PROGRAMME du C.M ALGEBRE L1 SEMESTRE 1.

Dr ASSANE

Contenu du cours :

ECU E1
I- Ensembles et Applications
II- Relations Binaires
III-groupes, Anneaux, Corps

ECUE2
IV-Arithmétique dans Z
V- Polynômes sur IR et sur $\mathbb{C}$
VI- Décomposition en éléments simples sur IR et sur $\mathbb{C}$

CHAPITRE 1 ENSEMBLES ET APPLICATIONS

A) ENSEMBLES

1. Définitions

un ensemble peut se définir comme un groupement d'objets déterminés et bien distincts, de notre perception ou de notre entendement, et que l'on appelle les éléments de l'ensemble.

Dans la pratique il y a deux façons de construire ou d'écrire des ensembles :

- en donnant la liste de ses éléments (l'extension) exemple $\mathrm{E} = \{0, 1, 2, 3, 5, 7, 8\}$

-en décrivant une caractérisation des éléments (la compréhension) exemple : $\mathbb{Q} = \left\{ \frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{Z}^* \right\}$

Le nombre d'éléments d'un ensemble E est appelé cardinal de E et se note : card(E)

si card(E)=0, on dit que E est l'ensemble vide noté : $\{\}$ ou $\varnothing$.

2.**Opérations usuelles sur les ensembles**

2.1 **Inclusion** ($\subset$)

On dit qu'un ensemble E est inclus dans un autre ensemble F (ce qu'on note E$\subset$ F),

si tous les éléments de E sont aussi dans F ; en d'autres termes si $x \in E \Longrightarrow x \in F$.

Deux ensembles sont égaux si ils ont les memes éléments ;

en particulier : E$\subset$F et F$\subset$E $\Longleftrightarrow$ E=F

Si E est inclu dans F, on dit que E est un sous ensemble (ou une partie) de F. L'ensemble des sous-ensembles d'un esemble E appelé aussi ensemble des parties de E se note $\mathcal{P}$ (E)=$\{$F,F $\subset$ E $\}$

On montre que card($\mathcal{P}$ (E))=$2^{\mathrm{card(E)}}$

exemple écrire $\mathcal{P}$ (E) si E=$\{0,1\}$

2.2 Complémentaire :

+Soit F un sous-ensemble de E ; on définit le complémentaire de F dans E que l'on note $\complement_E F$ (ou simplement $\complement F$ si E est sous-entendu) comme l'ensemble des éléments de E qui n'appartiennent pas) à F :

$\complement_E F=\{x \in E, x \notin F\}$ exemple : E=$\{0,1,2,3,4,5,6,7,8\}$ F=$\{0,1\}$,donner $\complement_E F=\{2,3,4,5,6,7,8\}$

remarque card$\complement_E F$ +cardF=cardE

Si F n'est plus nécessairement un sous-ensemble de E on emploiera la notation : E \ F

pour désigner $\{x \in E, x \notin F\}$.

2.3 Intersection :

si E et F sont deux ensembles on peut former un ensemble appelé leur intersection notée E ∩ F et définie par $\{x, x \in E$ et $x \in F\}$

exemple :i) E=$\mathbb{N}$, F=$\mathbb{Z}$ alors E ∩ F=$\{n \in \mathbb{Z}, n \geq 0\}$

ii) E=$\{\Delta, \Omega, \Gamma, a, b, 1, 2\}$, F=$\{\Delta, \alpha, \Gamma, 0, b, \beta, 2\}$

E ∩ F=$\{\Delta, \Gamma, b, 2\}$ ⊂E et E ∩ F⊂F

Exercice

determiner E ∩ F dans le cas :

E=$\left\{x \in \mathbb{R}, x^2 \geq 1\right\}$ F=$\{x, 2x-4 \geq 2\}$

2.4 Union :

si E et F sont deux ensembles on peut former un ensemble appelé leur union et notée E ∪ F et définie par : $\{x, x \in E$ ou $x \in F\}$

Exemple E=$\{\Delta, \Omega, \Gamma, a, b, 1, 2\}$, F=$\{\Delta, \alpha, \Gamma, 0, b, \beta, 2\}$

E ∪ F=$\{\Delta, \Omega, \Gamma, a, b, 1, 2, \alpha, 0, \beta\}$

E⊂E ∪ F et F⊂E ∪ F

card(E ∪ F)=cardE+cardF-card(E ∩F)

2.5 Produit cartésien :

Si x ∈ E et y ∈ F on peut fabriquer un nouvel élément appelé couple et note (x, y), caractérisé par le fait que

(x, y) = (z, t) si et seulement si x = z et y = t.

L'ensemble de ces couples s'appelle le produit (cartésien) de E et F et se note :

E×F=$\{(x,y), x \in E, y \in F\}$

Exemple : E=$\{a,b\}$ F=$\{1,2,3\}$

E×F=$\{(a,1),(a,2),(a,3),(b,1),(b,2),(b,3)\}$

card(E×F)=cardE×cardF

exercice

écrire $\emptyset \times \mathcal{P}(\emptyset)$ puis $\mathcal{P}(\mathcal{P}(\emptyset)) \times \mathcal{P}(\emptyset)$

Propriétés

A,B,C, . . . sont des ensembles

1) $A \cap B = B \cap A$ et $A \cup B = B \cup A$ (commutativité)

2)$A \cap (B \cap C) = (A \cap B) \cap C$ et

$A \cup (B \cup C) = (A \cup B) \cup C$ (associativité)

3) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (distributivité de l'intersection par rapport à la réunion)

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (distributivité de $\cup$ sur $\cap$)

4) $\complement_E(\complement_E A) = A$, $A \subset B \Longrightarrow \complement_E B \subset \complement_E A$

5) $\complement_E(A \cup B) = \complement_E A \cap \complement_E B$, $\complement_E(A \cap B) = \complement_E A \cup \complement_E B$ (loi de Morgan)

B.**APPLICATIONS**

1.Définition:

Une application (ou fonction) définie sur X et à valeurs dans Y est une loi

qui, à tout élément de X fait correspondre un unique élément de Y . Si on note f cette

application, l'élément associé à x par f est noté f(x). L'ensemble X s'appelle l'ensemble

de départ, l'ensemble Y s'appelle l'ensemble d'arrivé de f. On note souvent une fonction

f : X $\longrightarrow$ Y ou, si les ensembles X et Y sont sous-entendus x $\longmapsto$ f(x). L'élément f(x) = y

s'appelle l'image de x par f et x s'appelle un antécédent de y par f.

Le graphe d'une fonction f est l'ensemble des couples (x, f(x)) pour x $\in$ X.

2.Composition des applications :

Si f : X $\longrightarrow$ Y et g : Y $\longrightarrow$ Z sont deux applications, on peut définir la composée de f et g

par (go f)(x) = g(f(x)). Une propriété importante de la composition des applications est l'associativité :

C'est-'a-dire que si

h : X $\longrightarrow$ Y , g : Y $\longrightarrow$ Z et f : Z $\longrightarrow$ W sont trois applications, alors (fo g)o h = fo (go h)

(que l'on note donc simplement fo go h).

exemple : soit f(x)=$x^2 - 1$ g(x)=2x+4 de $\mathbb{R} \longrightarrow \mathbb{R}$

determiner fog et gof

fog(x)=f(g(x))=f(2x+4)=$(2x+4)^2 - 1 = 4x^2 + 16x + 15$

gof(x)=g(f(x))=g($x^2 - 1$)=$2\left(x^2 - 1\right) + 4 = 2x^2 + 2$

remarque fog$\neq$gof (pas de commutativité)

3.Définition (injection):

Une application f : X $\longrightarrow$ Y est injective si

(pour tout x, x' $\in$ X) l'égalité f(x) = f(x')$\Longrightarrow$ x = x'. En d'autres termes tout élément de Y a au plus un antécédent

ou encore est l'image d'au plus un élément de X.

exemple : $f(x)=x^2$

i)f est-elle injective de $\mathbb{R} \longrightarrow \mathbb{R}$?

ii)f est-elle injective de $[0,+\infty[\longrightarrow \mathbb{R}$?

4.Définition (surjection):

Une application f : X $\longrightarrow$ Y est surjective si,

pour tout y $\in$ Y, il existe x $\in$ X tel que y = f(x).

En d'autres termes tout élément de Y a au moins un antécédent.

exemple $f(x)=x^2$

i)f est-elle surjective de $\mathbb{R} \longrightarrow \mathbb{R}$?

ii)f est-elle surjective de $\mathbb{R} \longrightarrow [0,+\infty[$?

5.Définition (bijection):

Une application f : X $\longrightarrow$ Y est bijective si elle est à la fois injective et surjective.

En d'autres termes tout élément de Y a exactement un antécédent.

6.Définition (bijection réciproque):

On appelle bijection réciproque d'une bijection

f : X $\longrightarrow$ Y et on note f^{-1} : Y $\longrightarrow$ X l'application

caractérisée par : x = f^{-1}(y) $\iff$ y = f(x). Il est clair que f^{-1} est aussi une bijection.

exemple : $f(x)=\frac{2x+1}{x^2+1}$

i) f est -elle bijective de $\mathbb{R} \longrightarrow \mathbb{R}$?

ii) determiner deux parties A et B de telles que f soit bijective de A vers B et préciser sa bijection réciproque.

7.Définition(image directe-image réciproque)

i : Soit f : E $\longrightarrow$ F une application.

i) Si A est une partie de E on appelle image directe de A par f et on note f(A)

l'ensemble :

$f(A) = \{y \in F, \exists x \in A, f(x) = y\} = \{f(x), x \in A\}$

ii)Si B est une partie de F on appelle image réciproque de B par f et on note f^{-1}(B)

l'ensemble : $f^{-1}(B) = \{x \in E, f(x) \in B\}$

8.PROPOSITION:

Soit f : E $\longrightarrow$ F une application, on a les formules suivantes

(i) Pour toutes parties A,B de E
f(A $\cup$ B) =f(A) $\cup$ f(B) , A$\subset$ B $\Longrightarrow$ f(A)$\subset$ f(B) et
f(A $\cap$ B) $\subset$f(A) $\cap$ f(B)

Exemple : f(x)=$|x|$
A=$[-1, 0[$, B=$[0, 1]$
f(A)=$]0, 1]$ f(B)=
1(ii) Pour toutes parties A,B de F, on a f^{-1}(A$\cup$B) = f^{-1}(A)$\cup$$f^{-1}$(B) ,

f^{-1}(A$\cap$B) =f^{-1}(A) $\cap$ f^{-1}(B) ,
A$\subset$ B $\Longrightarrow$ f^{-1}(A)$\subset$ f^{-1}(B) et également $f^{-1}(\complement_F$ A) = $\complement_E f^{-1}$(A)

CHAPITRE II : **RELATION D'ORDRE ET RELATION D'EQUIVALENCE**

I) RELATION D'ORDRE

1.**Définitions**

i)Une relation(binaire) $\mathcal{R}$ sur un ensemble E est un énoncé $\mathcal{R}$(x, y) (ou x$\mathcal{R}$y) à deux variables x,y : si

si la relation est vraie pour deux éléments x et y on dira que x est relié à y par la relation R et on note : $\mathcal{R}$(x, y) (ou x$\mathcal{R}$y).

exemples sur $\mathbb{Z}$,on définit une relation $\mathcal{R}$ par : x$\mathcal{R}$y $\Longleftrightarrow$ $x^2 = y^2$

ii)On appelle graghe d'une relation binaire $\mathcal{R}$ sur un ensemble E l'ensemble noté G/$\mathcal{R}$ $=\{(x; y) \in E \times E, x\mathcal{R}y.\}$

Réciproquement une relation binaire sur un ensemble E, peut etre définie par la donnée d'une partie G de E$\times$E qui est le grahe de cette relation.

2.**Définition**:
Une relation $\mathcal{R}$ sur un ensemble E est dite :
(i) Réflexive si
Pour tout x $\in$ E on a x $\mathcal{R}$ x.
(ii) Transitive si
Pour tout x,y,z $\in$ E : x $\mathcal{R}$ y et y $\mathcal{R}$ z $\Longrightarrow$ x $\mathcal{R}$ z
(iii) symétrique Si
Pour tout x,y $\in$ E : x $\mathcal{R}$ y $\Longrightarrow$ y $\mathcal{R}$ x
(iv) Antisymétrique Si
Pour tout x,y $\in$ E : x $\mathcal{R}$ y et y $\mathcal{R}$ x $\Longrightarrow$ $x = y$

3.**Définition:**
Une relation d'ordre sur un ensemble E est une relation R qui est :
réflexive , transitive et antisymétrique

Exemples : $(\mathbb{R}, \leq), (\mathcal{P}(E), \subset)$
4.**Définition**

un ordre $\mathcal{R}$ sur un ensemble E est dit total (ou encore l'ensemble E est totalement

ordonné) si deux éléments sont toujours comparables i.e. si :

$\forall$x, y $\in$ E, x $\mathcal{R}$ y ou y $\mathcal{R}$ x

5.Définition :

Soit (E,$\leq$) un ensemble ordonné, un élément y de E est le plus grand (respect. le plus petit) élément de E si tous les autres éléments sont plus petits (respect. plus grands), c'est-à-dire

si $\forall$x$\in$ E, x$\leq$ y (respect.$\forall$x$\in$ E, y$\leq$ x)

Exemples :

Le plus petit élément de $\mathbb{N}$ est 0 mais $\mathbb{N}$ n'a pas de plus grand élément.

Considérons la relation d'inclusion sur l'ensemble $\mathcal{P}$(E) ; ce n'est pas un ensemble totalement

ordonné mais il a un plus petit élément : l'ensemble vide ; et un plus grand élément : l'ensemble E.

6.Définition:

Soit F$\subset$ E un sous-ensemble d'un ensemble ordonné (E,$\leq$), un élément M(respect.m) de E est un majorant(respect. un minorant) de F si pour tout x dans F on a x$\leq$ M(respect.m$\leq$ x) Le plus petit des majorants de F(respec.le pus grand des minorants) (s'il existe) s'appelle la borne supérieure(repecct.la borne inférieure) de F (dans E).

Notation : sup(E)=borne supérieure de E, inf(E)= borne inférieure de E

Max(E)=plus grand élément de E, min(E)=plus petit élément de E.

Exemples :

1)Soit $\mathbb{N} \subset \mathbb{R}$, tout nombre réel négatif est un minorant de $\mathbb{N}$ et sa borne inférieure est donc 0 (qui est aussi le plus petit élément de $\mathbb{N}$).

2)Soit E :=$[0, 1[\subset \mathbb{R}$ l'intervalle des nombres réels positifs et strictement plus petits que 1.

Il est clair que 0 est la borne inférieure de E (et son plus petit élément) et que 1

est sa borne supérieure bien que E n'ait pas de plus grand élément.

7.**PROPOSITION** :

Un réel M est la borne supérieure d'un ensemble E$\subset \mathbb{R}$ si et seulement si :

(i) $\forall$x $\in$ E, x$\leq$ M

(ii) $\forall$ ϵ> 0, $\exists$x $\in$ E, M - $\epsilon \leq$ x

Relation d'équivalence.

1.Définition :

Une relation d'équivalence sur un ensemble E est une relation $\mathcal{R}$ qui est :

réflexive , symétrique et transitive.

2.Définition :

i) La classe d'équivalence d'un élément x est l'ensemble des éléments qui lui sont reliés par $\mathcal{R}$:

C(x) = $\{y \in E, xRy\}$

ii) L'ensemble des classes d'équivalence de E pour la relation R s'appelle l'ensemble quotient de E par $\mathcal{R}$ et se note E/$\mathcal{R}$.

3.Théorème.

Soit E un ensemble non vide.

1) Si $\mathcal{R}$ est une relation d'´equivalence sur E, alors les différentes classes d'équivalence forment une partition de E.

E= $\underset{x\in E}{\cup}$ C(x) et C(x)$\cap$C(y)=$\varnothing$ si (x,y)$\notin$G/$\mathcal{R}$

2) Toute partition de E peut s'obtenir de façon unique à partir d'une relation d'équivalence .

CHAPITRE III GROUPES-ANNEAUX-CORPS

I loi de composition

1.1 Définition:

Une loi de composition interne sur un ensemble E est une application notée : $\star$, T,Δ, ...

de E $\times$ E vers E (x,y)$\longmapsto$x$\star$y

1.2 Définition:

Un groupe est la donnée d'un ensemble G et d'une loi de composition interne (x,y)$\longmapsto$x$\star$y

telle que :

(i) $\star$ admet un élément neutre e dans G tel que pour tout x dans G

on a e$\star$ x = x$\star$ e = x.

(ii) $\star$ est associative

Pour tout x, y, z dans G on a : (x$\star$ y)$\star$ z = x$\star$(y$\star$ z).

(iii) tout élément de G admet un symétrique

Pour tout x dans G il existe x' dans G tel que : x$\star$x' = x'$\star$x = e.

Si de plus pour tout x, y dans G on a : x$\star$ y = y $\star$x, on dit que la loi est commutative

et que le groupe (G, $\star$) est commutatif.

Exemples

1)Les ensembles $\mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$ et $\mathbb{C}$, munis de l'addition sont des groupes commutatifs

(noter que (ℕ, +) ne vérifie pas (iii)). Les ensembles $\mathbb{Q}^*$,$\mathbb{R}^*$ et $\mathbb{C}^*$ munis de la mutiplication sont des groupes

(noter que ($\mathbb{Z}^*$,×) ne vérifie pas (iii)).

2) Soit E un ensemble et soit S(E) l'ensemble des bijections de E vers E ; soit o la loi de composition naturelle de deux bijections, alors (S(E), o) est un groupe. En particulier l'ensemble des bijections de $\{1, 2, 3, ..., n\}$ vers lui-même, muni de la composition des applications, forme un groupe qu'on note S_n. C'est un groupe avec n! éléments, on l'appelle le groupe des permutations sur n éléments.

II LE GROUPE Sn.

2.1 Définition

Un élément s de S_n est une permutation de l'ensemble $\{1, 2, 3, ..., n\}$ et est donc défini par la suite

s(1), s(2), s(3), . . . , s(n). L'élément neutre sera noté id. On notera en général une permutation par un

tableau s= $\begin{pmatrix} 1 & 2 & .. & n \\ s(1) & s(2) & .. & s(n) \end{pmatrix}$

$$S_2 = \left\{ id, \tau_{12}^2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$$S_3 = \left\{ \begin{array}{c} id, s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \\ s_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, s_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \end{array} \right\}$$

Le tableau de la loi de groupe de S3 est (complèter) :

o	id	s_1	s_2	s_3	s_4	s_5
id						
s_1						
s_2						
s_3						
s_4						
s_5						

2.2 **Définition :**

Un m-cycle ou cycle de longueur m dans S_n est une permutation s de l'ensemble E := $\{1, ..., n\}$ qui laisse fixes n - m éléments et permute circulairement les autres.

Plus précisément, il existe un sous-ensemble à m éléments I = {i_1, . . . , i_m} de E

tel que : si i ∉ I alors s(i) = i mais s(i_k) = i_{k+1} (pour k = 1, . . . ,m - 1) et s(i_m) = i_1.

L'ensemble I s'appelle le support du cycle.

Une transposition est un cycle de longueur 2.

Nous noterons s = (i_1, . . . , i_m) le cycle décrit dans la définition.
Une transposition ayant pour support $\{i, j\}$ sera aussi notée τ_{ij}

2.3 THEOREME:
Toute permutation se décompose de manière unique (à l'ordre près) en produit de cycles dont les supports sont deux à deux disjoints.

Démonstration:
On utilise une récurrence sur l'entier n,
l'affirmation étant claire pour n$\leq$ 3 (puisque toutes les permutations sont alors des cycles).
Supposons donc l'énoncé démontré pour les permutations de k éléments avec k < n
et considérons s $\in$ S_n.
En regardant la suite 1, s(1), s^2(1) . . . on voit qu'il existe un plus petit entier m $\geq$1 tel que $s^m(1) = 1$
(on n'exclut pas que m = 1).
Définissons l'ensemble I := $\{1, s(1), s^2(1)..., s^{m-1}(1)\}$ et le m-cycle r := $(1, s(1), s^2(1)..., s^{m-1}(1))$;
alors la permutation t := sr^{-1} laisse fixe les éléments de I et pour i $\notin$ I on a t(i) = s(i).
La restriction de t à J := $\{1, ..., n\}\backslash$I est donc une permutation des éléments de J que nous notons s'.
Comme card(J)<n on sait (par l'hypothèse de récurrence) que
s' = s_1' . . . s'$_r$ avec s_i' des cycles de J 'à supports disjoints.
Définissons $s_i \in S_n$ par s_i(j) = s_i'(j) si j $\in$ J et s_i(j)= j si j $\notin$ J ;
on voit qu'alors on a t = s_1 . . . s_r et par conséquent s = s_1 . . . s_rr.
Ceci prouve l'existence de la décomposition en cycles ;

pour l'unicité on observe que le cycle r est uniquement déterminé par s
et que par hypothèse de récurrence s'$_1$, . . ., s'$_r$r (et par cons quent s_1, . . . ,s_r) sont uniques.

exemple
Soit $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 7 & 5 & 1 & 2 & 4 \end{pmatrix} \in S_7$
On choisit un premier élément disons 1 et on calcule ses images successives par ρ: on a $\rho(1) = 3$, $\rho^2(1) = \rho(3) = 7$,
$\rho^3(1) = \rho(7) = 4$, $\rho^4(1) = \rho(4) = 5$ et $\rho^5(1) = \rho(5) = 1$ et on obtient ainsi un premier cycle s' qui est le
5-cycle dans l'exemple précédant le théorème. On prend alors un autre élment qui n'est pas dans le suppport de s',
par exemple 2 et on recommence : $\rho(2) = 6$, $\rho^2(2) = \rho(6) = 2$.
on obtient ainsi la d´ecomposition ρ= s'τ_{26}.

2.4 PROPOSITION :

Tout cycle peut s'écrire comme produit de transpositions et donc toute permutation peut s'écrire comme produit de transpositions.

2.5 PROPOSITION:
Tout cycle peut s'écrire comme produit de transpositions et donc
toute permutation peut s'´ecrire comme produit de transpositions.

Démonstration:
Quitte à changer de notation il suffit de montrer que le cycle s = (1, 2, . . . ,m) s'écrit comme produit de transpositions. Or considérons le produit s' = $\tau_{12}\tau_{23}\tau_{34}.....\tau_{i,i+1}....\tau_{m-1,m}$
on vérifie que s'(m) = 1et que si i≤ m-1 alors s'(i) = i + 1 et finalement on a bien s = s',
ce qui achève la preuve.
Remarque :
la décomposition en produit de transpositions n'est pas du tout unique
mais la parité du nombre de transposition ne change pas comme on pourra le vérifier à
l'aide de la notion suivante.

Définition:
Le signe d'une permutation s ∈ S_n est défini par le produit :

$\epsilon(s) = \prod_{1\leq i<j\leq n} \left(\frac{s(j)-s(i)}{j-i}\right)$
Il est aisé de vérifier que $\epsilon(s) \in \{+1, -1\}$ et que le signe d'une transposition est -1 ;
la principale propriété est la suivante :
Soient s,$\sigma \in S_n$ alors $\epsilon(s\sigma) = \epsilon(s)\epsilon(\sigma)$
Remarque :
on voit donc ϵ(s) = +1 si ϵ est le produit d'un nombre pair de transpositions
et ϵ(s) = -1 si ϵ est le produit d'un nombre impair de transpositions. Plus généralement un cycle de longueur m aura donc un signe $(-1)^{m+1}$, ce qui donne une méthode de calcul du signe d'une permutation connaissant sa décomposition en cycles.

III Sous-Groupes
3.1 Définition:
Un sous-groupe d'un groupe (G,$\star$) est un sous-ensemble H de G tel que la loi $\star$ restreinte à H × H définisse une loi interne qui donne une loi de groupe sur H.
Ainsi un sous-groupe est stable pour la loi $\star$ (c'est-à-dire que si x, y ∈ H alors x$\star$ y ∈ H),
l'élément neutre e appartient à H et si x ∈ H alors x^{-1} ∈H.

3.2 PROPOSITION:

Soit H un sous-ensemble d'un groupe G, c'est un sous-groupe si et seulement si il satisfait :

(i) e $\in$ H

(ii) x, y $\in$ H $\Longrightarrow$ $xy^{-1} \in$ H.

Exemples :

1) L'ensemble des racines complexes de l'équation $X^n = 1$, muni de la multiplication des nombres complexes forme un sous-groupe de $\mathbb{C}$:

en effet si z, z' sont des racines de l'unité alors

(z/z') est une racine de l'unité

2) L'ensemble n$\mathbb{Z} = \{nx/x \in \mathbb{Z}\}$ muni de l'addition est un sous-groupe de $\mathbb{Z}$.

Nous verrons que ce sont les seuls sous-groupes de $\mathbb{Z}$.

3) les inclusions suivantes sont des inclusions de sous-groupes : $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ (pour la loi d'addition)

3.3 Définition:

Un homomorphisme de groupe est une application f : (G, $\star$)$\longrightarrow$ (H,$\circ$) telle que :

$\forall$x, y $\in$ G, f(x $\star$y) = f(x)$\circ$ f(y)

Si de plus f est une bijection, on dit que f est un isomorphisme de groupe et que G et H sont isomorphes.

3.4 Définition:

Le noyau d'un homomorphisme de groupe f : G $\longrightarrow$ H est l'ensemble $f^{-1}(\{e_H\}) = \{g \in G/f(g) = e_H\}$. On le note Ker(f)

Reùarque : Le noyau de f est toujours un sous-groupe de G.

3.5 THEOREME:

Un homomorphisme de groupe f : G $\longrightarrow$ H est injectif si et seulement si Ker(f) = $\{e_G\}$. Le noyau de f est toujours un sous-groupe de G.

IV STRUCTURE D'ANNEAU ET STRUCTURE DE CORPS.

4.1 Définition:

Un anneau est la donnée d'un ensemble A et de deux lois de composition notée : + (addition) et $\star$(Multiplication) telles que :

(i) (A, +) est un groupe commutatif (dont on note l élément neutre $0 = 0_A$).

(ii) La loi $\star$ est associative.

(iii) La loi $\star$ poss'ede un élément neutre (qu'on notera $1 = 1_A$)

(iv) La loi $\star$ est distributive par rapport à l'addition :

$\forall$ x, y, z $\in$ A, x $\star$(y + z) = (x$\star$ y) + (x$\star$ z) et (y + z)$\star$ x = (y$\star$ x) + (z$\star$ x)

Si de plus la loi $\star$ est commutative on dit que l'anneau A est commutatif.

4.2 Définition:
Un corps est un anneau tel que :
(v) Tout élément $x \in A \setminus \{0_A\}$ possède un symétrique (inverse) pour la loi $\star$(noté x^{-1})
Convention : Un anneau (ou un corps) est donc un triplet (A,+,$\star$)

Exemples : l'anneau des entiers relatifs (Z,+,$\times$) ;
ce n'est pas un corps car les seuls éléments de Z possédant un inverse pour la multiplication
sont +1 et -1

4.2 Sous-anneau
4.2.1 Définition
Soit (A,+, $\star$) un anneau et B une partie de A. On dit que B est un sous-anneau de l'anneau (A,+, $\star$) si :

(i) $1_A \in B$

(ii) B est stable pour les les deux lois de composition internes +, . et (B,+, .) est un anneau.

4.2.2 Proposition
Soit A un anneau et B une partie de A. B est un sous-anneau de A (au sens des
anneaux unitaires) si, et seulement si :

(i) $1_A \in B$

(ii) $\forall a, b \in B$, a - b $\in B$

(iii) $\forall a, b \in B$, a$\star$b $\in B$

4.2.3 Définition
Soit (K,+, .) un corps et L un sous-anneau de (K,+, .). On dit que L est un sous-corps du corps (K,+, .) si (L,+, .) est un corps.

4.2.4 Proposition
Soit (K,+, .) un corps et L une partie de K. L est un sous-corps du corps (K,+, .)
si, et seulement si :

(i) L est un sous-anneau de K

(ii) Pour tout a ∈ L ∖ {0}, $a^{-1} \in L$.

4.3 Homomorphismes d' Anneaux

4.3.1 Définition

Soit (A,+, .) et (B,+, .) deux anneaux (unitaires et non triviaux).

On dit qu'une application f de A dans B est un homomorphisme d'anneaux (ou morphisme d'anneaux) si :

(i) f(x + y) = f(x) + f(y) pour tout (x, y) élément de A^2

(ii) f(x.y) = f(x).f(y) pour tout (x, y) élément de A^2

(iii) $f(1_A) = 1_B$

CHAPITRE IV ARITHMETIQUE

I- Divisibilité dans $\mathbb{Z}$

1.1 Définition

Soient a et b deux entiers relatifs quelconques. On dit que a divise b et on écrit

a/b s'il existe un entier $k \in \mathbb{Z}$ tel que b = ka.

1.2 Proposition

Pour tous a, b, c éléments non nuls de $\mathbb{Z}$,

(i) a/a

(ii) Si a/b et b/a alors a = b ou a = -b

(iii) Si a/b et b/c alors a/c

(iv) Si a/b et a/c alors a/(b + c)

1.3 Théorème (Théorème de la Division Euclidienne)

Soit (a, b) ■ $\mathbb{Z} \times \mathbb{Z}^*$, alors il existe un couple (q, r) unique d'entiers relatifs vérifiant :

$a = bq + r$ et $0 \leq r < |b|$

PREUVE.

Existence : Si 0< b, on considère l'entier q tel que $bq \leq a \leq b(q+1)$

et l'entier r = a - bq. Si b < 0, alors, d'après ce qui précéde, $\exists q_1, r \in \mathbb{Z}$: $a = q_1(-b) + r$ avec

$0 \leq r < |b|$et ainsi il suffit de prendre le couple $(-q_1, r)$.

Unicité : Soient (q, r) et (q', r') deux couples d'entiers tels que $a = bq + r$ et $0 \leq r < |b|$

a = bq' + r', $0 \leq$ r' $< |b|$, alors b(q - q') = r' - r d'où $|b|\ |q - q\prime| = |r - r'|$. D'autre part, on a

$|r - r\prime| < |b|$ car $0 \leq$ r $< |b|$ et $0 \leq$ r' $< |b|$. Ainsi,$|b|\ |q - q\prime| = |r - r'| < |b|$ et par conséquent

$|q - q\prime| = 0$, i.e., q = q' et r = r'

1.4 Corollaire (Division Euclidienne dans $\mathbb{N}$)

Soit (a, b) $\in \mathbb{N} \times \mathbb{N}^*$, alors il existe un couple (q, r) unique d'entiers naturels vérifiant : a = bq + r et $0 \leq$ r$<$ b.

Preuve. Supposons que a $\geq$ b (si a$<$ b on pose r = a et q = 0), alors a $>$ r et ainsi q $\in \mathbb{N}$ (car

bq = a - r $\in \mathbb{N}$)

II Sous-groupes de $\mathbb{Z}$

Notation

Soit n un entier relatif, on note $n\mathbb{Z} = \{nm/m \in \mathbb{Z}\}$. On a ainsi $\{0\} = 0\mathbb{Z}$ et $\mathbb{Z} = 1\mathbb{Z}$.

2.1 Proposition

(i) Pour tout entier relatif n, (n$\mathbb{Z}$,+) est un sous-groupe du groupe ($\mathbb{Z}$,+).

(ii) Soit (a, b) $\in \mathbb{Z}^2$. a/b si, et seulement si, b$\mathbb{Z} \subset$ a$\mathbb{Z}$.

2.2 Conséquence

Soit (a, b)$\in \mathbb{Z}^2$, on a a$\mathbb{Z}$= b$\mathbb{Z}$ si, et seulement si, a = b ou a = -b. Ainsi pour

tout a $\in \mathbb{Z}$, il existe un unique entier naturel k tel que a$\mathbb{Z}$ = k$\mathbb{Z}$, (k = $|a|$). On appelle l'entier k le

générateur positif de a$\mathbb{Z}$.

2.3Théorème

Si H est un sous-groupe du groupe additif ($\mathbb{Z}$,+), alors il existe un unique entier

naturel n tel que H = n$\mathbb{Z}$.

Preuve. Supposons que H= $\neq \{0\}$ (si H = $\{0\}$ alors H = 0$\mathbb{Z}$), alors N = {m$\in \mathbb{Z}^*$ / m $\in$ H} est non vide.

Soit n le plus petit élément de N et montrons que H = n$\mathbb{Z}$. Puisque n $\in$ H, alors

n$\mathbb{Z} \subset$ H. D'autre part, soit h $\in$ H, alors, d'après le théorème de la division euclidienne dans Z,

$\exists$ un unique couple (q, r) $\in \mathbb{Z} \times \mathbb{Z}$: h = nq +r avec $0 \leq$ r $<$ n, ainsi r = h-nq$\in$ H et puisque n est le plus petit élément

de N, alors nécéssairement r = 0 et H $\subset$ n$\mathbb{Z}$.

L'unicité découle de la proposition 1.17 ii)

III. PGCD et PPCM

3.1Théorème et Définition
Soient a et b deux entiers relatifs non nuls. Alors,

(i) Il existe un unique entier naturel non nul d tel que : d/a et d/b et Si d' $\in \mathbb{Z}$ est tel que d'/a et d'/b, alors d'/d ;
d s'appelle le plus grand diviseur commun de a et b et se note d = pgcd(a,b), ou simplement d = a $\wedge$ b,

(ii) Il existe un unique entier naturel non nul m tel que : a/m et b/m et Si m' $\in \mathbb{Z}$ est tel que a/m' et b/m', alors m/m',
m s'appelle le plus petit multiple commun de a et b et se note m = ppcm(a,b), ou simplement m = a $\wedge$ b

(iii) Deux entiers a et b sont dits premiers entre eux si pgcd(a, b) = 1.

Preuve.
d (resp. m) est l'entier naturel tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ (resp.$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$)

Exercice
Soient a,b et c des entiers relatifs non nuls. Montrer que
1) a $\wedge$ (b $\wedge$ c) = (a$\wedge$ b)$\wedge$ c
2) ab$\wedge$ac = $|a|$.(b$\wedge$ c)
3) a $\vee$(b $\vee$ c) = (a $\vee$ b) $\vee$ c
4) ab $\vee$ ac = $|a|$.(b $\vee$ c)

3.2 Proposition
Soient a et b deux entiers naturels non nuls tels que a = bq+c, alors a$\wedge$b = b$\wedge$c.
En particulier, si r est le reste de la division euclidienne de a par b,alors a $\wedge$ b = b $\wedge$ r.

Preuve.
a = bq + c entraine que c $\in$ aZ + bZ et que a $\in$ bZ + cZ .
Ainsi, bZ + cZ = aZ + bZ et a $\wedge$ b = b $\wedge$ c

3.3. Algorithme (Algorithme d'Euclide)
Soient a, b deux entiers naturels non nuls tels que
b <a et b ne divise pas a. Alors, pgcd(a, b) est le dernier reste non nul obtenu en appliquant
l'algorithme d'Euclide. Cet algorithme consiste à :

i) Commencer par effectuer la division euclidienne de a par b : a = bq_1 + r_1

ii) Effectuer la division euclidienne de b par r_1 : $b = r_1q_2 + r_2$

iii) Effectuer la division euclidienne de r_1 par r_2 : $r_1 = r_2q_3 + r_3$

. . .

La suite (r_i) est telle que $0 \leq r_{i+1} < r_i$.

Ainsi il existe nécessairement n tel que $r_n \neq 0$ et $r_{n+1} = 0$.

D'autre part, d'après la proposition 3.2.1, $a \wedge b = b \wedge r_1 = \ldots = r_{n-1} \wedge r_n = r_n$.

Exemple

Considérons les entiers 1876 et 365. Alors,

$1876 = 365.5 + 51$,

$365 = 51.7 + 8$,

$51 = 8.6 + 3$,

$8 = 3.2 + 2$ et $3 = 2.1 + 1$.

Ainsi, les entiers 1876 et 365 sont premiers entre-eux.

Remarque

1) Si pgcd(a, b) = d, alors $dZ = aZ + bZ$ et ainsi, $\exists u, v \in Z$ tels que $au + bv = d$.

2) Une méthode pratique pour déterminer u et v consiste à les calculer en remontant les égalités

de l'algorithme d'Euclide.

3.4 Théorème (Théorème de Bezout)

Soient a et b deux entiers naturels non nuls. Alors, a et b sont premiers entre eux si, et seulement si, il existe deux entiers relatifs u et v tels que ua+vb = 1.

Preuve.

D'après la remarque 3.2.3 , si pgcd(a, b) = 1, il existe $u, v \in Z$: ua+vb = 1.

Réciproquement, s'il existe u et v tels que ua + vb = 1, alors $aZ + bZ = Z$ et ainsi $a \wedge b = 1$

Exercice

Soient a et b deux entiers naturels non nuls et d un diviseur commun de a et b.

Montrer que $a \wedge b = d$ si et seulement si, $\frac{a}{d} \wedge \frac{b}{d} = 1$.

IV Nombres Premiers

4.1 Définition

Soit p un entier naturel ≥ 2. On dit que p est un nombre premier, si 1 et p sont

les seuls diviseurs de p dans $\mathbb{N}$, (i.e., Si $a \in N$ et a/p alors a = 1 ou a = p).

On désigne par $\mathcal{P}$ l'ensemble de tous les nombres premiers.

4.2 Définition

Un entier relatif n est dit premier si $|n|$ est un nombre premier, i.e., si $n \geq 2$ et les seuls diviseurs de n sont 1, -1, n et -n.

Exercice

Montrer que

1) Si a $\in \mathbb{N}$ et p est un nombre premier, alors p/a ou p $\wedge$ a = 1.

2) Si p et q sont deux entiers naturels premiers et distincts, alors p $\wedge$ q = 1.

3) Montrer que tout entier n ≥ 2, admet un diviseur premier (Ind : considérer l'ensemble

D = $\{d \in \mathbb{N},\ d \geq 2\ et\ d/n\}$, montrer que D possède un plus petit élément p et que p est premier).

4.3 Théorème 1.35 (Premier Théorème d'Euclide)

Soient p un nombre premier, a et b deux entiers.

Si p divise ab, alors p divise a ou p divise b.

Preuve. Supposons que p$\nmid$ a, alors p $\wedge$ a = 1 ((i) de l'exercice précédent), d'où $\exists$ u,v $\in$ Z tels que

ua + vp = 1, ainsi b = uab + vpb et puisque p/ab, alors p/b

Une conséquence de ce résultat est l'important théorème suivant :

4.4 Théorème (Théorème fondamental de l'Arithmétique)

Tout entier naturel n $\geq$2 admet une factorisation unique en nombres premiers, à l'ordre des facteurs près,

i.e., $\forall n \in \mathbb{N}^\star - \{1\}, \exists! r \in \mathbb{N}^\star, \exists!(p_1, ..., p_r) \in \mathcal{P}^r$, avec $p_1 < \ldots < p_r$,

$n = p_1^{k_1} p_2^{k_2} ..... p_r^{k_r}\ k_i \geq 1$

Preuve.

Existence : Appelons P(n) la propriété « n est un produit de nombres premiers ». Puisque 2 est un nombre premier, 2 vérifie bien P(n). Supposons P(m) vraie pour tout entier m < n. Si n est premier, P(n) est évidement vraie.

Sinon, n = ab, avec a <n et b < n.

D'après l'hypothèse de récurrence, P(a) et P(b) sont vraies, i.e., a et b sont produits de nombres premiers, il en est de même de n = ab et P(n) est vraie ■n $\geq$ 2.

Unicité : Supposons que $n = p_1^{k_1} p_2^{k_2} ..... p_r^{k_r} = n = q_1^{l_1} q_2^{l_2} ..... q_{r'}^{l_{r'}}$

avec $p_1 < \ldots < p_r$ et $q_1 < \ldots < q_{r'}$.

Alors, p_1 divise $q_1^{l_1} q_2^{l_2} ..... q_{r'}^{l_{r'}}$ et en appliquant le théorème d'Euclide (p/ab . . . t alors p/a ou p/b. . . ou p/t), p_1

est égal à l'un des q_i, pour un certain i. Nécessairement $p_1 = q_1$ étant donné l'ordre imposé aux p_i et

aux $q_{\hat{i}}$ respectivement. D'où, on déduit que r = r', $p_i = q_i$ et $k_i = l_i$ pour tout i = 1, . . . , r

4.5 Lemme (Lemme de Gauss)

Soient a, b et c des éléments de Z. Si a/bc et a $\wedge$ b = 1, alors a/c.

Preuve.

Il suffit pour démontrer ce résultat de considérer la décomposition de chacun des nombres

a, b et c en nombres premiers et d'appliquer le théorème d'Euclide

4.5 Proposition

Soient a,b et c des entiers naturels non nuls. Si d = a $\wedge$ b et m = a$\vee$ b,

alors pgcd(a,b)$\times$ppmc(a,b) = ab. (En particulier, d = 1 si, et seulement si, m = ab).

V Congruences

5.1 Définition

Si a, b sont deux entiers relatifs, on dit que a est congru à b modulo m et on note

a $\equiv$ b[m] si et seulement si m divise a - b.

5.2 Proposition

Si a, b, c, d,m et n sont des entiers relatifs,

(i) a$\equiv$ a [m],

(ii) si a $\equiv$ b [m], alors b $\equiv$ a [m],

(iii) si a$\equiv$ b [m] et b$\equiv$ c [m], alors a$\equiv$ c[m] ,

(iv) si m est non nul et si b est le reste de la division euclidienne de a par m, alors on a : a $\equiv$ b[m],

(v) si a $\equiv$ b [m] et si n|m, alors on a : a $\equiv$ b [n]

(vi) si a $\equiv$b [m] et c $\equiv$d [m], alors a + c $\equiv$b + d[m],

(vii) si a $\equiv$ b [m] et c $\equiv$ d[m], alors ac $\equiv$ bd [m],

(viii) si a $\equiv$ b [m] et si n est un entier positif, alors $a^n \equiv b^n$ [m].

CHAPITRE V : POLYNÔMES, FRACTIONS RATIONNELLES ET DECOMPOSITION EN ELEMENTS SIMPLES

I) Décomposition d'un polynôme

1.1 Généralités:

Soit $K = \mathbb{R}$ ou $\mathbb{C}$. On appelle polynôme une somme de monômes $a_i X^i$ où X est une indéterminée et $a_i \in K$.

L'ensemble des polynômes est noté $K[X]$.

Exemple :

$5X^3-2X^2+9$ que l'on peut écrire : $9+0X+(-2)\,X^2+5X^3$est un polynôme de $\mathbb{R}[X]$ de degré 3 et dont les coefficients sont 9, 0, -2 et 5.

Un polynôme $P(X)$ s'écrit :

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n.$$

Si $a_n \neq 0$, $P(X)$ est dit de degré n et ses coefficients sont a_0, $a_1, \cdots, a_n \in K$.

On associe à $P(X)$ la fonction polynôme $f : x \longmapsto a_0 + a_1x + \cdots + a_nx^n$, cette fonction est aussi notée P.

1.2 Opération sur les polynômes

a) Somme de deux polynômes :

On fait la somme des coefficients des monômes de même degré.

Si $n \leq m$ on a : $(a_0+a_1X+a_2X^2+\cdots+a_nX^n)+(b_0+b_1X+\cdots+b_mX^m) = a_0+b_0+(a_1+b_1)X+\cdots+(a_n+b_n)X^n+b_{n+1}X^{n+1}+b_{n+2}X^{n+2}+\cdots+b_mX^m$.

b) Produit de deux polynômes :

On utilise la distributivité de la multiplication par rapport à l'addition et à la soustraction et le fait que $X^nX^m = X^{n+m}$.

Exemple :

$$\begin{aligned}(3X^2-5X+1)(X^4-X^2+1) &= \left(3X^2\left(X^4\right)+3X^2\left(-X^2\right)+3X^2\right)+ \\ &\quad +\left[(-5X)\left(X^4\right)-5X\left(-X^2\right)-5X\right]+\left[X^4-X^2+1\right] \\ &= \left(3X^6-3X^4+3X^2\right)+\left[-5X^5+5X^3-5X\right]+\left[X^4-X^2+1\right] \\ &= 3X^6-5X^5-2X^4+5X^3+2X^2-5X+1.\end{aligned}$$

Le produit de deux polynômes de degrés n et m est un polynôme de degré $n+m$.

On note $d^o\ P$ le degré du polynôme $P(X)$.

Si $d^o\ P = 0$ on dit que P est un polynôme constant.

On dit que a est un *zéro* (ou une racine) de P si $P(a) = 0$.

c) Divisions euclidiennes de deux polynômes

A) Suivant les puissances décroissantes

Si $P(X)$ et $Q(X)$ sont deux polynômes alors $P(X)$ s'écrit de manière unique sous la forme

$D(X)Q(X) + R(X)$ où $D(X)$ et $R(X)$ sont des polynômes avec $R(X) = 0$ oubien $d^o\ R < d^o\ Q$.

$D(X)$ est appelé le quotient et $R(X)$ le reste de la division euclidienne de P par Q (suivant les puissances décroissantes).

Exemple : $P(X) = -X^3 - 5X^2 + X - 3$ par $Q(X) = X^2 - X + 2$

$$\begin{array}{l|l} \boxed{-X^3} - 5X^2 + X - 3 & \boxed{X^2} - X + 2 \\ \underline{-\left[-X^3 + X^2 - 2X\right]} & \\ = 0 - 6X^2 + 3X - 3 & \boxed{-X} - 6 \\ \underline{-\left[-6X^2 + 6X - 12\right]} & \\ = 0 - 3X + 9 & \end{array}$$

$D(X) = -X - 6$ et $R(X) = -3X + 9$; $d^o\ R = 1 < d^o\ Q = 2$

on écrit: $P(X) = Q(X) D(X) + R(X)$:

$-X^3 - 5X^2 + X - 3 = (X^2 - X + 2)(-X - 6) + (-3X + 9)$

B) Suivant les puissances croissantes à l'ordre n :

Si $Q(0) \neq 0$ et pour tout entier naturel n

il existe un polynôme unique $D(X)$ et un polynôme unique $S(X)$ tels que

$$P(X) = D(X) \times Q(X) + X^{n+1} \times S(X) \text{ avec } d^o\ D \leq n$$

$D(X)$ est appelé le quotient et $R(X) = X^{n+1} \times S(X)$ le reste de la division euclidienne de P par Q suivant les puissances croissantes à l'ordre n.

Exemple: $P(X)=2X^3 - X + 1$; $Q(X)=X^2 - X + 1$

Division euclidienne suivant les puissances croissantes de $P(X)$ par $Q(X)$ à l'ordre 3 :

$P(X) = 1 - X + 2X^3$; $Q(X) = 1 - X + X^2$

$$\begin{array}{l|l} \boxed{1} - X + 2X^3 & \boxed{1} - X + X^2 \\ \underline{-1 \times \left(1 - X + X^2\right)} & \\ = \ -X^2 + 2X^3 & 1 - X^2 + X^3 = D(X) \\ \underline{-(-X^2 + X^3 - X^4)} & \\ = X^3 + \ X^4 & \\ \underline{-(X^3 - X^4 + X^5)} & \\ = 2X^4 - X = R(X) = & \\ X^4(2 - X) = X^4 S(X) & \end{array}$$

Division euclidienne suivant les puissances croissantes de $P(X)$ par $Q(X)$ à l'ordre 4 :

$P(X) = 1 - X + 2X^3$; $Q(X) = 1 - X + X^2$

$$\begin{array}{l|l}
\boxed{1}-X+2X^3 & \boxed{1}-X+X^2 \\
\underline{-1\times\left(1-X+X^2\right)} & \\
=-X^2+2X^3 & 1-X^2+X^3+2X^4=D(X) \\
\underline{-(-X^2+X^3-X^4)} & \\
=\ X^3+\ X^4 & \\
\underline{-(X^3-X^4+X^5)} & \\
=2X^4-X^5 & \\
\underline{-\left(2X^4-2X^5+2X^6\right)} & \\
=X^5-2X^6=R(X)= & \\
X^5\left(1-2X\right)=X^5S\left(X\right) &
\end{array}$$

Application : Le développement limité de $\dfrac{2x^3-x+1}{x^2-x+1}$ à l'ordre 4 au voisinage de 0 s'écrit:

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

En effet, $\dfrac{1-x+2x^3}{1-x+x^2}-\left(1-x^2+x^4\right)=\dfrac{x^5-x^6}{1-x+x^2}$

$$=x^4\left(\frac{x-x^2}{1-x+x^2}\right)=x^4\times\varepsilon(x) \text{ où } \lim_{x\to 0}\varepsilon(x)=0.$$

1.3) Décomposition d'un polynôme

1.3.1 Proposition

Tout polynôme non constant $P(X)$ à coefficients dans $\mathbb{R}$ s'écrit comme produit de polynômes de degrés 1 ou 2 :

$$P(X)=\lambda\times[(X-a_1)^{\alpha_1}\times(X-a_2)^{\alpha_2}\times\cdots\times(X-a_n)^{\alpha_n}]\times\left[(X^2+b_1X+c_1)^{\beta_1}\times\cdots\times(X^2-b_mX+c_m)^{\beta_m}\right]$$

$\sum_{i=1}^{n}\alpha_i+2\times\sum_{j=1}^{m}\beta_j=$ *degré de* P *et* a_i , b_j , $c_j\in\mathbb{R}$, $\lambda\in\mathbb{R}^*$ *et* $X^2+b_jX+c_j$ *n'admettant pas de zéro dans* $\mathbb{R}$ $(b_j^2-4c_j<0)$.

Les zéros de P *sont* a_1, a_2 ,$\cdots$,a_n.

1.3.2 Proposition

Tout polynôme non constant $P(X)$ de $\mathbb{C}[X]$, de degré m, s'écrit comme produit de m polynômes de degré 1 :

$$P(X)=\lambda\times(X-a_1)^{\alpha_1}\times(X-a_2)^{\alpha_2}\times\cdots\times(X-a_n)^{\alpha_n}$$

où $a_i\in\mathbb{C}$, $a_i\neq a_j\ \forall\ i\neq j$ *et* $\lambda\in\mathbb{C}^*$; $\sum_{i=1}^{n}\alpha_i=d^o\ P=m$.

Conséquence:

Un polynôme non nul de $\mathbb{C}[X]$ *de degré* $n \neq 0$ *admet* n *zéros (distincts ou non): on dit que* $\mathbb{C}$ *est algébriquement clos.*

(*Toute équation* $P(X) = 0$ *admet exactement* n *solutions (distinctes ou non) où* $n \neq 0$ *est le degré de* P).

1.3.3 Exemple

$P(X) = X^5 - 4X^4 + 6X^3 - 6X^2 + 5X - 2$; P est de degré 5.

Dans $\mathbb{R}[X]$: Les zéros de P sont : 1 et 2.

$P(X) = (X-1)^2(X-2)(X^2+1)$; 1 est un zéro d'ordre 2 et 2 est un zéro d'ordre 1.

Dans $\mathbb{C}[X]$: Les zéros de P sont : 1, 2, i et $-i$.

$P(X) = (X-1)^2(X-2)(X+i)(X-i)$

i, $-i$ et 2 sont des zéros d'ordre 1 ; et 1 est un zéro d'ordre 2 dit racine double.

1.3.4 Définition :

On dit que a *est un* zéro *d'ordre* $n \geq 1$ *de* P *si* $P(X) = (X-a)^n \times Q(X)$ *avec* $Q(a) \neq 0$.

1.3.5 Proposition :

a *est un zéro d'ordre* n *de* $P(X)$ *si et seulement si* $P(a) = 0$, $P'(a) = 0$, $P''(a) = 0, \cdots, P^{(n-1)}(a) = 0$ *et* $P^{(n)}(a) \neq 0$.

II) Fractions rationnelles

2.1 Définitions

On appelle *fraction rationnelle* à une indéterminée X le rapport d'un polynôme $P(X)$ par un polynôme $Q(X) \neq 0$ (c'est à dire différent du polynôme nul).

L'ensemble des fractions rationnelles à coefficients dans K est noté $K(X)$.

Deux fractions rationnelles $\dfrac{P_1}{Q_1}$ et $\dfrac{P_2}{Q_2}$ sont dites *égales* si $P_1 \times Q_2 = P_2 \times Q_1$.

Exemple :

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

2.2 Opération sur les fractions rationnelles

Si $\dfrac{P(X)}{Q(X)}$ et $\dfrac{R(X)}{S(X)}$ sont deux fractions rationnelles alors :

$\dfrac{P(X)}{Q(X)} + \dfrac{R(X)}{S(X)}$ est la fraction rationnelle $\dfrac{P(X)\times S(X) + R(X)\times Q(X)}{Q(X)\times S(X)}$.

$\dfrac{P(X)}{Q(X)} \times \dfrac{R(X)}{S(X)} = \dfrac{P(X)\times R(X)}{Q(X)\times S(X)}$

et si $R(X) \neq 0$ alors $\dfrac{\left(\dfrac{P(X)}{Q(X)}\right)}{\left(\dfrac{R(X)}{S(X)}\right)} = \dfrac{P(X)\times S(X)}{Q(X)\times R(X)}$.

Si $Q(X) = 1$, la fraction rationelle $\dfrac{P(X)}{Q(X)} = \dfrac{P(X)}{1}$ est identifiée au polynôme $P(X)$.

CHAPITRE VI : DECOMPOSITION EN ELEMENTS SIMPLES

Définition :

Soit $F(X) = \dfrac{P(X)}{Q(X)}$ une fraction rationnelle, on dit que l'écriture $\dfrac{P(X)}{Q(X)}$ est *irréductible* s'il n'existe pas de polynômes $P_1(X)$ et $Q_1(X)$ tels que $F(X) = \dfrac{P_1(X)}{Q_1(X)}$ avec $d^o\ P_1 < d^o\ P$ (c'est−à−dire si on ne peut simplifier davantage $F(X)$).

Exemple:

$\dfrac{2X^2+X}{X^3+X^2+3X} = \dfrac{2X+1}{X^2+X+3}$

La deuxième écriture est irréductible, la 1ère ne l'est pas.

I) Décomposition en éléments simples d'une fraction rationnelle dans $\mathbb{R}(X)$:

1.2 Définitions :

Soit $F(X) = \dfrac{P(X)}{Q(X)}$ une fraction rationelle écrite sous forme irréductible dans $\mathbb{R}(X)$.

Si $Q(X)$ s'écrit

$$\lambda\left[(X-a_1)^{\alpha_1}(X-a_2)^{\alpha_2}\cdots(X-a_n)^{\alpha_n}\right]\times\left[(X^2-b_1X+c_1)^{\beta_1}\times\cdots\times(X^2-b_mX+c_m)^{\beta_m}\right]$$

avec $a_i \neq a_k\ \forall i \neq k$ et $b_j^2 - 4c_j < 0\ \forall j$, on dit que a_i est un *pôle d'ordre* α_i de la fraction rationnelle $F(X)$.

On appelle *décomposition en éléments simples* de la fraction $F(X)$ l'écriture de $F(X)$ en somme :

– d'un polynôme $E(X)$

– d'*éléments de* $1^{ère}$ *espèce* :

$$\frac{A_{\alpha_i}}{(X-a_i)^{\alpha_i}} + \frac{A_{\alpha_i-1}}{(X-a_i)^{\alpha_i-1}} + \cdots + \frac{A_2}{(X-a_i)^2} + \frac{A_1}{X-a_i} \quad \rightarrow$$

partie principale relative au pôle a_i appelée *partie polaire relative au pôle* a_i.

– et d'*éléments de* $2^{ème}$ *espèce* :

$$\frac{B_{\beta_j}X + C_{\beta_j}}{(X^2+b_jX+c_j)^{\beta_j}} + \frac{B_{\beta_j-1}X + C_{\beta_j-1}}{(X^2+b_jX+c_j)^{\beta_{j-1}}} + \cdots + \frac{B_1X+C_1}{(X^2+b_jX+c_j)} \quad \rightarrow$$

partie principale relative au trinôme $X^2+b_jX+c_j$ avec $\Delta = b_j^2 - 4c_j < 0 \ \forall j$.

$E(X)$ est appelé *la partie entière* de la décomposition ; c'est le quotient de la division euclidienne de $P(X)$ par $Q(X)$ suivant les puissances décroissantes.

$E(X) = 0$ si et seulement si $d^o\ P < d^o\ Q$;

si $E(X) \neq 0$; $d^o\ E = d^o\ P - d^o\ Q$.

La décomposition d'une fraction rationnelle s'obtient de manière unique.

1.2) Exemples de décomposition en éléments simples d'une fraction dans $\mathbb{R}(X)$ rationnelle

Exemple 1: $F(X) = \dfrac{X^4+3X^3+X+2}{2X^3+14X^2+30X+18}$

Factorisons $Q(X)$: $Q(X) = 2X^3+14X^2+30X+18$

$Q(-1) = 0$

$2X^3+14X^2+30X+18 = (X+1)\left(2X^2+12X+18\right) = 2(X+1)\left(X^2+6X+9\right)$

$Q(X) = 2(X+1)(X+3)^2$

$F(X) = \dfrac{X^4+3X^3+X+2}{2X^3+14X^2+30X+18}$ est écrite sous forme irréductible car -3 et -1 ne sont pas racines de $P(X) = X^4+3X^3+X+2$.

On dit que -3 est un *pôle d'ordre* 2 de la fraction rationnelle $F(X)$ et -1 est un *pôle d'ordre* 1 de $F(X)$.

On appelle *décomposition en éléments simples* de la fraction $F(X)$

l'écriture de $F(X)$ en somme :

– d'un polynôme $E(X)$

– et d'éléments de $1^{ère}$ espèce:

$$\underbrace{\frac{A_2}{(X+3)^2}+\frac{A_1}{(X+3)^1}}_{\substack{\text{partie } \textit{polaire} \\ \text{relative au} \\ \text{pôle } -3}}+\underbrace{\frac{B}{X+1}}_{\substack{\text{partie } \textit{polaire} \\ \text{relative au} \\ \text{pôle } -1}}$$

où A_1, A_2 et B sont des constantes.

$E(X)$ est appelé *la partie entière* de la décomposition ; c'est le quotient de la division euclidienne de $P(X)$ par $Q(X)$.

Détermination de la partie entière $E(X)$ et des coefficients:
a) Détermination de $E(X)$ par division euclidienne:

$$\begin{array}{l|l} \boxed{X^4}+3X^3+X+2 & \boxed{2X^3}+14X^2+30X+18 \\ \underline{-(X^4+7X^3+15X^2+9X)} & \\ =-4X^3-15X^2-8X+2 & \boxed{\frac{1}{2}X}-2 \\ \underline{-\left(-4X^3-28X^2-60X-36\right)} & \\ =13X^2+52X+38 & \end{array}$$

$$P(X)=D(X)Q(X)+R(X)=$$

$$\left(\frac{1}{2}X-2\right)\left(2X^3+14X^2+30X+18\right)+13X^2+52X+38$$

$$\begin{aligned} F(X) &= \frac{1}{2}X-2+\frac{13X^2+52X+38}{2X^3+14X^2+30X+18} \\ &= E(X)+F_1(X) \end{aligned}$$

b) Calcul de B : Multiplions $F_1(X)$ par $X+1$ et faisons tendre X vers -1 :

$$\begin{aligned} F_1(X) &= \frac{13X^2+52X+38}{2(X+1)(X+3)^2} \\ &= \frac{A_2}{(X+3)^2}+\frac{A_1}{(X+3)}+\frac{B}{X+1} \end{aligned}$$

$\lim\limits_{X\longrightarrow -1}(X+1)F_1(X)=B=\lim\limits_{X\longrightarrow -1}\dfrac{13X^2+52X+38}{2(X+3)^2}=\dfrac{13-52+38}{2(2)^2}=-\dfrac{1}{8}$

b) Calcul de A_2 :

Multiplions par $(X+3)^2$ et faisons tendre X vers -3 :

$\lim\limits_{X\longrightarrow -3}(X+3)^2F_1(X)=A_2=\lim\limits_{X\longrightarrow -3}\dfrac{13X^2+52X+38}{2(X+1)}=\dfrac{13\times 9-52\times 3+38}{2(-3+1)}=\dfrac{1}{4}$.

b) Calcul de A_1 : Multiplions par X et

faisons tendre X vers ∞ :

$\lim\limits_{X\longrightarrow \infty}XF_1(X)=A_1+B=\lim\limits_{X\longrightarrow \infty}\dfrac{X\left(13X^2+52X+38\right)}{2X^3+14X^2+30X+18}=\lim\limits_{X\longrightarrow \infty}\dfrac{13X^3}{2X^3}=\dfrac{13}{2}\Rightarrow$

$A_1=\dfrac{13}{2}-B=\dfrac{13}{2}+\dfrac{1}{8}=\dfrac{53}{8}$.

ou encore

$$F_1(0)=\frac{38}{18}=\frac{19}{9}=\frac{A_2}{3^2}+\frac{A_1}{3}+\frac{B}{1}=\frac{\frac{1}{4}}{9}+\frac{A_1}{3}+\frac{\frac{-1}{8}}{1}=\frac{1}{3}A_1-\frac{7}{72}\Rightarrow$$

$$\begin{aligned}A_1 &= \frac{19}{3}+\frac{7}{24}=\frac{53}{8}\\ F_1(X) &= \frac{\frac{1}{4}}{(X+3)^2}+\frac{\frac{53}{8}}{(X+3)}+\frac{\frac{-1}{8}}{X+1}\end{aligned}$$

$$F(X)=E(X)+F_1(X)$$

$$\boxed{F(X)=\frac{1}{2}X-2+\frac{\frac{1}{4}}{(X+3)^2}+\frac{\frac{53}{8}}{(X+3)}+\frac{\frac{-1}{8}}{X+1}}$$

La décomposition d'une fraction rationnelle est unique.

Exemple 2 : $F(X)=\dfrac{X^4+3X^3+X+2}{2X^4-12X^3+22X^2-24X+36}$

$Q(X)=2X^4-12X^3+22X^2-24X+36=2\left(X^4-6X^3+11X^2-12X+18\right)$

$Q(3)=0$

$X^4-6X^3+11X^2-12X+18=(X-3)\left(X^3-3X^2+2X-6\right)$

$X^3-3X^2+2X-6=(X-3)\left(X^2+2\right)$

$Q(X)=2(X-3)^2\left(X^2+2\right)^1$.

$F(X)$ est écrite sous forme irréductible car la seule racine de Q est 3 qui n'est pas racine de P.

3 est un *pôle d'ordre* 2 de la fraction rationnelle $F(X)$ et X^2+2 est un *polynôme qui ne se décompose pas dans* $\mathbb{R}[X]$.

On appelle *décomposition en éléments simples* de la fraction $F(X)$ l'écriture de $F(X)$ en somme :

– d'un polynôme $E(X)$

– d'éléments de $1^{ère}$ espèce:

$$\underbrace{\frac{A_2}{(X-3)^2}+\frac{A_1}{(X-3)^1}}_{\text{partie polaire relative au pôle 3}}$$

– et d'un élément de $2^{ème}$ espèce:

$\frac{BX+C}{(X^2+2)^1}$: partie principale relative au trinôme X^2+2

avec $\Delta=-8<0$.

$$F(X)=E(X)+\frac{A_2}{(X-3)^2}+\frac{A_1}{(X-3)^1}+\frac{BX+C}{(X^2+2)^1}$$

Exemple 3:

$$F(X)=\frac{X^4+3X^3+X+2}{2X^5-11X^4+28X^3-40X^2+32X-12}$$

$$F(X)=\frac{X^4+3X^3+X+2}{(2X-3)(X^2-2X+2)^2}=\frac{P(X)}{Q(X)}$$

elle est écrite sous forme irréductible car 3/2 n'est pas racine de $P(X)$ et X^2-2X+2 n'a pas de racine dans $\mathbb{R}$.

3/2 est un *pôle d'ordre* 1 de la fraction rationnelle $F(X)$ et X^2-2X+2 est un *polynôme qui ne se décompose pas dans* $\mathbb{R}[X]$.

On appelle *décomposition en éléments simples* de $F(X)$ l'écriture de $F(X)$ en somme :

– d'un polynôme $E(X)$

– d'un élément de $1^{ère}$ espèce: $\underbrace{\frac{A}{(2X-3)^1}}_{\text{partie polaire relative au pôle 3/2}}$

– et de deux éléments de $2^{ème}$ espèce :

$\frac{B_2X+C_2}{(X^2-2X+2)^2}+\frac{B_1X+C_1}{(X^2-2X+2)}$ $\underline{\text{partie principale relative au trinôme}}$ X^2-2X+2 avec $\Delta=-4<0$.

$E(X)$ est appelé *la partie entière* de la décomposition.

Exemple 4 : $F(X)=\dfrac{2X^4-3X^2-X+2}{4X^3+X+5}$.

Soit $P(X)=2X^4-3X^2-X+2$ et $Q(X)=4X^3+X+5$

$d^o\ P-d^o\ Q=1$ d'où $E(X)$ est de $d^o\ \ 1$ qui sera déterminé par la division euclidienne

de $P(X)$ par $Q(X)$:

$$\begin{array}{l|l} \boxed{2X^4}-3X^2-X+2 & \boxed{4X^3}+X+5 \\ \hline -(2X^4+\frac{1}{2}X^2+\frac{5}{2}X) & \frac{1}{2}X \\ \hline =\frac{-7}{2}X^2-\frac{7}{2}X+2 & \end{array}$$

$$\begin{aligned} P\left(X\right) &= \left(\frac{1}{2}X\right)Q\left(X\right)+R\left(X\right) \\ P(X) &= \left(\frac{1}{2}X\right)(4X^3+X+5)+\left[\frac{-7}{2}X^2-\frac{7}{2}X+2\right] \end{aligned}$$

$$\frac{P(X)}{Q\left(X\right)}=\frac{1}{2}X+\frac{\frac{-7}{2}X^2-\frac{7}{2}X+2}{4X^3+X+5}$$

$E\left(X\right)=\dfrac{1}{2}X.$

Faisons la décomposition en éléments simples de $G(X)=\dfrac{\frac{-7}{2}X^2-\frac{7}{2}X+2}{4X^3+X+5}$

(dont la partie entière est nulle) .

$Q\left(X\right)=4X^3+X+5=(X+1)\left(4X^2-4X+5\right)$

$4X^2-4X+5$ a pour discriminant:

$\Delta=16-4\times 20=-64<0$

-1 est un *pôle* d'ordre 1 de $G\left(X\right)$ dit simple. $G(X)=\dfrac{A}{X+1}+\dfrac{BX+C}{4X^2-4X+5}$.

a) Détermination de A :

Multiplions par $X+1$et faisons tendre X vers -1 :

$$(X+1)\,G(X) = A+\frac{(BX+C)\,(X+1)}{4X^2-4X+5}$$

$$\begin{aligned}(X+1)\,G(X) &= \frac{(X+1)\left[\dfrac{-7}{2}X^2-\dfrac{7}{2}X+2\right]}{(X+1)\,(4X^2-4X+5)}\\ &= \frac{\dfrac{-7}{2}X^2-\dfrac{7}{2}X+2}{4X^2-4X+5}\end{aligned}$$

$$A+\frac{(X+1)\,(BX+C)}{4X^2-4X+5} = \frac{\dfrac{-7}{2}X^2-\dfrac{7}{2}X+2}{4X^2-4X+5}$$

$$\lim_{X\longrightarrow -1}(X+1)\,G(X) = A = \lim_{X\longrightarrow -1}\frac{\dfrac{-7}{2}X^2-\dfrac{7}{2}X+2}{4X^2-4X+5} = \frac{2}{13}.$$

b) Multiplions $G(X)$ par X et faisons tendre X vers ∞ :

$$XG(X) = \frac{AX}{X+1}+\frac{X\,(BX+C)}{4X^2-4X+5} = \frac{X\left[\dfrac{-7}{2}X^2-\dfrac{7}{2}X+2\right]}{4X^3+X+5}$$

$$\begin{aligned}\lim_{X\longrightarrow\infty} XG(X) &= A+\lim_{X\longrightarrow\infty}\frac{BX^2}{4X^2} = \lim_{X\longrightarrow\infty}\frac{\dfrac{-7}{2}X^3}{4X^3}\\ &= A+\frac{B}{4} = \frac{-7}{8}\end{aligned}$$

$$4A+B = \frac{-7}{2} \Rightarrow B = \frac{-8}{13}-\frac{7}{2} = -\frac{107}{26}.$$

Il reste C.

c) Donnons à X une valeur qui n'est pas un pôle :

0 par exemple

$$G(0) = A+\frac{C}{5} = \frac{2}{5} \Rightarrow C = 2-5A = 2-5\times\frac{2}{13} = \frac{16}{13}$$

$$G(X) = \frac{\dfrac{2}{13}}{X+1}+\frac{\dfrac{-107}{26}X+\dfrac{16}{13}}{4X^2-4X+5}$$

$$\boxed{F(X) = \frac{1}{2}X + \frac{\frac{2}{13}}{X+1} + \frac{-\frac{107}{26}X + \frac{16}{13}}{4X^2 - 4X + 5}}$$

$$\downarrow$$

Décomposition de $F(X)$ dans $\mathbb{R}(X)$

II) Décomposition en éléments simples d'une fraction rationnelle dans $\mathbb{C}(X)$:

Les mêmes définitions de A) sont valables sauf qu'il n'y a plus d'éléments de $2^{ème}$ espèce.

Si la fraction rationnelle est à coefficients réels on peut avoir la décomposition dans $\mathbb{R}(X)$ à partir de la décomposition dans $\mathbb{C}(X)$ et puis regrouper les parties polaires relatives à des pôles conjugués pour avoir des fractions de $\mathbb{R}(X)$.

Exemple : $F(X) = \dfrac{2X^4 - 3X^2 - X + 2}{4X^3 + X + 5}$.

Soit $P(X) = 2X^4 - 3X^2 - X + 2$ et $Q(X) = 4X^3 + X + 5$.

$d^o\ P - d^o\ Q = 1$ d'où $E(X)$ est de $d^o\ 1$. Faisons la division euclidienne de $P(X)$ par $Q(X)$:

$$\begin{array}{l|l} 2X^4 - 3X^2 - X + 2 & 4X^3 + X + 5 \\ \hline -(2X^4 + \frac{1}{2}X^2 + \frac{5}{2}X) & \frac{1}{2}X \\ \hline = \frac{-7}{2}X^2 - \frac{7}{2}X + 2 & \end{array}$$

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

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

On fait la décomposition pour $G(X) = \dfrac{\frac{-7}{2}X^2 - \frac{7}{2}X + 2}{4X^3 + X + 5}$ (qui n'a pas de partie entière) .

Dans $\mathbb{C}(X)$:

$4X^3 + X + 5$ admet -1 comme racine; $(4x^3 + x + 5)' = 12x^2 + 1$ qui ne n'annule pas en -1 donc -1 est un zéro d'ordre 1 dit simple de $4x^3 + x + 5$. On a :

$4x^3+x+5=(x+1)(4x^2-4x+5)$

$\dfrac{4X^3+X+5}{X+1}=4X^2-4X+5$: n'admet pas de racine dans $\mathbb{R}$.

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

$\Delta=(-4)^2-4\times4\times5=-64=(8i)^2$

$x_1=\dfrac{4+8i}{8}=\dfrac{1}{2}+i$; $x_2=\dfrac{4-8i}{8}=\dfrac{1}{2}-i$.

$$4X^2-4X+5=4(X-x_1)(X-x_2)=4\left(X-\frac{1}{2}-i\right)\left(X-\frac{1}{2}+i\right).$$

La décomposition dans $\mathbb{C}(X)$ est de la forme :

$$F(X)=\frac{1}{2}X+\frac{A}{X+1}+\frac{B}{X-\dfrac{1}{2}-i}+\frac{C}{X-\dfrac{1}{2}+i}=\frac{1}{2}X+G(X)$$

$a=-1$; $\dfrac{1}{2}+i$ et $\dfrac{1}{2}-i$ sont des pôles simples. On multiplie par $(X-a)$, on simplifie et on fait tendre X vers a (ou bien on le remplace par a).

$$F(X)=\frac{P(X)}{(X+1)(4X^2-4X+5)}$$

$$(X+1)F(X)=\frac{1}{2}X(X+1)+A+\frac{B(X+1)}{X-\dfrac{1}{2}-i}+\frac{C(X+1)}{X-\dfrac{1}{2}+i}\text{ donc}$$

$$\frac{2X^4-3X^2-X+2}{4X^2-4X+5}=\frac{1}{2}X(X+1)+A+\frac{B(X+1)}{X-\dfrac{1}{2}-i}+\frac{C(X+1)}{X-\dfrac{1}{2}+i}.$$

$$\lim_{x\to-1}\frac{2X^4-3X^2-x+2}{4X^2-4X+5}=A\text{ d'où }A=\frac{2}{13}.$$

On pouvait écrire :

$$(X+1)G(X)=(X+1)\left[\frac{A}{X+1}+\frac{B}{X-\dfrac{1}{2}-i}+\frac{C}{X-\dfrac{1}{2}+i}\right]$$

$$(X+1)\frac{\dfrac{-7}{2}X^2-\dfrac{7}{2}X+2}{(X+1)\,(4X^2-4X+5)}=A+\frac{B(X+1)}{X-\dfrac{1}{2}-i}+\frac{C(X+1)}{X-\dfrac{1}{2}+i}$$

$$\frac{\frac{-7}{2}X^2-\frac{7}{2}X+2}{4X^2-4X+5}=A+\frac{B(X+1)}{X-\frac{1}{2}-i}+\frac{C(X+1)}{X-\frac{1}{2}+i}$$

En remplaçant X par -1 on a : $\dfrac{\frac{-7}{2}+\frac{7}{2}+2}{4+4+5}=A$ d'où $A=\dfrac{2}{13}$

$$G(X) \quad = \quad \frac{\frac{2}{13}}{X+1}+\frac{B}{X-\frac{1}{2}-i}+\frac{C}{X-\frac{1}{2}+i}.$$

De même

$$\left(X-\frac{1}{2}-i\right)G(X)=\frac{2}{13}\frac{X-\frac{1}{2}-i}{X+1}+B+\frac{C\left(X-\frac{1}{2}-i\right)}{X-\frac{1}{2}+i}$$

$$\begin{aligned}\frac{\left(X-\frac{1}{2}-i\right)\left(\frac{-7}{2}X^2-\frac{7}{2}X+2\right)}{4\left(X+1\right)\left(X-\frac{1}{2}-i\right)\left(X-\frac{1}{2}+i\right)} &= \left(X-\frac{1}{2}-i\right)G(X)\\ &= \frac{2}{13}\frac{X-\frac{1}{2}-i}{X+1}+B+\frac{C\left(X-\frac{1}{2}-i\right)}{X-\frac{1}{2}+i}\end{aligned}$$

$$\frac{\frac{-7}{2}X^2-\frac{7}{2}X+2}{4\left(X+1\right)\left(X-\frac{1}{2}+i\right)}=\frac{2}{13}\frac{X-\frac{1}{2}-i}{X+1}+B+\frac{C\left(X-\frac{1}{2}-i\right)}{X-\frac{1}{2}+i}$$

En remplaçant X par $\dfrac{1}{2}+i$ on a :

$$\frac{\frac{-7}{2}\left(\frac{1}{2}+i\right)^2-\frac{7}{2}\left(\frac{1}{2}+i\right)+2}{4\left[\left(\frac{1}{2}+i\right)+1\right]\left[\left(\frac{1}{2}+i\right)-\frac{1}{2}+i\right]}=B$$

$$\text{d'où} \quad B = \frac{\frac{23}{8} - 7i}{8i\left(\frac{3}{2} + i\right)} = \frac{\frac{23}{8} - 7i}{-8 + 12i}$$

$$\boxed{B = \frac{-107}{208} + \frac{43}{416}i}$$

Calcul de C :

On peut procéder de la même manière que pour B ou considérer que $G(X)$ est une fraction de $\mathbb{R}(X)$ donc en prenant les conjugués,

$$G(X) = \overline{G(X)} = \frac{\frac{2}{13}}{X+1} + \frac{\overline{B}}{X - \frac{1}{2} + i} + \frac{\overline{C}}{X - \frac{1}{2} - i}$$

or,

$$G(X) = \frac{\frac{2}{13}}{X+1} + \frac{B}{X - \frac{1}{2} - i} + \frac{C}{X - \frac{1}{2} + i} \ ,$$

la décomposition d'une fraction rationnelle étant unique on a : $C = \overline{B}$ (et $B = \overline{C}$)

$$\boxed{C = \frac{-107}{208} - \frac{43}{416}i}$$

La décomposition de $G(X)$ dans $\mathbb{C}(X)$ s'écrit :

$$G(X) = \frac{\frac{2}{13}}{X+1} + \frac{\frac{-107}{208} + \frac{43}{416}i}{X - \frac{1}{2} - i} + \frac{\frac{-107}{208} - \frac{43}{416}i}{X - \frac{1}{2} + i}$$

$$\boxed{F(X) = \frac{1}{2}X + G(X) = \frac{1}{2}X + \frac{\frac{2}{13}}{X+1} + \frac{\frac{-107}{208} + \frac{43}{416}i}{X - \frac{1}{2} - i} + \frac{\frac{-107}{208} - \frac{43}{416}i}{X - \frac{1}{2} + i}.}$$

En regroupant les parties principales relatives aux pôles complexes non réels on a :

$$\frac{\left(\frac{-107}{208} + \frac{43}{416}i\right)\left(X - \frac{1}{2} + i\right) + \left(\frac{-107}{208} - \frac{43}{416}i\right)\left(X - \frac{1}{2} - i\right)}{\left(X - \frac{1}{2} - i\right)\left(X - \frac{1}{2} + i\right)} = \frac{\frac{-107}{104}X + \frac{4}{13}}{X^2 - X + \frac{5}{4}}$$

d'où

$$G(X) = \frac{\frac{2}{13}}{X+1} + \frac{\frac{-107}{104}X + \frac{4}{13}}{X^2 - X + \frac{5}{4}}$$

et

$$\boxed{F(X) = \frac{1}{2}X + \frac{\frac{2}{13}}{X+1} + \frac{\frac{-107}{104}X + \frac{4}{13}}{X^2 - X + \frac{5}{4}}}$$

$$\downarrow$$

Décomposition de $F(X)$ dans $\mathbb{R}(X)$

Pour décomposer $F(X)$ dans $\mathbb{R}(X)$ on peut procéder comme suit :

On extrait la partie entière $\frac{1}{2}X$ et on écrit:

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

$$F(X) = \frac{1}{2}X + \frac{A}{X+1} + \frac{E'X + E"}{X^2 - X + \frac{5}{4}} = \frac{1}{2}X + G(X)$$

E et E' étant des réels à déterminer.

$$A = \lim_{X \to -1}(X+1)F(X) = \frac{2}{13}$$

Pour déterminer E et E' on peut:

1) procéder par soustraction

$$\begin{aligned} F(X) - \frac{1}{2}X - \frac{A}{X+1} &= \frac{2X^4 - 3X^2 - X + 2}{4X^3 + X + 5} + \frac{-2X^4 + \frac{-1}{2}X^2 - \frac{5}{2}X}{4X^3 + X + 5} \\ &\quad + \frac{\frac{-2}{13} \times 4(X^2 - X + \frac{5}{4}}{4X^3 + X + 5} \\ F(X) - \frac{1}{2}X - \frac{A}{X+1} &= \frac{\frac{-107}{26}X^2 - \frac{75}{26}X + \frac{16}{13}}{4X^3 + X + 5} \end{aligned}$$

-1 annule le numérateur et le dénominateur de cette fraction ; on simplifie par $X + 1$:

$$F(X) - \frac{1}{2}X - \frac{\frac{2}{13}}{X+1} = \frac{\frac{-107}{26}X + \frac{16}{13}}{4\left(X^2 - X + \frac{4}{5}\right)}$$

d'où

$$F(X) - \frac{1}{2}X - -\frac{\frac{2}{13}}{X+1} = \frac{\frac{-107}{104}X + \frac{4}{13}}{X^2 - X + \frac{5}{4}}$$

2) procéder par identification après avoir réduit au même dénominateur :

$$\begin{aligned} F(X) &= \frac{1}{2}X + \frac{\frac{2}{13}}{X+1} + \frac{E'X + E"}{X^2 - X + \frac{5}{4}} \\ &= \frac{\frac{1}{2}X(4X^3 + X + 5) + \frac{2}{13}(4X^2 - 4X + 5)}{4(X+1)\left(X^2 - X + \frac{5}{4}\right)} + \frac{(4E'X + 4E")(X+1)}{4(X+1)\left(X^2 - X + \frac{5}{4}\right)} \end{aligned}$$

$$\begin{aligned} F(X) &= \frac{2X^4 + \left(\frac{1}{2} + \frac{8}{13} + 4E'\right)X^2 + \left(\frac{5}{2} - \frac{8}{13} + 4E' + 4E"\right)X + \frac{10}{13} + 4E"}{4X^3 + X + 5} \\ F(X) &= \frac{2X^4 - 3X^2 - X + 2}{4X^3 + X + 5} \end{aligned}$$

D'où , par identification on a :

$$\begin{cases} \dfrac{1}{2}+\dfrac{8}{13}+4E'=-3 \\ \dfrac{5}{2}-\dfrac{8}{13}+4E'+4E''=-1 \\ \text{et} \quad \dfrac{10}{13}+4E''=2 \end{cases} \Longrightarrow \begin{cases} E'=\dfrac{-107}{104} \\ E''=\dfrac{4}{13} \end{cases}$$

3) procéder par remplacements de X par des valeurs 0, 1, -1, 2, $\cdots$ et par résolutions.

Par 0 on a :

$$\frac{2}{5}=F(0)=\frac{2}{13}+\frac{E''}{\frac{5}{4}}$$

d'où

$$E''=\frac{5}{4}\left(\frac{2}{5}-\frac{2}{13}\right)=\frac{5}{4}\left(\frac{26-10}{5\times 13}\right)=\frac{4}{13}$$

4) procéder par multiplication de $G(X)$ par X et faire tendre X vers l'infini :

on a

$$\frac{2}{13}+E'=\lim_{X\to\infty} XG(X)=\frac{\frac{-7}{2}}{4}$$

$$E'=\frac{-7}{8}-\frac{2}{13}=\frac{-107}{104}$$

C) Techniques de décomposition en éléments simples

1) Recherche de la partie entière $E(X)$:
si $d^o\ P \geq d^o\ Q$ alors $d^o\ E = d^o\ P - d^o\ Q$ et on peut déterminer $E(X)$ par division euclidienne de P par Q.

2) S'il existe un pôle simple α on multiplie par $X-\alpha$, on simplifie et on fait tendre X vers α; alors on trouve le coefficient A tel que la partie polaire relative à α s'écrit $\dfrac{A}{X-\alpha}$.

3) Si α est un pôle multiple d'ordre $k \geq 2$, la fraction s'écrit $\dfrac{P(X)}{(X-\alpha)^k Q_1(X)}$ (avec $Q_1(\alpha) \neq 0$), on détermine un coefficient en multipliant par $(X-\alpha)^k$ et en faisant tendre X vers α après simplifications.

4) On peut parfois simplifier les calculs par des conditions de parité.

Exemple: $F(X) = \dfrac{X^2-2}{(X^2-4)^2}$

$$F(X) = \frac{X^2-2}{[(X-2)(X+2)]^2} = \frac{X^2-2}{(X-2)^2(X+2)^2}$$

La partie entière est nulle car $d^o\ P < d^o\ Q$.

$$F(X) = \frac{A_2}{(X-2)^2} + \frac{A_1}{X-2} + \frac{B_2}{(X+2)^2} + \frac{B_1}{X+2}$$

car les pôles sont 2 et -2 et ils sont d'ordre 2;

F est paire: $F(-X) = F(X)$ d'où

$$\begin{aligned} F(-X) &= \frac{A_2}{(-X-2)^2} + \frac{A_1}{-X-2} + \frac{B_2}{(-X+2)^2} + \frac{B_1}{-X+2} \\ &= F(X) \end{aligned}$$

d'où

$$\begin{aligned} F(-X) &= \frac{A_2}{(X+2)^2} + \frac{-A_1}{X+2} + \frac{B_2}{(X-2)^2} + \frac{-B_1}{X-2} = F(X) \\ F(X) &= \frac{B_2}{(X+2)^2} + \frac{B_1}{X+2} + \frac{A_2}{(X-2)^2} + \frac{A_1}{X-2} \end{aligned}$$

or, la décomposition d'une fraction rationnelle est unique, on a alors (par identification):

$$\left\{\begin{array}{l} B_2 = A_2 \\ B_1 = -A_1 \end{array}\right.$$

Détermination de A_1 et A_2 :

$$F(X)=\frac{X^2-2}{(X^2-4)^2} = \frac{A_2}{(X-2)^2}+\frac{A_1}{X-2}+\frac{A_2}{(X+2)^2}+\frac{-A_1}{X+2}$$

a) Multiplions par $(X-2)^2$ et faisons tendre X vers 2 :

$$\begin{aligned}\lim_{X\to 2}(X-2)^2 F(X) &= \lim_{X\to 2}\left(A_2+A_1(X-2)+\frac{A_2(X-2)^2}{(X+2)^2}+\frac{-A_1(X-2)^2}{X+2}\right) \\ &= \lim_{X\to 2}\frac{(X-2)^2\left(X^2-2\right)}{(X-2)^2(X+2)^2} = \lim_{X\to 2}\frac{X^2-2}{(X+2)^2}\end{aligned}$$

d'où

$$A_2 = \frac{2}{16} = \frac{1}{8}.$$

$$F(X) = \frac{1/8}{(X-2)^2}+\frac{A_1}{X-2}+\frac{1/8}{(X+2)^2}+\frac{-A_1}{X+2}.$$

On peut remplacer X par 0 :

$$F(0) = \frac{-2}{16} = \frac{1/8}{4}+\frac{A_1}{-2}+\frac{1/8}{4}+\frac{-A_1}{2}$$

$$A_1 = \frac{3}{16}.$$

$$\boxed{F(X) = \frac{1/8}{(X-2)^2}+\frac{\frac{3}{16}}{X-2}+\frac{1/8}{(X+2)^2}+\frac{-\frac{3}{16}}{X+2}}$$

5) Pour la détermination des éléments de $2^{ème}$ espèce dans $\mathbb{R}(X)$ on peut faire tendre X vers l'infini après avoir multiplié par des X^n ou remplacer X par 0, 1, -1, 2, $-2, \cdots$ s'ils ne sont pas pôles de la fraction rationnelle et par résolution.

6) On peut aussi procéder par identification.

Références

M. Serfati, Exercices de mathématiques. 1. Algèbre, Belin, Collection DIA, 1987.

D. Duverney, S. Heumez, G. Huvent, Toutes les mathématiques – Cours, exercices corrigés – MPSI,

FICHE n°1
Ensembles et Applications

Exercice 1

Donner des exemples d'applications de R dans R (puis de R2 dans R) injective

et non surjective, puis surjective et non injective.

Exercice 2

Soit f : R $\mathbb{R} \longrightarrow \mathbb{R}$ R définie par f(x) = $x^3 -$ x.

f est-elle injective? surjective? Déterminer $f^{-1}1([-1;1])$ et $f(\mathbb{R}_+)$.

Exercice 3

Soit f :$\mathbb{R} \longrightarrow \mathbb{R}$ dé nie par f(x) = $2x/(1+x^2)$.

1. f est-elle injective? surjective?

2. Montrer que $f(\mathbb{R}) = [-1;1]$.

3. Montrer que la restriction g :$[-1;1] \longrightarrow [-1;1]$, g(x) = f(x) est une bijection.

4. Retrouver ce résultat en étudiant les variations de f.

Exercice 4

Soit f : $[0;1] \longrightarrow [0;1]$ telle que

f(x) =$\begin{cases} x \text{ si x} \in [0,1] \cap \mathbb{Q} \\ 1-x \text{ si } \notin [0,1] \cap \mathbb{Q} \end{cases}$

Déterminer fof.

EXERCICE 5

Soit A, B étant deux sous-ensembles d'un ensemble E, $\overline{A}$ désigne le complémentaire de A.

1°) a) Montrer que : A⊂B$\Longrightarrow$A∩B=A

b) Montrer que : A⊂B$\Longrightarrow$A∪B=B

2°) Simplifier : ; ; (A∩B)∩(A∪B) ; A∪(A∩B) :(A∪B)∩(A∪$\overline{B}$) : (A∩B)∪($\overline{A}$∩B).

Exercice 6

Soit E un ensemble et A,B,C trois parties de E.

1. Montrer que (A∪ B) ∩ (B∪ C) ∩ (C∪ A) = (A∩ B)∪ (B ∩ C)∪ (C∩ A).

2.On définit sur P(E) l'ensemble des parties de E une opération o par :

AoB=$\overline{A} \cap \overline{B}$. Exprimer à l'aide de la seule opération o : $\overline{A}$, A∪B, A∩B.

Exercice 7

. Soient deux ensembles E=$\{1, a\}$, F=$\{a, b\}$.Determiner et comparer
P(E $\times$F) avec P(E) $\times$P(F), P(E $\cap$ F) avec P(E) $\cap$ P(F) et P(E $\cup$ F) avec P(E) $\cup$ P(F).

Exercice 8(**MI**)
Soit E un ensemble, et soit A, B $\in$P(E) deux parties de E.
Soit f la fonction :
f : P(E) $\longrightarrow$P(A) $\times$(A^c)
X $\longmapsto$(X$\cap$ A, X $\cap$ A^c)
Montrer que f est bijective.

Exercice 9(**MI**) :
Soit X et Y deux ensembles et une application $f : X \longrightarrow Y$.
Prouver l'équivalence suivante :
f est injective $\Longleftrightarrow(\forall A, B \subset X, A \cap B = \varnothing \Longrightarrow f(A) \cap f(B) = \varnothing)$.

Exercice 10(**MI**)
Soit f une application d'un ensembie E dans un ensemble F.
Démontrer l'équivalence des propositions suivantes :
1. (pour toute partie X de E, $f^{-1}(f(X)) = X$)$\Longleftrightarrow$ f est injective
2. (pour toute partie Y de B , $f\left(f^{-1}(Y)\right) = Y) \Longleftrightarrow$ f est est surjective

FICHE n^0 2
Relations binaires

Exercice 1.
On définit sur un groupe multiplicatif G une relation $\mathcal{R}$ par :
$\forall$x,y $\in$G, x$\mathcal{R}$y $\Longleftrightarrow$xy^{-1} $\in$H où H est un sous-groupe de G.
La relation $\mathcal{R}$ est-elle
1) reflexive ?
2) symétrique ?
3) antisymétique ?
4) transitive ?

Exercice 2
Soit E un ensemble, on note P(E) l'ensemble des parties de E.
On définit sur P(E) une relation $\mathcal{R}$ par :
$\forall A, B \in$P(E) , $A\mathcal{R}B \Longleftrightarrow A \cap \overline{B} = \emptyset$ où $\overline{B}$ désigne le complémentaire de B dans E.
La relation $\mathcal{R}$ est-elle
1) une relation d'équivalence ?
2) une relation d'ordre?
Justifiez vos réponses.

Exercice 3 :

1)Soit X = {a,b ,c }.
Sur X on considère la relation $\Re$ dont le graphe est l'ensemble G suivant :
G = {(a, a), (a, b),(b,b), (b, a) , (c,c),(b,c) }.
Cette relation est-elle réflexive ? symétrique ? antisymétrique ? transitive ?

Exercice 4
On définit sur $\mathbb{R}^*$ une relation R par : xRy $\iff$ xe^y=ye^x.
1. Montrer que R est une relation d'équivalence.

2.Déterminer le cardinal de la classe d'un élément $x \in \mathbb{R}^*$.

Exercice 5

Soit X = {1, 2, 3, 4}.
Sur X on consid'ere la relation dont le graphe est l'ensemble G suivant :
G = {(1, 1), (1, 2), (2, 1), (2, 2), (2, 4), (3, 4), (4, 2), (4, 3), (4, 4)}.
Cette relation est-elle réflexive ? symétrique ? antisymétrique ? transitive ?

Exercice 6
On d´efinit une relation R sur $\mathbb{R}$en posant, pour tous réels x et y :

$$x \ R \ y \Leftrightarrow x^2 - y^2 = x - y.$$

1) Montrer que R est une relation d'´equivalence.
2) Quel est le graphe de R?
3) Déterminer les classes d'équivalence des réels 0, 1,2.

Exercice 7
On dit qu'une relation R sur un ensemble X est circulaire lorque pour tous a, b et c de X :

$$(a \ R \ b \text{ et } b \ R \ c) \Rightarrow c \ R \ a.$$

1) Montrer qu'une relation est une relation d'équivalence si et seulement si elle est réflexive et circulaire.
2) Donner un exemple de relation circulaire qui ne soit pas une relation d'équivalence.

Exercice 8
On définit une relation R sur $\mathbb{N}^2$ en posant, pour tous entiers naturels a, b, c et d :

$$(a, b) \ R \ (c, d) \Leftrightarrow a + d = b + c.$$

1) Montrer que R est une relation d'´equivalence.

2) Déterminer les classes d'équivalence respectives de (0, 0), de (3, 1), de (2, 4).

3) Décrire l'ensemble-quotient $\mathbb{N}^2/\mathrm{R}$.

Exercice 9

Soit E un ensemble.

Sur l'ensemble P(E) on définit une relation R en posant, pour tous A, B inclus dans E

ARB $\Leftrightarrow$ ((A = B) ou (A est le complémentaire de B dans E)).

Montrer que R est une relation d'´equivalence sur P(E).

Exercice 10

On définit dans $\mathbb{Q}$ une relation$\ll$ en posant, pour tous x, y de $\mathbb{R}_+^{\bigstar}$:x$\ll$ y $\Leftrightarrow$ $\exists$n$\in$ $\mathbb{Q}$, y = x^n.

Montrer que $\ll$ est une relation d'equivalence sur $\mathbb{Q}$.

FICHE n^{o}3 Groupes-Anneaux-Corps

Exercice 1

1) Soit (G,$\star$) un groupe et f une bijection de G dans G. On définit sur G une loi notée T par :

$$\mathrm{a\ T\ b} = \mathrm{f}(\mathrm{f}^{-1}(\mathrm{a}) \star \mathrm{f}^{-1}(\mathrm{b}))$$

(G,T) est-il un goupe?

2) On définit sur I=$]-1,1[$ une loi $\star$ par x$\star$y=$\frac{\mathrm{x+y}}{\mathrm{1+xy}}$. (I,$\star$) est-il un goupe?

Exercice 2

1)Soient $a \in \mathbb{R}^*, b \in \mathbb{R}$ et $f : \mathbb{R} \longrightarrow \mathbb{R}, x \longmapsto ax + b$.

Montrer que f est une bijection dont on déterminera la bijection réciproque .

2) Montrer que l'ensemble $H = \{f_{a,b} : \mathbb{R} \longrightarrow \mathbb{R}, x \longmapsto ax + b, a \in \mathbb{R}^*, b \in \mathbb{R}\}$ est un sous groupe du goupe G des applications bijectives de $\mathbb{R}$ vers $\mathbb{R}$ muni de la loi de composition des applications.

3) Montrer que l'application $\varphi : (H, o) \longrightarrow (H, o)$, $f_{a,b} \longmapsto f_{a,-b}$ est un automorphisme du groupe H..

Exercice 3.

Soit E =$\{-1, 1\}$.

1)Montrer que E est un groupe pour la multipliction usuelle

Exercice 4

On définit sur $\mathbb{R}^2$ une loi $\star$ par $(x_1, y_1)\star(x_2 , y_2)=(x_1, y_1)\star(x_2 , y_2)=(x_1x_2 , x_2y_1+x_1y_2)$

Montrer que $(\mathbb{R}^2, +, \star)$ est un anneau commutatif. + étant l'addition usuelle sur $\mathbb{R}^2$.

Exercice 5

On définit sur $\mathbb{R}$ les deux lois T et Δ par xTy=x+y-1 et xΔy=x+y-xy.

Montrer que $(\mathbb{R}, T, \Delta)$ est un corps.

EX 6

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 2 & 5 & 7 & 8 & 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$$

Les décomposer en produit de cycles à supports disjoints, puis en produits de transpositions.

Calculer la signature des permutations ci-dessus.

FICHE 4 Arithmétique

Exercice 1

Soient m> 1 et n > 2 des entiers; montrer que :

1. n - 1 | n^m - 1 ;
2. $(n-1)^2$ | n^m - 1 ; si et seulement si n -1 | m.

Exercice 2

Soit a un entier relatif quelconque, démontrer que le nombre a(a^2- 1) et, plus généralement, a(a^{2n}- 1) est divisible par 6.

Exercice 3

Démontrer que le nombre $7^n + 1$ est divisible par 8 si n est impair; dans le cas n pair, donner le reste de sa division par 8.

Exercice 4

Trouver tous les entiers relatifs n tels que $n^2 + n + 7$ soit divisible par 13.

Exercice 5

On considère le nombre $m = 2^n p$, dans lequel n désigne un entier naturel quelconque et p un nombre premier. Dresser la liste des diviseurs de m, y compris 1 et m lui-même, et calculer, en fonction de m et p, la somme S de tous ces diviseurs.

Exercice 6

Soient a et b deux entiers tels que a > b > 1 et pgcd(a; b) = 1.

1. Montrer que pgcd(a + b; a - b) = 1 ou 2,

2. Si pgcd(a; b) = 1, montrer que pgcd(a + b; ab) = 1,

3. Si pgcd(a; b) = 1, montrer que pgcd(a + b; $a^2 + b^2$) = 1 ou 2.

4. Soit m et n deux entiers positifs.
Si pgcd(m; 4) = 2 et pgcd(n; 4) = 2, montrer que pgcd(m + n; 4) = 4.

Exercice 7
Calculer par l'algorithme d'Euclide :pgcd (18480, 9828).
En déduire une écriture de 84 comme combinaison linéaire de 18480 et 9828.

FICHE n°5
-Décomposition en éléments simples

Exercice 1
1)Décomposer sur $\mathbb{R}$ les fractions rationnelles suivantes :
a) $\dfrac{2X^5 - 8X^3 + 8X^2 - 4X + 1}{X^3 (X-1)^2}$ $\quad b) \dfrac{16}{(1-X^2)^3}$
Décomposer en éléments simple dans $\mathbb{R}$ la fraction rationnelle suivante :
$F(X) = \dfrac{X^2 + X + 1}{(X-1)^2 (X+1)^2 (X^2+1)}$

2)Décomposer sur $\mathbb{R}$ et sur $\mathbb{C}$ les fractions rationnelles suivantes :

$$\frac{X^2 - 6}{(X^2+1)(4+X^2)}$$

Exercice 2
Décomposer en éléments simples sur $\mathbb{R}$ et sur $\mathbb{C}$ les fractions rationnelles suivantes:

$$\frac{3}{(X+1)^4 (X+3)} \quad ; \quad \frac{X^5 + X + 1}{X^4 - 1}$$

Exercice 3
Décomposer les fractions rationnelles suivantes :

$$\frac{3}{X^3+1} \text{ sur } \mathbb{C} \text{ puis sur } \mathbb{R}$$

$$\frac{X^3}{X^3-1} \text{ sur } \mathbb{R}$$

$$\frac{X^2 + X + 1}{(X-1)^2 (X+1)^2} \text{ sur } \mathbb{R}$$

$$F(X) = \frac{1}{(X^3-1)^2} \text{ sur } \mathbb{C} \text{ en remarquant que } F(jX) = F(X)$$

$$\frac{X^7+1}{(X^2+1)(X^2+X+1)} \text{ sur } \mathbb{R}$$

$$\frac{3X^5+2X^4+X^2+3X+2}{X^4+1} \text{ sur } \mathbb{R}$$

$$\frac{1}{X^{2n}+1} \text{ sur } \mathbb{C} \text{ puis sur } \mathbb{R}$$

$$\frac{X^3+X}{(X^2+X+1)^2} \text{ sur } \mathbb{R}$$

Exercice 4

Effectuer la division euclidienne du polynôme (puissances décroissantes) $P = X^5 - X^4 + 2X^3 + X^2 + 4$ par $Q = X^2 - 1$. Même exercice lorsque $P = X^4 - 2X\cos(2\varphi) + 1$ et $Q = X^2 - 2X\cos(\varphi) + 1$.

Exercice 5

Calculer le reste de la division euclidienne du polynôme X^n par le polynôme $Q = X^2 + 1$ et $X^n + X + 1$ par le polynôme $(X-1)^2$(puissances décroissantes)