toute fraction rationnelle $\frac{P}{Q}$ peut s'écrire d'une façon et d'une seule sous la forme $\frac{P}{Q} = A + \frac{R}{Q}$ où A est un polynôme et $d^\circ R < d^\circ Q$: Cela est clair, A n'est autre que le quotient dans la division euclidienne de P par Q.

b) Toute fraction rationnelle $\frac{P}{Q}$ telle que $d°P < d°Q$ et telle que $Q = R_1R_2...R_k$ est le produit de k polynômes premiers entre eux deux à deux peut s'écrire d'une manière et d'une seule sous la forme $P = \sum_{i=1}^{n} \frac{P_i}{R_i}$ avec $d°P_i < d°R_i$: Par une récurrence immédiate on peut supposer que $k = 2$. Donc $\frac{P}{Q} = \frac{P}{R_1R_2}$. Par Bezout on sait qu'il existe deux polynômes U_1 et U_2 tels que $U_2R_1+U_1R_2 = 1$. Donc

$$\frac{P}{Q} = \frac{P(U_2R_1+U_1R_2)}{R_1R_2} = \frac{PU_1}{R_1} + \frac{PU_2}{R_2} .$$

En appliquant le résultat a) ci-dessus à $\frac{PU_1}{R_1} + \frac{PU_2}{R_2}$ on a :

$$\frac{PU_1}{R_1} = A_1 + \frac{P_1}{R_1} \quad (d°P_1 < d°R_1) \quad \text{et} \quad \frac{PU_2}{R_2} = A_2 + \frac{P_2}{R_2} .$$

Donc $$\frac{P}{Q} = A_1+A_2+ \frac{P_1}{R_1} + \frac{P_2}{R_2} .$$

Les conditions sur les degrés impliquent que A_1+A_2 est la partie entière de $\frac{P}{Q}$ donc que $A_1+A_2 = 0$ (puisque $d°P < d°Q$).

c) Toute fraction rationnelle $\frac{P}{Q^\alpha}$ avec $d°P < d°Q^\alpha$ peut s'écrire d'une manière et d'une seule sous la forme $\sum_{j=1}^{\alpha} \frac{B_j}{Q^j}$ où B_j est un polynôme tel que $d°B_j < d°Q$: En divisant P par Q il vient $P = QU_1+B_\alpha$ avec $d°B_\alpha < d°Q$.
Donc $\frac{P}{Q^\alpha} = \frac{U_1}{Q^{\alpha-1}} + \frac{B_\alpha}{Q^\alpha}$. Si $d°U_1 < d°Q$ on a fini, sinon on pose $U_1 = QU_2+B_{\alpha-1}$ $(d°B_{\alpha-1} < d°Q)$ et $\frac{P}{Q^\alpha} = \frac{U}{Q^{\alpha-2}} + \frac{B_{\alpha-1}}{Q^{\alpha-1}} + \frac{B_\alpha}{Q^\alpha}$ et on on itère le procédé.

Ainsi on a le résultat cherché en appliquant à une fraction rationnelle $\frac{P}{Q}$ chacune des 3 étapes qui précèdent (dans la $2^{ème}$ étape, si $Q = Q_1^{\alpha_1}...Q_k^{\alpha_k}$ on prend $R_i = Q_i^{\alpha_i}$).

Nous laissons au lecteur le soin de se convaincre de l'unicité de la décomposition.

3.- Pratique de la décomposition en éléments simples sur $\mathbb{C}$ et $\mathbb{R}$

Commençons par indiquer la plus mauvaise méthode, celle des coefficients indéterminés.

Exemple 1 : Décomposer en éléments simples sur $\mathbb{R}$ la fraction

$$\frac{1}{(x^2-2x\cos\alpha+1)(x^2-2x\cos\beta+1)} = f(x).$$

Le théorème général nous indique :

$$f(x) = \frac{ax+b}{x^2-2x\cos\alpha+1} + \frac{cx+d}{x^2-2x\cos\beta+1}.$$

En chassant les dénominateurs, on trouve :

$$1 = (ax+b)(x^2-2x\cos\beta+1)+(cx+d)(x^2-2x\cos\alpha+1)$$

et les quatres nombres a,b,c,d sont déterminés par les relations :

$$\begin{cases} a+c = 0 \\ b+d-2a\cos\beta-2c\cos\beta = 0 \\ a+c-2B\cos\beta-2d\cos\alpha = 0 \\ b+d = 1 \end{cases}$$

Le système est simple à résoudre et on trouve :

$$f(x) = \frac{1}{2(\cos\alpha-\cos\beta)}\left(\frac{-x+2\cos\alpha}{x^2-2x\cos\alpha+1} + \frac{x-2\cos\beta}{x^2-2x\cos\beta+1}\right).$$

En général cette méthode aboutit à des calculs assez compliqués.

Pour cette méthode comme pour les suivantes des simplifications peuvent parfois être apportées en utilisant certaines propriétés de la fonction rationnelle f. Par exemple si $f = \frac{P}{Q}$ est une fonction paire, si A est sa partie entière, on a :

$$f(x) = A(x)+g(x) = f(-x) = A(-x)+g(-x).$$

Donc A et g sont paires. Si α est un pôle de f d'ordre r, $-\alpha$ est aussi un pôle d'ordre r. Si on fait la somme des parties polaires relatives à α et $-\alpha$ on arrive à :

$$\sum_{k=1}^{r} \left(\frac{a_k}{(x-\alpha)^k} + \frac{b_k}{(x+\alpha)^k} \right).$$

Cette quantité est invariante par la substitution de x à -x ce qui donne $b_k = (-1)^k a_k$.

De la même manière et avec les mêmes notations, si f est <u>impaire</u>, on doit avoir $b_k = (-1)^{k-1} a_k$.

Si f est à <u>coefficients réels</u> et qu'on la décompose sur $\mathbb{C}$, au pôle α est associé le pôle $\bar{\alpha}$ et, avec les notations analogues, $b_k = \bar{a}_k$.

<u>Exercice 1</u> : Décomposer sur $\mathbb{R}$ la fraction rationnelle $\frac{x^2+2}{x^4+1}$.
(Remarquer que cette fraction est paire et utiliser $x^4+1 = (x^2+1)^2-2x^2$).

<u>Recherche de la partie entière</u>

Cela se fait simplement en divisant le numérateur par le dénominateur comme il résulte du théorème 2.

Avant d'aborder la pratique de la décomposition, nous établissons un résultat qui nous sera utile chaque fois que l'on aura à déterminer la partie polaire d'une fraction rationnelle relative à un pôle (c'est-à-dire à un dénominateur de la forme $(X-a)^2$).

<u>Proposition</u> (Division des polynômes selon les puissances croissantes)

Soient n un entier naturel, A et B deux polynômes de K[X]. On suppose B(0) ≠ 0. Il existe un couple Q,R et un seul de polynômes de K[X] tels que $A = BQ+X^{n+1}R$ *avec* $Q = 0$ *ou* $d^\circ Q \leq n$.

On dit que l'on a divisé le polynôme A par le polynôme B suivant les puissances croissantes de X. Q est le quotient à l'ordre n et $X^{n+1}R$ *le reste à l'ordre n.*

Remarque : Dans la division euclidienne de A par B on cherchait un polynôme Q tel que le degré de $A-BQ$ soit aussi petit que possible. Dans la division selon les puissances croissantes on cherche à rendre la valuation de $A-BQ$ supérieure à un nombre n donné à l'avance. (Rappelons que la valuation du polynôme $P(X) = a_n X^n+\ldots+a_1 X+a_0$, notée $\omega(P)$, est le plus petit des indices k tels que $a_k \neq 0$ - cf 3ème Partie, exercice 3). Notons aussi que la division euclidienne est parfois appelée division selon les puissances décroissantes.

Si $A = 0$ ou si $\omega(A) > n$, on pose $A = X^{n+1}R$ et le couple (Q,R) avec $Q = 0$ répond à la question. Posons $A = \sum_{k=o}^{p} a_k X^k$ et $B = \sum_{k=o}^{q} b_k X^k$. Par hypothèse on a $b \neq 0$. Nous démontrons le résultat par récurrence sur n.

Pour $n = 0$, on prend $Q_0 = \frac{a_0}{b_0}$ et $R_0 = \frac{A-BQ_0}{X}$. Le couple (Q_0,R_0) répond à la question avec $n = 0$. Supposons que nous ayons trouvé Q_n et R_n tels que :

$$A = BQ_n+X^{n+1}R_n \quad \text{et} \quad d^\circ Q_n \leq n.$$

En appliquant le résultat pour $n = 0$ au polynôme R_n on a : $R_n = \alpha B+XS$ et en reportant dans l'égalité précédente :

$$A = BQ_n+\alpha X^{n+1}B+X^{n+2}S.$$

On prend alors $Q_{n+1} = Q_n+\alpha X^{n+1}$ et $R_{n+1} = S$ et on a une solution.

L'unicité de la solution est claire : si on a $A = BQ+X^{n+1}R = BQ'+X^{n+1}R'$, par différence on trouve $B(Q-Q')+X^{n+1}(R-R') = 0$. Comme $B(0) \neq 0$, le polynôme X^{n+1} est premier avec B donc X^{n+1} divise $Q-Q4$. Mais $d^\circ Q$ et $d^\circ Q'$ sont majorés par n donc $Q = Q'$ et par suite $R = R'$.

Pratiquement la disposition d'un calcul de division suivant les puissances croissantes suit le raisonnement ci-dessus. Il est d'ailleurs analogue à un calcul de division euclidienne, sauf que les polynômes sont ordonnés selon les puissances croissantes :

$$
\begin{array}{l|l}
1+2X \quad +X^3 & 1+X+2X^2 \\
\underline{-(1+X+2X^2)\qquad\qquad} & \hline 1+X-3X^2 \\
X-2X^2 \ +X^3 & \\
\underline{-(X+X^2 \ +2X^3)} & \\
-3X^2 \ -X^3 & \\
\underline{-(-3X^2-3X^3-6X^4)} & \\
2X^3+6X^4 &
\end{array}
$$

On a ici calculé le quotient et le reste à l'ordre 2 de $1+2X+X^3$ par $1+X+2X^2$.

Dans la décomposition en éléments simples sur $\mathbb{R}$ on a deux types de parties polaires : les unes sont relatives à des dénominateurs de la forme $(x-a)^r$, les autres à des dénominateurs de la forme $(x^2+ax+b)^r$ où x^2+ax+b est irréductible. Les premières sont somme de fractions $\frac{b}{(x-a)^k}$ qui sont les éléments simples de <u>première espèce</u>. Les autres donnent naissance aux éléments simples de <u>seconde espèce</u> qui sont de la forme $\frac{cx+d}{(x^2+ax+b)^k}$ ... Sur $\mathbb{C}$ on conserve cette terminologie (tous les éléments sont donc de première espèce).

<u>Détermination des éléments simples de première espèce</u>

Soit $f = \frac{P}{Q}$ une fraction rationnelle appartenant à $\mathbb{C}(X)$ ou $\mathbb{R}(X)$. Désignons par a un pôle d'ordre r de f et posons $Q(x) = (x-a)^r S(x)$. En posant $y = x-a$ on a $P(x) = P(y+a) = R(y)$ et $S(x) = S(y+a) = T(y)$. La fraction rationnelle initiale s'écrit $g(y) = \frac{R(y)}{y^r T(y)}$. En divisant R par T suivant les puissances croissantes à l'ordre $r-1$ on a :

$$R(y) = (b_r+b_{r-1}y+\ldots+b_2y^{r-2}+b_1y^{r-1})T(y)+y^rU(y).$$

Donc : $$g(y) = \frac{R(y)}{y^rT(y)} = \frac{b_r}{y^r}+\ldots+\frac{b_1}{y}+\frac{U(y)}{T(y)}.$$

La substitution de $x-a$ à y donnera la partie polaire de f par rapport à $(x-a)$.

<u>Remarque</u> : Lorsqu'on détermine le quotient à l'ordre $r-1$ de la division de R par T, seuls les termes de degré plus petit que $r-1$ de T interviennent : on fait donc une économie d'écriture en négligeant les autres

(qui bien entendu sont utiles pour calculer le reste).

Exemple 2 : Décomposer sur $\mathbb{C}$ la fraction rationnelle $\frac{1}{(x^2+x+1)^2}$.

La partie entière est 0. Les racines du dénominateur sont $j = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$ et $\bar{j}$. La partie polaire relative à j est de la forme $\frac{a}{(x-j)^2} + \frac{b}{(x-j)}$.

En posant $y = x-j$ la fraction rationnelle devient :

$$\frac{1}{(x^2+x+1)^2} = \frac{1}{(x-j)^2(x-\bar{j})^2} = \frac{1}{y^2(j-\bar{j}+y)^2}$$

Avec les notations précédentes on a : $R = 1$ et $T = (j-\bar{j})^2+2y(j-\bar{j})+y^2$ et compte tenu de la remarque on doit diviser 1 par $-3+2yi\sqrt{3}$ à l'ordre 1. Le quotient est $-\frac{1}{3} - \frac{2}{9} iy\sqrt{3}$. Donc la partie polaire relative à j est $-\frac{1}{3(x-j)^2} - \frac{2i\sqrt{3}}{9(x-j)}$. D'autre part j et $\bar{j}$ sont conjugués donc les coefficients correspondants des éléments simples le seront aussi. Par suite :

$$\frac{1}{(x^2+x+1)^2} = -\frac{1}{3(x-j)^2} - \frac{2i\sqrt{3}}{9(x-j)} - \frac{1}{3(x-\bar{j})^2} + \frac{2i\sqrt{3}}{9(x-\bar{j})}$$

Calcul direct de b_r

Avec les notations ci-dessus on a :

$$\frac{P(x)}{Q(x)} = \frac{P(x)}{(x-a)^r S(x)} = \frac{b_r}{(x-a)^r} + \ldots + \frac{b_1}{(x-a)} + g(x)$$

où a n'est pas un pôle de g. En multipliant par $(x-a)^r$ les deux membres de cette égalité et en faisant $x = a$, on trouve :

$$b_r = \frac{P(a)}{S(a)} \quad \text{ou encore} \quad b_r = \lim_{x \to a} \frac{(x-a)^r P(x)}{Q(x)}$$

(la deuxième forme est supérieure à la première en ce sens que la connaissance de S est superflue).

En particulier sur $\mathbb{R}$ si a est un pôle simple on a :

$$b = \lim_{x \to a} \frac{P(x)}{\frac{Q(x)}{(x-a)}} = \frac{P(a)}{Q'(a)}, \quad Q' \text{ étant le polynôme dérivé de } Q.$$

On pourra utiliser cette formule sur $\mathbb{C}$ (le polynôme dérivé de $a_k x^k + \ldots + a_0$ étant bien entendu $k\,a_k x^{k-1} + \ldots + 2a_2 x + a_1$) : cela sera justifié plus tard.

Exercice 2 : Décomposer sur $\mathbb{R}$ la fraction $\dfrac{x^4+x+1}{x(x-1)(x-2)}$.

Exercice 3 : Décomposer sur $\mathbb{R}$ la fraction $\dfrac{x^4+1}{(x^2-1)^3}$ (utiliser la parité).

Exercice 4 : Décomposer sur $\mathbb{R}$ la fraction $\dfrac{1}{x^n(1-x)}$.

Détermination des éléments simples de seconde espèce

Si la fraction rationnelle n'admet que deux pôles complexes conjugués on procède comme dans la partie c) de la démonstration du théorème 2.

Exemple 3 :

Ainsi, soit à décomposer $\dfrac{2x^5+3x^2-1}{(x^2+x+1)^3} = \dfrac{P(x)}{Q(x)}$.

On divise $P(x)$ par x^2+x+1 (division euclidienne) :

$$P(x) = (x^2+x+1)(2x^3-2x^2+5)+(-5x-6).$$

Donc : $$\frac{P(x)}{Q(x)} = \frac{2x^3-2x^2+5}{(x^2+x+1)^2} - \frac{5x+6}{(x^2+x+1)^3}.$$

Puis on divise $2x^3-2x^2+5$ par x^2+x+1 :

$$2x^3-2x^2+5 = (x^2+x+1)(2x-4)+2x+9.$$

D'où : $$\frac{P(x)}{Q(x)} = \frac{2x-4}{x^2+x+1} + \frac{2x+9}{(x^2+x+1)^2} - \frac{5x+6}{(x^2+x+1)^3}.$$

Si on n'est pas dans ce cas, on détermine les éléments simples de proche en proche comme dans l'exemple ci-dessous.

Exemple 4 :

Soit à décomposer $\dfrac{P(x)}{Q(x)} = \dfrac{x^2+1}{(x-1)^2(x^2-x+1)^2}$. Le résultat général nous indique qu'il existe a,b tels que :

$$\frac{P(x)}{Q(x)} - \frac{ax+b}{(x^2-x+1)^2} = \frac{R(x)}{(x-1)^2(x^2-x+1)}$$

ou encore :

$$x^2+1-(ax+b)(x-1)^2 = R(x)(x^2-x+1).$$

Dans cette relation on remplace x successivement par α et $\bar{\alpha}$, racines de x^2-x+1 (en remarquant que $\alpha^2 = \alpha-1$) ce qui donne

$$(a+b+1)\alpha-a = 0$$
$$(a+b+1)\bar{\alpha}-a = 0$$

Comme a et b sont réels cela donne $a = 0$ et $b = -1$.

On en déduit que $R(x) = 2$ (en portant ces valeurs de a et b dans $\frac{P(x)}{Q(x)} - \frac{ax+b}{(x^2+x+1)^2}$). Donc :

$$\frac{P(x)}{Q(x)} = \frac{-1}{(x^2-x+1)^2} + \frac{2}{(x-1)^2(x^2-x+1)}$$

On détermine alors c et d tels que :

$$\frac{2}{(x-1)^2(x^2-x+1)} - \frac{cx+d}{x^2-x+1} = \frac{S(x)}{(x-1)^2}.$$

Par la même méthode, on trouve $c = 2$, $d = -2$ et on en déduit $S(x) = -2x+4$. Donc :

$$\frac{P(x)}{Q(x)} = \frac{-1}{(x^2-x+1)^2} + \frac{2x-2}{(x^2-x+1)} + \frac{-2x+4}{(x-1)^2}$$

Et finalement (en posant $-2x+4 = -2(x-1)+2$) :

$$\frac{P(x)}{Q(x)} = \frac{-1}{(x^2-x+1)^2} + \frac{2x-2}{(x^2-x+1)} + \frac{2}{(x-1)^2} - \frac{2}{x-1}$$

On peut aussi remarquer que si $(x^2+ax+b)^r$ est un facteur irréductible du dénominateur, si α et $\bar{\alpha}$ sont les racines complexes de x^2+ax+b, la partie polaire de la fraction rationnelle relative à $(x^2+ax+b)^r$ (dans une décomposition sur $\mathbb{R}$) et la somme des parties polaires relatives à

$(x-\alpha)^r$ et $(x-\bar{\alpha})^r$ (dans une décomposition sur $\mathbb{C}$). D'où : on décompose $\frac{P}{Q}$ dans $\mathbb{C}(X)$ puis on regroupe les parties polaires associées à des pôles conjugués.

Exemple 5 :

Décomposer sur $\mathbb{R}$ la fraction $\frac{1}{x^7-1}$.

Les racines complexes non réelles du dénominateur sont $\alpha_1, \alpha_2, \alpha_3$ et leur conjugués avec $\alpha_k = e^{\frac{2i\pi k}{7}}$.

Sur $\mathbb{C}$ on a :

$$\frac{1}{x^7-1} = \frac{a}{x-1} + \sum_{k=1}^{3} \left(\frac{b_k}{x-\alpha_k} + \frac{\overline{b_k}}{x-\overline{\alpha_k}} \right).$$

Les numérateurs sont donnés par les formules $b_k = \frac{1}{7\alpha_k}$ (c'est-à-dire $\frac{P(a)}{Q'(a)}$) et les formules analogues.

D'où :

$$\frac{1}{x^7-1} = \frac{1}{7(x-1)} + \frac{1}{7} \sum_{k=1}^{3} \left(\frac{\alpha_k}{x-\alpha_k} + \frac{\overline{\alpha_k}}{x-\overline{\alpha_k}} \right)$$

En regroupant les termes conjugués on arrive à :

$$\frac{1}{x^7-1} = \frac{1}{7(x-1)} + \frac{2}{7} \sum_{k=1}^{3} \frac{x \cos \frac{2k\pi}{7} - 1}{x^2 - 2x \cos \frac{2k\pi}{7} + 1}$$

Exercice 5 : Décomposer en éléments simples sur $\mathbb{C}$ la fraction $f(x) = \frac{2x^4+1}{(x-1)^3(x^2+1)}$. Indications : on sait que

$$f(x) = \frac{a_3}{(x-1)^3} + \frac{a_2}{(x-1)^2} + \frac{a_1}{x-1} + \frac{b}{x-i} + \frac{c}{x+i}.$$

On remarque que $c = \bar{b}$. En multipliant les 2 membres de l'égalité par x et en faisant tendre x vers l'infini, on a $2 = a + b + \bar{b}$. On calcule ensuite a_3 et b comme indiqué plus haut.

Exercice 6 : Décomposer sur $\mathbb{C}$ la fonction $\frac{1}{x^4+1}$.

Exercice 7 : Décomposer $\frac{x^2+1}{x(x-1)^4(x^2-2)^2}$ sur $\mathbb{R}$.

Exercice 8 : Décomposer $\frac{1}{(x+1)^3(x^2+x+1)^2}$ sur $\mathbb{R}$.

Exercice 9 : Décomposer $\frac{8}{(x^2-1)(x^2+1)^2}$ sur $\mathbb{R}$.

Exercices : Résultats

1) $\frac{x^2+2}{x^4+1} = \frac{1}{2\sqrt{2}}\left(\frac{x+2\sqrt{2}}{x^2+x\sqrt{2}+1} + \frac{-x+2\sqrt{2}}{x^2-x\sqrt{2}+1}\right)$.

2) $\frac{x^4+x+1}{x(x-1)(x-2)} = x+3+\frac{1}{2x} - \frac{3}{x-1} + \frac{19}{2(x-2)}$.

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

4) $\frac{1}{x^n(1-x)} = \frac{1}{1-x} + \frac{1}{x^n} + \frac{1}{x^{n-1}} + \ldots + \frac{1}{x}$.

5) $a_3 = \frac{3}{2}$, $a_2 = \frac{3}{4}$, $a_1 = \frac{11}{4}$, $b = -\frac{3}{8}(1+i)$, $c = \bar{b}$.

6) Avec $\alpha_k = e^{\frac{i\pi}{4} + k\frac{\pi}{2}}$ $(k = 0,1,2,3)$ on a $\frac{1}{x^4+1} = \sum_{k=0}^{3} \frac{b_k}{x-\alpha_k}$ avec $b_k = -\frac{\alpha_k}{4}$.

7) La fraction s'écrit $\frac{a}{x} + \frac{b_4}{(x-1)^4} + \frac{b_3}{(x-1)^3} + \frac{b_2}{(x-1)^2} + \frac{b_1}{x-1} + \frac{c_2}{(x-\sqrt{2})^2} +$

$$+ \frac{c_1}{x-\sqrt{2}} + \frac{d_2}{(x+\sqrt{2})^2} + \frac{d_1}{x+\sqrt{2}}$$

avec $a = \frac{1}{4}$, $b_4 = 2$, $b_3 = 8$, $b_2 = 29$, $b_1 = 91$, $c_2 = \frac{3}{16}(24+17\sqrt{2})$,

$c_1 = -\frac{1}{8}(365+258\sqrt{2})$, $d_2 = \frac{3}{16}(24-17\sqrt{2})$, $d_1 = -\frac{1}{8}(365-258\sqrt{2})$.

(d_2 et d_1 sont déduits de c_2 et c_1 en remplaçant $\sqrt{2}$ par $-\sqrt{2}$).

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

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

(on peut écrire a priori que les numérateurs des éléments simples de seconde espèce sont des constantes à cause de la parité de la fraction rationnelle).

APPENDICE : PETIT VOCABULAIRE ALGÉBRIQUE

Groupes

- Un groupe G est un ensemble muni d'une opération (notée souvent comme une multiplication) vérifiant :

  - $\forall x,y,z \in G$, $(xy)z = x(yz)$ (Associativité)
  - $\exists e \in G$, $\forall x \in G$, $xe = ex = x$ (e est l'élément neutre de G)
  - $\forall x \in G$, $\exists y \in G$, $xy = yx = e$ (y est l'élément symétrique de x. On le note en général x^{-1}. Si l'opération de G est notée additivement le symétrique de x est noté $-x$ et dans ce cas on note 0 l'élément neutre).
  - De plus si $\forall x,y \in G$, $xy = yx$, G est dit commutatif ou abélien.

- Quelques exemples : $\mathbb{Z}$ muni de l'addition, $\mathbb{Q}$ muni de l'addition, $\mathbb{R}-\{0\}$ muni de la multiplication, les nombres complexes de module 1 munis de la multiplication, les matrices carrées inversibles d'ordre n à coefficients réels, l'ensemble des bijections d'un ensemble sur lui-même (et en particulier les permutations d'un ensemble fini) avec la composition des applications. Les deux derniers exemples sont des groupes non abéliens.

- Un sous-groupe H d'un groupe G est une partie non vide de G telle que l'opération de G restreinte à H fait de H un groupe : c'est-à-dire que $x,y \in H$ on a $xy \in H$ et $x^{-1} \in H$.

Anneaux

- Un anneau A est un ensemble muni de 2 opérations notées usuellement $+$ et $\times$ telles que :

  - A muni de $+$ est un groupe abélien (on note 0 son élément neutre).
  - $\forall x,y,z$: $x(yz) = (xy)z$ (Associativité)
    $x(y+z) = xy+xz$ (Distributivité de la multiplication par rapport à l'addition).

• Très souvent il existe un élément neutre pour la multiplication. Il est usuellement noté 1 et vérifie donc : $\forall x,\ 1x = x1 = x$. On dit dans ce cas que A est un anneau unitaire.

Si de plus la multiplicité de A est commutative ($\forall x,y,\ xy = yx$) on dit que A est commutatif.

- Exemples : $\mathbb{Z}$, $\mathbb{R}[X]$, les endomorphismes d'un espace vectoriel. Ces anneaux sont unitaires, le dernier est non commutatif.

- Un sous-anneau B de A est une partie de A telle que la restriction à B des opérations de A fait de B un anneau. Notons que A peut être unitaire sans que B le soit : ainsi l'ensemble des entiers pairs est un sous-anneau non unitaire de $\mathbb{Z}$.

- Un idéal I de A est une partie de A qui est un sous-groupe pour l'addition et qui vérifie :

$$\forall x \in I,\ \forall y \in A,\ xy \in I.$$

(En particulier si $y \in I$, $xy \in I$ donc I est un sous-anneau).

Corps

- Un corps K est un anneau unitaire dans lequel tout élément différent de 0 est inversible pour la multiplication. (c'est-à-dire que si $x \neq 0$, il existe x^{-1} vérifiant $xx^{-1} = x^{-1}x = 1$).

- Exemples : • $\mathbb{R}$, $\mathbb{C}(X)$, $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

• Désignons par 1,i,j,k une base de l'espace vectoriel $\mathbb{R}$. On définit les produits 2 à 2 des éléments de cette base par : $1^2 = 1$, $1i = i1 = i$, $1j = j1 = j$, $1k = k1 = k$, $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$.
Tout élément de $\mathbb{R}^4$ s'écrit $\alpha 1+\beta i+\gamma j+\delta k$ ($\alpha,\beta,\gamma,\delta \in \mathbb{R}$).
On prolonge la multiplication définie sur la base (1,i,j,k) à $\mathbb{R}^4$ tout entier en utilisant associativité et distributivité (de même que l'on a procédé pour construire $\mathbb{C}$).

Ainsi $ji = (ki)i = ki^2 = k(-1)$ et d'autre part $k(1)+k(-1) = k(1-1) = 0$ donc $k(-1) = -k$ et finalement $ji = -k$. On obtient ainsi un corps H, non commutatif, appelé corps des quaternions.

Morphismes

Si E et F sont deux ensembles munis d'une même structure algébrique (deux groupes sur deux anneaux ...), un morphisme f de E dans F est une application qui "conserve" la structure : par exemple si E et F sont des groupes, f vérifie $f(xy) = f(x)f(y)$ $\forall x,y \in E$. Si E et F sont des anneaux f vérifie $f(xy) = f(x)f(y)$ et $f(x+y) = f(x)+f(y)$.

On vérifie facilement que si E et F sont des groupes dont les éléments neutres sont e_1 et e_2 et si f est un morphisme, $f(e_1) = e_2$ et $f(x^{-1}) = (f(x))^{-1}$. (Par contre si E et F sont des anneaux unitaires à éléments unités 1_E et 1_F il n'est pas nécessaire que $f(1_E) = 1_F$).

Un morphisme est aussi appelé homomorphisme. Si f est un morphisme et est bijective, c'est un isomorphisme. Si $E = F$, si f est un morphisme on dit que c'est un endomorphisme et si f est bijective, c'est un automorphisme.

Relations

Rappelons qu'une relation R sur un ensemble E est une relation d'équivalence si elle vérifie :

- xRx $\quad \forall x \in E$ (Réflexivité)
- $xRy \Rightarrow yRx$ $\quad \forall x,y \in E$ (Symétrie)
- xRy et $yRz \Rightarrow xRz$ $\quad \forall x,y,z \in E$ (Transitivité).

Une relation d'ordre vérifie :

- xRx
- xRy et $yRx \Rightarrow x = y$ (antisymétrie)
- xRy et $yRz \Rightarrow xRz$.

INDEX

Affixe d'un point 48
Algorithme d'Euclide ... 13
Anneau 103
Anneau quadratique 38
Anneau unitaire 104
Argument 49
Arrangement 2
Automorphisme 105
Bezout (Théorème de) ... 11
" " ... 77
Binôme (Formule du) 68
Chinois (Théorème) 33
Classe modulo n 23
Combinaison 3
Congruence 23
Conjugué 46
Corps 104
Crible d'Eratosthène ... 8
Degré d'un polynôme 67
De Moivre (Formule de) . 53
Division euclidienne ... 1
Elément simple de 1ère espèce ... 96
Elément simple de 2ème espèce ... 96
Endomorphisme 105
Equivalence (Relation d') 105
Entier de Gauss 40
Entier naturel 1
Entier rationnel 1
Entier relatif 1
Euclide (Lemme d') 12
Euler (Formules d') 30
Fermat (petit théorème de) 29
Fermat (Grand théorème de) .. 35
Fonction polynomiale 64
Groupe abélien, commutatif . 103
Idéal 104
Idéal de $\mathbb{Z}$ 9
Image d'un nombre complexe . 48
Isomorphisme 105
Module 46
Morphisme 105
Multiplicité d'une racine .. 81
Nombres premiers 6
N ombres premiers entre eux 11
Ordre (Relation d') 105
Partie polaire 91
Pascal (Triangle de) 4
Permutation 2
PGCD de deux entiers 9
PGCD de deux polynômes 76
Pôle 90
Polynôme 66
Polynôme irréductible 75
Polynômes premiers entre eux 77
PPCM de deux entiers 19
Racine d'un polynôme 80
Représentation cartésienne d'un complexe 46
Représentation algébrique d'un complexe 46
Résidu modulo n 23
Sous-anneau 104
Sous-groupe 103
Système de représentants modulo n 24
Unité dans un anneau 38
Valuation d'un polynôme 68