Algèbre générale

I. Groupes

I.1. Généralités

Définition. *Soit G un ensemble. On dit que $(G,*)$ est un **groupe** si*
- (G_1) *$*$ est une loi de composition interne sur G, c'est-à-dire une application de $G\times G$ dans G ;*
- (G_2) *$*$ est associative :* $\forall (a,b,c)\in G^3 \quad (a*b)*c = a*(b*c)$;
- (G_3) *$*$ admet un élément neutre e :* $\exists e\in G \quad \forall a\in G \quad e*a=a*e=a$;
- (G_4) *chaque élément de G admet un symétrique :* $\forall a\in G \quad \exists b\in G \quad a*b = b*a = e$.

I.2. Sous-groupes

Définition. *Soit $(G,*)$ un groupe. Une partie H de G est appelée un **sous-groupe** de $(G,*)$ si $(H,*)$ est un groupe.*

Proposition I.1. *Une partie H est un sous-groupe de $(G,*)$ si et seulement si elle vérifie les trois conditions :*
- (S_1) *$H\neq\varnothing$ (ou $e\in H$) ;*
- (S_2) *H est stable par $*$:* $\forall (a,b)\in H^2 \quad a*b\in H$;
- (S_3) *H est stable par passage au symétrique :* $\forall a\in H \quad a^{-1}\in H$.

Il est équivalent de dire :
- (S_1') *$H\neq\varnothing$ (ou $e\in H$) ;*
- (S_2') $\forall (a,b)\in H^2 \quad a*b^{-1}\in H$.

Théorème I.2. *Soit $(H_i)_{i\in I}$ une famille (éventuellement infinie) de sous-groupes de $(G,*)$. Alors, $\bigcap_{i\in I} H_i$ est un sous-groupe de $(G,*)$.*

Théorème I.3. *Les sous-groupes de $(\mathbb{Z},+)$ sont exactement les ensembles*

$$a\mathbb{Z} = \{ka \ ;\ k\in\mathbb{Z}\} \qquad \text{où } a\in\mathbb{N}$$

I.3. Morphismes de groupes

Définition. *Soient $(G,*)$ et $(H,\triangle)$ deux groupes, et φ une application de G dans H. On dit que φ est un **morphisme de groupes** de $(G,*)$ dans $(H,\triangle)$ si*

$$\forall (a,b)\in G^2 \quad \varphi(a*b) = \varphi(a)\mathbin{\triangle}\varphi(b)$$

*On dit que φ est un **isomorphisme** de groupes si c'est un morphisme bijectif.*

Proposition I.4. *Si φ est un morphisme de groupes de $(G,*)$ dans $(H,\triangle)$, alors*
- $\varphi(e_G) = e_H$;
- $\forall a\in G \quad \varphi(a^{-1}) = \varphi(a)^{-1}$.

Proposition I.5. *La composée de deux morphismes de groupes est un morphisme de groupes ; la réciproque d'un isomorphisme de groupes est un isomorphisme.*

Proposition I.6. *Soit φ un morphisme de groupes de $(G,*)$ dans $(H,\triangle)$.*
- *Si G_1 est un sous-groupe de G, alors $\varphi(G_1)$ est un sous-groupe de H.*
- *Si H_1 est un sous-groupe de H, alors $\varphi^{-1}(H_1)$ est un sous-groupe de G.*

Définition. *Soit φ un morphisme de groupes de $(G,*)$ dans $(H,\triangle)$. Alors :*
- *$\varphi(G)$, qui est un sous-groupe de H, est appelé **image** de φ, et noté $\operatorname{Im}\varphi$;*
- *$\varphi^{-1}(\{e_H\})$, qui est un sous-groupe de G, est appelé **noyau** de φ, et noté $\operatorname{Ker}\varphi$.*

Proposition I.7. *Soit φ un morphisme de groupes de $(G,*)$ dans $(H,\triangle)$.*

Deux éléments a et b de G ont la même image si et seulement si $a*b^{-1}\in\operatorname{Ker}\varphi$, c'est-à-dire si et seulement si il existe $h\in\operatorname{Ker}\varphi$ tel que $a = h*b$.

Le morphisme φ est donc injectif si et seulement si $\operatorname{Ker}\varphi = \{e_G\}$.

I.4. Produit de groupes

Proposition I.8. *Soient $(G,*)$ et $(H,\triangle)$ deux groupes. L'ensemble $G\times H$, muni de la loi $\otimes$ définie par*

$$\forall (a_1,a_2)\in G^2 \quad \forall (b_1,b_2)\in H^2 \quad (a_1,b_1)\otimes(a_2,b_2) = (a_1*a_2, b_1\mathbin{\triangle} b_2)$$

*est un groupe, appelé **groupe produit** des groupes G et H. Son neutre est (e_G,e_H) ; le symétrique d'un élément (a,b) est (a^{-1},b^{-1}).*

II. Le groupe $\mathbb{Z}/n\mathbb{Z}$

II.1. Congruences

Définition. *Soient $n\in\mathbb{N}^*$ et $(a,b)\in\mathbb{Z}^2$. On dit que a est **congru** à b modulo n si n divise $b-a$, c'est-à-dire s'il existe $k\in\mathbb{Z}$ tel que $b = a+nk$; on écrit alors $a\equiv b\ [n]$.*

Proposition II.1. *Soit $n\in\mathbb{N}^*$. La relation de congruence modulo n est une relation d'équivalence ; autrement dit, elle est*
- *réflexive :* $\forall a\in\mathbb{Z} \quad a\equiv a\ [n]$;
- *symétrique :* $\forall (a,b)\in\mathbb{Z}^2 \quad a\equiv b\ [n] \Longrightarrow b\equiv a\ [n]$;

- *transitive :* $\forall (a,b,c)\in\mathbb{Z}^3 \quad (a\equiv b\ [n] \text{ et } b\equiv c\ [n]) \Longrightarrow a\equiv c\ [n]$.

Définition. *Soit $n\in\mathbb{N}^*$. La **classe de congruence** modulo n d'un entier a, est sa classe d'équivalence pour cette relation de congruence, c'est-à-dire l'ensemble*

$$\{b\in\mathbb{Z}\,|\,b\equiv a\ [n]\}=\{a+nk\ ;\ k\in\mathbb{Z}\}$$

*S'il n'y a pas d'ambiguïté sur la valeur de n, cette classe sera notée $\overline{a}$. Si C est la classe d'un entier a, on dit que a est un **représentant** de la classe C.*

Proposition II.2. *Soit $n\in\mathbb{N}^*$; chaque entier $a\in\mathbb{Z}$ appartient à une et une seule des n classes $\overline{0}$, $\overline{1}$, $\overline{2}$,…, $\overline{n-1}$, qui sont donc deux à deux distinctes.*

Définition. *Soit $n\in\mathbb{N}^*$. L'ensemble des classes de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$; il a pour cardinal n. Plus précisément, $\mathbb{Z}/n\mathbb{Z}=\{\overline{0},\overline{1},\overline{2},\dots,\overline{n-1}\}$.*

II.2. Le groupe $\mathbb{Z}/n\mathbb{Z}$

Proposition II.3. *Soit $n\in\mathbb{N}^*$. La relation de congruence modulo n est compatible avec l'addition et la multiplication dans $\mathbb{Z}$; autrement dit, pour tout $(a,b,c)\in\mathbb{Z}^3$,*
- $a\equiv b\ [n] \implies a+c\equiv b+c\ [n]$;
- $a\equiv b\ [n] \implies ac\equiv bc\ [n]$.

Définition. *Soient C_1 et C_2 deux classes de congruence modulo n ; soient $a\in C_1$ et $b\in C_2$. La classe $\overline{a+b}$ ne dépend alors que des classes C_1 et C_2, et pas des représentants a et b choisis ; on peut donc définir la somme C_1+C_2 comme étant $\overline{a+b}$. Autrement dit, on définit la loi $+$ sur $\mathbb{Z}/n\mathbb{Z}$ par*

$$\forall (a,b)\in\mathbb{Z}^2 \quad \overline{a}+\overline{b}=\overline{a+b}$$

Proposition II.4. *Soit $n\in\mathbb{N}^*$. Alors, $\mathbb{Z}/n\mathbb{Z}$ muni de la loi $+$ est un groupe commutatif. Son neutre est $\overline{0}$; le symétrique d'un élément $\overline{a}$ est $\overline{-a}=\overline{n-a}$.*

Proposition II.5. *Soit $n\in\mathbb{N}^*$. L'application $a\longmapsto\overline{a}$ est un morphisme de groupes de $(\mathbb{Z},+)$ dans $(\mathbb{Z}/n\mathbb{Z},+)$.*

III. Sous-groupe engendré par une partie

III.1. Définition

Définition. *Soient $(G,*)$ un groupe, et A une partie de G. L'intersection de tous les sous-groupes contenant A est encore un sous-groupe de G ; on l'appelle **sous-groupe engendré** par A.*

Proposition III.1. *Soient A et H deux parties d'un groupe G. Alors, H est le sous-groupe engendré par A si et seulement si il vérifie les deux conditions :*

i. *H est un sous-groupe de G et $A\subset H$;*

ii. *tout sous-groupe K de G qui contient A, contient aussi H.*

Proposition III.2. *Soit $(G,*)$ un groupe ; soit $(a,b)\in G^2$.*
- *Le sous-groupe engendré par $\{a\}$ dans G est $\{a^n\ ;\ n\in\mathbb{Z}\}$.*
- *Si $a*b=b*a$, le sous-groupe engendré par $\{a,b\}$ est $\{a^n*b^p\ ;\ (n,p)\in\mathbb{Z}^2\}$.*

III.2. Groupe monogène, groupe cyclique

Définition. *Un groupe $(G,*)$ est dit **monogène** s'il existe $a\in G$ tel que le sous-groupe engendré par $\{a\}$ soit G tout entier ; on dit alors que a est un **générateur** de G. Un groupe est dit **cyclique** s'il est monogène et fini.*

Proposition III.3. *Soit $n\in\mathbb{N}^*$. Alors, $\mathbb{Z}/n\mathbb{Z}$ est cyclique ; ses générateurs sont les classes $\overline{a}$ des entiers a premiers avec n.*

Théorème III.4. *Soit $(G,*)$ un groupe monogène, et a un générateur de G. Alors, l'application $\varphi:\mathbb{Z}\longrightarrow G,\ n\longmapsto a^n$ est un morphisme de groupes surjectif. De plus :*
- *si $\operatorname{Ker}\varphi=\{0\}$, alors φ est un isomorphisme, et donc G est isomorphe à $\mathbb{Z}$;*
- *sinon, il existe un unique $n\in\mathbb{N}^*$ tel que $\operatorname{Ker}\varphi=n\mathbb{Z}$; G est alors isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Corollaire III.5. *Soit $n\in\mathbb{N}^*$. Le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$; ses générateurs sont les $\exp(2ik\pi/n)$ vérifiant $k\wedge n=1$.*

III.3. Ordre d'un élément

Définition. *Soit $(G,*)$ un groupe, et $a\in G$. On dit que a est **d'ordre fini** s'il existe $p\in\mathbb{N}^*$ tel que $a^p=e$. Le plus petit des éléments $p\in\mathbb{N}^*$ vérifiant $a^p=e$ est alors appelé **ordre** de a.*

Proposition III.6. *Soit a un élément d'ordre fini d du groupe $(G,*)$. Alors :*
- *d est le cardinal du sous-groupe engendré par a ;*
- *pour tout $p\in\mathbb{Z}$, on a $a^p=e\Longleftrightarrow d|p$.*

Proposition III.7. *Soit G un groupe **fini**. Alors, tout élément de G est d'ordre fini, et son ordre divise le cardinal de G. En particulier : $\forall a\in G \quad a^{\operatorname{Card}(G)}=e_G$.*

IV. Anneaux et corps

IV.1. Généralités

Définition. *On dit que $(A, +, *)$ est un* ***anneau*** *si*
- *(A1) $+$ et $*$ sont deux lois de composition internes sur A ;*
- *(A2) $(A, +)$ est un groupe abélien ;*
- *(A3) $*$ est associative ;*
- *(A4) $*$ est distributive sur $+$: pour tout $(a, b, c) \in A^3$ $\quad a*(b+c) = a*b + a*c$ et $\quad (b+c)*a = b*a + c*a$;*
- *(A5) $*$ admet un élément neutre 1_A.*

L'anneau est dit ***commutatif*** *si la loi $*$ est commutative.*

Définition. *Un élément a d'un anneau $(A, +, *)$ est dit* ***inversible*** *s'il admet un symétrique pour la loi $*$; ce symétrique est alors unique.*

Proposition IV.1. *Soit $(A, +, *)$ un anneau. L'ensemble A^* des inversibles de A, muni de la loi $*$, est un groupe.*

Définition. *On dit que $(K, +, *)$ est un* ***corps*** *si*
- *$(K, +, *)$ est un anneau commutatif ;*
- *tout élément non nul de K est inversible.*

IV.2. Anneau produit

Définition. *Soient $(A, +, *)$ et $(B, +, \triangle)$ deux anneaux. L'ensemble $A \times B$, muni des lois $+$ et $\otimes$ définies par $\quad (a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \quad$ et $\quad (a_1, b_1) \otimes (a_2, b_2) = (a_1 * a_2, b_1 \triangle b_2)$, $\quad$ est un anneau, appelé* ***anneau produit*** *des anneaux A et B.*

Proposition IV.2. *Avec les notations précédentes, un élément (a, b) de l'anneau produit $A \times B$ est inversible si et seulement si a est inversible dans A et b est inversible dans B.*

IV.3. Sous-anneaux

Soit $(A, +, *)$ un anneau. Une partie B de A est appelée un **sous-anneau** si $(B, +, *)$ est un anneau contenant 1_A.

Proposition IV.3. *Soit $(A, +, *)$ un anneau. Une partie B de A est un sous-anneau si et seulement si*
- *B est un sous-groupe de $(A, +)$;*
- *$1_A \in B$;*
- *B est stable pour la loi $*$.*

IV.4. Morphismes d'anneaux

Définition. *Soient $(A, +, *)$ et $(B, +, \triangle)$ deux anneaux. Une application φ de A dans B est appelée un* ***morphisme d'anneaux*** *si*
- *$\varphi(1_A) = 1_B$;*
- *$\forall (a, b) \in A^2 \quad \varphi(a + b) = \varphi(a) + \varphi(b) \quad$ et $\quad \varphi(a * b) = \varphi(a) \triangle \varphi(b)$.*

On dit que c'est un ***isomorphisme*** *si c'est un morphisme bijectif.*

Proposition IV.4. *La composée de deux morphismes d'anneaux est encore un morphisme d'anneaux ; la réciproque d'un isomorphisme d'anneaux est encore un isomorphisme d'anneaux.*

Définition. *Soit φ un morphisme d'anneaux de $(A, +, *)$ dans $(B, +, \triangle)$. On appelle* ***image*** *de φ l'ensemble $\varphi(A) \subset B$, noté $\operatorname{Im} \varphi$; on appelle* ***noyau*** *de φ l'ensemble $\varphi^{-1}(\{0_B\}) \subset A$, noté $\operatorname{Ker} \varphi$.*

Proposition IV.5. *Avec les hypothèses et notations précédentes,*
- *l'image $\operatorname{Im} \varphi$ du morphisme φ est un sous-anneau de B ;*
- *le noyau de φ est un sous-groupe de $(A, +)$; et le morphisme φ est injectif si et seulement si $\operatorname{Ker} \varphi = \{0_A\}$.*

IV.5. Idéaux d'un anneau commutatif

Définition. *Soit $(A, +, *)$ un anneau commutatif. Une partie I de A est appelée un* ***idéal*** *de A si*
- *I n'est pas vide ;*
- *I est stable pour la loi $+$: $\quad \forall (a, b) \in I^2 \quad a + b \in I$;*
- *I est absorbant pour la loi $*$: $\quad \forall a \in I \quad \forall b \in A \quad a * b \in I$.*

Proposition IV.6. *Soient b et c deux éléments de l'anneau commutatif A. Les ensembles $\quad bA = \{b*x \; ; \; x \in A\} \quad$ et $\quad bA + cA = \{b*x + c*y \; ; \; (x, y) \in A^2\} \quad$ sont deux idéaux de A, respectivement appelés idéal engendré par b et idéal engendré par $\{b, c\}$.*

Proposition IV.7. *Le noyau d'un morphisme d'anneaux commutatifs est toujours un idéal.*

Proposition IV.8. *Soit $(A, +, *)$ un anneau commutatif. Alors*
- *tout idéal de A est un sous-groupe de $(A, +)$;*
- *l'intersection d'une famille d'idéaux de A, est encore un idéal de A.*

IV.6. Anneaux intègres

Définition. *Soit $(A,+,*)$ un anneau commutatif. On dit qu'un élément a de A est un **diviseur de zéro** si $a \neq 0_A$ et $\exists b \in A \setminus \{0_A\}$ $a*b = 0_A$.*

*On dit que A est un anneau **intègre** s'il ne contient aucun diviseur de zéro, c'est-à-dire si*

$$\forall (a,b) \in A^2 \quad a*b = 0_A \Longrightarrow (a = 0_A \text{ ou } b = 0_A)$$

Proposition IV.9. *Dans un anneau intègre $(A,+,*)$, tout élément **non nul** a est **régulier**, c'est-à-dire vérifie $\forall (b,c) \in A^2 \quad a*b = a*c \Longrightarrow b = c$.*

Proposition IV.10. *Si $(A,+,*)$ est un corps, alors c'est un anneau intègre.*

Définition. *Soient $(A,+,*)$ un anneau intègre, et $(a,b) \in A^2$. On dit que a **divise** b, et on écrit $a \mid b$, s'il existe $c \in A$ vérifiant $b = ac$.*

Proposition IV.11. *Soient $(A,+,*)$ un anneau intègre, et $(a,b) \in A^2$. Alors, a divise b si et seulement si l'idéal bA engendré par b, est inclus dans l'idéal aA engendré par a.*

Proposition IV.12. *Soit $(A,+,*)$ un anneau intègre. Alors :*
- $\forall (x,y,z) \in A^3 \quad (x \mid y \text{ et } x \mid z) \Longrightarrow x \mid (y+z)$;
- *$(x \mid y$ et $y \mid x)$ si et seulement si il existe $u \in A$ **inversible** vérifiant $y = ux$.*

V. L'anneau $\mathbb{Z}/n\mathbb{Z}$

V.1. Généralités

Définition. *Soit $n \in \mathbb{N}^*$. De même que pour l'addition, on peut définir une multiplication dans $\mathbb{Z}/n\mathbb{Z}$ par $\forall (a,b) \in \mathbb{Z}^2 \quad \overline{a}.\overline{b} = \overline{(a.b)}$, la classe produit ne dépendant pas des représentants a et b choisis.*

Proposition V.1. *Soit $n \in \mathbb{N}^*$. Alors, $\big(\mathbb{Z}/n\mathbb{Z},+,.\big)$ est un anneau commutatif; ses éléments inversibles sont les classes des entiers premiers avec n.*

Corollaire V.2. *Soit $n \in \mathbb{N}^*$; $\big(\mathbb{Z}/n\mathbb{Z},+,.\big)$ est un corps si et seulement si n est un nombre premier.*

V.2. Le théorème chinois

Théorème V.3. *Soit $(p,q) \in (\mathbb{N}^*)^2$. Si $p \wedge q = 1$, alors $\mathbb{Z}/pq\mathbb{Z}$ est isomorphe à l'anneau produit $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.*

Corollaire V.4. *Soient $(p,q) \in (\mathbb{N}^*)^2$, et $(a,b) \in \mathbb{Z}^2$. Si $p \wedge q = 1$, alors le système de congruences*

$$x \equiv a \ [p], \quad x \equiv b \ [q]$$

admet une et une seule solution x_0 dans $[\![0, pq-1]\!]$; les autres solutions sont les entiers x congrus à x_0 modulo pq.

V.3. L'indicateur d'Euler

Définition. *On appelle **fonction indicatrice d'Euler**, ou **indicateur d'Euler**, la fonction φ qui, à tout $n \in \mathbb{N}^*$, associe le nombre $\varphi(n)$ d'inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$; c'est aussi le nombre d'entiers premiers avec n dans $[\![0, n-1]\!]$.*

Théorème V.5 (Théorème d'Euler)**.** *Soit $n \in \mathbb{N}^*$. Si $a \in \mathbb{Z}$ est premier avec n, alors $a^{\varphi(n)} \equiv 1 \ [n]$.*

Proposition V.6.
- *Si $(p,q) \in \mathbb{Z}^2$ et $p \wedge q = 1$, alors $\varphi(pq) = \varphi(p)\varphi(q)$.*
- *Si p est un nombre premier et $n \in \mathbb{N}^*$, alors $\varphi(p^n) = p^n - p^{n-1}$.*
- *Si $n \in \mathbb{N}^*$, alors $\displaystyle \varphi(n) = n \prod_{p \in P_n} \Big(1 - \frac{1}{p}\Big)$ où P_n est l'ensemble des diviseurs premiers de n.*

VI. Arithmétique dans $\mathbb{Z}$ et $\mathbb{K}[X]$

VI.1. Arithmétique dans $\mathbb{Z}$

Théorème VI.1. *Soit $(a,b) \in \mathbb{Z}^2$. Alors $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ où $d = a \wedge b$. En particulier,*
- *il existe $(u,v) \in \mathbb{Z}^2$ tel que $a \wedge b = au + bv$;*
- *$a \wedge b = 1$ si et seulement s'il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.*

Proposition VI.2. *Soit $(a,b,c) \in \mathbb{Z}^3$. Si $a \mid bc$ et a est premier avec b, alors $a \mid c$.*

VI.2. Arithmétique dans $\mathbb{K}[X]$

Théorème VI.3. *Si I est un idéal de $\mathbb{K}[X]$ non réduit à $\{0\}$, alors il existe un unique polynôme unitaire A vérifiant $I = A\mathbb{K}[X] = \big\{AQ \ ; \ Q \in \mathbb{K}[X]\big\}$.*

Théorème VI.4. *Soit $(A,B) \in \mathbb{K}[X]^2$. Alors $A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$ où $D = A \wedge B$. En particulier,*
- *il existe $(U,V) \in \mathbb{K}[X]^2$ tel que $A \wedge B = AU + BV$;*
- *$A \wedge B = 1$ si et seulement s'il existe $(U,V) \in \mathbb{K}[X]^2$ tel que $AU + BV = 1$.*

Proposition VI.5. *Soit $(A,B,C) \in \mathbb{K}[X]^3$. Si $A \mid BC$ et A est premier avec B, alors $A \mid C$.*