Algèbre générale

Ce document n'est pas un cours mais présente seulement quelques notions à connaître sur le sujet.

1 Groupes

1.1 Généralités

Définition 1 *Soit G un ensemble non-vide muni d'une loi interne $\star$*
$$\begin{array}{ccc} G\times G & \to & G \\ (x,y) & \mapsto & x\star y \end{array}$$
(c'est à dire d'une application $\star$:),
$(G,\star)$ est un groupe si la loi $\star$ vérifie :

- $\forall (x,y,z)\in G\times G\times G,\ x\star(y\star z)=(x\star y)\star z$ *(on dit $\star$ est associative)*
- $\exists e\in G,\ \forall x\in G,\ x\star e=e\star x=x$ *(on dit que e est élément neutre pour $\star$)*
- $\forall x\in G,\ \exists x^{'}\in G,\ x\star x^{'}=x^{'}\star x=e$ *(on dit que tout élément de G possède un symétrique).*

Si de plus $\forall (x,y)\in G^2,\ x\star y=y\star x$ (on dit que $\star$ est commutative), on dit que le groupe $(G,\star)$ est commutatif ou abélien.

Remarque 1 *On montre que l'élément neutre est unique, de même que le symétrique d'un élément.*

Notations :

- La loi d'un groupe abélien est souvent notée additivement $+$:
  - l'élément neutre est noté 0 ou 0_G
  - le symétrique d'un élément x est noté $-x$ et est appelé l'opposé de x
  - La puissance d'ordre $n\in\mathbb{N}$ d'un élément x, $x+\cdots+x$ (n termes) est notée $n\cdot x$ (avec $0\cdot x=0$).
- Lorsque la loi d'un groupe est notée multiplicativement$\cdot$ ou $\times$:
  - l'élément neutre est noté 1 ou 1_G
  - le symétrique d'un élément x est noté x^{-1}.
  - La puissance d'ordre $n\in\mathbb{N}$ d'un élément x, $x\times\cdots\times x$ (n termes) est notée x^n (convention $x^0=1$).

Définition 2 *Si $(G,\star)$ est un groupe de cardinal fini $n\in\mathbb{N}^*$, on note* $\operatorname{card} G=n$ *ou $|G|=n$, on dit que G est un groupe fini et que G est un groupe d'ordre n.*

Exemple 1 *Dans $(\mathbb{C}^*,\times)$, pour $n\in N^*$ l'ensemble des racines n-ième de l'unité $\mathbb{U}_n$ est un sous-groupe fini de $(\mathbb{C}^*,\times,)$, c'est un groupe d'ordre n.*

Définition 3 *Soit $(G,\star)$ un groupe et $a\in G$, s'il existe $k\in\mathbb{N}^*$ tel que $a^k=e_G$ on dit que a est un élément d'ordre fini, le plus petit entier $p\geqslant 1$ tel que $a^p=e_G$ est appelé l'ordre de a.*

Exercice 1
Dans un groupe fini $(G,\star)$ d'ordre n montrer que tout élément est d'ordre fini et d'ordre inférieur ou égal à n

Définition 4 *Soit $(G,\star)$ un groupe et G' une partie de G*
G' est un sous-groupe de $(G,\star)$ si

1. *G' est non vide*
2. *$(G',\star)$ est un groupe*

Proposition 1 *Soit $(G,\star)$ un groupe et G' une partie non vide de G*
G' est un sous-groupe de $(G,\star)$ si et seulement si $\forall (x,y)\in G'^2,\quad x\star y^{-1}\in G'$.

Proposition 2 *Si G' est un sous-groupe d'un groupe $(G,\star)$ alors $(G',\star)$ et $(G,\star)$ ont même élément neutre et tout élément de G' a même symétrique dans $(G',\star)$ et dans $(G,\star)$.*

Proposition 3 *Soit $(G,\star)$ un groupe et $(G_i)_{i\in I}$ une famille de sous-groupes de G*
$\bigcap\limits_{i\in I} G_i$ *est un sous-groupe de G*

Proposition 4
Les sous-groupes de $(\mathbb{Z},+)$ sont les sous-groupes de la forme $a\mathbb{Z}$ où $a\in\mathbb{Z}, a\mathbb{Z}=\{ax,\ x\in\mathbb{Z}\}$.

Définition 5 *Soit $(G,\star)$ et $(G',\star')$ deux groupes,*
on appelle morphisme de groupe toute application f de G dans G' telle que $\forall (x,y)\in G^2,\ f(x\star y)=f(x)\star' f(y)$

On a aussi :

- Un morphisme de groupe bijectif s'appelle un isomorphisme de groupe.
- Pour $G'=G$ un morphisme de groupe s'appelle un endomorphisme de groupe.
- Pour $G'=G$ un isomorphisme de groupe s'appelle un automorphisme de groupe.

Proposition 5
Si $Aut(G)$ désigne l'ensemble des automorphismes du groupe $(G,\star)$ Alors $(Aut(G),\circ)$ est un groupe

Proposition 6 *Pour $a\in G$ l'application h_a : $\begin{array}{ccc} G & \to & G \\ g & \mapsto & h_a(g)=a\star g\star a^{-1}\end{array}$ est un automorphisme de $(G,\star)$ appelé automorphisme intérieur.*

Définition 6 *Soit $(G,\star)$ et $(G',\star')$ deux groupes et f un morphisme de groupe*

- *On appelle noyau de f la partie de G, $\ker f=\{g\in G,\ f(g)=e_{G'}\}$ où $e_{G'}$ est l'élément neutre de G'*
- *On appelle image de f la partie de G', $\mathrm{Im}f=\{g'\in G',\ \exists g\in G,\ f(g)=g'\}$.*

Proposition 7 *Soit $(G,\star)$ et $(G',\star')$ deux groupes et f un morphisme de groupe.*
Le noyau de f est un sous-groupe de $(G,\star)$ et l'image de f est un sous-groupe de $(G',\star')$

Proposition 8 *Soit $(G,\star)$ et $(G',\star')$ deux groupes et f un morphisme de groupe.*

1. *f est injectif si et seulement si $\ker f=\{e_G\}$ où e_G est l'élément neutre de G.*
2. *f est surjectif si et seulement si $\mathrm{Im}f=G'$.*

1.2 Groupes monogènes et groupes cycliques

Proposition 9 *Soit $(G,\star)$ un groupe et $A\subset G$.*
Il existe un plus petit sous-groupe (au sens de l'inclusion) G' de G contenant A, on dit que G' est le sous-groupe de G engendré par A, on note $G'=<A>$

Définition 7 *Soit $(G,\star)$ un groupe et $A\subset G$.*
On dit que A est une partie génératrice de G si $G=<A>$

Exemple 2

1. *On considère le groupe $(\mathbb{Z},+)$, $<\{1\}>$ est une partie génératrice de $(\mathbb{Z},+)$, on note aussi $<1>=\mathbb{Z}$*
2. *On considère le groupe des permutations d'un ensemble à n éléments, $n\in\mathbb{N}$, $n\geqslant 2$, $(\mathbb{S}_n,\circ)$, soit A l'ensemble des transpositions de $\mathbb{S}_n$, $A=\{t=(i,j)\in\mathbb{S}_n,\ (i,j)\in[\![1,n]\!]^2\ i<j\}$,*
   A est une partie génératrice de $\mathbb{S}_n$, $<A>=\mathbb{S}_n$
3. *Dans le plan vectoriel euclidien $\vec{P}$, on considère $G=O(\vec{P})$ le groupe des isométries vectorielles et A l'ensemble des réflexions (symétries orthogonales par rapport à une droite), A est une partie génératrice de $O(\vec{P})$, plus précisément toute isométrie vectorielle du plan est la composée d'au plus deux réflexions.*

Définition 8 *Soit $(G,\star)$ un groupe*
G est un groupe monogène s'il existe $a\in G$ tel que $G=<\{a\}>$, on note aussi $G=<a>$,
si de plus G est fini on dit que G est cyclique.

Exemple 3

1. *Pour $n\in\mathbb{N}^*$, dans $(\mathbb{C}^*,\times)$ le sous-groupe $\mathbb{U}_n$ des racines n-ième de l'unité est un groupe cyclique d'ordre n.*
2. *$(\mathbb{Z},+)$ est un groupe monogène.*

Proposition 10 *Un groupe monogène ou cyclique est commutatif.*

1.3 Produit de deux groupes

Proposition 11 *Soit $(G_1,\star_1)$ et $(G_2,\star_2)$ deux groupes, on muni le produit cartésien $G_1\times G_2$ de la loi interne $\star$ définie par : $\forall (x_1,x_2)\in G_1\times G_2,\ \forall (y_1,y_2)\in G_1\times G_2,\quad (x_1,x_2)\star(y_1,y_2)=(x_1\star_1 y_1, x_2\star_2 y_2)$, on a :*
$(G_1\times G_2,\star)$ est un groupe appelé groupe produit de $(G_1,\star_1)$ et $(G_2,\star_2)$.

L'élément neutre de $(G_1\times G_2,\star)$ est (e_{G_1},e_{G_2}) et le symétrique de $(x,y)\in G_1\times G_2$ est (x^{-1},y^{-1})
Plus généralement on peut définir le produit de p groupes $p\in\mathbb{N}^*$.

Proposition 12
Si $(G_1,\star_1)$ et $G_2,\star_2$ sont deux groupe finis alors $(G_1\times G_2,\star)$ est un groupe fini et $\mathrm{card}\, G_1\times G_2=\mathrm{card}\, G_1.\mathrm{card}\, G_2$

2 Anneaux

Définition 9 *Soit A un ensemble non vide muni de deux loi internes $+$ et $\times$.*
$(A,+,\times)$ est un anneau si

1. *$(A,+)$ est un groupe abélien*
2. *la loi $\times$ vérifie :*
   a) *$\times$ est associative*
   b) *$\times$ possède un élément neutre*
   c) *la multiplication $\times$ est distributive sur l'addition à droite et à gauche :*
   $\forall (x,y,z)\in A^3,\ x\times(y+z)=x\times y+x\times z$ et $(x+y)\times z=x\times y+x\times z$

- *Si $\times$ est commutative on dit que l'anneau est commutatif.*
- *Si $\times$ est commutative et n'a pas de diviseur de 0, c'est à dire que $\forall (x,y)\in A^2,\ x\times y=0\Rightarrow x=0$ ou $y=0$ on dit que l'anneau est intègre.*

L'élément neutre de $(A,+)$ se note en général 0 ou 0_A et l'élément neutre de la multiplication se note 1 ou 1_A
Comme pour les groupes on définit les sous-anneaux et les morphismes d'anneaux :

Définition 10 *Si $(A,+,\times)$ est un anneau et A' est une partie non-vide de A, A' est un sous-anneau de $(A,+,\times)$ si $(A',+,\times)$ est un anneau et $1_A\in A'$*

Proposition 13 *Si $(A,+,\times)$ est un anneau et A' est une partie non-vide de A*
A' est un sous-anneau de $(A,+,\times)$ si et seulement si

1. *$(A',+)$ est un sous-groupe de $(A,+)$*
2. *$\forall (x,y)\in {A'}^2,\ x\times y\in A'$*
3. *$1_A\in A'$*

Définition 11 *Soit $(A,+,\times)$ et $(A',+,\times)$ deux anneaux,*
on appelle morphisme d'anneaux toute application f de A dans A' telle que :
$\forall (x,y)\in A^2,\ f(x+y)=f(x)+f(y)$, $f(x\times y)=f(x)\times f(y)$ et $f(1_A)=1_{A'}$

On a aussi :

- Un morphisme d'anneau bijectif s'appelle un isomorphisme d'anneau.
- si f est un morphisme d'anneau alors $f(0_A)=0_{A'}$, $f(1_A)=1_{A'}$, $\forall x\in A$, $f(-x)=-f(x)$
- Pour $A'=A$ un morphisme de groupe s'appelle un endomorphisme d'anneau.
- Pour $A'=A$ un isomorphisme de groupe s'appelle un automorphisme d'anneau.

Pour un anneau on définit la notion d'idéal

Définition 12 *Soit $(A,+,\times)$ un anneau commutatif et $J\subset A$, J est un idéal de A si*

- *$(J,+)$ est un sous-groupe de $(A,+)$*
- *$\forall (a,b)\in A\times J,\ a\times b\in J$*

Exemple 4
Pour un anneau comutatif $(A,+,\times))$ et $a\in A$, $\quad aA=\{ax,\ x\in A\}$ est un idéal de A, c'est le plus petit idéal (au sens de l'inclusion) de A contenant a, on dit que c'est l'idéal de A engendré par a, un idéal de la forme aA est appelé un idéal principal.

Remarque 2
Lorsque tous les idéaux d'un anneau commutatif $(A,+,\times)$ sont des idéaux principaux, on dit que $(A,+,\times)$ est un anneau principal.

Remarque 3 *Si J est un idéal d'un anneau $(A,+,\times)$ et $1_A\in J$ alors $J=A$*

Proposition 14 *Dans un anneau commutatif $(A,+,\times)$, une intersection d'idéaux de A est un idéal de A.*

Proposition 15 *Les idéaux de l'anneau $(\mathbb{Z},+,\times)$ sont les parties $n\mathbb{Z}=\{n\times m,\ m\in\mathbb{Z}\}$ de $\mathbb{Z}$ pour $n\in\mathbb{N}$.*

Proposition 16
Soit $(A,+,\times)$ et $(A',+,\times)$ deux anneaux, un morphisme d'anneaux est une application f de A dans A' telle que :

1. $\forall (a,b)\in A^2,\ f(a+b)=f(a)+f(b)$
2. $\forall (a,b)\in A^2,\ f(a\times b)=f(a)\times f(b)$
3. $f(1_A)=1_{A'}$

Proposition 17 *Si f est un morphisme d'un anneau A sur un anneau A' alors*

- *Le noyau de f, $\ker f=f^{-1}(\{0_{A'}\})$ est un idéal de A*
- *L'image de A par f, $\mathrm{Im}f=f(A)$ est un sous-anneau de $(A',+,\times)$*

Proposition 18 *Soit $(A,+,\times)$ et $(A^{'},+,\times)$ deux anneaux et f un morphisme d'anneaux.*

1. *f est injectif si et seulement si $\ker f=\{0_A\}$ où 0_A est l'élément neutre de $(A,+)$.*
2. *f est surjectif si et seulement si $\mathrm{Im}f=A'$.*

Proposition 19 *Soit $(A,+,\times)$ un anneau, l'application : $\varphi :\ \begin{array}{ccc}\mathbb{Z}&\to&A\\ n&\mapsto&n.1_A\end{array}$*
est un homorphisme d'anneau de noyau $n_0\mathbb{Z}$ où $n_0\in\mathbb{N}$

Définition 13 (caractéristique d'un anneau) *Pour un anneau $(A,+,\times)$*
l'unique entier n_0 de la proposition précédente s'appelle la caractéristique de l'anneau A

Proposition 20
Soit $(A,+,\times)$ un anneau et $C=\{n\in\mathbb{N}^*,\ n.1_A=0\}$:

- *Si $C\neq\varnothing$ alors la caractéristique de A est l'entier n_0 tel que $n_0.1_A=0$ et $\forall k\in[\![1,n_0-1]\!],\ k.1_A\neq 0$.*
- *Si $C=\varnothing$ alors A est de caractéristique nulle.*

Notation
Pour un anneau $(A,+,\times)$ on note A^* l'ensemble des éléments inversibles pour la multiplication,
$A^*=\{a\in A,\ \exists a'\in A,\ a\times a'=a'\times a=1_A\}$
Par exemple : $\mathbb{Z}^*=\{-1,1\}$, $\mathbb{K}^*=\mathbb{K}\setminus\{0\}$, $\mathbb{K}[X]^*=\mathbb{K}^*$

Proposition 21 *Si f est un morphisme d'un anneau A dans un anneau A' et $x\in A^*$ alors $f(x^{-1})=f(x)^{-1}$*

Proposition 22 *Pour un anneau $(A,+,\times)$, $(A^*,\times)$ est un groupe.*

Proposition 23 (produit d'anneaux) *Soit $(A,+,\times)$ et $(A',+,\times)$ deux anneaux :*
On définit une structure d'anneau sur $A\times A'$ en définissant l'addition et la multiplication par :
$\forall (a,b)\in A\times A',\ \forall (a',b')\in A\times A',\ (a,b)+(a',b')=(a+a',b+b')$ *et* $(a,b)\times(a',b')=(a\times a',b\times b')$

Divisibilité dans un anneau intègre

Dans ce paragraphe $(A,+,\times)$ désigne un anneau intègre, c'est à dire un anneau commutatif sans diviseur de zéro.

Définition 14 *Soit $(x,y)\in A^2$, on dit que x divise y s'il existe $q\in A$ tel que $y=qx$, on note $x\,|\,y$.*

Proposition 24 *Soit $(x,y)\in A^2$, on a : x divise y si et seulement si $Ay\subset Ax$*

3 Corps

Définition 15 *Soit $\mathbf{K}$ un ensemble muni de deux lois de compositions internes $+$ et $\times$*
$(\mathbf{K},+,\times)$ est un corps si

1. *$(\mathbf{K},+,\times)$ est un anneau*
2. *les éléments de $\mathbf{K}\setminus\{0\}$ possède un inverse pour la multiplication, c'est à dire que $\mathbf{K}^*=\mathbf{K}\setminus\{0\}$*

Si la multiplication $\times$ est commutative on dit que le corps est commutatif

Un corps est un anneau intègre.
On définit la caractéristique d'un corps $(\mathbf{K},+,\times)$ comme étant la caractéristique de l'anneau $(\mathbf{K},+,\times)$.

Exemples :$(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$ sont des corps.

On définit aussi les notions de sous-corps et de morphisme de corps

4 Anneau $\mathbb{Z}$

Proposition 25
Pour tout idéal J de $\mathbb{Z}$, il existe un unique entier naturel n tel que $J = n\mathbb{Z}$.

Proposition 26
Si $(a,b) \in \mathbb{N}^2$ *et* $d \in \mathbb{N}$
Alors *d est le pgcd de a et b, on note $d = a \wedge b$ si et seulement si $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.*

Proposition 27
Si $(a,b) \in \mathbb{N}^2$ *et* $m \in \mathbb{N}$
Alors *m est le ppcm de a et b, on note $m = a \vee b$ si et seulement si $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.*

Théorème 1 (théorème de Bezout)
Soit $(a,b) \in \mathbb{Z}^2$, a et b sont premier entre eux, on note $a \wedge b = 1$ si et seulement si $\exists (u,v) \in \mathbb{Z}^2$, tel que $au + bv = 1$

Théorème 2 (théorème de Gauss)
Soit $(a,b,c) \in \mathbb{Z}^3$, **Si** *a divise bc avec a et b premiers entre eux* **Alors** *a divise c*

5 Anneaux $\mathbb{Z}/n\mathbb{Z}$

5.1 Notions sur les relations binaires

Définition 16
Soit E et F deux ensembles non vides, on appelle relation binaire $\mathcal{R}$ de E dans F, la donnée d'une partie G de $E \times F$ appelée graphe de la relation $\mathcal{R}$.
Pour $(x,y) \in E \times F$ on dit que x est en relation avec y, on note souvent $x\mathcal{R}y$, si $(x,y) \in G$. On dit alors que :

- *y est une image de x*
- *x est un antécédent de y*
- *E est l'ensemble de départ de la relation $\mathcal{R}$*
- *F est l'ensemble d'arrivée de la relation $\mathcal{R}$*
- *Si $E = F$ on dit aussi que $\mathcal{R}$ est une relation binaire sur E.*

Une relation binaire $\mathcal{R}$ de E dans F se définit souvent à l'aide d'une proposition $\mathcal{P}$ sur $E \times F$, on a alors :
$G = \{(x,y) \in E \times F, \text{ tq } \mathcal{P}(x,y) \text{ est vraie}\}$

Exemple 5
$E = F = \mathbb{R}$, $\mathcal{P}(x,y) : x^2 - y^2 = 1$, on a par exemple :

- *$G = \{(x,y) \in \mathbb{R}^2,\ x^2 - y^2 = 1\}$*
- *$\forall x \in]-\infty,-1[\cup]1,+\infty[$, x a deux images : $\sqrt{x^2-1}$ et $-\sqrt{x^2-1}$*
- *$x \in \{-1,+1\}$, x a pour seule image 0*
- *Si $x \in]-1,+1[$, x n'a pas d'image.*
- *$\forall y \in \mathbb{R}$, y a deux antécédents : $\sqrt{1+y^2}$ et $-\sqrt{1+y^2}$*

Définition 17
Soit E et F deux ensembles non vides et f une relation binaire de E dans F de graphe G

1. *Si tout élément de l'ensemble de départ E possède au plus une image dans F on dit que f est une* **fonction** *de E dans F. Pour $(x,y) \in E \times F$ si $(x,y) \in G$, $x\,f\,y$ se note alors $y = f(x)$.*
   On appelle ensemble de définition de f la partie de E définie par $D_f = \{x \in E,\ x \text{ possède une image}\}$, on a alors $G = \{(x, f(x)) \in E \times F,\ x \in D_f\}$.
2. *Si tout élément de l'ensemble de départ E possède exactement une image dans F on dit que f est une* **application** *de E dans F.*

Définition 18
Soit f une **application** *de E dans F :*

1. *Si tout élément de l'ensemble d'arrivée F possède au moins un antécédent on dit que f est une* **surjection**
2. *Si tout élément de l'ensemble d'arrivée F possède au plus un antécédent on dit que f est une* **injection**
3. *Si tout élément de l'ensemble d'arrivée F possède exactement un antécédent on dit que f est une* **bijection**

Proposition 28

Soit f une application de E dans F, pour $y \in F$ on considère l'équation : $(E_y) : \left\{ \begin{array}{l} f(x) = y \\ x \in E \end{array} \right.$,

résoudre E_y revient à déterminer les antécédents de y.

- *Si $\forall y \in F$, E_y possède au moins une solution alors f est surjective*
- *Si $\forall y \in F$, E_y possède au plus une solution alors f est injective*
- *Si $\forall y \in F$, E_y possède exactement une solution alors f est bijective*

5.2 Notions sur les relations d'équivalence

Définition 19 *soit E un ensemble non vide et $\mathcal{R}$ une relation binaire sur E :*

- *$\mathcal{R}$ est une relation réflexive si $\forall x \in E$, $x\mathcal{R}x$ est vraie.*
- *$\mathcal{R}$ est une relation symétrique si $\forall (x, y) \in E^2$, $x\mathcal{R}y \Rightarrow y\mathcal{R}x$*
- *$\mathcal{R}$ est une relation transitive si $\forall (x, y, z) \in E^3$, $x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z$*

Si $\mathcal{R}$ est réflexive, symétrique et transitive on dit que $\mathcal{R}$ est une relation d'équivalence.

Définition 20

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E et $x \in E$, on appelle classe d'équivalence de x la partie de E définie par : $\mathcal{O}(x) = \{y \in E,\ x\mathcal{R}y\}$

Définition 21

Soit E un ensemble non vide et $(E_i)_{i\in I}$ une famille de parties de E, on dit que $(E_i)_{i\in I}$ est une partition de E si :

- $\forall i \in I$, $E_i \neq \varnothing$
- $\forall (i, j) \in I^2$, $i \neq j$, $\quad E_i \cap E_j = \varnothing$
- $\bigcup_{i\in I} E_i = E$

Proposition 29

Soit E un ensemble non vide et $\mathcal{R}$ une relation d'équivalence sur E, la famille des classes d'équivalence distinctes 2 à 2 forme une partition de E.

Remarque 4 *Soit E un ensemble non vide*

- *L'égalité sur E est une relation d'équivalence. Les classes d'équivalence ne contiennent qu'un seul élément.*
- *La relation binaire $\mathcal{R}$ sur E définie par : $x\mathcal{R}y \Leftrightarrow (x, y) \in E^2$ c'est à dire $G = E \times E$ est une relation d'équivalence sur E qui ne possède qu'une classe d'équivalence, on l'appelle la relation grossière sur E.*
- *Toute partition $(O_i)_{i\in I}$ de E définit une relation d'équivalence sur E par $x\mathcal{R}y \Leftrightarrow \exists i \in I$, $(x, y) \in O_i^2$. Les O_i, $i \in I$ sont alors les classes d'équivalence de la relation $\mathcal{R}$.*

5.3 $\mathbb{Z}/n\mathbb{Z}$

5.3.1 Congruence modulo n

Soit $n \in \mathbb{N}$

Définition 22

On considère dans $\mathbb{Z}$ la relation binaire : $x\mathcal{R}y$ si et seulement si $x - y \in n\mathbb{Z}$.
Pour $(x, y) \in \mathbb{Z}^2$, $x\mathcal{R}y$ se note $x \equiv y \,[\mathrm{mod}\, n]$ ou $x \equiv y \,[n]$ et on dit : x est congru à y modulo n

Proposition 30

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

Remarque 5

- *Pour $n = 0$ la relation de congruence modulo n est équivalente à la relation d'égalité sur $\mathbb{Z}$:* $x \equiv y \,[\mathrm{mod}\, 0] \Leftrightarrow x = y$
- *Pour $n = 1$ la relation de congruence modulo n est équivalente à la relation grossière sur $\mathbb{Z}$,* $\forall (x, y) \in \mathbb{Z}^2$ *on a* $x \equiv y \,[\mathrm{mod}\, 1]$

Dans la suite on prendra $n \geqslant 2$

Proposition 31
Pour $n \in \mathbb{N}$, $n \geqslant 2$:
- $\forall (x,y) \in \mathbb{Z}^2$, $x \equiv y \,[\mathrm{mod}\, n]$ *si et seulement si x et y ont le même reste dans la division euclidienne par n*
- *La relation de congruence modulo n est une relation d'équivalence qui possède n classes d'équivalence, elles forment une partition de $\mathbb{Z}$.*
- *Si pour $x \in \mathbb{Z}$ on note $\bar{x}$ la classe de x modulo n, on a : $\bar{x} = \{x + kn,\, k \in \mathbb{Z}\}$, on note aussi $\bar{x} = x + n\mathbb{Z}$*
- *On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence modulo n et on a :*

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$$

5.3.2 Stucture de Groupe

Proposition 32
Si $(x,y,x',y') \in \mathbb{Z}^4$, $x \equiv x' \,[\mathrm{mod}\, n]$ *et* $y \equiv y' \,[\mathrm{mod}\, n]$
Alors $\overline{x+y} \equiv \overline{x'+y'} \,[\mathrm{mod}\, n]$

On définit alors l'addition dans $\mathbb{Z}/n\mathbb{Z}$ par $\bar{x} + \bar{y} = \overline{x+y}$

Théorème 3
$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique de cardinal n.

Proposition 33
Soit $z \in \mathbb{Z}$, $\bar{z}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $z \wedge n = 1$
On a alors $\mathbb{Z}/n\mathbb{Z} = \{k\bar{z},\, k \in [\![0, n-1]\!]\}$

Théorème 4
- *Si $(G,*)$ est un groupe monogène avec $G =< a >$,*
  $$\begin{array}{ccccc} (\mathbb{Z},+) & \to & (G,*) \\ k & \mapsto & a^k \end{array}$$
  l'application est un isomorphisme de groupe.
- *Si $(G,*)$ est un groupe cyclique d'ordre n avec $G =< a >$,*
  $$\begin{array}{ccccc} (\mathbb{Z},+) & \to & (G,*) \\ k & \mapsto & a^k \end{array}$$
  - *est un morphisme de groupe de noyau $n\mathbb{Z}$*
  $$\begin{array}{ccccc} (\mathbb{Z}/n\mathbb{Z},+) & \to & (G,*) \\ \bar{k} & \mapsto & a^k \end{array}$$
  - *est un isomorphisme de groupe.*

5.3.3 Stucture d'anneau

Proposition 34
Si $(x,y,x',y') \in \mathbb{Z}^4$, $x \equiv x' \,[\mathrm{mod}\, n]$ *et* $y \equiv y' \,[\mathrm{mod}\, n]$
Alors $\overline{x \times y} \equiv \overline{x' \times y'} \,[\mathrm{mod}\, n]$

On définit alors la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ par $\bar{x} \times \bar{y} = \overline{x \times y}$

Théorème 5
$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif de caractéristique n.

Proposition 35
Si *$(A, +, \times)$ un anneau de caractéristique n avec $n \in \mathbb{N}$*
Alors
$$\begin{array}{ccccc} \mathbb{Z} & \to & A \\ n & \mapsto & n.1_A \end{array}$$
- *est un morphisme d'anneau, le noyau est* $\ker\varphi = n\mathbb{Z}$ *et l'image $\varphi(\mathbb{Z})$ est un sous-anneau commutatif de $(A, +, \times)$.*
- *Si $n = 0$ alors φ est injective, $\mathbb{Z}$ et $\varphi(\mathbb{Z})$ sont deux anneaux isomorphes.*
  $$\begin{array}{ccccc} \mathbb{Z}/n\mathbb{Z} & \to & A \\ \bar{x} & \mapsto & y.1_A \end{array}$$
  où $y \in \bar{x}$ est un morphisme d'anneaux et $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\bar{\varphi}(\mathbb{Z}/n\mathbb{Z}) = \varphi(\mathbb{Z})$

Proposition 36
Soit $(A, +, \times)$ un anneau de caractéristique $n \in \mathbb{N}$

- *Si $n = 0$ alors A contient un sous-anneau isomorphe à $\mathbb{Z}$*
- *Si $n \geqslant 1$ alors A contient un sous-anneau isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Théorème 6
Pour $n \geqslant 2$ on a équivalence entre les trois propositions suivantes :
- $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ *est un corps*
- $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ *est un anneau intègre*
- n *est un nombre premier.*

Exercice 2 *Soit $(A, +, \times)$ un anneau fini et intègre. Montrer que $(A, +, \times)$ est un corps.*

Théorème 7
Soit $n \geqslant 2$ et $m \in \mathbb{Z}$, on a : $\bar{m} \in (\mathbb{Z}/n\mathbb{Z})^*$ si et seulement si $n \wedge m = 1$.

Théorème 8
Si $(\mathbf{K}, +, \times)$ *est un corps de caractéristique n ($\mathbf{K} \neq \{0\}$ soit $n = 0$ ou $n \geqslant 2$)*
Alors

- *Si $n \neq 0$ alors n est un nombre premier et* $\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mathbf{K} \\ \bar{x} & \mapsto & y.1_{\mathbf{K}} \text{ où } y \in \bar{x} \end{array}$ *est un morphisme de corps injectif.*
- *Si $n = 0$ alors* $\begin{array}{ccc} \mathbb{Q} & \to & \mathbf{K} \\ \frac{p}{q} & \mapsto & (p.1_{\mathbf{K}})(q.1_{\mathbf{K}})^{-1} = (q.1_{\mathbf{K}})^{-1}(p.1_{\mathbf{K}}) \end{array}$ *est un morphisme de corps injectif.*

5.4 Indicatrice d'Euler

Définition 23
On appelle indicatrice d'Euler l'application : $\varphi : \begin{array}{ccc} \mathbb{N}^* & \to & \mathbb{N}^* \\ n & \mapsto & \varphi(n) = \left\{ \begin{array}{l} \varphi(1) = 1 \\ \text{pour } n \geqslant 2,\ \varphi(n) = \operatorname{card}(\mathbb{Z}/n\mathbb{Z})^* \end{array} \right. \end{array}$

Théorème 9
- *Soit $(m, n) \in \mathbb{N}^2$,* **Si** $m \wedge n = 1$ **Alors** *l'anneau $\mathbb{Z}/mn\mathbb{Z}$ est isomorphe à l'anneau $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$*
- $\begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \bar{x}^{mn} & \mapsto & (\bar{x}^m, \bar{x}^n) \end{array}$ *est un isomorphisme d'anneaux.*

Propriétés

Propriété 1
Si $(a, b) \in {\mathbb{N}^*}^2$, $a \wedge b = 1$ **Alors** $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

Propriété 2
Si $p \in \mathbb{N}$ *est premier et* $\alpha \in \mathbb{N}^*$ **Alors** $\varphi(p) = p - 1$ *et* $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$

Propriété 3
Si $n \in \mathbb{N}$, $n \geqslant 2$, $\quad n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ *(décomposition en produit de facteurs premiers)* **Alors** $\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$.

Propriété 4
Si $n \in \mathbb{N}$, $n \geqslant 2$ **Alors** $n = \sum_{d \mid n} \varphi(d)$

6 Anneau de polynômes $\mathbf{K}[X]$

Soit $(\mathbf{K}, +, \times)$ un corps

Proposition 37
$(\mathbf{K}[X], +, \times)$ *est un anneau dont les éléments inversibles sont les éléments non-nul de* $\mathbf{K}$, $\mathbf{K}[X]^* = \mathbf{K}^*$

Définition 24
Deux polynômes P *et* Q *de* $\mathbf{K}[X]$ *sont dits associés s'il existe* $k \in \mathbf{K}^*$ *tel que* $Q = kP$

Théorème 10 (division euclidienne)
Si $(A, B) \in \mathbf{K}[X]^2$, $B \neq 0$
Alors *il existe un unique couple* $(Q, R) \in \mathbf{K}[X]^2$ *tel que* $A = BQ + R$ *tel que* $R = 0$ *ou* $\mathrm{d}^\circ R < \mathrm{d}^\circ B$

Théorème 11 (idéaux de $\mathbf{K}[X]$)
- *Les idéaux de* $\mathbf{K}[X]$ *sont les idéaux principaux.*
- **Si** $\mathcal{I}$ *est un idéal de* $\mathbf{K}[X]$ *non réduit à* $\{0\}$ **Alors** *il existe un unique polynôme unitaire* P *tel que* $\mathcal{I} = P\mathbf{K}[X]$

Théorème 12 (PGCD) *Soit* A *et* B *deux polynômes de* $\mathbf{K}[X]$ *non-nuls.*
Il existe un unique polynôme unitaire D *tel que* $A\mathbf{K}[X] + B\mathbf{K}[X] = D\mathbf{K}[X]$,
D *est appelée le* $PGCD$ *de* A *et* B, *on note* $D = A \wedge B$ *ou* $D = PGCD(A, B)$ *et si* D_1 *est un polynôme associé à* D *on dit que* D_1 *est un* $PGCD$ *de* A *et* B.

Théorème 13 (PPCM) *Soit* A *et* B *deux polynômes de* $\mathbf{K}[X]$ *non-nuls.*
Il existe un unique polynôme unitaire P_m *tel que* $A\mathbf{K}[X] \cap B\mathbf{K}[X] = P_m\mathbf{K}[X]$,
P_m *est appelée le* $PPCM$ *de* A *et* B, *on note* $P_m = A \vee B$ *ou* $P_m = PPCM(A, B)$ *et si* P_1 *est un polynôme associé à* P_m *on dit que* P_1 *est un* $PPCM$ *de* A *et* B

Proposition 38
Soit $(A, B) \in \mathbf{K}[X]^2$ *deux polynômes non-nuls,*
- *Les diviseurs communs à* A *et* B *sont les diviseurs de* $A \wedge B$.
- *Les multiples communs à* A *et* B *sont les multiples de* $A \vee B$.

Définition 25 *Soit* $(A, B) \in \mathbf{K}[X]^2$ *deux polynômes non-nuls,*
On dit que A *et* B *ont premiers entre eux si* $A \wedge B = 1$

Proposition 39
Soit $(A, B) \in \mathbf{K}[X]^2$ *deux polynômes non-nuls,*
A *et* B *sont premiers entre eux si et seulement si les seuls diviseurs communs à* A *et* B *sont les polynômes inversibles c'est à dire les éléments de* $\mathbf{K}^*$

Théorème 14 (théorème de Bezout) *Soit* $(A, B) \in \mathbf{K}[X]^2$,
A *et* B *sont premiers entre eux, on note* $A \wedge B = 1$ *si et seulement si* $\exists (U, V) \in \mathbf{K}[X]^2$, *tel que* $AU + BV = 1$

Théorème 15 (théorème de Gauss)
Soit $(A, B, C) \in \mathbf{K}[X]^3$, **Si** A *divise* BC *avec* A *et* B *premiers entre eux* **Alors** A *divise* C