Saint Rémi : MP (programme 2022)
David Corneillie

Chap AG1 : Structures algébriques

Rappels préliminaires :

1°) Relation sur un ensemble :

Soit R une relation sur un ensemble E, on dit que

R *est réflexive* $\Leftrightarrow \forall x \in E,\ xRx$

R *est symétrique* $\Leftrightarrow \forall (x,y) \in E^2,\ xRy \Rightarrow yRx$

R *est antisymétrique* $\Leftrightarrow \forall (x,y) \in E^2,\ xRy$ *et* $yRx \Rightarrow x = y$

R *est transitive* $\Leftrightarrow \forall (x,y,z) \in E^3,\ xRy$ *et* $yRz \Rightarrow xRz$

Une relation R est dite relation d'équivalence si et seulement si elle est réflexive, symétrique et transitive.

Def : On appelle classe d'équivalence de x, l'ensemble des éléments de E qui sont équivalents à x

Exo : Sur $\mathbb{C}$, *la relation* $\forall (z,z') \in \mathbb{C}^2,\ zRz' \Leftrightarrow \exists \theta \in \mathbb{R},\ z' = \dfrac{z\cos\theta + \sin\theta}{-z\sin\theta + \cos\theta}$

Déterminer la classe de 0

Th : L'ensemble des classes d'équivalence forme une partition de E, c'est-à-dire que la réunion de toutes les classes forme E et que toutes les classes sont disjointes

Dem : $\overline{x} \subset E \Rightarrow \bigcup \overline{x} \subset E$ *et* $\forall y \in E, y \in \overline{y} \subset \bigcup \overline{x}$ *(car R est réflexive)*

Soit $x \in \overline{y} \cap \overline{z}$ *alors* xRy *et* $xRz \Rightarrow yRz$ *et* $\overline{y} = \overline{z}$

Une relation R est dite d'ordre si et seulement si elle est réflexive, antisymétrique et transitive
L'ordre est dit total si $\forall (x,y) \in E^2$, *on a soit* xRy *ou* yRx

Exo : Soit $(A,+,\times)$ *un anneau tel que* $\forall x \in A,\ x^2 = x$.

On définit la relation R sur A par $\forall (x,y) \in A^2,\ xRy \Leftrightarrow xy = x$

Montrer que R est une relation d'ordre sur A

2°) Application sur un ensemble :

f une application de E dans F est dite injective si et seulement si tout élément de F a au plus un antécédent dans E , on peut caractériser une injection par : $\forall (x,y) \in E^2,\ f(x) = f(y) \Rightarrow x = y$

f une application de E dans F est dite surjective si et seulement si tout élément de F a au moins un antécédent dans E . $\forall y \in F, \exists x \in E$ *tel que* $y = f(x)$

f une application de E dans F est dite bijective si et seulement si tout élément de F a un antécédent unique dans E, on peut caractériser une bijection par une application qui est à la fois injective et surjective.

Exo : Soit f une application de E dans E telle que $fofof = f$.
Montrer que f est surjective si et seulement si f est injective

Def : Soit A une partie de E et f une application de E dans F.

On note $f(A)=\{y\in F \text{ tel que } y=f(x) \text{ où } x\in A\}$ *l'image de A*
Soit B une partie de F, on note $f^{-1}(B)=\{x\in E \text{ tel que } f(x)\in B\}$ *l'image réciproque de B.*

I) Les groupes :

1°) Définition :

$(G,+)$ *est un groupe si G est un ensemble muni d'une loi de composition + interne, associative, qui possède un élément neutre et telle que tout élément de G possède un symétrique ; et si de plus la loi est commutative, le groupe est dit abélien.*
Ex : $(\mathbb{Z},+),(\mathbb{Q}^*,\times),(\mathbb{R},+)$ *sont des groupes*

Exo : Soit $E=\mathbb{Q}-\{1\}$ *;* $a*b=a+b-ab$ *; montrer que* $(E,*)$ *est un groupe*
Exo : $(G,\times)$ *un groupe tel que* $\forall(x,y)\in G^2,\ x^2y^2=(xy)^2$ *. Montrer que G est abélien*

$(H,+)$ *est un sous groupe de* $(G,+)$ *si et seulement si*

$$H\subset G,\ H\neq\varnothing,\ \forall(x,y)\in H^2,\ x-y\in H$$

Rem : Le neutre du groupe appartient à tous les sous groupes.
Exo : Soit $(G,*)$ *un groupe non abélien*
Montrer que $\Gamma=\{\alpha\in G,\forall x\in G,\alpha*x=x*\alpha\}$ *est un sous groupe de G*

Th : Les sous groupes de $(\mathbb{Z},+)$ *sont les* $(n\mathbb{Z},+)$ *où* $n\mathbb{Z}=\{np,p\in\mathbb{Z}\}$

Dem : On montre d'abord que $(n\mathbb{Z},+)$ *est un sous groupe de* $(\mathbb{Z},+)$

Puis on considère H un sous groupe de $(\mathbb{Z},+)$

Si $H=\{0\}$ *alors* $H=0\mathbb{Z}$

Si $H\neq\{0\}$ *alors il existe au moins un élément de H strictement positif, l'ensemble des éléments strictement positifs de H est une partie non vide de* $\mathbb{N}$ *, donc elle admet un plus petit élément n*
On a immédiatement $n\mathbb{Z}\subset H$
Soit $x\in H$*, si x est positif on effectue la division euclidienne de x par n :*
$x=np+r$ *où* $0\le r<n$*, ainsi* $r=x-np\in H$*, r est positif et strictement plus petit que n donc r est nul donc* $x=np\in n\mathbb{Z}$

2°) Intersection et groupe engendré :

Th : Toute intersection de sous groupes de $(G,*)$ *est un sous groupe de* $(G,*)$

Def : Soit A une partie de G, l'intersection de tous les sous groupes de $(G,*)$ *contenant A est le plus petit sous groupe contenant A, c'est le sous groupe engendré par A, noté* $Gr(A)$

Exo : Soit $(G,+)$ *un groupe abélien, H et F deux sous groupes de G*
On définit : $H+F=\{x=h+f\in G \text{ tel que } h\in H \text{ et } f\in F\}$
c'est un sous groupe de G, c'est le sous groupe engendré par la réunion de H et F

Exo : $(G_1,*)$ *et* $(G_2,*)$ *sont 2 groupes*
Montrer que $(G_1 \cup G_2,*)$ *est un groupe si et seulement si* $G_1 \subset G_2$ *ou* $G_2 \subset G_1$

3°) Morphisme de groupes (Rappel MPSI):

Soient $(G,*),(F,\Delta)$ *deux groupes, f une application de G dans F est un morphisme de groupes de G dans F si et seulement si* $\forall (x,y) \in G^2, f(x*y) = f(x) \Delta f(y)$
Ex : La fonction ln est un morphisme de $(\mathbb{R}^{*+},\times)$ *dans* $(\mathbb{R},+)$ *et l'application déterminant est un morphisme de* $(GL_n(\mathbb{R}),\times)$ *dans* $(\mathbb{R}^*,\times)$

Si un morphisme f est bijectif, f est alors appelé isomorphisme
Si f est un morphisme d'un ensemble dans lui même, alors f est appelé endomorphisme
Un endomorphisme bijectif est un automorphisme

Prop : Si $f : G \to F$ *est un morphisme de groupe alors* $f(e_G) = e_F$ *et* $f(x') = (f(x))'$
Dem : $\forall x \in G$, $f(x*e_G) = f(x) \Delta f(e_G) = f(x)$ *or* $f(x)$ *admet un symétrique dans F donc on obtient* $f(e_G) = e_F$
De plus $f(x*x') = f(e_G) = e_F = f(x) \Delta f(x')$

Prop : L'image d'un sous groupe de $(G,*)$ *par un morphisme est un sous groupe de* (F,Δ)*, l'image réciproque d'un sous groupe de* (F,Δ) *par un morphisme est un sous groupe de* $(G,*)$.
Dem : Soit $(A,*)$ *un sous groupe de* $(G,*)$
$f(A) \subset F$, $f(A) \neq \varnothing$ *car* $e_F \in f(A)$
$\forall (x,y) \in (f(A))^2$, $\exists (a,b) \in A^2$ *tel que* $x = f(a)$ *et* $y = f(b)$
$x \Delta y' = f(a) \Delta f(b') = f(a*b') \in f(A)$ *car* $a*b' \in A$. $(f(A),\Delta)$ *est bien un groupe*
Soit (B,Δ) *un sous groupe de* (F,Δ)
$f^{-1}(B) \subset G$, $f^{-1}(B) \neq \varnothing$ *car* $e_G \in f^{-1}(B)$
$\forall (x,y) \in (f^{-1}(B))^2$, $(f(x), f(y)) \in B^2$ *donc* $f(x) \Delta (f(y))' = f(x*y') \in B$
Donc $x*y' \in f^{-1}(B)$, $(f^{-1}(B),*)$ *est bien un groupe*

Def : Soit $f : G \to F$ *un morphisme de groupes, on appelle image et noyau de f les ensembles* $\mathrm{Im}\, f = \{y \in F, \exists x \in G \text{ tel que } y = f(x)\}$, $\ker f = \{x \in G \text{ tel que } f(x) = e_F\}$

Prop : Le noyau d'un morphisme est un sous groupe de $(G,*)$
L'image d'un morphisme est un sous groupe de (F,Δ)
Dem : $\{e_F\}$ *est un sous groupe de F donc* $\ker f = f^{-1}(\{e_F\})$ *est un sous groupe*
$\mathrm{Im}\, f = f(G)$ *est donc un sous groupe*
Exo : $SL(E) = \{f \in \ell(E), \det(f) = 1\}$ *est un sous groupe de* $GL(E)$

Th : Un morphisme est injectif si et seulement si son noyau est réduit à l'élément neutre

Dem : $(\Rightarrow)$ *Soit* $x \in \ker f \Rightarrow f(x) = e_F = f(e_G) \Rightarrow x = e_G$ *car f est injective*

$(\Leftarrow)$ $f(x) = f(y) \Rightarrow f(x * y') = e_F \Rightarrow x * y' \in \ker f \Rightarrow x = y$ *donc f est injective*

Th : (transport de structure)

$(G,*)$ *un groupe, F un ensemble muni d'une loi de composition* Δ, *soit une application f de G dans F surjective telle que* $\forall (x,y) \in G^2,\ f(x*y) = f(x) \Delta f(y)$. *Alors* (F,Δ) *est un groupe*

Dem : Soit $(x',y') \in F^2 \Rightarrow x' = f(x)$ *et* $y' = f(y)$ *car f est surjective*

$x' \Delta y' = f(x) \Delta f(y) = f(x*y)$ *or* $x*y \in G$ *: la loi est interne*

$(x' \Delta y') \Delta z' = f(x*y) \Delta f(z) = f(x*y*z) = f(x) \Delta f(y*z) = x' \Delta (y' \Delta z')$

$f(e_G)$ *est neutre dans F et* $f(sym(x))$ *est le symétrique de* $f(x)$

Exo : L'ensemble des matrices de permutation forme un groupe multiplicatif

4°) Groupes isomorphes :

Def : Deux groupes sont dits isomorphes s'il existe un isomorphisme de l'un vers l'autre

Exo : L'ensemble des matrices $M_x = \begin{pmatrix} 1 & 0 & 0 \\ x^2 & 1 & x \\ 2x & 0 & 1 \end{pmatrix}$, $x \in \mathbb{R}$ *est un sous groupe de* $(GL_3(\mathbb{R}), \times)$ *isomorphe à* $(\mathbb{R}, +)$

5°) Groupe monogène :

Soit G un groupe multiplicatif d'élément neutre $1,\ x \in G$

On définit $\varphi_x : \mathbb{Z} \to G$ *tq* $\varphi_x(n) = x^n$, *c'est un morphisme de groupe* $(\mathbb{Z},+) \to (G,\times)$

Son image est un sous groupe de G, c'est le sous groupe engendré par x, c'est donc le plus petit sous groupe de G contenant x .

Dem : On sait que $\operatorname{Im} \varphi_x$ *est un sous groupe en tant qu'image d'un morphisme*

$x = \varphi_x(1) \in \operatorname{Im} \varphi_x$ *montrons qu'il s'agit du plus petit sous groupe contenant* $\{x\}$

Soit H un sous groupe de G contenant $\{x\}$ *alors toutes les puissances de x sont aussi dans H donc* $\operatorname{Im} \varphi_x \subset H$

Def : G est un groupe monogène si et seulement si il existe x de G tel que $G = \operatorname{Im} \varphi_x$, *donc si G est engendré par un seul élément, soit* $Gr(\{x\})$

Si le noyau (qui est un sous groupe de $\mathbb{Z}$ *) est réduit à 0, le groupe monogène est infini*

Th : Tout groupe monogène infini est isomorphe à $(\mathbb{Z},+)$

Dem : $Gr(\{x\})$ *est infini donc* φ_x *est injectif car son noyau est réduit à* $\{0\}$, *donc il réalise un isomorphisme de* $\mathbb{Z}$ *sur son image* $\operatorname{Im} \varphi_x = Gr(\{x\})$

Si le noyau (qui est un sous groupe de $\mathbb{Z}$ *) n'est pas réduit à 0, alors il existe un entier p tel que* $\ker \varphi_x = p\mathbb{Z}$, *on dit alors que x est un élément d'ordre p de G, p étant le plus petit entier strictement positif tel que* $x^p = 1$

Exo : Dans $GL_2(\mathbb{R})$, $A=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ *est d'ordre 4 ,* $B=\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}$ *est d'ordre 3, quel est l'ordre de AB ?*

Th : Si G est un groupe multiplicatif, si x est d'ordre d alors $x^n=1\Leftrightarrow d$ *divise n*

Dem : $(\Leftarrow)$ *si d divise n alors* $n=dp$ *et* $x^n=\left(x^d\right)^p=1$

$(\Rightarrow)$ $n\in\ker\varphi_x=d\mathbb{Z}$, *donc* $n=dp$

Def : Un groupe monogène de cardinal fini p est appelé groupe cyclique d'ordre p, l'ordre du groupe est l'ordre de son générateur

Ex : Les racines $n^{ièmes}$ *de 1 dans* $\mathbb{C}$

Th : Soit G un groupe cyclique d'ordre n engendré par a, les générateurs de G sont les a^k *où* $k\wedge n=1$

Dem : Si a^k *engendre G, comme a appartient à G, il existe p tel que* $\left(a^k\right)^p=a$ *donc* $kp\equiv 1[n]$ *donc* $k\wedge n=1$

Réciproquement si $k\wedge n=1$ *alors* $a^{kp}=a$ *et* $\forall b\in Gr(a)$, $b=a^q=\left(a^k\right)^{qp}$

Application : Les générateurs de l'ensemble des racines $n^{ièmes}$ *d'un complexe de module* 1

Exo : Soit G un groupe cyclique d'ordre n et x un générateur de G.
Montrer que l'ordre de x^r *est* $\dfrac{n}{n\wedge r}$

Th : L'ordre d'un élément d'un groupe fini divise le cardinal du groupe
Pour tout élément a d'un groupe fini de cardinal n, on a : $a^n=1$

Dem : Soit H un sous groupe fini du groupe fini G, on montre que le cardinal de H divise celui de G (c'est le théorème de Lagrange)

Soit $a\in G$, $\varphi: H\to G$ *telle que* $\varphi(x)=ax$, *comme a est inversible on montre que* φ *est injective,* φ *est une bijection de H sur* $aH=\{ah\ ,\ h\in H\}$ *donc* $card(H)=card(aH)$

On considère la relation sur G : $xRy\Leftrightarrow x^{-1}y\in H$ *c'est une relation d'équivalence*

On montre que aH est une classe d'équivalence de R, donc que $\bar{a}=aH$ *en effet*

si $x\in aH$, *alors* $x=ah$ *où* $h\in H$ *alors* $a^{-1}x=h\in H\Rightarrow aRx$ *et* $x\in\bar{a}$

si $x\in\bar{a}\Rightarrow a^{-1}x\in H$ *or* $x=aa^{-1}x\in aH$

Toutes les classes d'équivalences sont du type aH, elles ont donc le même cardinal, or par le théorème de partition tout élément de G appartient à une classe et une seule, si on note p le nombre de classe (c'est en réalité l'indice de H sur G) on aura

$Card(G)=p\times Card(aH)=p\times Card(H)$

Enfin si a est d'ordre p dans G de cardinal n, $Gr(a)$ *est un sous groupe de cardinal p et par le théorème précédent p divise n*

Rem : Dans le cas d'un groupe additif, on définit également un groupe monogène comme étant un sous groupe engendré par un seul élément, par exemple dans $(\mathbb{Z},+)$, $Gr(\{n\})=n\mathbb{Z}$

II) Les anneaux et les corps :

1°) Anneaux (rappel MPSI) :

$(A,+,\times)$ *est un anneau si A est un ensemble muni de 2 lois de composition telles que* $(A,+)$ *soit un groupe abélien et que la loi* $\times$ *soit interne, associative, distributive par rapport à + et possède un élément neutre. Si de plus elle est commutative l'anneau est commutatif.*

$(A,+,\times)$ *est un anneau si et seulement si*

$(A,+)$ *est une groupe abélien*

$\forall (x,y)\in A^2,\ x\times y\in A$

$\forall (x,y,z)\in A^3,\ (x\times y)\times z = x\times(y\times z)$

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

$\exists 1\in A$ *tel que* $\forall x\in A,\ 1\times x = x\times 1 = x$

Ex : $(\mathbb{Z},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$, $(\mathbb{R}[X],+,\times)$ *sont des anneaux commutatifs, et* $(M_n(\mathbb{R}),+,\times)$ *est un anneau*

$(B,+,\times)$ *est un sous anneau de* $(A,+,\times)$ *si et seulement si* $(B,+)$ *est un sous groupe de* $(A,+)$, $\forall (x,y)\in B^2,\ x\times y\in B$ *et* $1_A\in B$.

$(B,+,\times)$ *est un sous anneau de* $(A,+,\times)$ *si et seulement si*

$B\subset A,\ B\neq\varnothing$

$\forall (x,y)\in B^2,\ x-y\in B$

$\forall (x,y)\in B^2,\ x\times y\in B$

$1\in B$

Rem : On utilise souvent $1\in B$ *pour montrer que B est non vide.*
Bien qu'on aura toujours $0\in B$ *si* $(B,+)$ *est un sous groupe*

Exo : Soit $A=\left\{m+n\sqrt{5},(m,n)\in\mathbb{Z}^2\right\}$, *montrer que (A,+,.) est un anneau*

Def : Soit $(A,+,\times)$ *un anneau, un élément a de A est un diviseur de zéro, lorsque* $a\neq 0$ *et s'il existe* $b\neq 0$ *tel que* $a\times b = 0$

Ex : $A=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$ *et* $B=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$ *alors* $AB=0$

Def : Un anneau est intègre s'il est commutatif et ne possède pas de diviseur de zéro
Ainsi dans un anneau intègre ($a\times b=0\Rightarrow a=0$ *ou* $b=0$ *)*
Contre-ex : $M_n(\mathbb{R})$ *n'est pas intègre*

Prop : L'ensemble des éléments inversibles $U(A)$ *d'un anneau* $(A,+,\times)$ *est un groupe pour la loi* $\times$

Dem : $1_A\in U(A)$ *car* $1_A\times 1_A = 1_A$, *le neutre pour* $\times$ *est élément de U(A)*

On montre que la loi est interne si $(x,y)\in(U(A))^2$ $xy\times y^{-1}x^{-1}=1_A$ *donc* $xy\in U(A)$

De plus $x^{-1}\in U(A)$ *car* $\left(x^{-1}\right)^{-1}=x$

L'associativité est respectée dans A donc dans U(A)

Ex : $\left(GL_n(\mathbb{R}),\times\right)$ *est un groupe*

Def : Soient $\left(A,+,\times\right)$ *et* $\left(B,+,\times\right)$ *deux anneaux*

On définit le produit cartésien $A\times B=\left\{(x,y),x\in A,y\in B\right\}$

Sur cet ensemble on pose les lois $\bullet$ *telles que* $(x,y)\bullet(x',y')=(x\bullet x',y\bullet y')$ *(où* $\bullet$ *vaut + ou* $\times$*) alors* $\left(A\times B,+,\times\right)$ *est un anneau*

Cette notion se généralise à un produit fini d'anneaux

Ex : $\left(\mathbb{Z}^2,+,\times\right)$ *est un anneau*

2°) Morphisme d'anneaux

Def : Soient $\left(A,+,\times\right)$ *et* $\left(B,+,\times\right)$ *deux anneaux*

L'application $f:\ A\to B$ *est un morphisme d'anneaux si et seulement si*

$$\begin{cases}\forall(x,y)\in A^2,\ f(x+y)=f(x)+f(y)\\ f(x\times y)=f(x)\times f(y)\\ f(1_A)=1_B\end{cases}$$

Rem : Le déterminant n'est pas un morphisme d'anneaux

Prop : Si $\left(C,+,\times\right)$ *est un sous anneau de* $\left(A,+,\times\right)$*, alors* $\left(f(C),+,\times\right)$ *est un sous anneau de* $\left(B,+,\times\right)$

Dem : $f(C)\subset B,\ 1_B=f(1_A)$ *or* $1_A\in C\Rightarrow 1_B\in f(C)\neq\varnothing$

$\forall(x,y)\in\left(f(C)\right)^2,\ x=f(a),\ y=f(b)$ *où* $(a,b)\in C^2$

$x-y=f(a)-f(b)=f(a-b)\in f(C)$ *car* $a-b\in C$

$x\times y=f(a)\times f(b)=f(a\times b)\in f(C)$ *car* $a\times b\in C$

Conséquence : $\left(\mathrm{Im}\,f,+,\times\right)$ *est un sous anneau de* $\left(B,+,\times\right)$

Prop : Si $\left(C,+,\times\right)$ *est un sous anneau de* $\left(B,+,\times\right)$*, alors* $\left(f^{-1}(C),+,\times\right)$ *est un sous anneau de* $\left(A,+,\times\right)$

Dem : $f^{-1}(C)\subset A,\ 1_B=f(1_A)$ *or* $1_B\in C\Rightarrow 1_A\in f^{-1}(C)\neq\varnothing$

$\forall(x,y)\in\left(f^{-1}(C)\right)^2\Rightarrow\left(f(x),f(y)\right)\in C^2$

$f(x)-f(y)=f(x-y)\in C\ \Rightarrow x-y\in f^{-1}(C)$

$f(x)\times f(x)=f(x\times y)\in C\Rightarrow x\times y\in f^{-1}(C)$

Rem : $\ker f=f^{-1}\left(\{0_B\}\right)$ *n'est pas un sous anneau de A (car* $1\notin\ker f$ *)*

Exo : L'ensemble des matrices carrées d'ordre 2 qui commutent avec $M_1=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ *est un anneau isomorphe à* $\mathbb{C}$

3°) Corps :

$\left(C,+,\times\right)$ *est un corps s'il est un anneau commutatif et si de plus tout élément non nul admet un symétrique pour la loi* $\times$

$\left(K,+,\times\right)$ *est un sous corps de* $\left(C,+,\times\right)$ *si et seulement si*

$\left(K,+,\times\right)$ *est un sous anneau de* $\left(C,+,\times\right)$

$\forall x\in K\ ,\ x^{-1}\in K$

$(K,+,\times)$ *est un sous corps de* $(C,+,\times)$ *si et seulement si*

$$K \subset C,\ K \neq \varnothing$$

$$\forall (x,y) \in K^2,\ x-y \in K \text{ et } x \times y^{-1} \in K$$

Rem : Il n'est plus utile de vérifier que $1 \in K$ *car* $x \times x^{-1} \in K$

Une application f de C dans D est un morphisme de corps lorsque :

$\forall (x,y) \in C^2,\ f(x+y) = f(x) + f(y)$ *et* $f(xy) = f(x) f(y)$

Rem : On ne doit plus vérifier que $f(1) = 1$

En effet $\forall x \in C,\ f(x) = f(x \times 1) = f(x) \times f(1)$ *or* $f(x)$ *est inversible*

On aura aussi $f(x \times x^{-1}) = f(x) \times f(x^{-1}) = f(1) = 1$ *et* $f(x^{-1} \times x) = f(x^{-1}) \times f(x) = f(1) = 1$

Soit $f(x^{-1}) = (f(x))^{-1}$

Prop : Tout corps est un anneau intègre (la réciproque est fausse)

Dem : Si $xy = 0$ *avec* $x \neq 0$ *alors x est inversible et* $x^{-1}xy = y = 0$

$(\mathbb{Z},+,\times)$ *est un anneau intègre mais pas un corps*

<u>4°) Idéal d'un anneau commutatif :</u>

Def : Soit $(A,+,\times)$ *un anneau commutatif. On appelle idéal I de A tout sous groupe de* $(A,+)$*, stable par le produit de tout élément de A , c'est-à-dire :*

$$I \neq \varnothing,\ I \subset A$$

$$\forall (x,y) \in I^2\ x-y \in I$$

$$\forall x \in A,\ \forall y \in I \text{ on a } xy \in I$$

Ex : $\{0\}$ *et* A *sont des idéaux de A*

Prop : Soit f un morphisme d'anneau de A dans B, I un idéal de A alors $f(I)$ *est un idéal de* $\operatorname{Im} f$ *, si J est un idéal de B alors* $f^{-1}(J)$ *est un idéal de A, le noyau de f est un idéal de A*

Dem : Les démonstrations sont déjà établies pour les sous groupes

Soit $y \in f(I), b \in \operatorname{Im} f \Rightarrow by = f(a) f(x) = f(ax) \in f(I)$ *car* $ax \in I$

Soit $x \in f^{-1}(J), a \in A$ *on a* $f(ax) = f(a) f(x) \in J \Rightarrow ax \in f^{-1}(J)$

Soit $x \in \ker f, a \in A$ *on a* $f(ax) = f(a) f(x) = 0 \Rightarrow ax \in \ker f$

Exo : A un anneau et I un idéal de A, on définit le radical de I comme suit :

$\sqrt{I} = \{x \in A / \exists n \in \mathbb{N}^*, x^n \in I\}$ *montrer que* $\sqrt{I}$ *est un idéal de A*

L'ensemble xA = $\{ax, a \in A\}$*, où x est élément de A est un idéal de A, c'est le plus petit idéal contenant x, on l'appelle l'idéal principal engendré par x*

Dem : $xA \subset A,\ x = x \times 1 \in xA \neq \varnothing$

$\forall (y,z) \in (xA)^2,\ y = ax$ *et* $z = bx$ *où* $(a,b) \in A^2$

$y - z = (a-b)x \in xA,\ \forall c \in A,\ yc = acx \in xA$

Donc xA est un idéal de A contenant x

Soit I un idéal de A contenant x

$\forall y \in xA,\ y = ax$ *où* $a \in A$ *or* $x \in I \Rightarrow y \in I$ *donc* $xA \subset I$

Th : Les idéaux de $(\mathbb{Z},+,\times)$ *sont les* $n\mathbb{Z}$

Def : Un anneau intègre dont tous les idéaux sont principaux est appelé anneau principal
Ex : $(\mathbb{Z},+,\times)$ *est un anneau principal*

Th : Dans un anneau principal, on dit que b divise a si et seulement si $aA \subset bA$
Dem : $(\Rightarrow)$ *soit* $x \in aA$ *alors* $x = ah$ *or* $a = bp \Rightarrow x = bph \in bA$
$(\Leftarrow)$ $a \in aA \subset bA$ *donc* $a = bp$

Exo : Soit $(A,+,\times)$ *un anneau commutatif, montrer que A est un corps si et seulement si* $\{0\}$ *et A sont les seuls idéaux de A*

5°) Arithmétique dans un anneau principal

Def : Soit $(a,b) \in A^2$, $aA+bA$ *est un idéal de A, or* $(A,+,\times)$ *est un anneau principal, ses idéaux sont donc principaux. Il existe donc d tel que* $aA+bA = dA$, *d est le pgcd de a et b.*
On notera $d = a \wedge b$. *(cette définition se généralise à n éléments de A)*
Dem : On montre que $aA+bA$ *est un idéal*
$aA+bA \subset A,\ 0 = 0\times a + 0\times b \in aA+bA \neq \varnothing$
$\forall (x,y) \in aA+bA,\ x-y = au+bv-au'-bv' = a(u-u')+b(v-v') \in aA+bA$
$(aA+bA,+)$ *est un sous groupe de* $(A,+)$
$\forall x \in aA+bA,\ \forall c \in A,\ cx = c(au+bv) = acu+bcv \in aA+bA$

Def : Deux éléments sont premiers entre eux si et seulement si leur pgcd vaut 1 *, autrement dit si* $aA+bA = A$

Th de Bezout (1730-1783) : a et b sont premiers entre eux si et seulement si il existe deux entiers u et v tels que $au+bv = 1$
Dem : $(\Rightarrow)$ $aA+bA = A$ *, or* $1 \in A \Rightarrow 1 = au+bv$
$(\Leftarrow)$ $aA+bA \subset A$ *, soit* $x \in A \Rightarrow x = x\times 1 = axu+bxv \in aA+bA$

Th de Gauss (1777-1855) : si a divise bc et si a est premier avec b alors a divise c
Dem : On va montrer que $cA \subset aA$, $c = c\times 1 = acu+bcv$ *or* $bc \in aA \Rightarrow bc = aw$
donc $c = a(cu+wv) \in aA \Rightarrow cA \subset aA$

Def : Soit $(a,b) \in A^2$, $aA \cap bA$ *est un idéal de* A *or* $(A,+,\times)$ *est un anneau principal, ses idéaux sont donc principaux. Il existe donc* m *tel que* $aA \cap bA = mA$ *, m est le ppcm de a et b*
On notera $m = a \vee b$. *(cette définition se généralise à n éléments)*
Dem : L'intersection de 2 sous groupes est un sous groupe, donc $(aA \cap bA,+)$ *est un sous groupe de* $(A,+)$
$\forall x \in aA \cap bA,\ \forall c \in A,\ cx = cau = cbv \in aA \cap bA$

Th : On a pour tout couple $(a,b) \in A^2$ *:* $(a \wedge b)(a \vee b) = ab$
Dem : On note $d = a \wedge b \Rightarrow a = da'$ *et* $b = db'$ *où* $a' \wedge b' = 1$

On considère $a'b'd$ *on va montrer que* $a'b'd = m = a \vee b$

$a'b'd = a'b = ab' \in aA \cap bA$

Soit $M \in a\mathbb{Z} \cap b\mathbb{Z} \Rightarrow M = ap = bq \Rightarrow a'p = b'q$

$a' / b'q$ *et* $a' \wedge b' = 1 \Rightarrow a'$ *divise* q *(Gauss)* $q = a'x \Rightarrow M = bq = b'dq = a'b'dx \in a'b'dA$

Finalement $md = a'b'dd = a'db'd = ab$

Application : trouver le pgcd et le ppcm de $a = 17640$ *et* $b = 3300$

Réponse : On va décomposer a et b en facteurs premiers

$a = 2^3.3^2.5.7^2$, $b = 2^2.3.5^2.11 \Rightarrow a \wedge b = 2^2.3.5 = 60$ *et* $a \vee b = \dfrac{ab}{60} = 2^3.3^2.5^2.7^2 11 = 970200$

III) L'anneau Z/nZ :

1°) La relation de congruence (rappel MPSI):

Soit n un entier naturel non nul, soient a et b deux éléments de $\mathbb{Z}$ *.*

On définit alors la relation suivante : $a \equiv b \ [n] \Leftrightarrow b - a \in n\mathbb{Z}$

Prop : Cette relation est une relation d'équivalence, appelée relation de congruence modulo n qui est compatible avec les lois + et $\times$

On a donc $\begin{cases} a \equiv b \ [n] \\ c \equiv d \ [n] \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d \ [n] \\ a \times c \equiv b \times d \ [n] \end{cases}$

Dem : $a - a = 0 \in n\mathbb{Z} \Rightarrow a \equiv a \ [n]$*, la congruence est réflexive*

Si $a \equiv b \ [n] \Rightarrow a - b = -(b - a) \in n\mathbb{Z} \Rightarrow b \equiv a \ [n]$*, la congruence est symétrique*

Si $a \equiv b \ [n]$ *et* $b \equiv c \ [n] \Rightarrow c - a = c - b + b - a \in n\mathbb{Z} \Rightarrow a \equiv c \ [n]$*, d'où la transitivité*

$$\begin{cases} a \equiv b \ [n] \\ c \equiv d \ [n] \end{cases} \Rightarrow \begin{cases} b + d - (a + c) = b - a + d - c \in n\mathbb{Z} \\ bd - ac = b(d - c) + c(b - a) \in n\mathbb{Z} \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d \ [n] \\ a \times c \equiv b \times d \ [n] \end{cases}$$

Th : Deux entiers sont congrus modulo n si et seulement si ils ont le même reste dans la division euclidienne par n

Dem : $(\Rightarrow)$ *On a* $x \equiv y \ [n]$*, on note r et r' les restes respectifs de x et y dans leur division euclidienne par n.*

$r - r' = x - np - (y - nq) = x - y + n(q - p) \in n\mathbb{Z}$ *or* $-n < r - r' < n \Rightarrow r - r' = 0$

$(\Leftarrow)$ *on a* $x = np + r$ *et* $y = nq + r \Rightarrow x - y = n(p - q) \in n\mathbb{Z}$

Exo : Quel est le dernier chiffre de $a = 1987^{1995^{1998}}$ *(vous avez une chance sur 10) ?*

2°) L'anneau quotient :

Soit n un entier naturel non nul, l'ensemble des classes d'équivalence pour la relation de congruence modulo n est noté $\mathbb{Z} / n\mathbb{Z}$*, chaque classe est caractérisée par un entier compris entre* 0 *et* $n - 1$*, correspond au reste de la division euclidienne par n. La classe de l'élément p sera notée* $\overline{p}$

Soit l'application $f : \mathbb{Z} \to \mathbb{Z} / n\mathbb{Z} : p \to \overline{p}$ *, f est un morphisme surjectif pour les lois + et* $\times$

Th : Par transport de structure, $(\mathbb{Z} / n\mathbb{Z}, +, \times)$ *est un anneau*

Prop : $\bigcup_{p \in \ 0, n-1} \overline{p} = \mathbb{Z}$

Exo : Réaliser les tables d'addition et multiplication de $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

c'est un anneau non intègre, $\bar{2}$ *et* $\bar{3}$ *sont diviseurs de zéro, il possède 2 éléments inversibles* $\bar{1}$ *et* $\bar{5}$

Th : $\bar{p}$ *est un élément inversible de* $\mathbb{Z}/n\mathbb{Z}$ *si et seulement si p est premier avec n*

Dem : $\bar{p}$ *est inversible* $\Leftrightarrow \exists q \in \mathbb{N}$ *tel que* $\bar{p}.\bar{q} = \bar{1} \Leftrightarrow pq = 1 + nr \Leftrightarrow p \wedge n = 1$

Conséquence : $\mathbb{Z}/n\mathbb{Z}$ *est un corps si et seulement si n est premier, on le notera* F_p

Intérêt : Résoudre des équations dans $\mathbb{Z}/n\mathbb{Z}$

$\overline{5x} = \bar{5}$ *et* $\overline{5x} = \bar{4}$ *dans* $\mathbb{Z}/7\mathbb{Z}$

$\overline{5x} = \bar{3}$ *et* $\overline{4x} = \bar{1}$ *dans* $\mathbb{Z}/8\mathbb{Z}$

$\begin{cases} \overline{7x} + \overline{5y} = \bar{2} \\ \overline{5x} + \overline{4y} = \bar{1} \end{cases}$ *dans* $\mathbb{Z}/8\mathbb{Z}$

$\bar{x}^2 + \bar{x} + \bar{1} = \bar{0}$ *dans* $\mathbb{Z}/7\mathbb{Z}$

3°) Théorèmes d'isomorphismes :

Th : Soit G un groupe multiplicatif et x un élément d'ordre p dans G alors $(Gr(x), \times) \simeq (\mathbb{Z}/p\mathbb{Z}, +)$

(i.e. tout groupe monogène fini de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ *)*

Dem : On construit l'application $\varphi : Gr(x) \to \mathbb{Z}/p\mathbb{Z}$ *telle que* $\varphi(x^k) = \bar{k}$

$\varphi(x^k x^{k'}) = \varphi(x^{k+k'}) = \overline{k+k'} = \bar{k} + \bar{k'} = \varphi(x^k) + \varphi(x^{k'})$, φ *est un morphisme de groupe*

$x^k \in \ker\varphi \Rightarrow \bar{k} = \bar{0} \Rightarrow x^k = x^{pq} = 1$ *donc* φ *est injectif or* $card(G(x)) = p = card(\mathbb{Z}/p\mathbb{Z})$

Donc φ *est un isomorphisme de groupe*

Conséquence : Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ *sont* $\bar{p}$ *telles que* $p \wedge n = 1$

Th : Soient n et p deux entiers premiers entre eux alors l'anneau produit $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, +, \times)$ *est isomorphe à* $(\mathbb{Z}/np\mathbb{Z}, +, \times)$ *(c'est le lemme chinois)*

Dem : On construit un isomorphisme d'anneaux de l'un vers l'autre

$f : \mathbb{Z}/np\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, $x \mapsto (a,b)$ *telle que* $\begin{cases} x = a[n] \\ x = b[p] \end{cases}$

f est clairement un morphisme d'anneaux

Si $f(x) = f(y)$ *alors* $x \equiv y[n]$ *et* $x \equiv y[p] \Rightarrow x - y = nq = pr$

p divise nq et est premier avec n donc p divise q $\Rightarrow q = pz \Rightarrow x - y = nq = npz$

Finalement $x \equiv y[np]$*, donc f est injectif or les deux anneaux ont le même nombre d'éléments, ce qui assure la bijectivité de f*

Exo : Résoudre dans $\mathbb{Z}$ $\begin{cases} x \equiv 3[17] \\ x \equiv 4[11] \end{cases}$*, et résoudre l'équation dans* $\mathbb{Z}/21\mathbb{Z}$, $\bar{x}^2 - \overline{3x} - \bar{7} = 0$

4°) Indicatrice d'Euler :

Def : On appelle indicatrice d'Euler, l'application φ *de* $\mathbb{N}$ *dans* $\mathbb{N}$ *qui à tout entier naturel n non nul fait correspondre le nombre d'éléments inversibles dans* $\mathbb{Z}/n\mathbb{Z}$

Par convention : $\varphi(1)=1$

$\varphi(n)=card\left(p\in\ 1,n-1\ \ tel\ que\ \ p\wedge n=1\right)$

Prop : Si p est premier alors $\varphi(p)=p-1$ *et* $\forall k\in\mathbb{N},\ \varphi\left(p^k\right)=p^{k-1}(p-1)$

Dem : Si p est premier, les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ *sont inversibles donc* $\varphi(p)=p-1$

Les éléments non premiers avec p^k *sont* $p,\ 2p,\ 3p,....,\ p^{k-1}\times p$

Donc $\varphi\left(p^k\right)=p^k-p^{k-1}=p^{k-1}(p-1)$

Prop : Si p et q sont premiers alors $\varphi(pq)=(p-1)(q-1)$

Dem : Le nombre de multiples de p inférieurs à pq est q, pour ceux de q on en dénombre p. Seuls les multiples de p et q ne sont pas premiers avec pq

$\varphi(pq)=pq-p-q+1=(p-1)(q-1)$

Prop : Si p et q sont premiers entre eux alors $\varphi(pq)=\varphi(p)\varphi(q)$

Dem : $(\mathbb{Z}/pq\mathbb{Z},+,\times)$ *est isomorphe à* $(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z},+,\times)$

Soit x tel que $\bar{x}$ *soit inversible dans* $\mathbb{Z}/pq\mathbb{Z}$ *alors* $\exists y$ *tel que* $xy\equiv1[pq]\Rightarrow xy\equiv1[p]$ *et* $xy\equiv1[q]$, *les classes de x modulo p et q seront inversibles respectivement dans* $\mathbb{Z}/p\mathbb{Z}$ *et* $\mathbb{Z}/q\mathbb{Z}$

Réciproquement, si (a,b) *est inversible dans* $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$, *il existe un unique x' de* $\mathbb{Z}/pq\mathbb{Z}$ *associé à* (a',b') *c'est l'inverse de* (a,b) *et x' sera bien l'inverse de x, ainsi*

$card\left(U\left(\mathbb{Z}/pq\mathbb{Z}\right)\right)=card\left(U\left(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}\right)\right)=card\left(U\left(\mathbb{Z}/p\mathbb{Z}\right)\right)card\left(U\left(\mathbb{Z}/q\mathbb{Z}\right)\right)$

Conséquence : Si $n=\prod_{i=1}^{k}p_i^{\alpha_i}$ *alors* $\varphi(n)=\prod_{i=1}^{k}p_i^{\alpha_i-1}(p_i-1)$

Dem : $p_i^{\alpha_i}$ *et* $p_j^{\alpha_j}$ *sont premiers entre eux car les* p_i *sont des nombres premiers, donc on peut affirmer que* $\varphi(n)=\prod_{i=1}^{k}\varphi\left(p_i^{\alpha_i}\right)=\prod_{i=1}^{k}p_i^{\alpha_i-1}(p_i-1)$

Th d'Euler : Si n est un entier supérieur à 2, si a est premier avec n alors $a^{\varphi(n)}\equiv1[n]$

Corollaire : (le petit théorème de Fermat) si p est premier et $1\le k\le p-1$ *alors* $k^{p-1}\equiv1\ [p]$

Dem : Si a est premier avec n, a appartient au groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ *qui est un groupe fini de cardinal* $\varphi(n)$ *donc nécessairement* $a^{\varphi(n)}\equiv1[n]$

Si p est premier, si k est strictement inférieur à p alors p et k sont premiers entre eux, or $\varphi(p)=p-1$ *donc* $k^{p-1}\equiv1\ [p]$

Exo : Déterminer les deux derniers chiffres de 2^{2006}

Exo : Montrer que $\sum_{d\ diviseur\ de\ n}\varphi(d)=n$

Exo (pour aller plus loin) : Théorème de Wilson

Montrer que p est premier si et seulement si $(p-1)!\equiv-1[p]$

IV) L'anneau K[X] des polynômes :

(on identifiera toujours le polynôme et sa fonction polynômiale)

1°) Division Euclidienne :

Th : $A\in K[X]$, *B un polynôme non nul, alors il existe un unique couple* $(Q,R)\in K[X]^2$ *tel que :* $A=BQ+R$ *et* $d°R<d°B$

Dem : Unicité (sous réserve d'existence)

$B(Q-Q')=R'-R$ *or* $d^\circ\big(B(Q-Q')\big)=d^\circ B+d^\circ(Q-Q')$

Si $R\neq R'\Rightarrow Q\neq Q'\Rightarrow d^\circ\big(B(Q-Q')\big)\geq d^\circ B$

Or $d^\circ(R-R')<d^\circ B$ *ce qui est contradictoire donc* $R=R'$ *et* $Q=Q'$

Existence

Si $A=0\Rightarrow Q=R=0$

Sinon on effectue une récurrence sur n le degré de A, on note p le degré de B ($p\leq n$ *)*

On suppose l'existence assurée pour tout polynôme de degré inférieur à n

On pose $A(X)=\sum_{k=0}^{n+1}a_kX^k$, $Q_1(X)=\frac{a_{n+1}}{b_p}X^{n+1-p}$ *et* $A_1(X)=A(X)-B(X)Q_1(X)$

On a $d^\circ(A_1)\leq n\Rightarrow A_1=BQ_2+R$ *où* $d^\circ R<p$

Finalement $A=B(Q_1+Q_2)+R$

Exo : Déterminer le reste de la division euclidienne de X^n *par* $(X-1)^2(X-2)$

Def : B est diviseur de A s'il existe $Q\in K[X]$, $A=BQ$ *(i.e. le reste est nul), on dit aussi que A est un multiple de B*

Def : A et B sont dits associés si chacun d'eux est un multiple de l'autre, il existe donc un scalaire $\lambda\in K^*$ *tel que* $A=\lambda B$

<u>*2°) Notion de racines de polynôme (Rappel MPSI)*</u> *:*

Def : α *est racine d'ordre r du polynôme P si et seulement si il existe un polynôme Q tel que* $P(x)=(x-\alpha)^rQ(x)$ *où* $Q(\alpha)\neq 0$

Th : α *est racine d'ordre r du polynôme P si et seulement si*

$P(\alpha)=P'(\alpha)=....=P^{(r-1)}(\alpha)=0$ *et* $P^{(r)}(\alpha)\neq 0$

Dem : $(\Rightarrow)$ *On a* $P(x)=(x-\alpha)^rQ(x)$ *donc* $P'(x)=(x-\alpha)^{r-1}\big[rQ(x)+(x-\alpha)Q'(x)\big]$ *donc* α *est racine d'ordre* $r-1$ *de la dérivée, en itérant r fois ce procédé le résultat est établi*

$(\Leftarrow)$ *On applique la formule de Taylor en* α *à l'ordre n (le degré de P)*

$$P(x)=\sum_{k=0}^{n}\frac{P^{(k)}(\alpha)}{k!}(x-\alpha)^k=\sum_{k=r}^{n}\frac{P^{(k)}(\alpha)}{k!}(x-\alpha)^k=(x-\alpha)^rQ(x)$$

Or $Q(x)=\sum_{k=r}^{n}\frac{P^{(k)}(\alpha)}{k!}(x-\alpha)^{k-r}\Rightarrow Q(\alpha)=\frac{P^{(r)}(\alpha)}{r!}\neq 0$

Exo : Soit l'équation (E) *:* $x^3+px+q=0$ *où p et q sont deux réels quelconques.*
Déterminer une condition nécessaire et suffisante sur p et q pour que (E) *ait une racine double.*

<u>*3°) Factorisation*</u>

Th de D'Alembert-Gauss : Tout polynôme non constant de $\mathbb{C}[X]$ *admet au moins une racine, tout polynôme de* $\mathbb{C}[X]$ *est donc scindé.* $\forall P\in\mathbb{C}[X]$, $P(x)=\lambda\prod_{i=1}^{n}(x-\alpha_i)^{r_i}$

Dem (HP pour info) : Soit P un polynôme à coefficients complexes de degré d, $\left\{\left|P(z)\right|, z\in\mathbb{C}\right\}$ *est une partie non vide et minorée de* $\mathbb{R}^+$*, elle admet une borne inférieure, que nous noterons* α

On considère une suite $(u_n)\in\mathbb{C}^{\mathbb{N}}$ *, telle que* $\left|P(u_n)\right|\to\alpha$ *définition de la borne inférieure*

Soit $z\in\mathbb{C}$*, tel que* $|z|=r$ *,* $\left|P(z)\right|=\left|\sum_{k=0}^{d}a_k z^k\right|\geq\left|a_d z^d\right|-\left|\sum_{k=0}^{d-1}a_k z^k\right|\geq|a_d|r^d-\sum_{k=0}^{d-1}|a_k|r^k=Q(r)$

Q est un polynôme de $\mathbb{R}[X]$ *qui admet une limite infinie quand* $r\to+\infty$ *(car* $a_d\neq 0$ *) ,ce qui prouve que si* $|z|\to+\infty$ *alors* $\left|P(z)\right|\to+\infty$

Il existe donc $r_0>0$ *tel que si* $|z|>r_0$ *alors* $\left|P(z)\right|>\alpha+1$

Alors la suite $(u_n)\in\mathbb{C}^{\mathbb{N}}$*, telle que* $\left|P(u_n)\right|\to\alpha$ *est à partir d'un certain rang dans le disque D de centre 0 et de rayon* r_0 *qui est une partie bornée de l'ensemble des complexes.*

Il existe donc une sous suite $\left(u_{\varphi(n)}\right)$ *qui converge vers un complexe* z_0 *(Th de Bolzano Weiertrass)*

Comme $P\left(u_{\varphi(n)}\right)=\sum_{k=0}^{d}a_k\left(u_{\varphi(n)}\right)^k\Rightarrow\lim_{n\to\infty}P\left(u_{\varphi(n)}\right)=P(z_0)=\alpha$

Montrons que $P(z_0)=0$ *par l'absurde, on suppose donc que* $\alpha>0$

En considérant le polynôme $A(z)=\dfrac{P(z_0+z)}{P(z_0)}$*, on a alors* $\inf_{z\in\mathbb{C}}\left(\left|A(z)\right|\right)=1=\left|A(0)\right|$

$A(z)=1+b_q z^q+\sum_{k=q+1}^{d}b_k z^k$ *où* $b_q\neq 0$*, on pose* $b_q=-\rho e^{i\theta}$ *et on choisit* $z=re^{-i\frac{\theta}{q}}$

Alors $A(z)=1-\rho r^q+\sum_{k=q+1}^{d}b_k r^k e^{-ik\frac{\theta}{q}}$ *et* $\left|A(z)\right|\leq\left|1-\rho r^q\right|+\sum_{k=q+1}^{d}|b_k|r^k$

Si on prend maintenant $r\leq\left(\dfrac{1}{\rho}\right)^{1/q}$ *alors* $\left|1-\rho r^q\right|=1-\rho r^q$

Et $\left|A(z)\right|-1\leq-\rho r^q+\sum_{k=q+1}^{d}|b_k|r^k<0$ *si r est suffisamment petit ce qui est impossible*

Prop : Si $\alpha\in\mathbb{C}$ *est racine d'ordre r d'un polynôme P de* $\mathbb{R}[X]$ *alors* $\overline{\alpha}$ *est aussi racine d'ordre r de P*

Dem : Il suffit de conjuguer $P(\alpha)=P'(\alpha)=....=P^{(r-1)}(\alpha)=0$ *et* $P^{(r)}(\alpha)\neq 0$

Or $P\in\mathbb{R}[X]\Rightarrow\overline{P(\alpha)}=P\left(\overline{\alpha}\right)$

Th : Tout polynôme P de $\mathbb{R}[X]$ *peut s'écrire sous la forme*

$P(x)=\lambda\prod_{i=1}^{n}(x-\alpha_i)^{r_i}\prod_{k=1}^{q}\left(x^2+b_k x+c_k\right)^{r_k}$ *où* $b_k{}^2-4c_k<0$

Dem : Soit w une racine complexe (d'ordre r) de P alors $\overline{w}$ *est aussi racine d'ordre r*

Or $(x-w)\left(x-\overline{w}\right)=x^2-2\mathrm{Re}(w)x+|w|^2=x^2+bx+c$

De plus $b^2-4c=4\mathrm{Re}(w)^2-4\left[\mathrm{Re}(w)^2+\mathrm{Im}(w)^2\right]<0$*, finalement avec les racines réelles de P, on obtient* $P(x)=\lambda\prod_{i=1}^{n}(x-\alpha_i)^{r_i}\prod_{k=1}^{q}(x-w_k)^{r_k}\prod_{k=1}^{q}\left(x-\overline{w_k}\right)^{r_k}=\lambda\prod_{i=1}^{n}(x-\alpha_i)^{r_i}\prod_{k=1}^{q}\left(x^2+b_k x+c_k\right)^{r_k}$

4°) Les idéaux de K[X] :

On note $(A) = A.K[X]$*, l'idéal engendré par A dans l'anneau* $(K[X],+,\times)$

Th : Pour tout I idéal de $(K[X],+,\times)$*, il existe P de K [X], tel que* $I = (P)$*, l'anneau* $(K[X],+,\times)$ *est principal*

Dem : Si I est réduit au polynôme nul alors $I = (0)$

Sinon on considère $E = \{d^\circ(A), A \in I, A \neq 0\}$ *c'est une partie non vide de* $\mathbb{N}$*, on note d son plus petit élément , il existe alors un polynôme P de I tel que* $d^\circ(P) = d$

On a toujours $(P) \subset I$

On considère un polynôme Q de I et on effectue la division euclidienne de Q par P

$Q = AP + R$ *où* $d^\circ R < d$ *or* $R = Q - AP \in I \Rightarrow R = 0$ *donc* $I \subset (P)$

5°) Arithmétique dans l'anneau des polynômes :

Def : On dit qu'un polynôme est unitaire lorsque son coefficient dominant vaut 1

Def : Soient A et B deux polynômes de K[X], il existe un polynôme D tel que l'idéal engendré par $\{A,B\}$ *soit l'idéal engendré par le polynôme unitaire D, D est le pgcd de A et B, de même, l'intersection des idéaux* (A) *et* (B) *est l'idéal engendré par le polynôme unitaire appelé le ppcm de A et B*

Def : Deux polynômes P et Q sont premiers entre eux si et seulement si $(P)+(Q) = K[X]$

Ou encore si et seulement si il existe deux polynômes U et V tels que $UP + VQ = 1$

(c'est-à-dire qu'ils n'ont pas de diviseur commun de degré non nul)

Th : Si P et Q sont premiers entre eux alors pour tous entiers n et m, les polynômes P^n *et* Q^m *sont premiers entre eux*

Th : Soient P, Q et R trois polynômes tels que P divise QR, si P et Q sont premiers entre eux alors P divise R

Def : Un polynôme est dit irréductible si son degré est > 0 et si ses seuls diviseurs unitaires sont 1 *et lui-même*

Th : Tout polynôme non constant de $K[X]$ *est le produit d'un scalaire par un produit de polynômes irréductibles unitaires de* $K[X]$*, de plus cette décomposition est unique*

Dem : On démontre l'existence par récurrence sur le degré du polynôme P

Si P est de degré 1 *alors P est irréductible*

On suppose que tout polynôme de degré inférieur à n se décompose en produit de polynômes irréductibles.

Soit P un polynôme de degré $n+1$*, s'il est irréductible, alors c'est bien un produit d'un seul polynôme irréductible, sinon P = AB où A et B sont deux polynômes non constants donc de degré inférieur à n, on peut donc appliquer l'hypothèse de récurrence à A et à B*

En mettant en facteurs les coefficients dominants des polynômes irréductibles, on obtient la décomposition souhaitée

Pour l'unicité on suppose dans un premier temps que $P = \lambda \prod_{i=1}^{k} P_i = \mu \prod_{j=1}^{p} Q_j$

Les polynômes irréductibles étant unitaires, $\mu = \lambda$ et valent le coefficient dominant de P
Comme P_i divise P alors il divise l'un des Q_j, étant tous les deux irréductibles et unitaires alors ils sont égaux

Th : Sur $\mathbb{R}$ les polynômes irréductibles sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est strictement négatif

Th : Sur $\mathbb{C}$ les polynômes irréductibles sont les polynômes de degré 1

Exo : Décomposer en éléments irréductibles dans $\mathbb{R}[X]$ le polynôme $x^8 + x^4 + 1$

6°) Un exemple de polynômes : Les polynômes de Lagrange

Soient $(x_i)_{i=0..n}$ $n+1$ réels 2 à 2 distincts
On définit pour $i \in 0,n$, le polynôme $L_i \in \mathbb{R}_n[X]$ tel que $L_i(x_j) = \delta_{i,j}$

On a alors $\forall i \in 0,n$, $L_i(x) = \prod_{j\neq i,\, j=0}^{n} \frac{x - x_j}{x_i - x_j}$

Dem : Le polynôme L_i admet n racines $(x_j)_{j\neq i}$, il est donc factorisable par $\prod_{j\neq i,\, j=0}^{n} (x - x_j)$

Les 2 polynômes étant de degré n, on a $L_i(x) = k.\prod_{j\neq i,\, j=0}^{n} (x - x_j)$ où $k \in \mathbb{R}$

Or $L_i(x_i) = 1 = k \prod_{j\neq i,\, j=0}^{n} (x_i - x_j) \Rightarrow k = \frac{1}{\prod_{j\neq i,\, j=0}^{n} (x_i - x_j)}$, d'où l'expression de L_i

Prop : Pour tout polynôme P de $\mathbb{R}_n[X]$, on a $P(x) = \sum_{i=0}^{n} P(x_i) L_i(x)$

Dem : On démontre que la famille $(L_i)_{i=0..n}$ est libre, c'est donc une base de $\mathbb{R}_n[X]$.

$\forall P \in \mathbb{R}_n[X]$, $P(x) = \sum_{i=0}^{n} \lambda_i L_i(x)$, or $P(x_k) = \sum_{i=0}^{n} \lambda_i \delta_{i,k} = \lambda_k$

V) La structure d'algèbre :

1°) Définition :

On appelle K-algèbre un ensemble E muni de deux lois internes notées + et × et d'une loi externe sur le corps K notée • telles que :

$(E,+,.)$ est un espace vectoriel sur K

$(E,+,\times)$ est un anneau $\forall \alpha \in K, \forall (x,y) \in E^2$ $(\alpha.x)\times y = x \times (\alpha.y) = \alpha.(x \times y)$

Ex : $(K[X],+,\times,.)$, $(\ell(E),+,o,.)$, $(M_n(K),+,\times,.)$

Def : L'algèbre est commutative si la loi × est commutative

Def : Si l'espace vectoriel est de dimension p, on dit que l'algèbre est de dimension p

2°) Sous algèbre :

Th : $(F,+,\times,.)$ *est une sous algèbre de* $(E,+,\times,.)$ *si et seulement si* $(F,+,\times)$ *est un sous anneau de* $(E,+,\times)$ *et* $(F,+,.)$ *est un sous espace vectoriel de* $(E,+,.)$

i.e. : $\forall \lambda \in K, \forall (x,y) \in F^2,\ x+\lambda y \in F,\ x \times y \in F$ *et* $1 \in F$

3°) Morphisme d'algèbre :

Def : Une application de l'algèbre $(F,+,\times,.)$ *vers l'algèbre de* $(E,+,\times,.)$ *est un morphisme d'algèbre si et seulement si :*

$\forall \lambda \in K, \forall (x,y) \in E^2,\ f(x+\lambda y) = f(x) + \lambda f(y),\ f(x \times y) = f(x) \times f(y)$ *et* $f(1_E) = 1_F$

4°) Un exemple d'algèbre :

Dans $M_2(\mathbb{R})$, *on note* $F = \begin{pmatrix} a & -b \\ b & c \end{pmatrix}$, *où* $(a,b,c) \in \mathbb{R}^3$ *avec* $b \neq 0$

On considère $\Gamma = \{M = xI + yF, (x,y) \in \mathbb{R}^2\}$

Montrer que $(\Gamma,+,\times,.)$ *est une algèbre commutative*

Solution : $\Gamma = Vect(I,F)$, *donc* $(\Gamma,+,.)$ *est un sous espace vectoriel de* $(M_2(\mathbb{R}),+,.)$

$\forall (M,M') \in (\Gamma)^2,\ M = xI + yF$ *et* $M' = x'I + y'F$

$MM' = xx'I + (xy' + x'y)F + yy'F^2$

or $F^2 = \begin{pmatrix} a^2 - b^2 & -ab - bc \\ ab + bc & -b^2 + c^2 \end{pmatrix} = (a+c)F + (-ac - b^2)I$

Donc $MM' = (xx' - yy'(ac + b^2))I + (xy' + x'y + yy'(a+c))F \in \Gamma$

Comme $I \in \Gamma$, *on a* $(\Gamma,+,\times,.)$ *une sous algèbre de* $(M_2(\mathbb{R}),+,\times,.)$

De plus (I,F) *forme une famille libre donc une base de* Γ, *finalement* $(\Gamma,+,\times,.)$ *est une algèbre de dimension* 2