Compléments d'algèbre

I. Relation d'équivalence

1°) Relation binaire

Déf : On appelle relation binaire $\mathcal{R}$ sur E toute propriété vraie pour certains couples (x,y) d'éléments de E et fausse pour les autres. Lorsqu'un couple (x,y) vérifie la relation $\mathcal{R}$, on écrit $x\mathcal{R}y$. Sinon, on écrit $x\not\mathcal{R}y$.

Déf : Soit $\mathcal{R}$ une relation binaire sur E. On dit que :
$\mathcal{R}$ est réflexive ssi $\forall x\in E, x\mathcal{R}x$,
$\mathcal{R}$ est symétrique ssi $\forall x,y\in E, x\mathcal{R}y\Rightarrow y\mathcal{R}x$,
$\mathcal{R}$ est transitive ssi $\forall x,y,z\in E, x\mathcal{R}y$ et $y\mathcal{R}z\Rightarrow x\mathcal{R}z$,
$\mathcal{R}$ est antisymétrique ssi $\forall x,y\in E, x\mathcal{R}y$ et $y\mathcal{R}x\Rightarrow x=y$.

2°) Relation d'équivalence

Déf : On appelle relation d'équivalence toute relation binaire à la fois réflexive, symétrique et transitive.

3°) Classe d'équivalence

$\mathcal{R}$ désigne une relation d'équivalence sur E.

Déf : Soit $x\in E$. On appelle classe d'équivalence de x pour la relation $\mathcal{R}$, le sous-ensemble noté $Cl(x)$ (formé des éléments qui sont en relation avec x : $Cl(x)=\{y\in E / x\mathcal{R}y\}$. La classe d'équivalence de x est encore parfois notée $\dot{x},\overline{x},\hat{x}$,…

Prop : $\forall x\in E, x\in Cl(x)$ et par suite une classe d'équivalence n'est jamais vide.

Prop : $\forall x,y\in E$, $x\mathcal{R}y\Rightarrow Cl(x)=Cl(y)$.

Déf : Tout élément y d'une classe d'équivalence est appelé représentant de celle-ci.

Prop : $\forall x,y\in E$, $x\not\mathcal{R}y\Rightarrow Cl(x)\cap Cl(y)=\varnothing$.
Ainsi deux classes d'équivalence distinctes sont disjointes.

Déf : On appelle ensemble quotient de E par $\mathcal{R}$ l'ensemble des classes d'équivalence pour relation $\mathcal{R}$.

4°) Ensemble $\mathbb{Z}/n\mathbb{Z}$

Soit $n\in\mathbb{N}^*$.

Déf : Deux entiers a,b sont dits congrus modulo n ssi $n\mid a-b$. On note alors $a\equiv b\ \ [n]$.

Prop : La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Déf : Pour $a\in\mathbb{Z}$, on note $\overline{a}$ la classe d'équivalence de $a\in\mathbb{Z}$ pour la relation de congruence modulo n.
Ainsi $\overline{a}=\{a+kn / k\in\mathbb{Z}\}$.

Déf : On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n.

Théorème :
$\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini à n éléments qui sont $\overline{0},\overline{1},\ldots,\overline{(n-1)}$.

Prop : $\forall a,b,a',b'\in\mathbb{Z}$, $a\equiv a'\ \ [n]$ et $b\equiv b'\ \ [n]\Rightarrow a+b\equiv a'+b'\ \ [n]$ et $ab\equiv a'b'\ \ [n]$.

Déf : On définit deux lois de composition internes notées $+$ et $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ en posant : $\overline{a}+\overline{b}=\overline{a+b}$ et $\overline{a}\times\overline{b}=\overline{ab}$.

II. Groupes

1°) Généralités

a) définition

Déf : On appelle groupe tout couple $(G,\star)$ formé d'un ensemble G et d'une loi de composition interne $\star$ sur G vérifiant :

1) $\star$ est associative i.e. $\forall a,b,c \in G,(a\star b)\star c = a\star(b\star c)$,

2) $\star$ possède un neutre i.e. $\exists e \in G,(a\star e) = a = (e\star a)$,

3) tout élément de G est inversible pour $\star$ i.e. $\forall a \in G,\exists b \in G, a\star b = e = b\star a$.

Si de plus $\star$ est commutative, on parle de groupe abélien.
Lorsque la loi est notée $\times$ ou., on dit que le groupe est noté multiplicativement.
Lorsque la loi est notée +, on dit que le groupe est noté additivement (réservé au groupe commutatif).

Théorème :

$(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe abélien de neutre $\overline{0}$.

b) sous-groupe

Déf : On appelle sous-groupe d'un groupe $(G,\star)$ toute partie H de G vérifiant :

1) $H \neq \varnothing$.

2) $\forall x,y \in H, x\star y^{-1} \in H$.

Théorème :

Les sous-groupes de $(\mathbb{Z},+)$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

c) morphisme de groupes

Déf : On appelle morphisme d'un groupe $(G,\star)$ vers un groupe $(H,\top)$ toute application $f : G \to H$ vérifiant $\forall x,y \in G, f(x\star y) = f(x) \top f(y)$.

$\ker f = f^{-1}(\{e_H\})$ et $\mathrm{Im} f = f(G)$ sont alors des sous-groupes de $(G,\star)$ et $(H,\top)$.

2°) Produit de deux groupes

Déf : Etant données deux loi de compositions internes $\top$ et $\perp$ définies sur des ensembles E et F, on appelle loi produit sur $E\times F$ la loi $\star$ définie par la relation $(x,y)\star(x',y') = (x\top x', y\perp y')$.

Prop : Si $(G,\top)$ et $(H,\perp)$ sont deux groupes de neutres e et f alors $G\times H$ muni de la loi produit $\star$ est un groupe de neutre $\varepsilon = (e,f)$. De plus l'inverse d'un élément $(x,y) \in G\times H$ est donné par la relation $(x,y)^{-1} = (x^{-1},y^{-1})$.

3°) Groupe engendré par un élément

Soit $(G,\star)$ un groupe de neutre e.

Soit $a \in G$. Pour tout $k \in \mathbb{Z}$, on note a^k itéré d'ordre k de l'élément a :

Pour $k > 0$: $a^k = a\star\cdots\star a$ (k termes)
Pour $k = 0$: $a^0 = e$
Pour $k < 0$: $a^k = a^{-1}\star\cdots\star a^{-1}$ ($|k|$ termes).

Prop : L'application $\varphi_a : \mathbb{Z} \to G$ définie par $\varphi_a(k) = a^k$ est un morphisme de groupes.

Déf : On note $< a >= \{a^k / k \in \mathbb{Z}\}$, l'image de ce morphisme appelé groupe engendré par a.

Théorème :

$< a >$ est le plus petit sous-groupe qui contient l'élément a.

4°) Ordre d'un élément

Soit a un élément d'un groupe $(G,\star)$ de neutre e.

Déf : On dit que l'élément a est d'ordre fini ssi $\exists n \in \mathbb{N}^*, a^n = e$.

Prop : Si a n'est pas un élément d'ordre fini alors $< a >$ est un sous-groupe infini isomorphe à $(\mathbb{Z},+)$.

Déf : Si a est un élément d'ordre fini, on appelle ordre de a le plus petit $n \in \mathbb{N}^*$ tel que $a^n = e$.

Prop : Si a est un élément d'ordre fini égal à n : $\forall k, \ell \in \mathbb{Z}, a^k = a^\ell \Leftrightarrow k = \ell \quad [n]$.

Théorème :

Si a est un élément d'ordre fini égal à n alors $< a >= \left\{e, a, a^2, \ldots, a^{n-1}\right\}$ est un sous-groupe à n éléments isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

5°) Groupe cyclique

Déf : Un groupe $(G, \star)$ est dit monogène ssi il existe $a \in G$ tel que $< a >= G$. Cet élément a est alors appelé générateur du groupe.

Déf : Un groupe est dit cyclique ssi il est monogène et fini.

Théorème :

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique dont les générateurs sont les $\overline{m}$ avec $m \wedge n = 1$.

Théorème :

Tout groupe cyclique de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Cor : Les générateurs de $(U_n, \times)$ sont les $\omega^k = \mathrm{e}^{2ik\pi/n}$ avec $k \wedge n = 1$

Ces éléments sont appelés racines primitives n ème de l'unité.

6°) Partie génératrice d'un groupe

Soit $(G, \star)$ un groupe de neutre e.

Prop : Pour toute partie A de G, il existe un unique sous-groupe H de $(G, \star)$ contenant A et inclus dans tout sous-groupe contenant A.

Déf : Avec les notations précédentes, on dit que H est le sous-groupe engendré par A.

Déf : On appelle partie génératrice d'un groupe toute partie engendrant le groupe en question.

III. Anneaux et corps

1°) Généralités

a) définition

Déf : On appelle anneau tout triplet $(A, +, \times)$ formé d'un ensemble A et de deux lois de composition interne $+$ et $\times$ sur A vérifiant :

(1) $(A, +)$ est un groupe abélien de neutre 0,

(2) $\times$ est associative et possède un neutre 1,

(3) $\times$ est distributive sur $+$ i.e. $\forall a, b, c \in A, a(b+c) = ab + ac$ et $(b+c)a = ba + ca$.

Prop : Si a et b sont deux éléments commutant d'un anneau A on a pour $n \in \mathbb{N}$:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \text{ et } a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}.$$

Déf : Un élément a d'un anneau $(A, +, \times)$ est dit inversible ssi il existe $b \in A$ tel que $ab = ba = 1$. Cet élément est alors unique et est noté a^{-1}.

Prop : L'ensemble $U(A)$ des éléments inversibles de l'anneau est un groupe multiplicatif.

b) sous-anneau

Déf : On appelle sous-anneau d'un anneau $(A, +, \times)$ toute partie B de A vérifiant :

(1) $1 \in B$,

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

(3) $\forall a, b \in B, ab \in B$.

c) morphisme d'anneaux

Déf : On appelle morphisme d'un anneau $(A, +, \times)$ vers un anneau $(B, +, \times)$ toute application $f : A \to B$ vérifiant :

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

(2) $\forall a,b\in A, f(a+b)=f(a)+f(b)$,

(3) $\forall a,b\in A, f(ab)=f(a)f(b)$.

Prop : L'image d'un morphisme d'anneaux est un sous-anneau.

d) produit de deux anneaux

Prop : Si $(A,+,\times)$ et $(B,+,\times)$ sont des anneaux alors en notant encore $+$ et $\times$ les lois produits sur $A\times B$ alors $(A\times B,+,\times)$ est un anneau de neutre $(0_A,0_B)$ et $(1_A,1_B)$.

De plus un élément $(a,b)\in A\times B$ est inversible ssi a et b le sont et son inverse est alors (a^{-1},b^{-1}) .

2°) L'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$

Théorème :

$(\mathbb{Z}/n\mathbb{Z},+,\times)$ est un anneau commutatif de neutres $\overline{0}$ et $\overline{1}$.

De plus l'application $p_n:\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$ définie par $p_n(x)=\overline{x}$ est un morphisme d'anneaux surjectif. On l'appelle surjection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.

Théorème :

Les éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$ sont les $\overline{m}$ avec $m\wedge n=1$.

3°) Idéal d'un anneau commutatif

Soit $(A,+,\times)$ un anneau commutatif.

Déf : On appelle idéal de l'anneau $(A,+,\times)$ toute partie I de A vérifiant :

(1) $0\in I$,

(2) $\forall x,y\in I, x+y\in I$,

(3) $\forall a\in A,\forall x\in I, ax\in I$ (propriété d'absorption)

Prop : Si I et J sont deux idéaux de $(A,+,\times)$ alors $I+J=\{x+y/x\in I,y\in J\}$ et $I\cap J$ sont des idéaux de $(A,+,\times)$.

4°) Idéaux principaux

Déf : Soit $x\in A$, on note Ax (ou xA) l'ensemble $\{xa/a\in A\}$.

Prop : Ax est le plus petit idéal de $(A,+,\times)$ contenant x : on l'appelle idéal (principal) engendré par x .

Théorème :

Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n\in\mathbb{N}$.

Théorème :

Les idéaux de $\mathbb{K}[X]$ sont les $P\mathbb{K}[X]$ avec P polynôme.

5°) Anneau intègre

Soit $(A,+,\times)$ un anneau.

Déf : On appelle diviseur de zéro d'un anneau $(A,+,\times)$ tout élément $a\in A\setminus\{0\}$ tel qu'il existe un élément $b\in A\setminus\{0\}$ tel que $ab=0$ ou $ba=0$.

Déf : Un anneau $(A,+,\times)$ est dit intègre ssi il est commutatif, non réduit à $\{0\}$ et ne possède pas de diviseurs de zéros.

Prop : Si $(A,+,\times)$ est un anneau intègre alors $\forall a,b\in A, ab=0\Rightarrow a=0$ ou $b=0$.

Théorème :

Pour $p\geq 2$, l'anneau $(\mathbb{Z}/p\mathbb{Z},+,\times)$ est intègre ssi p est un nombre premier.

6°) Corps

a) définition

Déf : On appelle corps tout anneau commutatif $(K,+,\times)$ non réduit à $\{0\}$ dont tous les éléments, sauf le nul, sont inversibles.

Prop : Les seuls idéaux d'un corps sont $\{0\}$ et lui-même.

Prop : Tout corps est intègre.

Théorème :

Pour $p \geq 2$, l'anneau $(\mathbb{Z}/p\mathbb{Z},+,\times)$ est un corps ssi p est un nombre premier

b) sous-corps

Déf : On appelle sous-corps d'un corps $(K,+,\times)$ toute partie L de K vérifiant :

1) L est un sous-anneau de $(K,+,\times)$,

2) $\forall x \in L \setminus \{0\}, x^{-1} \in L$.

c) caractéristique d'un corps

Soit $(K,+,\times)$ un corps. L'application $f : \mathbb{Z} \to K$ définie par $f(k) = k.1_K$ (itéré additif de 1_K) est un morphisme d'anneau. Son noyau est un idéal de $\mathbb{Z}$ donc il existe un unique $n \in \mathbb{Z}$ tel que $\ker f = n\mathbb{Z}$.

Déf : L'entier n est appelé caractéristique du corps K.

Prop : La caractéristique d'un corps est soit nulle, soit égale à un nombre premier.

IV. Application à l'arithmétique

1°) Arithmétique dans un anneau intègre

Soit $(A,+,\times)$ un anneau intègre.

Déf : On dit que $a \in A$ divise $b \in A$ ssi il existe $c \in A$ tel que $ac = b$. On note alors $a \mid b$.

Prop : $\forall a,b,c \in A$, $a \mid b$ et $b \mid c \Rightarrow a \mid c$.

Prop : Si $a \mid b$ et $b \mid a$ alors il existe u inversible tel que $b = au$.

Prop : $\forall a,b,c \in A$, $a \mid b \Rightarrow a \mid bc$, $a \mid b$ et $a \mid c \Rightarrow a \mid (b+c)$.

Prop : $\forall x,y \in A$, $x \mid y \Rightarrow Ay \subset Ax$.

2°) Arithmétique dans $\mathbb{Z}$

Théorème :

$\forall a,b \in \mathbb{Z}, \exists ! d \in \mathbb{N}, a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Déf : Cet entier d est appelé le pgcd de a et b.

Théorème :

$\forall a,b \in \mathbb{Z}, \exists ! m \in \mathbb{N}, a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$

Cet entier m est appelé le ppcm de a et b.

Théorème de Bézout

Pour $a,b \in \mathbb{Z}$, on a équivalence entre :

(i) a et b sont premiers entre eux,

(ii) $\exists u,v \in \mathbb{Z}, au + bv = 1$.

Théorème de Gauss

Pour tout $a,b,c \in \mathbb{Z}$. $a \mid bc$ et $a \wedge b = 1 \Rightarrow a \mid c$.

3°) Arithmétique dans $\mathbb{K}[X]$

Théorème :

$\forall A,B \in \mathbb{K}[X], \exists ! D \in \mathbb{K}[X]$ unitaire ou nul tel que $A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$.

Déf : Ce polynôme D est appelé pgcd de A et B.

Théorème :

$\forall A,B\in\mathbb{K}[X],\exists! M\in\mathbb{K}[X]$ unitaire ou nul tel que $A\mathbb{K}[X]\cap B\mathbb{K}[X]=M\mathbb{K}[X]$.

Déf : Ce polynôme M est appelé ppcm de A et B.

4°) Lemme chinois

Soit n et m deux entiers naturels non nuls.

Pour $k\in\mathbb{Z}$, on note $\overline{k}$, $\hat{k}$ et $\dot{k}$ les classes d'équivalence de k dans $\mathbb{Z}/nm\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$.

Pour tout $k,\ell\in\mathbb{Z}$, $k=\ell\ \ [mn]\Rightarrow k=\ell\ \ [m]$ et $k=\ell\ \ [n]$.

On peut donc considérer l'application $f:\mathbb{Z}/mn\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ définie par $f(\overline{k})=(\dot{k},\hat{k})$.

f est un morphisme d'anneaux.

Théorème

Si n et m sont premiers entre eux alors l'application $f:\mathbb{Z}/mn\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ ci-dessus définie un isomorphisme d'anneaux.

5°) Fonction indicatrice d'Euler

Déf : Pour $n\in\mathbb{N}^*$, on pose $\varphi(n)$ le nombre d'entiers $k\in\{1,\ldots,n\}$ premiers avec n. La fonction $\varphi:\mathbb{N}^*\to\mathbb{N}^*$ ainsi définie est appelée fonction indicatrice d'Euler.

Prop : Si p est un nombre premier et $\alpha\in\mathbb{N}^*$ alors $\varphi(p^\alpha)=p^{\alpha-1}(p-1)$.

Prop : Si n et m sont deux entiers naturels non nuls premiers entre eux alors $\varphi(nm)=\varphi(n)\varphi(m)$.

Théorème :

Si n est entier supérieur à 2 de décomposition primaire $n=p_1^{\alpha_1}\ldots p_N^{\alpha_N}$ (avec $p_1,\ldots,p_N$ nombres premiers deux à deux distincts et $\alpha_1,\ldots,\alpha_n\in\mathbb{N}^*$) alors $\varphi(n)=n\prod_{i=}^{N}\left(1-\frac{1}{p_i}\right)$.