RÉVISION ET COURS : GROUPES - ANNEAUX - POLYNÔMES

I. GROUPES

1. **Définition 1**

Soit G un ensemble non vide. On appelle **loi de composition interne** sur G toute application de $G \times G$ dans G.

On la note en général : $*$, $+$, $\cdot$, $\times$, $\circ$ ...

Remarque : Lorsque la loi est notée $\cdot$, le produit $x \cdot y$ est noté xy.

2. **Définition 2**

Soit G un ensemble non vide muni d'une loi de composition interne $\cdot$ sur G.

On dit que $(G, \cdot)$ est un **groupe** si

> i) La loi $\cdot$ est associative : $\forall (x, y, z) \in G^3,\ \ (xy)z = x(yz)$
> ii) G admet un élément neutre pour la loi $\cdot$: $\exists e \in G$ tel que $\forall x \in G,\ xe = ex = \ldots x$.
> iii) Tout élément de G admet un symétrique pour la loi $\cdot$:
> $\forall x \in G,\ \exists x' \in G$ tel que $xx' = x'x = \ldots e$.

On dit que le groupe $(G, \cdot)$ est **commutatif** (ou **abélien**) si la loi $\cdot$ est commutative : $\forall (x, y) \in G^2 : yx = \ldots xy$

Remarque 1 : S'il n'y a pas d'ambiguïté sur la loi on dira simplement que G est un groupe au lieu de $(G, \cdot)$.

Remarque 2 : L'élément neutre est noté généralement e ou e_G ou 1_G ou 1 pour une loi multiplicative et 0_G ou 0 pour une loi additive.

Remarque 3 : Le symétrique est appelé **..inverse** pour une loi multiplicative et noté x^{-1} (et même noté $\frac{1}{x}$ si la loi est commutative). Il est appelé **..opposé** pour une loi additive et noté $-x$.

Exercice : Rayer les intrus *(qui ne sont pas des groupes)*

$(\mathbb{N}, +)$ $(\mathbb{Z}, +)$ $(\mathbb{Q}^*, \times)$ $(\mathbb{R}, \times)$ $(\mathbb{R}, +)$ $(\mathbb{R}, -)$ $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +)$ $(\mathcal{M}_n(\mathbb{R}), \times)$
$(\mathbb{R}^{\mathbb{N}}, +)$ $(\mathbb{K}[X], \times)$ $(\mathcal{L}(E, F), +)$ $(\mathcal{L}(E), \circ)$ $(GL(E), \circ)$ $E \neq \emptyset, (\mathcal{P}(E), \bigcup)$ $(\mathcal{P}(E), \Delta)$

3. **Propriétés**

Proposition 1 : L'inverse de xy dans le groupe $(G, \cdot)$ est $\ldots y^{-1}x^{-1}$.

Proposition 2 : Dans un groupe tout élément est **simplifiable**. C'est-à-dire que si $(G, \cdot)$ est un groupe alors :

$$\forall a \in G,\ \forall (x, y) \in G^2 : \qquad ax = ay \Longrightarrow x = y \qquad \text{et} \qquad xa = ya \Longrightarrow x = y.$$

Démonstration 1

4. **Règles de calcul** :

Soit $(G, \cdot)$ un groupe. Soit $x \in G$ et $n \in \mathbb{N}^*$.

Le produit $x \cdot x \cdot \cdots \cdot x$ (n exemplaires de x) est noté x^n et x^0 est par convention égal à e.

Rigoureusement x^n est définit récursivement par $\begin{cases} x^0 = e \\ x^{n+1} = x^n \cdot x \end{cases}$

Le produit $x^{-1} \cdot x^{-1} \cdot \cdots \cdot x^{-1}$ ($n \in \mathbb{N}$ exemplaires de x^{-1}) est noté x^{-n}.

Proposition : $\forall x \in G$ et $\forall (n, p) \in \mathbb{Z}^2 : x^n x^p = x^{n+p}$ et $(x^n)^p = x^{np}$.

Démonstration 2

Remarque : Si la loi est additive, x^n est alors noté $\ldots nx$.

5. **Sous-Groupe**

Définition : H est un **sous-groupe** de $(G, \cdot)$ si H est stable pour la loi $\cdot$ et si $(H, \cdot)$ est lui même un groupe.

Théorème : Soit $(G,\cdot)$ un groupe et soit $H \subset G$. On a :

$$H \text{ est un sous groupe de } (G,\cdot) \quad \boxed{\text{SSI}} \quad \begin{cases} H \neq \emptyset \quad (e_G \in H) \\ \forall (x,y) \in H^2 \ : \ \bullet\bullet xy \in H \ \text{ et } \ \bullet\bullet x^{-1} \in H \end{cases}$$

Démonstration 3

Remarque : On peut contracter avec $\forall (x,y) \in H^2 \ : \ \bullet\bullet xy^{-1} \in H$.

Corollaire : Pour montrer **qu'un ensemble E est un groupe** il suffit de prouver qu'il est inclus dans un groupe connu G et de montrer que c'est un sous groupe de G.

6. **Morphisme de groupes**

Définition : L'application f de $(G,\cdot)$ dans $(G',*)$ est un **morphisme de groupes** si

$$\boxed{\forall (x,y) \in G^2 \ : \ \bullet\bullet f(xy) = f(x) * f(y)}$$

Proposition 1 : Si f est un morphisme de G dans G' alors

$$\boxed{f(e_G) = e_{G'} \text{ et pour tout } x \text{ dans } G,\ f(x^{-1}) = \bullet\bullet f(x)^{-1}}$$

Démonstration 4

Proposition 2 : La composée de morphismes est un morphisme et la réciproque d'un morphisme bijectif est un morphisme (bijectif).

Démonstration 5

Définition : Un morphisme bijectif est appelé $\bullet\bullet$ **isomorphisme** et si de surcroit $G = G'$ alors ce morphisme est appelé $\bullet\bullet$ **automorphisme**.

Définition : Soit f un morphisme de groupes de $(G,\cdot)$ dans $(G',*)$.

On appelle $\bullet\bullet$ **noyau** de f le sous-ensemble de G noté $\ker f = \{x \in G \ , \ f(x) = e_{G'}\}$.

On appelle $\bullet\bullet$ **image** de f le sous-ensemble de G' noté $\text{im } f = \{y \in G' \text{ tel que } \exists x \in G \text{ et } y = f(x)\}$

Proposition 1 : Si f un morphisme de $(G,\cdot)$ dans $(G',*)$ alors on a :

$$\boxed{\ker f \text{ est un sous-groupe de } G \qquad \text{et} \qquad \text{im } f \text{ est un sous-groupe de } G'.}$$

Démonstration 6

Proposition 2 : Si f un morphisme de $(G,\cdot)$ dans $(G',*)$ alors on a :

$$\boxed{f \text{ est injective SSI } \bullet\bullet \ker f = \{e_G\} \qquad \text{et} \qquad f \text{ est surjective SSI } \bullet\bullet \text{im } f = G'.}$$

Démonstration 7

II. ANNEAUX

1. **Définition** :

Soit A un ensemble non vide muni de 2 **L.C.I.** notées $+$ et $*$ (très souvent $* = \times$ ou $* = \circ$).

On dit que $(A,+,*)$ est un **anneau** si :

i) $(A,+)$ est un **groupe abélien** et on note 0 l'élément neutre de $+$,

ii) $*$ est **associative** et A possède un élément **neutre** pour la loi $*$ (noté e ou 1 ou id ...) ,

iii) $*$ **est distributive par rapport à** $+$ **:**

$\forall (x,y,z) \in A^3 \ : (x+y)*z = x*z + y*z \quad$ et $\quad z*(x+y) = z*x + z*y.$

Si de plus $*$ est **commutative** alors l'anneau est dit **commutatif**.

2. **Exemples** : Rayer les intrus

$(\mathbb{N},+,\times)$; $(\mathbb{Z},+,\times)$; $(\mathbb{Q},+,\times)$; $(\mathbb{R},+,\times)$; $(\mathbb{C},+,\times)$; $(\mathbb{K}[X],+,\times)$; $(\mathcal{L}(E),+,\circ)$; $(\mathcal{M}_{n,p}(\mathbb{R}),+,\times)$ (avec $n \neq p$).
$(\mathcal{M}_n(\mathbb{R}),+,\times)$; $(\mathcal{F}(I,\mathbb{R}),+,\times)$; $(\mathcal{F}(\mathbb{R},\mathbb{R}),+,\circ)$

3. **Propriétés** :

i) $\forall x \in A \ : \ x * 0 = 0 * x = 0$ (0 : élément **absorbant**).

ii) $\forall (x,y) \in A^2 \ : \ -(x*y) = (-x)*y = x*(-y)$.

iii) $\forall (x,y,z,t) \in A^4 \ : \ (x+y)*(z+t) = x*z + x*t + y*z + y*t$.

Démonstration 8

Attention : On peut avoir $x*y = 0$ avec $x \neq 0$ et $y \neq 0$. (Exemple : dans $\mathcal{M}_n(\mathbb{R})$ avec $n \geqslant 2$). Soient $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix}$. On a $AB = \ldots \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et $BA = \ldots \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$.

Définition : Un anneau A est dit **intègre** si $\forall (x,y) \in A^2,\ xy = 0_A \implies \ldots x = 0_A$ ou $y = 0_A$.

4. **Éléments inversibles** :

Soit $(A,+,*)$ un anneau et a un élément de A. On dit que a est un élément **inversible** de A,

s'il **existe un élément** b de A tel que $a*b = b*a = 1_A$ (1_A : élément neutre pour $*$).

Notation : a^{-1}.

Définition : On appelle **groupe des éléments inversibles** de A, noté : A^*, l'ensemble des éléments inversibles de $(A,+,*)$.

$$A^* = \{a \in A \text{ tel que : } \exists b \in A \text{ tel que } a*b = b*a = 1_A\}.$$

Proposition :

$$(A^*, *) \text{ est un } \ldots \text{groupe}.$$

Démonstration 9

Exemples : Déterminer $\mathbb{Z}^* = \{$ $\mathbb{R}^* =$ $\mathbb{R}[X]^* =$ $\mathcal{L}(E)^* =$

5. **Binôme de Newton** :

Notation : Soit $(A,+,*)$ un anneau et a élément de A, on note :

$\forall n \in \mathbb{N}^* \ : \ na = \underbrace{a + a + \cdots + a}_{n \ fois}$, $(-n)a = -(na)$ et $0a = 0$.

$\forall n \in \mathbb{N}^* \ : \ a^n = \underbrace{a * a * \cdots * a}_{n \ fois}$, $a^0 = e$ et si a est inversible $a^{-n} = (a^n)^{-1} = (a^{-1})^n$.

Théorème :

$\forall (a,b) \in A^2$, $\forall n \in \mathbb{N}^*$, si $\ldots a*b = b*a$, alors :

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b^1 + \binom{n}{2} a^{n-2}b^2 + \cdots\cdots + \binom{n}{n-1} a^1 b^{n-1} + b^n = \sum_{k=0}^{n} \ldots \binom{n}{k} a^{n-k}b^k.$$

Démonstration 10

Remarque :

Ne **jamais oublier de vérifier** que $\ldots a*b = b*a$.

Dans le cas contraire, on développe par distributivité, exemple :

$(a+b)^2 = a^2 + b^2 + \ldots a*b + b*a$.

6. **Morphismes d'anneaux** :

Définition :

Soit $(A,+,*)$ et $(B,+,\perp)$ deux anneaux et soit f une application de A dans B.

On dit que f est un **morphisme d'anneaux** de A dans B si :

i) $\forall (x,y) \in A^2 \ : \ f(x+y) = \ldots f(x) + f(y)$

ii) $\forall (x,y) \in A^2 \ : \ f(x*y) = \ldots f(x) \perp f(y)$

iii) $f(1_A) = \ldots 1_B$ **à ne pas oublier !**

7. **Idéaux d'un anneau commutatif**

Définition :

Soit $(A,+,\times)$ un anneau **commutatif** . On dit que $I \subset A$ est un **idéal** de A si

i) I est un sous groupe de $(A,+)$

ii) $\forall x \in I$ et $\forall a \in A$: $ax \in I$ (on dit que I est **super-stable** pour $\times$)

Exemples :

$*$ $\{0\}$ et A sont des **idéaux** (triviaux) de A.

$*$ Si $n \in \mathbb{N}$, $n\mathbb{Z}$ est un **idéal** de l'anneau $\mathbb{Z}$ (ce sont les seuls car les seuls sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$).

$*$ Le noyau d'un morphisme d'anneaux f de A dans B :

$$\ker f = \{\ x \in A \text{ tel que } f(x) = 0_B\ \} \text{ est un } \textbf{idéal} \text{ de } A \ .$$

Démonstrations 11

Attention : L'image d'un morphisme d'anneaux f de A dans B n'est pas toujours un idéal de B.

Propriété très importante :

Soit I un idéal de A. On a $I = A$ ssi $1_A \in I$. Donner une autre C.N.S. du même type :
$I = A$ ssi $\exists a \in \ldots A^* \bigcap I$.

Démonstration 12

Idéal engendré par un élément :

Soit $(A,+,\times)$ un anneau **commutatif**. Soit $x_0 \in A$. On appelle **idéal engendré** par x_0 l'ensemble

$$x_0 \cdot A = \{x_0\, a\ ,\ a \in A\}.$$

Proposition : C'est évidemment un idéal de A.

Démonstration 13

Définition :

On dit qu'un idéal I de A est **principal** s'il existe $x_0 \in A$ tel que $I = x_0 A$. x_0 est alors appelé **générateur** de I.

Définition :

On dit qu'un anneau commutatif A est un **anneau principal** si tous ses idéaux sont principaux.

Exemple : Donner un exemple d'anneau principal : $\ldots\mathbb{Z}$.

8. **Divisibilité dans un anneau commutatif et intègre**

Définition :

Soit A un anneau commutatif et intègre.

On dit que $b \in A$ **divise** $a \in A$ s 'il existe $c \in A$ tel que $a = bc$. On note $b \mid a$.

9. **Corps**

(a) **Définition :** Soit K un ensemble non vide muni de 2 L.C.I. notées + et $\times$. On dit que $(K,+,\times)$ est un corps si :

a) $(K,+,\times)$ est un anneau commutatif.

b) Tout les éléments non nul de K sont $\ldots$inversibles

(c'est à dire : $\forall a \in K - \{0\}$, $\exists b \in K$ tel que $a \times b = \ldots 1$ (1 : élément neutre pour $\times$).

(b) **Exemples :**

$(\mathbb{Q}\ ,+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$, $(\mathbb{K}(X),+,\times)$, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}\ (a,b) \in \mathbb{Q}^2\}$, $(\mathbb{Z}/7\mathbb{Z},\dot{+},\dot{\times})$.

III. POLYNÔMES

Tous les polynômes du programme sont à coefficients dans un corps $\mathbb{K}$ **inclus dans $\mathbb{C}$**.

Exemples : $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ mais aussi $\mathbb{Q}(\sqrt{7})\cdots\cdots$ *(il y en a une infinité)*

I. GÉNÉRALITÉS

1. **Définitions**

Définition 1 :

Un **polynôme** est une expression $P = a_0 + a_1X + \cdots + a_nX^n$ avec $(a_0, a_1, \ldots, a_n) \in \mathbb{K}^{n+1}$. Cette expression sous-entend que $a_i = 0$ pour tout $i \geqslant n+1$.

Attention : Cette écriture ne sous-entend pas que $a_n \neq 0$.

X est appelé : **l'indéterminée**.

Ensemble des polynômes à coefficients dans $\mathbb{K}$: ..$\mathbb{K}[X]$

Définition 2 : Une **fonction polynômiale** est une fonction du type

$$P : \mathbb{K} \longrightarrow \mathbb{K}$$
$$x \longmapsto a_0 + a_1x + \cdots + a_nx^n \qquad \text{avec } (a_0, a_1, \ldots, a_n) \in \mathbb{K}^{n+1}$$

Remarque très importante : Dans les **concours**, on ne fait pas de distinction entre polynôme et fonction polynômiale. On pourra donc écrire $P = P(X) = -1+2X+5X^2$. Parfois on verra X comme une indéterminée et parfois X comme un réel.

Exemple ultra-classique :

$$f : \mathbb{K}[X] \longrightarrow \mathbb{K}[X]$$
$$P \longmapsto P(X+1) - P(X)$$

A gauche on voit plutôt un polynôme et à droite plutôt une fonction polynomiale.

Équation algébrique : Toute équation de la forme $\boxed{P(z) = 0}$ avec P un polynôme fixé (exemple $z^3 = 1$).

2. **Lois**

Définition de $P+Q$, λP et PQ. Soit $P = a_0 + a_1X + \cdots + a_nX^n$, $Q = b_0 + b_1X + \cdots + b_mX^m$ et $\lambda \in \mathbb{K}$.

$P + Q = \sum_{i=..0}^{N} (..a_i + b_i)X^i$, avec $N = ..\max(n, m)$

$\lambda P = \sum_{i=..0}^{N} (..\lambda a_i)X^i$, avec $N = ..n$

$PQ = \sum_{i=..0}^{N} \left(\sum_{\alpha+\beta=i} ..a_\alpha b_\beta \right) X^i$, avec $N = ..n + m$.

3. **Degré - Division euclidienne**

Définition 3 : On appelle **degré** de $P = a_0 + a_1X + \cdots + a_nX^n \neq 0$:

$d^oP = \deg P = ..\max\{i \in [\![0, n]\!] \text{ tel que } a_i \neq 0\}$; $d^o0 = ..-\infty$; $d^o(PQ) = ..d^oP + d^oQ$;

$$d^o(\lambda P) = \begin{cases} ..d^oP & \text{si } ..\lambda \neq 0 \\ ..-\infty & \text{si } ..\lambda = 0 \end{cases} , \quad d^o(P+Q) \leqslant ..\max(d^oP, d^oQ) \text{ avec égalité si } ..d^oP \neq d^oQ.$$

Proposition : $\boxed{\mathbb{K}[X] \text{ est un anneau } \textbf{intègre}}$.

Démonstration 14

Ensemble des polynômes de degré inférieur ou égal à n noté : $\mathbb{K}_n[X]$.

Structure de $(\mathbb{K}_n[X], +, \cdot)$: $\dim \mathbb{K}_n[X] =$

Division euclidienne de A par $B \neq 0$:

$$\forall (A, B) \in \mathbb{K}[X]^2 \text{ , } B \neq 0 \quad : \quad \exists (..Q, ..R) \in \mathbb{K}[X] \text{ tel que } \begin{cases} ..A = BQ + R \\ ..d^oR < d^oB \end{cases}$$

Démonstration 15

Algorithme de cette division :

Définition 4 : Soient A et B deux polynômes.

	a_nX^n	$+$	$a_{n-1}X^{n-1}$	$+$	$\cdots$	$+$	$\cdots$	$+$	a_1X	$+$	a_0	$b_pX^p+\cdots+b_0$
$-$	a_nX^n		$\cdots$		$\cdots$	$\cdots$	$\cdots$	$\cdots$				$\frac{a_n}{b_p}X^{n-p}$ $+\cdots$
			$[\cdots]X^{n-1}$		$\cdots$	$\cdots$	$\cdots$	$\cdots$				

TABLE 1 – Première étape de l'algorithme de la division euclidienne de $P(X)$ par $Q(X)$.

	X^5	$+$	X^4	$+$	αX^3	$+$	βX^2	$+$	$5X$	$-$	2	X^3-2X+1
$-$	X^5			$-$	$2X^3$	$+$	X^2					$X^2+X+..\alpha+2$
			X^4	$+$	$(\alpha+2)X^3$	$+$	$(\beta-1)X^2$	$+$				
$-$			X^4			$-$	$2X^2$	$+$	X			
				$+$	$(\alpha+2)X^3$	$+$	$(\beta+1)X^2$	$+$	$4X$			
$-$					$(\alpha+2)X^3$			$-$	$(2\alpha+4)X$	$+$	$\alpha+2$	
							$(\beta+1)X^2$	$+$	$2(\alpha+4)X$	$-$	$(\alpha+4)$	

TABLE 2 – Un exemple complet

On dit que $\boxed{B \text{ **divise** } A}$ si $\exists Q \in \mathbb{K}[X]$ tel que $A = BQ$. **Notation** : $B \mid A$.

Remarque : On dit également que A est un **multiple** de B ou que B est un **diviseur** de A. L'ensemble des multiples de B sera noté $B\,\mathbb{K}[X]$.

Définition 5 : Les polynômes A et B sont dits $\boxed{\textbf{associés}}$ si A divise B et B divise A.

Définition 6 : Un polynôme A est dit **unitaire** s'il est non nul et si son coefficient dominant est égal à 1.

Définition 7 : Un polynôme A est dit **normalisé** s'il est nul ou s'il est unitaire.

4. **Racines - Ordre de multiplicité**

Le reste de la division de P par $(X-\alpha)$ est : $..P(\alpha)$.

Définitions : $\boxed{\alpha \in \mathbb{K} \text{ est } \textbf{racine} \text{ de } P \text{ si : } ..P(\alpha)=0}$

Conséquence : **Factorisation** de P : Si α est racine de P alors $\exists Q \in \mathbb{K}[X]$ tel que $P = ..(X-\alpha)Q$.

$\alpha \in \mathbb{K}$ est **racine simple** de P si : $\exists Q \in \mathbb{K}[X]$ tel que $P = ..(X-\alpha)Q$ avec $..Q(\alpha) \neq 0$,

$\alpha \in \mathbb{K}$ est **racine double** de P si : $\exists Q \in \mathbb{K}[X]$ tel que $P = ..(X-\alpha)^2Q$ avec $..Q(\alpha) \neq 0$,

$\alpha \in \mathbb{K}$ est **racine d'ordre** $s \in \mathbb{N}^*$ de P si : $\exists Q \in \mathbb{K}[X]$ tel que $P = ..(X-\alpha)^sQ$ avec $..Q(\alpha) \neq 0$.

Proposition :

Soient $(\alpha_1, \cdots, \alpha_p) \in \mathbb{K}^p$ **2 à 2 distincts**, on a alors :
$\alpha_1, \cdots, \alpha_p$ racines de P **si et seulement si** $\exists Q \in \mathbb{K}[X]$ tel que $..P = (X-\alpha_1)\cdots(X-\alpha_p)Q$

Démonstration 16

Théorème :

Soit P, un polynôme de $\mathbb{K}[X]$, tel que $\boxed{\deg P \leqslant n}$.
Si P admet au moins $n+1$ racines 2 à 2 distinctes (en particulier s'il en admet une $..$infinité) alors $P = ..0$

Démonstration 17

Polynôme dérivé de $P = a_0 + a_1X + \cdots + a_nX^n$: $P' = a_1 + \cdots + na_nX^{n-1}$.

$(P+Q)' = ..P' + Q'$ $\qquad$ $(\lambda P)' = ..\lambda P'$ $\qquad$ $(PQ)' = ..P'Q + PQ'$.

Dérivée **successive** de P : $P^{(0)} = ..P$, $P^{(n+1)} = ..(P')^{(n)} = ..(P^{(n)})'$.

Formule de **Leibniz** [1] : $(PQ)^{(n)} = \sum_{k=}$

1. Leibniz comme Schwarz n'aiment pas le t !

Formule de **Taylor** en $a \in \mathbb{K}$: si $d^oP = n$ alors :

$$\boxed{P(X) = P(a) + P\ (a)(X-a) + \frac{P^{..''}(a)}{..2!}(X-a)^{..2} + \cdots + \frac{P^{..(n)}(a)}{..n!}(X-a)^{..n}}$$

Démonstration 18

Remarque : On peut aussi la démontrer grâce à la formule de Taylor - R..este intégrale ou bien l'inégalité de Taylor - ..Lagrange .

Caractérisation des racines d'ordre $s \geqslant 1$ de P :

$\alpha \in \mathbb{K}$ est **racine double** de P **si et seulement si** $..P(\alpha) = 0$, $P'(\alpha) = 0$ et $P''(\alpha) \neq 0$,

$\alpha \in \mathbb{K}$ est **racine d'ordre** $s \in \mathbb{N}^*$ de P **si et seulement si** $..P(\alpha) = P'(\alpha) = \cdots = P^{(s-1)}(\alpha) = 0$ et $P^{(s)}(\alpha) \neq 0$.

Démonstration 19

Définition : On considère un corps $\mathbb{K} \subset \mathbb{C}$. On dit que P est un polynôme **scindé dans $\mathbb{K}$** si toutes ses racines (à priori complexes) **sont dans $\mathbb{K}$**.

Conséquence :

Si $P \in \mathbb{K}[X]$, $d^oP = p \geqslant 1$, est **scindé** dans $\mathbb{K}$ alors

$$\boxed{\exists \lambda \in \mathbb{K}^* \text{ et } \exists (\alpha_1, \cdots, \alpha_p) \in \mathbb{K}^p \text{ tel que } P = ..\lambda(X-\alpha_1)\cdots(X-\alpha_p)}$$

Exemples : Dire si ces polynômes sont scindés dans $\mathbb{K}$:

X^2+1 avec $\mathbb{K} = \mathbb{C}$, $(X-7)(X^2+1)$ avec $\mathbb{K} = \mathbb{R}$, X^2-2 avec $\mathbb{K} = \mathbb{Q}$.

Relations coefficients-racines :

Exemples

- $P = aX^2+bX+c = a(X-\alpha)(X-\beta)$ avec $a \neq 0$. Donner les 2 relations coefficients-racines :
$$\begin{cases} \alpha+\beta = ..-\dfrac{b}{a} \\ \alpha\beta = ..\dfrac{c}{a} \end{cases}$$
- $P = X^3+bX^2+cX+d = (X-\alpha)(X-\beta)(X-\gamma)$ avec $a \neq 0$. Donner les 3 relations coefficients-racines :
$$\begin{cases} \alpha+\beta+\gamma = ..-b \\ \alpha\beta+\alpha\gamma+\beta\gamma = ..c \\ \alpha\beta\gamma = ..-d \end{cases}$$
- $P = X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1X + a_0 = (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$.

Donner les n relations coefficients-racines :
$$\begin{cases} \sigma_1 = \alpha_1 + \cdots + \alpha_n = ..-a_{n-1} \\ \sigma_2 = \displaystyle\sum_{1 \leqslant i < j \leqslant n} \alpha_i\alpha_j = ..a_{n-2} \\ \vdots \qquad\qquad \vdots \\ \sigma_p = \displaystyle\sum_{1 \leqslant i_1 < \cdots < i_p \leqslant n} \alpha_{i_1}\cdots\alpha_{i_p} = ..(-1)^p a_{n-p} \\ \vdots \qquad\qquad \vdots \\ \sigma_n = \alpha_1\cdots\alpha_n = ..(-1)^n a_0 \end{cases}$$

Exercice : Déterminer les racines de $X^4 - 5X^3 - 7X^2 + 41X - 30$ *(On cherchera deux racines évidentes).*

Théorème de **d'Alembert-Gauss** :

$$\boxed{\text{Tout polynôme } ..\text{non constant de } \mathbb{C}[X] \text{ possède au moins } ..\text{une racine dans } \mathbb{C}}.$$

Démonstration 20 :

Corollaire : Pour tout polynôme $P \in \mathbb{C}[X]$ de degré $n \geqslant 1$, $\exists \lambda \in \mathbb{C}^*$ et $\exists (\alpha_1, \cdots, \alpha_n) \in \mathbb{C}^n$ tel que $P = \lambda(X-\alpha_1)\cdots(X-\alpha_n)$ (***Attention*** *: les $\alpha_1, \cdots, \alpha_n$ ne sont pas forcément deux à deux distinctes*)

II. ARITHMÉTIQUE DES POLYNÔMES

1. Divisibilité définitions

(a) **Proposition** : Soient $(A,B) \in \mathbb{K}[X]^2$ on a alors $A|B$ SSI $B \in A\mathbb{K}[X]$.

Démonstration 21

Proposition : A et B sont associés dans $\mathbb{K}[X]$ SSI $\exists \lambda \in \mathbb{K}^*$ tel que $A = \lambda B$.

Démonstration 22

Proposition : Tout polynôme A est associé à un unique polynôme normalisé.

Démonstration 23

2. Idéaux de $\mathbb{K}[X]$

Théorème de structure des idéaux de $\mathbb{K}[X]$

Pour tout idéal I de $\mathbb{K}[X]$, il existe un **unique** polynôme P_0 **normalisé** tel que $I = P_0\,\mathbb{K}[X]$.

Remarque : Autrement dit $\mathbb{K}[X]$ est un anneau principal.

Démonstration 24

3. PGCD - PPCM

(a) **Lemme** :

Soit A un anneau commutatif et soient n idéaux $I_1, \dots, I_n$ de A.
i) La somme $I_1 + \cdots + I_n = \{x_1 + \cdots + x_n \ , \ (x_1, \dots, x_n) \in I_1 \times \cdots \times I_n\}$ est un idéal de A
ii) $I_1 \cap \cdots \cap I_n$ est un idéal de A.

Démonstration 25

(b) **Rappels** : On a vu en MPSI les définitions du PGCD et du PPCM de **deux** polynômes :

$[D = A \wedge B]$ si $\forall P \in \mathbb{K}[X]$: $[\ P|A \text{ et } P|B \iff P|D\ ]$

$[M = A \vee B]$ si $\forall P \in \mathbb{K}[X]$: $[\ A|P \text{ et } B|P \iff M|P\ ]$

On a vu aussi que les PGCD et PPCM était définit à une constante multiplicative non nulle près (exemple : $7X-7$ est un PGCD de X^2-1 et de X^3-1). On va imposer en MP que les PGCD et PPCM soient unitaires (exemple : $(X^2-1) \wedge (X^3-1) = X-1$ et rien d'autre)

On se propose de généraliser la notion de PGCD à $n \geqslant 2$ polynômes et de voir que cette nouvelle définition (plus algébrique) du PGCD coïncide avec la définition vue en MPSI (idem pour le PPCM).

(c) **PGCD**

Proposition-définition

Soit $A_1, \dots, A_n$, n polynômes de $\mathbb{K}[X]$. On appelle **PGCD** de $A_1, \dots, A_n$ le **générateur normalisé** de l'idéal $A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X]$. Notation : $D = A_1 \wedge \cdots \wedge A_n$.
On a donc $A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X] = D\mathbb{K}[X]$.
On a pour tout $P \in \mathbb{K}[X]$, $[\ \forall i \in [\![1,n]\!] : P|A_i \iff P|D\ ]$
On retrouve donc bien lorsque $n=2$, la définition de MPSI.

Démonstration 26

Définitions : On dit que $A_1, \dots, A_n$ sont premiers entre eux dans leur ensemble si $A_1 \wedge \cdots \wedge A_n = 1$.

On dit que $A_1, \dots, A_n$ sont premiers entre eux deux à deux si $\forall (i,j) \in [\![1,n]\!]^2$ tel que $i \neq j$: $A_i \wedge A_j = 1$.

(d) **PPCM**

Proposition-définition

Soit $A_1, \dots, A_n$, n polynômes de $\mathbb{K}[X]$. On appelle **PPCM** de $A_1, \dots, A_n$ le **générateur normalisé** de l'idéal $A_1\mathbb{K}[X] \cap \cdots \cap A_n\mathbb{K}[X]$. Notation : $M = A_1 \vee \cdots \vee A_n$.
On a donc $A_1\mathbb{K}[X] \cap \cdots \cap A_n\mathbb{K}[X] = M\mathbb{K}[X]$.
On a pour tout $P \in \mathbb{K}[X]$, $[\ \forall i \in [\![1,n]\!] : A_i|P \iff M|P\ ]$
On retrouve donc bien lorsque $n=2$, la définition de MPSI.

Démonstration 27

Remarque pratique : Pour déterminer le PGCD de deux polynômes, soit on décompose les deux polynômes en facteurs irréductibles soit on utilise l'algorithme d'Euclide (vu en MPSI). Pour la détermination d'un PGCD d'au moins 3 polynômes, on utilise l'associativité et la récursivité :

$$A_1 \wedge \cdots \wedge A_n = [A_1 \wedge \cdots \wedge A_{n-1}] \wedge A_n.$$

4. **Bezout - Gauss - Équation $AU + BV = 1$**

(a) **Bezout** : $A \wedge B = 1 \iff \exists (U, V) \in \mathbb{K}[X]^2$ tel que $..AU + BV = 1$.

(b) **Gauss** : Si A divise le produit BC et si $A \wedge B = 1$ alors $..A$ divise C.

Corollaire 1 : Un polynôme est premier avec un produit si et seulement s'il est premier avec chacun des facteurs.

Démonstration 28

Corollaire pratique 2 :

On a les deux relations pour le PGCD et le PPCM de deux polynômes :

i) si $A \wedge B = D$ alors $\exists (A_1, B_1) \in \mathbb{K}[X]^2$ tel que $\begin{cases} A = ..DA_1 \\ B = ..DB_1 \\ A_1 \wedge B_1 = ..1 \end{cases}$

ii) $c(A \wedge B)(A \vee B) = ..AB$ (c le produit des coefficients dominants de A et B).

Démonstration 29

(c) **Équation du type Bezout** : $AU + BV = 1$ $(**)$

Si $A \wedge B = 1$ alors par Bezout il existe une **solution particulière** :

$$(U_0, V_0) \in \mathbb{K}[X]^2 \text{ tel que } AU_0 + BV_0 = 1 \quad (*).$$

Pour obtenir toutes les solutions $(**)$ on soustrait $(**)$ - $(*)$ on obtient alors :

$..A(U - U_0) + B(V - V_0) = 0$ donc $A(U - U_0) = -B(V - V_0)$ donc A $..$divise $B(V - V_0)$ et par $..$Gauss, A $..$divise $(V - V_0)$ d'où il existe $Q \in \mathbb{K}[X]$ tel que $..V - V_0 = AQ$. On reporte dans $A(U - U_0) = -B(V - V_0)$ d'où $..U - U_0 = -BQ$.

On a donc $U = ..U_0 - BQ$ et $V = ..V_0 + AQ$ la réciproque (**à ne pas oublier !**) est évidente et facile à vérifier. On en conclut que **l'ensemble des solutions** de $AU + BV = 1$ $(**)$ est

$$\{ (U_0 - ..BQ, V_0 + ..AQ) \ , \ Q \in \mathbb{K}[X] \}.$$

Exercice : Résoudre dans $\mathbb{R}[X]^2$ les équations :

$(X^6 + 3X^5 - X^4 + X^3 + 3X)U + (X^4 + 1)V = 1$ et $(X^3 + 3X^2 + 2X + 2)U + (X^2 + 1)V = 1$

5. **Polynômes irréductibles**

(a) **Définition**

On appelle **polynôme irréductible** de $\mathbb{K}[X]$ tout polynôme P vérifiant :

- $\deg(P) \geqslant 1$
- les seuls diviseurs de P sont les éléments de $\mathbb{K}^*$ et les polynômes λP avec $\lambda \in \mathbb{K}^*$.

Donc si P est irréductible alors $P = Q_1 Q_2 \Longrightarrow \deg Q_1 = 0$ ou $\deg Q_2 = 0$

(b) **Propriétés** :

$\bullet_1$ Tout polynôme de $\mathbb{K}[X]$ **de degré 1** est irréductible dans $\mathbb{K}[X]$.

Démonstration 30

$\bullet_2$ Tout polynôme de $\mathbb{K}[X]$ **de degré supérieur ou égal à 2** ayant une racine n'est pas irréductible dans $\mathbb{K}[X]$.

Réciproque fausse !

Démonstration 31

•$_3$ Soit P un polynôme irréductible et A un polynôme quelconque. Alors A et P sont premiers entre eux **si et seulement si** P ne divise pas A.

Démonstration 32

(c) **Théorème fondamental** :

On note $\mathcal{P}_{\mathbb{K}}$ l'ensemble des polynômes irréductibles et unitaires de $\mathbb{K}[X]$, les éléments de $\mathcal{P}_{\mathbb{K}}$ sont deux à deux non associés et tout polynôme irréductible est associé à un unique élément de $\mathcal{P}_{\mathbb{K}}$.

Exemple 1 : $\mathcal{P}_{\mathbb{C}} = \left\{X-3\ ,\ X+i\ ,\ X-\sqrt{2}\ ,\ X-j\ ,\ \dots\right\}$

Exemple 2 : $\mathcal{P}_{\mathbb{R}} = \left\{X-3\ ,\ X-7\ ,\ X+\sqrt{2}\ ,\ X^2+1\ ,\ X^2+X+1\ ,\ \dots\right\}$

Tout polynôme P non constant de $\mathbb{K}[X]$ se décompose en produit d'un élément de $\mathbb{K}^*$ et de polynômes unitaires et irréductibles de $\mathbb{K}[X]$.

De plus cette écriture est unique à une permutation près de ces facteurs.

Pour tout polynôme P non constant de $\mathbb{K}[X]$,

$\exists!\lambda \in \mathbb{K}^*\ ,\ \exists! k \geqslant 1\ ,\ \exists!(P_1,\dots,P_k) \in \mathcal{P}_{\mathbb{K}}^k$ et $\exists!(s_1,\dots,s_k) \in (\mathbb{N}^*)^k$ tel que $\boxed{P = \lambda \cdot P_1^{s_1} \cdots P_k^{s_k}}$

Démonstration 33

(d) **Exemples** :

- Décomposer $X^4 - X^3 - X + 1$ dans $\mathbb{C}[X]$.
- Montrer que X^2+1 est irréductible dans $\mathbb{R}[X]$, l'est-il dans $\mathbb{C}[X]$?
- Montrer que X^4+1 n'est pas irréductible dans $\mathbb{R}[X]$ (*on pourra rajouter et retrancher* $2X^2$).
- Montrer que X^3-2 est irréductible dans $\mathbb{Q}[X]$, l'est-il dans $\mathbb{R}[X]$?
- On pose $P = \lambda \cdot P_1^{n_1} \cdots P_k^{n_k}$ et $Q = \mu \cdot P_1^{m_1} \cdots P_k^{m_k}$ avec $(\lambda,\mu) \in (\mathbb{K}^*)^2$, $(P_1,\dots,P_k) \in \mathcal{P}_{\mathbb{K}}^k$ et $(n_1,\dots,n_k,m_1\dots,m_k) \in (\mathbb{N}^*)^{2k}$. Déterminer $P \wedge Q$ et $P \vee Q$.

$P \wedge Q = P_1^{r_1} \cdots P_k^{r_k}$ avec $r_i = ..\min(n_i,m_i)$ et $P \vee Q = P_1^{s_1} \cdots P_k^{s_k}$ avec $s_i = ..\max(n_i,m_i)$.

(e) **Cas de $\mathbb{C}$**

Proposition :

Les Polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes . . de degré 1

Démonstration 34

Corollaire : Deux polynômes de $\mathbb{C}[X]$ sont premiers entre eux si et seulement s'ils n'ont pas de racines communes.

Démonstration 35

(f) **Cas de $\mathbb{R}$**

Lien factorisation entre $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

Lemme : Si $\alpha \in \mathbb{C}$ est racine de $P \in \mathbb{R}[X]$ alors $\overline{\alpha}$ est . . aussi racine de P.

Démonstration 36

Corollaire 1 :

Soit $P \in \mathbb{R}[X]$ et α une racine de P avec $\alpha \in \mathbb{C} \setminus \mathbb{R}$. Alors P se factorise **dans $\mathbb{R}[X]$** par :

$P = (X^2 - ..2\mathcal{R}e(\alpha)X + ..|\alpha|^2)Q$ et $Q \in \mathbb{R}[X]$.

Corollaire 2 : Deux racines complexes conjuguées d'un polynôme de $\mathbb{R}[X]$ ont même ordre de multiplicité.

Démonstration 37

Les Polynômes irréductibles de $\mathbb{R}[X]$ sont :

i) Les Polynômes de degré . . 1

ii) Les Polynômes de degré . . 2 avec . . un discriminant strictement négatif.

Démonstration 38

Conséquence : Tous les autres polynômes de $\mathbb{R}[X]$ sont donc **NON irréductibles**

(exemples : $P = X^4+1$, $P = X^3+X+1$)

Expression pratique de la factorisation d'un polynôme :

Dans $\mathbb{C}[X]$, $P = ..\lambda(X-\alpha_1)^{s_1}\cdots(X-\alpha_p)^{s_p}$, avec $\lambda \in \mathbb{C}^*$, $(\alpha_1,\ldots,\alpha_p) \in \mathbb{C}^p$ (2 à 2 distincts) et $\forall i : s_i \geqslant 1$.

Dans $\mathbb{R}[X]$, $P = ..\lambda(X-\alpha_1)^{s_1}\cdots(X-\alpha_p)^{s_p}(X^2+a_1X+b_1)^{t_1}\cdots(X^2+a_qX+b_q)^{t_q}$, avec

$\lambda \in \mathbb{R}^*$, $(\alpha_1,\ldots,\alpha_p) \in \mathbb{R}^p$ (2 à 2 $\neq$) et $\forall i : s_i \geqslant 1$, [$(a_1,b_1),\ldots,(a_q,b_q)$] $\in (\mathbb{R}^2)^q$ (2 à 2 $\neq$) et $\forall i : t_i \geqslant 1$.

Remarque : Pour factoriser dans $\mathbb{R}[X]$ on peut commencer par factoriser dans $\mathbb{C}[X]$.

"Méga-astuce" pour factoriser les polynômes bi-carrés du quatrième degré tel que $P = X^4+X^2+9$.

On écrit $P = X^4+X^2+9$

$= [X^4+9]+X^2$

$= [X^4+3^2+6X^2-6X^2]+X^2$

$..\quad = [X^4+3^2+6X^2]-6X^2+X^2$

$= [X^2+3]^2-5X^2$

$= [X^2+3]^2-[\sqrt{5}X]^2$

$= (X^2+3+\sqrt{5}X)(X^2+3-\sqrt{5}X) = (X^2+\sqrt{5}X+3)(X^2-\sqrt{5}X+3)$

Exemples : Décomposer

i. Dans $\mathbb{C}$ $[X]$, $X^n-1 = ..\prod_{k=0}^{n-1}(X-\omega_k)$ avec $\omega_k = ..e^{\frac{2ik\pi}{n}}$.

ii. Dans $\mathbb{R}[X]$,(sans passer dans $\mathbb{C}$ $[X]$), $X^6-1 = ..(X-1)(X+1)(X^2-X+1)(X^2+X+1)$

iii. Dans $\mathbb{R}[X]$ (en passant dans $\mathbb{C}$ $[X]$), $X^6-1 = ..(X-1)(X+1)(X^2-X+1)(X^2+X+1)$

iv. Dans $\mathbb{R}[X]$, $X^4+2X^2+4 = ..(X^2-\sqrt{2}X+2)(X^2+\sqrt{2}X+2)$

v. Dans $\mathbb{Q}[X]$, $X^4+X^3-2X-2 = ..(X+1)(X^3-2)$

6. **Polynômes interpolateurs de LAGRANGE** :

Lemme :

Soient $(a_1,\cdots,a_n)$ n éléments de $\mathbb{K}$ deux à deux distincts. Alors **l'unique polynôme** L_i de degré $n-1$ tel que

$\forall (i,j) \in [\![1,n]\!]^2 : L_i(a_j) = \delta_{i,j}$ est $L_i = \prod_{k=1,k\neq..i}^{n}\left(\frac{..X-a_k}{..a_i-a_k}\right)$.

Proposition :

Soient $(a_1,\cdots,a_n)$ n éléments de $\mathbb{K}$ deux à deux **distincts** et soient $(b_1,\cdots,b_n)$ n éléments **quelconques** de $\mathbb{K}$.

Alors il existe un unique polynôme L de $\mathbb{K}[X]$ tel que $d^oL \leqslant n-1$ et $\forall i \in \{1,\cdots,n\}$, $L(a_i) = b_i$:

$$L = \sum_{i=1}^{n}..b_i\cdot L_i \quad = \quad \sum_{i=1}^{n}..b_i\cdot\prod_{k=1,k\neq..i}^{n}\left(\frac{..X-a_k}{..a_i-a_k}\right)$$

Donner à l'aide de L **tous** les polynômes P de $\mathbb{K}[X]$ tel que $\forall i \in \{1,\cdots,n\}$, $P(a_i) = b_i$:

$$P = ..L+Q\prod_{i=1}^{n}(X-a_k) \quad \text{avec} \quad Q \in \mathbb{K}[X]$$

Démonstration 39

Remarque : Hermite a généralisé "Lagrange" en montrant (par exemple) que si $(a_1,\cdots,a_n)$ sont n éléments de $\mathbb{K}$ deux à deux distincts et si $(b_1,\cdots,b_n),(c_1,\cdots,c_n)$ sont $2n$ éléments quelconques de $\mathbb{K}$, alors il existe des polynômes H tels que

$$\forall i \in \{1,\cdots,n\} : \ H(a_i) = b_i \quad \text{et} \quad H'(a_i) = c_i$$

ANNEXE

DÉMONSTRATION DU THÉORÈME DE D'ALEMBERT - GAUSS

Soit $P \in \mathbb{C}[X]$, $\mathrm{d}^o P \geqslant 1$. Montrons qu'il existe z_0 tel que $P(z_0) = 0$. Posons $\alpha = \inf_{z \in \mathbb{C}} |P(z)|$.

1. Montrer que α existe.
2. Montrer que $\exists r > 0$ tel que $\forall z \in \mathbb{C}$, $|z| > r \Longrightarrow |P(z)| > |P(0)|$.
3. En déduire que $\alpha = \inf_{z \in D} |P(z)|$ où $D = D_F(0, r) = \{z \in \mathbb{C} \text{ tel que } |z| \leqslant r\}$.
4. Justifier l'existence d'une suite (u_n) dans D telle que $\alpha = \lim_{n \to +\infty} |P(u_n)|$.
5. Démontrer qu'il existe une suite (v_n) dans D telle que $\alpha = \lim_{n \to +\infty} |P(v_n)|$ et (v_n) convergente vers $z_0 \in \mathbb{C}$.
6. En déduire que $|P(z_0)| = \alpha$.

Supposons que $\alpha > 0$, posons alors $Q(z) = \dfrac{P(z_0 + z)}{P(z_0)}$

7. Montrer, à l'aide de Q que "SNALG" , on peut supposer que $\alpha = 1$ et $z_0 = 0$.

On a donc $P(z) = 1 + a_q z^q + z^{q+1} R(z)$ avec $1 \leqslant q$ et $a_q \neq 0$

8. En posant $a_q = -\rho e^{i\theta_0}$, prouver qu'il existe z proche de 0 tel que $|P(z)| < 1$. Conclure.