Table des matières

Chapitre I : Groupes, anneaux : Rappels et compléments

I. Groupes

On donnera des rappels sur les groupes et quelques compléments, notamment les groupes finis, groupes monogènes (les groupes cycliques en particulier).

I.1. Définitions, exemples

On suppose connues les notions de lois de composition interne et leurs propriétés vues en première année.

I.1.1. Définitions

Définition 1

Un groupe est un couple $(G, \star)$ tel que G est un ensemble non vide et $\star$ une loi de composition interne sur G tel que :

1. $\star$ est associative.
2. admet un élément neutre (celui-ci est alors unique noté e).
3. Tout élément de G est symétrisable (Il y'a alors unicité du symétrique d'un élément x de G, on le note x').

Formellement, $(G, \star)$ est un groupe si :

1. $\forall (a, b, c) \in G^3, \quad (a \star b) \star c = a \star (b \star c)$.
2. $\exists e \in G, \forall x \in G, \quad x \star e = e \star x = x$.

3. $\forall x \in G, \exists x' \in G, \quad x \star x' = x' \star x = e.$

Remarques On retient les remarques suivantes :

1. Si de plus $\star$ est commutative, on dit que $(G, \star)$ est un groupe commutatif ou abelien.
2. On adopte en général une notation multiplicative ou additive et le tableau ci-dessous résume les diverses notations associées :

Générale	Additive	Multiplicative
$(G, \star)$	$(G, +)$	$(G, \times)$ ou $(G, .)$
$x \star y$	$x + y$	$x \times y$ ou $x.y$ ou xy
e	0	1 ou e
symétrique	opposé	inverse
x'	$-x$	x^{-1}
$x \star y'$	$x - y$	xy^{-1}
$\underbrace{x \star \cdots \star x}_{n \text{ fois}}$, $n \in \mathbb{N}^*$	nx	x^n
$\underbrace{x' \star \cdots \star x'}_{n \text{ fois}}$, $n \in \mathbb{N}^*$	$-nx$	x^{-n}

3. Quand la lois du groupe est connue, on confond par abus le groupe $(G, \star)$ et l'ensemble G. On dit par exemple : le groupe G.
4. Dans un groupe, tout élément est régulier à droite et à gauche.
5. Si $(G, \star)$ est un groupe et $x, y \in G$, alors le symétrique de $x \star y$ est : $(x \star y)' = y' \star x'$. En notation multiplicative (resp.additive), cela donne : $(xy)^{-1} = y^{-1}x^{-1}$ (resp. $-(x + y) = (-y) + (-x) = -y - x$).

I.1.2. Exemples

Voici des exemples de groupes : Ce sont les groupe les plus utilisés et les plus connus. On peut trouver d'autres exemples intéressants.

1. $(\mathbb{C}, +), (\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{Z}, +)$ sont des groupes commutatifs.
2. $(\mathbb{C}^*, \times), (\mathbb{R}^*, \times), (\mathbb{Q}^*, \times)$ Sont aussi des groupes commutatifs.
3. Si E est un ensemble non vide, on note $\mathscr{S}_E$ l'ensemble des bijections de E vers E. Muni de la composition des applications, $\mathscr{S}_E$ est un groupe non commutatif en général appelé groupe des permutations de E. Si $E = [\![1, n]\!]$ avec $n \in \mathbb{N}^*$, on adopte la notation $\mathscr{S}_n$ et on l'appelle groupe symétrique.
4. $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$. Soit $n \in \mathbb{N}^*$, on dispose de $GL_n(\mathbb{K})$ l'ensemble des matrices carrées de taille n inversibles à coefficients dans $\mathbb{K}$. Muni de la multiplication usuelle des matrices carrées, c'est un groupe non commutatif (sauf si $n = 1$), appelé groupe linéaire.

I.2. Sous-groupes

I.2.1. Définitions

a) Lois induite :
Soit $(G, \star)$ un groupe et H une partie non vide de G tel que :

$$\forall (x, y) \in G^2 \quad (x, y) \in H^2 \Rightarrow x \star y \in H$$

On dit que H est stable et on remarque qu'on dispose d'une loi de composition interne $*$ sur H tel que :

$$\forall (x, y) \in H^2 \quad x * y = x \star y$$

Dans la pratique, on adopte la même notation pour les deux lois.
b) Sous-groupe :

Définition 2

Soit $(G, \star)$ un groupe. On appelle sous-groupe de $(G, \star)$ toute partie H non vide stable tel que $(H, \star)$ est un groupe.

Proposition 1

Si H est un sous-groupe de $(G, \star)$ alors :
- Si e_G et e_H sont les éléments neutres respectifs de G et H alors : $e_G = e_H$.
- Si $x \in H$ et x', x'' les symétriques respectifs de x dans G et H alors $x' = x''$.

Preuve:

On a $e_G \star e_H = e_H$ et $e_H \star e_H = e_H$ et e_H est régulier dans G donc $e_G = e_H$.
Notons alors e l'élément neutre commun de G et H et soit $x \in H$ alors : comme $x \in G$, on a : (1) $x \star x' = e$, et comme $x \in H$, on a : (2) $x \star x'' = e$. De (1) et (2) et la régularité de x dans G on déduit : $x \star x' = x \star x''$ puis $x' = x''$.

Proposition 2

Soit $(G, \star)$ un groupe et H une partie de G, alors :

1. H est un sous-groupe de $(G, \star)$ si et seulement si : $\begin{cases} H \neq \emptyset \\ \forall (x, y) \in H^2, \quad x \star y \in H \\ \forall x \in H, \quad x' \in H \end{cases}$
2. H est un sous-groupe de $(G, \star)$ si et seulement si : $\begin{cases} H \neq \emptyset \\ \forall (x, y) \in H^2, \quad x \star y' \in H \end{cases}$

I.2.2. Exemples

1. On considère le groupe linéaire $GL_2(\mathbb{R})$ et on note :
$$O_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos\theta & -\varepsilon\sin\theta \\ \sin\theta & \varepsilon\cos\theta \end{pmatrix} / \theta \in \mathbb{R} \quad \text{et} \quad \varepsilon = \pm 1 \right\}$$
Alors, $O_2(\mathbb{R})$ est un sous-groupe de $GL_2(\mathbb{R})$. En effet, en prenant $\theta = 0$ et $\varepsilon = 1$, on obtient $I_2 \in O_2(\mathbb{R})$. Pour tout $(\theta, \varepsilon) \in \mathbb{R} \times \{-1, 1\}$, notons :
$$M_{\theta,\varepsilon} = \begin{pmatrix} \cos\theta & -\varepsilon\sin\theta \\ \sin\theta & \varepsilon\cos\theta \end{pmatrix}$$
Alors pour tout $\theta, \theta' \in \mathbb{R}$ et $\varepsilon, \varepsilon' \in \{-1, 1\}$, on a :
$$M_{\theta,\varepsilon} \times M_{\theta',\varepsilon'} = M_{\theta+\varepsilon\theta',\varepsilon\varepsilon'}$$
2. Pour tout groupe $(G, \star)$, $\{e\}$ et G sont des sous-groupes de $(G, \star)$.
3. $\mathbb{Z}$ est un sous-groupe du groupe additif $\mathbb{R}$.
4. $\{-1, 1\}$ est un sous-groupe du groupe multiplicatif $\mathbb{Q}^*$.
5. Soit $G = \bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$, alors G est un sous-groupe de $(\mathbb{C}^*, \times)$
6. Exercice : Montrer que les seuls sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$:
Rep : Soit $n \in \mathbb{N}$, il est aisé de prouver que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Réciproquement, si H est un sous-groupe de $\mathbb{Z}$ deux cas sont possibles :
- Soit $H \cap \mathbb{N}^* = \emptyset$, dans ce cas on a $H \cap \mathbb{Z}^* = \emptyset$ car si $k \in \mathbb{Z}$, on a $k \in H \Rightarrow |k| \in H$. Donc $H = \{0\} = 0\mathbb{Z}$.
- Soit $H \cap \mathbb{N}^* \neq \emptyset$, soit alors $n = \min(H \cap \mathbb{N}^*)$ alors $n \in H$ donc $n\mathbb{Z} \subset H$. Soit $x \in H$ et $x = qn + r$ la division euclidienne de x par n alors $r = x - nq \in H \cap \mathbb{N}$ donc $r = 0$ car sinon on aurait $r \geq n$, donc $H = n\mathbb{Z}$.

I.3. Groupe engendré par une partie

I.3.1. Intersection de sous-groupes

Proposition 3

Soit G un groupe. Si $(H_i)_{i\in I}$ est une famille de sous-groupes alors $H = \bigcap_{i\in I} H_i$ est un sous groupe de G.

I.3.2. Définition, exemples

Par convention, quand on dit : soit G un groupe, on sous-entends une notation multiplicative pour sa loi, on adoptera la notation $\prod_{k=1}^{m} x_k$ pour le composé $x_1 \times \cdots \times x_m$, pour tout $m \in \mathbb{N}^*$ et $x_1, \cdots, x_m \in G$. Si A est une partie non vide de G alors on définit : $A^{-1} = \{x^{-1}/x \in A\}$

Proposition 4

Soit G un groupe et A une partie de G. On note

$$\mathscr{G}_A = \{H/A \subset H \quad \text{et} \quad H \text{ sous-groupe de } G\}$$

et soit $\langle A\rangle$ le sous-groupe :

$$\langle A\rangle = \bigcap_{H\in\mathscr{G}_A} H$$

Alors $\langle A\rangle$ est le plus petit sous-groupe de G contenant A. Il est appelé le sous-groupe de G engendré par A. On a : Si $A = \emptyset$ alors $\langle A\rangle = \{e\}$ et si $A \neq \emptyset$ alors :

$$\langle A\rangle = \left\{\prod_{k=1}^{m} x_k / m \in \mathbb{N}^*, x_k \in A \cup A^{-1}, \forall k \in [\![1, m]\!]\right\}$$

Preuve:

Posons $K = \bigcap_{H\in\mathscr{G}_A} H$. D'après le proposition 3, $\langle A\rangle$ est un sous-groupe de G. Comme $\langle A\rangle$ est une intersection de groupes contenant A, on a $A \subset \langle A\rangle$. Ainsi on a $\langle A\rangle \in \mathscr{G}_A$ et $\langle A\rangle \subset H$ pour tout $H \in \mathscr{G}_A$. Donc $\langle A\rangle$ est le plus petit sous-groupe de G contenant A.

• Posons

$$K = \left\{\prod_{k=1}^{m} x_k / m \in \mathbb{N}^*, x_k \in A \cup A^{-1}, \forall k \in [\![1, m]\!]\right\}$$

et prouvons que $K = \langle A\rangle$. Soit $m \in \mathbb{N}^*$, et $x_1, \cdots, x_m \in A \cup A^{-1}$, alors $x_1, \cdots, x_m \in \langle A\rangle$, donc le produit $x = \prod_{k=1}^{m} x_k$ réalise $x \in \langle A\rangle$, Ainsi $K \subset \langle A\rangle$. Pour démontrer que $\langle A\rangle \subset K$, il suffit de prouver que K est un sous-groupe de G contenant A. Il est clair que $A \subset K$. Comme $A \subset K$ et $A \neq \emptyset$, on a $K \neq \emptyset$. Soit $x, y \in K$, alors $x = \prod_{k=1}^{n} a_k$ et $y = \prod_{j=1}^{n} b_j$ avec $a_k, b_j \in A \cup A^{-1}$ pour tout $k \in [\![1, m]\!]$ et tout $j \in [\![1, n]\!]$. On a :

$$xy = \prod_{i=1}^{n+m} c_i$$

avec pour tout $i \in [\![1, m+n]\!]$: $c_i = \begin{cases} a_i & \text{si} \quad i \in [\![1, m]\!] \\ b_{i-m} & \text{si} \quad i \in [\![m+1, m+n]\!] \end{cases}$, donc $c_i \in A \cup A^{-1}$, pour tout $i \in [\![1, n+m]\!]$. Par ailleurs, $x^{-1} = \prod_{k=0}^{m-1} (a_{m-k})^{-1}$ avec $a_{m-k}^{-1} \in A \cup A^{-1}$ car $a_{m-k} \in A \cup A^{-1}$, donc $x^{-1} \in K$. Ainsi K est un sous-groupe de G, ce qui termine la démonstration.

Remarques Dans le cas où$A \neq \emptyset$,on peut faire les remarques suivantes :

1. En notation additive on note
$$(-A) = \{-a/a \in A\}$$
et on a alors :
$$\langle A\rangle = \left\{ \sum_{k=1}^{m} x_k / m \in \mathbb{N}^*, x_k \in A \cup (-A), \forall k = 1, ..., m \right\}$$
2. Si la condition suivante est réalisée :
$$(1) \quad \forall a, b \in A \quad ab = ba$$
alors $\langle A\rangle = \left\{ \prod_{j=1}^{m} a_j^{k_j} / m \in \mathbb{N}^*, a_j \in A,\ 2\,\text{à}\,2\,\text{distincts}\,, k_j \in \mathbb{Z} \right\}$.
3. Si $G = \langle A\rangle$, on dit que G est le groupe engendré par A et que A est une partie génératrice de G. On a toujours : $G = \langle G\rangle$, mais il est plus intéressant de trouver des parties génératrices A de G minimales au sens de l'inclusion.

I.3.3. Exemples

On donne les exemples importants suivants :

1. Le groupe symétrique $\mathscr{S}_n$ est engendré :
   (a) Par les transpositions.
   (b) Par les transpositions de la forme $\tau_{i,i+1}, i \in [\![1, n-1]\!]$.
   (c) Par les transpositions de la forme $\tau_{1,i}, i \in [\![2, n]\!]$.
   (d) par la paire $\{\tau, s\}$ où $\tau = \tau_{1,2}$ et $s = (12\cdots n)$ (cycle).

Preuve:

La preuve des points 2,3 et 4 est basée sur la propriété importante suivante : Pour tout $i, j \in [\![1, n]\!]$ tel que $i \neq j$, si $\sigma \in \mathscr{S}_n$ alors $\sigma\tau_{i,j}\sigma^{-1} = \tau_{\sigma(i),\sigma(j)}$

2. Le groupe orthogonal $O_2(\mathbb{R})$ est engendré par les matrices de symétries orthogonales, à savoir les matrices de la forme :
$$S_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}, \quad \text{avec} \quad \theta \in \mathbb{R}.$$
3. $GL_n(\mathbb{K})$ est engendré par les matrices de transvections et de dilatations. On rappelle qu'une matrice de transvection est une matrice de la forme $T_{i,j}(\alpha) = I_n + \alpha E_{ij}$ avec $(i, j) \in [\![1, n]\!]^2$ tel que $i \neq j$ et $\alpha \in \mathbb{K}$ et une matrice de dilatation est une matrice de la forme $D_i(\alpha) = I_n + (\alpha - 1)E_{ii}$ avec $i \in [\![1, n]\!]$ et $\alpha \in \mathbb{K}^*$.

I.3.4. Cas particulier : Groupes monogène, groupe cyclique

Définition 3

Un groupe G engendré par un singleton $\{a\}$ s'appelle groupe monogène, et on note $G = \langle a \rangle$. Un groupe monogène fini est dit cyclique.

Exemples On retient les exemples suivants de groupes monogènes :

1. Le groupe additif $\mathbb{Z}$ est un groupe monogène non cyclique engendré par 1.
2. Pour tout $n \in \mathbb{N}^*$, le groupe additif $\mathbb{Z}/n\mathbb{Z}$) est un groupe cyclique dont $\overline{1}$ est un générateur.
3. Le groupe multiplicatif $\mathbb{U}_n$ des racines n èmes de l'unité est un groupe cyclique de cardinal n engendré par $e^{i\frac{2\pi}{n}}$

I.4. Morphismes de groupes

I.4.1. Definitions, propriétés

Définition 4

Soient $(G, \perp)$ et $(G', \top)$ deux groupes. On appelle morphisme de $(G, \perp)$ vers $(G', \top)$, toute application f de G vers G' tel que :

$$\forall (x, y) \in G^2, f(x \perp y) = f(x) \top f(y).$$

Exemples Voici quelques exemples :

1. L'application $f : \mathbb{Z} \to \mathbb{R}^*$ tel que $f(k) = 2^k$ est un morphisme de $(\mathbb{Z}, +)$ vers $(\mathbb{R}^*, \times)$.
2. L'application : $\ln : \mathbb{R}_+^* \to \mathbb{R}, x \mapsto \ln(x)$ est un morphisme de $(\mathbb{R}_+^*, \times)$ vers $(\mathbb{R}, +)$
3. L'application : det est un morphisme de $GL_n(\mathbb{K})$ vers $\mathbb{K}^*$.
4. La signature $\varepsilon : \mathscr{S}_n \to \{-1, 1\}, \sigma \mapsto \varepsilon(\sigma)$ est un morphisme de groupes.

Proposition 5

Si $f : G \to G'$ est un morphisme de groupe et e et e' les éléments neutres respectifs de G et G' et pour $(x, y) \in G \times G'$, x' et y' les symétriques de x et y respectivement alors : $f(e) = e'$ et $\forall x \in G, f(x') = (f(x))'$

Preuve:

On ne nuit pas à la généralité si on choisit une notation multiplicative pour chacune des deux lois.

• Comme $e^2 = e$, on a $(f(e))^2 = f(e)$. Or $f(e)e' = f(e)$, donc $f(e).f(e) = f(e).e'$ et par régularité de $f(e)$, on a $f(e) = e'$.

• Soit $x \in E$ et x' son symétrique. Comme $xx' = x'x = e$, on a $f(xx') = f(x'x) = f(e)$. Compte tenu de $f(e) = e'$, il vient : $f(x)f(x') = f(x')f(x) = e'$, donc $f(x')$ est le symétrique

- dans G' de $f(x)$, donc $(f(x))' = f(x')$

Proposition 6

Soit $f : G \to G'$ un morphisme de groupes. Si f est bijective en tant qu'application de G vers G' alors f^{-1} est un morphisme de groupe de G' vers G

Définition 5

On dit alors que f est un isomorphisme de groupes et que f^{-1} est le morphisme réciproque de f. On dit que les groupes G et G' sont isomorphes.

Remarque Deux groupes isomorphes ont les mêmes propriétés relevant de la structure de groupe.

Exemple Il y'a aux moins deux groupes de cardinal 4, non isomorphes à savoir $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^2$. En effet, pour tout $x \in (\mathbb{Z}/2\mathbb{Z})^2$, on a $2x = (\overline{0}, \overline{0})$, ce qui n'est pas le cas dans $\mathbb{Z}/4\mathbb{Z}$ puisque par exemple : $2.\overline{3} = \overline{2} \neq \overline{0}$.
On peut, en fait prouver qu'à isomorphisme près, il y a exactement deux groupes de cardinal 4, à savoir $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^2$.

I.4.2. Image , image réciproque , noyau , image

Proposition 7

Soit $f : G \to G'$ un morphisme de groupes. Si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de G'. Si H' est un sous-groupe de G' alors $f^{-1}(H')$ est un sous-groupe de G.

Proposition 8

Soit $f : G \to G'$ un morphisme de groupes. Alors $\ker(f) = f^{-1}(\{e'_G\})$ est un sous-groupe de G appelé noyau de f et $\mathrm{Im}(f) = f(G)$ est un sous-groupe de G' appelé image de f. On a les équivalences :

1. f est injectif si et seulement si $\ker(f) = \{e_G\}$.
2. f est surjectif si et seulement si $\mathrm{Im}(f) = G'$

Exemples Les exemples importants ci-dessous sont à retenir :

1. $\det : GL_n(\mathbb{K}) \to \mathbb{K}^*$ est un morphisme surjectif et non injectif, son noyau est l'ensemble des matrices inversibles de determinant 1, appelé groupe linéaire spécial et noté $SL_n(\mathbb{K})$.
2. La signature $\varepsilon : \mathscr{S}_n \to \mathbb{R}^*$ est un morphisme de groupe qui n'est ni surjectif ni injectif. On a $\ker(\varepsilon) = \mathscr{A}_n$ appelé groupe symétrique alterné.

3. Soit $(G,\star)$ un groupe quelconque. Pour tout $x \in G$, on note t_x et τ_x les applications de G vers G définies par :
$$\forall g \in G, \quad \begin{cases} t_x(g) = g \star x \\ \tau_x(g) = x \star g \end{cases}$$
Les applications t_x et τ_x sont bijectives de G vers G, pour tout $x \in G$, ce qui permet de définir les applications :
$$t : G \to \mathscr{S}(G); x \mapsto t_x$$
et
$$\tau : G \to \mathscr{S}(G); x \mapsto \tau_x$$
Alors τ est un morphisme de groupe de $(G,\star)$ vers $(\mathscr{S}(G),\circ)$. Cependant, ce n'est pas le cas pour t. Toutefois, on peut dire que t est un morphisme de $(G,\perp)$ vers $(\mathscr{S}(G),\circ)$ où l'on a définit $\perp$ par :
$$\forall (x,y) \in G^2, \quad x \perp y = y \star x.$$
Notons que les applications τ et t sont injectives, ce qui permet de dire que tout groupe G est isomorphe à un sous-groupe du groupe symétrique $\mathscr{S}(G)$ des bijections de G vers G. Plus précisément, on a :
$$(G,\star) \simeq (\tau(G),\circ).$$

I.5. Produit fini de groupes

Soient $(G_i,\top_i)$ où $i \in [\![1,m]\!], m \in \mathbb{N}, m \geq 2$ une famille de groupe et $G = \prod_{i=1}^{m} G_i$ muni de la loi $\top$ tel que pour tout $x = (x_i), y = (y_i) \in G$, on aie : $x \top y = (x_i \top_i y_i)$.

Proposition 9

$(G,\top)$ est un groupe. De plus si les G_i sont commutatifs G est commutatif. Si pour tout $i \in [\![1,m]\!]$, l'élément neutre de G_i est e_i alors $e = (e_i)_{1\leq i\leq m}$ est l'élément neutre de G.Si $x = (x_i) \in G$ alors le symétrique de x est $x' = (x_i')$ où x_i' est le symétrique de x_i dans G_i, pour tout $i \in [\![1,m]\!]$.

Remarque Un cas usuel est quand les G_i sont égaux et ont même loi : $G_1 = \cdots = G_m = H$ alors $G = H^m$. Comme exemples : $\mathbb{Z}^m, \mathbb{R}^m, \mathbb{Q}^m, \mathbb{C}^m, (\mathbb{Z}/n\mathbb{Z})^m$.

I.6. Element d'ordre fini d'un groupe

Dans tout ce qui suit G est un groupe dont la notation pour la loi est multiplicative et l'élément neutre est e.

I.6.1. Définitions

Définition 6

Soit $x \in G$. On dit que x est d'ordre fini s'il existe $d \in \mathbb{N}^*$ tel que $x^d = e$. Si c'est le cas, le plus petit $d \in \mathbb{N}^*$ tel que $x^d = e$ s'appelle l'ordre de x.

Remarques 1) Avec une notation additive x est d'ordre fini s'il existe $d \in \mathbb{N}^*$ tel que $dx = 0$.
2) l'élément neutre de G est d'ordre 1.

Exemples

1. Dans $\mathbb{Z}/n\mathbb{Z}$ tout élément est d'ordre fini puisque $\forall x \in \mathbb{Z}/n\mathbb{Z}, nx = \overline{0}$.
2. Aucun élément non nul de $\mathbb{Z}$ n'est d'ordre fini.
3. Dans $\mathbb{C}^*$, pour tout n$\in \mathbb{N}^*$, le nombre complexe $\omega_n = e^{i\frac{2\pi}{n}}$ est d'ordre n
4. Soit $G = \bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$. On peut démontrer que G est un sous-groupe de $\mathbb{C}^*$. On a G est infini mais tout élément est d'ordre fini.

I.6.2. Propriétés

Proposition 10

Soit $x \in G$ et $d \in \mathbb{N}^*$. Alors :

$$x \text{ est d'ordre } d \text{ si et seulement si } \begin{cases} x^d = e \\ \forall k \in \mathbb{Z}, x^k = e \Rightarrow d|k \end{cases}$$

Proposition 11

Soit $x \in G$ et $d \in \mathbb{N}^*$. Alors x est d'ordre d si et seulement si $\langle x \rangle$ est cyclique de cardinal d.

I.6.3. Cas des groupes finis

Proposition 12

Si G est un groupe fini de cardinal n alors : $\forall x \in G, x^n = e$

Corollaire 1

Si G est un groupe finie de cardinal n alors tout élément x de G est d'ordre fini et si d est l'ordre de x alors d divise n.

I.7. Etude des groupes monogène

I.7.1. Les groupes monogène $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$

Proposition 13

Le groupe monogène $\mathbb{Z}$ admet exactement deux générateurs à savoir 1 et -1. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique dont les générateurs sont $\overline{k}$ tel que $k \in [\![1, n]\!]$ et $k \wedge n = 1$.

Preuve:

Si a est un générateur de $\mathbb{Z}$, comme $1 \in \mathbb{Z}$, il existe $k \in \mathbb{Z}$ tel que $1 = ka$ donc $a|1$, donc $a \in \{-1, 1\}$.
Soit $k \in \{1, \cdots, n\}$. Si $\overline{k}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ alors $\overline{1} = u\overline{k}$ avec $u \in \mathbb{Z}$ donc $u\overline{k} \equiv 1\ [n]$ donc il existe $v \in \mathbb{Z}$ tel que $uk - 1 = -vn$ c'est-à-dire $uk + vn = 1$; par le lemme de Bezout $k \wedge n = 1$. Si réciproquement $k \wedge n = 1$ alors par Bezout il existe $u, v \in \mathbb{Z}$ tel que $uk + vn = 1$ donc pour tout $x \in \mathbb{Z}$ on a $x = xuk + xvn$ donc $\overline{x} = (xu)\overline{k}$ donc $\overline{k}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$.

I.7.2. Classification et générateurs

Proposition 14

Si $G = \langle a \rangle$ est un groupe monogène alors $\varphi_a : \mathbb{Z} \to G, k \mapsto a^k$ est un morphisme surjectif de groupes.

Preuve:

Surjectif par construction. Morphsme car si $k, \ell \in \mathbb{Z}$ alors $\varphi_a(k + \ell) = a^{k+\ell} = a^k a^\ell$

Proposition 15

Si $G = \langle a \rangle$ est un groupe monogène alors soit G est infini auquel cas G est isomorphe à Z et les générateurs de G sont a et a^{-1}, soit G est fini auquel cas G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ où $n = \text{card}(G)$ et les générateurs de G sont a^k avec $k \in [\![1, n]\!]$ et $k \wedge n = 1$.

Preuve:

Soit $G = \langle a \rangle$ un groupe monogène. D'après la proposition 14 $\varphi_a : \mathbb{Z} \to G; k \mapsto a^k$ est un morphisme surjectif de groupes.
• Si φ_a est injectif alors φ_a est un isomorphisme de groupe. Soit alors b un générateur de G. Pour tout $x \in \mathbb{Z}$ on a $\varphi_a(x) \in G$ donc il existe $k \in \mathbb{Z}$ tel que $\varphi_a(x) = b^k$ donc $x = \varphi_a^{-1}(b^k) =$

$k\varphi_a^{-1}(b)$ de sorte que $\varphi_a^{-1}(b)$ est un générateur de $\mathbb{Z}$, donc $\varphi_a^{-1}(b) \in \{-1, 1\}$ par suite $b = a$ ou $b = a^{-1}$. Ainsi G est monogène infini isomorphe à $\mathbb{Z}$ dont les seuls générateurs sont a et a^{-1}.
• Si φ_a n'est pas injectif alors $\ker(\varphi_a) \neq \{0\}$ donc il existe $k \in \mathbb{Z}$ tel que $k \neq 0$ et $\varphi_a(k) = e$ donc $a^k = e$ donc $a^{-k} = (a^k)^{-1} = e$ donc $a^m = e$ où $m = |k|$, donc a est d'ordre fini. Soit alors n l'ordre de a et ψ l'application :

$$\psi : \mathbb{Z}/n\mathbb{Z} \to G; \overline{k} \mapsto a^k.$$

Tout d'abord, ψ est bien définie car si $k \equiv \ell[n]$ alors il existe $q \in \mathbb{Z}$ tel que $\ell = k + qn$ donc $a^\ell = a^k(a^n)^q = a^k$ donc a^k ne dépends pas du représentant de la classe $\overline{k}$.
Ensuite ψ est surjectif par construction et finalement injectif car si $\overline{k} \in \ker\psi$ alors $a^k = e$ donc $n|k$ donc $\overline{k} = \overline{0}$. Ainsi G est un groupe cyclique isomorphe à $\mathbb{Z}/nZ$. Si b est un générateur de G alors comme $b \in G$, on a $b = a^k$ avec $k \in \{1, \cdots, n\}$. Si $x \in \mathbb{Z}/n\mathbb{Z}$ alors $\psi(x) \in G$ donc il existe $\ell \in \mathbb{Z}$ tel que $\psi(x) = b^\ell = a^{\ell k}$ donc $x = \psi^{-1}(x) = \overline{\ell k} = \ell\overline{k}$, ce qui prouve que $\overline{k}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$, donc par la proposition 13 il vient que $k \wedge n = 1$. Ainsi les générateurs de $G = \langle a \rangle$ sont les a^k avec $k \in [\![1, n]\!]$ et $k \wedge n = 1$.

Corollaire 2

Tout groupe monogène est commutatif.

Preuve:

Un tel groupe est isomorphe soit à $\mathbb{Z}$ soit à un certain $\mathbb{Z}/n\mathbb{Z}$, lesquels sont commutatifs.

I.8. Exercices

Exercice 1 : Soit G un groupe monogène. Démontrer que si G est monogène infini, tout sous-groupe de G est monogène infini et si G est cyclique tout sous-groupe de G est cyclique.
Exercice 2 : Démontrer que tout groupe de cardinal un nombre premier est cyclique.
Exercice 3 : Montrer que si $a, b \in G$ tel que $ab = ba$ et a et b d'ordres respectifs m et n et $m \wedge n = 1$ alors ab est d'ordre mn.

II. Anneaux et corps

II.1. Anneaux

II.1.1. Généralité sur les anneaux

Définition 7

Un anneau est un triplet $(A, \perp, \star)$ tel que

1. A est un ensemble non vide.
2. $(A, \perp)$ est un groupe commutatif.
3. $\star$ est associative.
4. $\star$ admet un élément neutre.
5. $\star$ est distributive par rapport à $\perp$.

Remarque On adoptera par la suite la notation additive pour la première loi et la notation multiplicative pour le seconde et on abrégera en disant l'anneau A.

Exemples 1. L'anneau $\mathbb{Z}$ des entiers relatifs.

2. L'anneau $\mathscr{A}(X, A)$ des application d'un ensemble non vide X vers un anneau A.
3. L'anneau $\mathbb{K}[X]$ des polynômes.

Définition 8

Soit A un anneau. On appelle sous-anneau de A toute partie B de A tel que :

1. B est un sous-groupe de A
2. B stable par $\times$
3. $1_A \in B$.

II.1.2. Groupe des inversibles d'un anneau

Si A est un anneau, on note $A^\times$ l'ensemble des éléments inversibles de $(A, \times)$.

Proposition 16

$A^\times$ est stable par $\times$ et $(A^\times, \times)$ est un groupe appelé groupe des inversibles de l'anneau A.

Exemples $\mathbb{Z}^\times = \{-1, 1\}$, $\mathbb{R}^\times = \mathbb{R}^*$, $\mathbb{K}[X]^\times = \mathbb{K}$, $\mathcal{M}_n(\mathbb{K})^\times = GL_n(\mathbb{K})$

II.1.3. Produit fini d'anneau

Proposition 17

Si $(A_k, +_k, \times_k), k \in [\![1, m]\!]$ sont des anneaux, on munit $A = \prod_{k=1}^{m} A_k$ des lois : $(x_k) + (y_k) =$

$(x_k +_k y_k)$ et $(x_k) \times (y_k) = (x_k \times_k y_k)$ alors $(A, +, \times)$ est un anneau. On a $A^\times = \prod_{k=1}^{m} A_k^\times$.

II.1.4. Morphismes d'anneaux

Définition 9

A et A' sont deux anneaux. Une application $f : A \to A'$ est un morphisme d'anneau si :
$$\begin{cases} \forall (x,y) \in A^2, \begin{cases} f(x+y) = f(x) + f(y) \\ f(x \times y) = f(x) \times f(y) \end{cases} \\ f(1_A) = 1_{A'} \end{cases}$$

Proposition 18

Soit $f : A \to A'$ un morphisme d'anneaux. Si f est bijective alors f^{-1} est un morphisme d'anneau de A' vers A

Proposition 19

$f : A \to A'$ un morphisme d'anneau. f est injectif si et seulement si $\ker(f) = \{x \in A / f(x) = 0\}$ est réduit à $\{0\}$. f est surjectif si et seulement si $\mathrm{Im}(f) = A'$

II.1.5. Anneau intègre

Définition 10

Soit A un anneau. On appelle diviseur de zero tout élément $a \in A$ tel que $a \neq 0$ et il existe $b \in A$ tel que $b \neq 0$ et $ab = 0$ ou $ba = 0$ A est intègre s'il n' a pas de diviseur de zero.

Remarque A est intègre si :

$$\forall (x,y) \in A^2, xy = 0 \Rightarrow x = 0 \quad \text{ou} \quad y = 0$$

II.2. Corps

Définition 11

On appelle corps tout anneau commutatif A tel que $A^\times = A^*$

Définition 12

Soit K un corps. On appelle sous-corps de K toute partie K' de K tel que K' est stable par les lois de K et muni des lois induites K' est un corps.

Remarque Si K' est un sous-corps de K alors K'^* est un sous-groupe de K^* par suite on a en particulier le même élément neutre pour la multiplication pour K et K' et le même inverse pour tout $x \in K'$.

II.3. Idéal d'un anneau

II.3.1. Généralités

Définition 13

Soit A un anneau commutatif. On appelle idéal de A toute partie I de A tel que :

1. I est un sous-groupe de $(A, +)$
2. $\forall (a, x) \in A \times I, ax \in I$

Remarque $\{0\}$ et A sont deux idéaux de A (les idéaux triviaux)

Proposition 20

Soient A un anneau commutatif et A' un anneau. Pour tout morphisme d'anneau $f : A \to A'$ on a $\ker(f)$ est un idéal de A.

Proposition 21

Soit A un anneau commutatif et $x \in A$. Alors $xA = \{xa / a \in A\}$ est un idéal de A appelé idéal engendré par x.

Si $I_1, \cdots, I_m$ ($m \geq 2$) sont des idéaux de A, on note :

$$\sum_{k=1}^{m} I_k = I_1 + \cdots + I_m = \{x_1 + \cdots + x_m / (x_1, \cdots, x_m) \in I_1 \times \cdots \times I_m\}.$$

Proposition 22

Si I et J sont deux idéaux de A alors $I + J$ et $I \cap J$ sont deux idéaux de A.

Généralement, si $(I_k)_{1 \leq k \leq m}$ est une famille d'idéaux de A alors $\sum_{k=1}^{m} I_k$ et $\bigcap_{k=1}^{m} I_k$ sont des idéaux de A.

Remarque On a $I \cap J \subset I \subset I + J$.

Généralement pour tout $k \in [\![1, m]\!]$, on a : $\bigcap_{j=1}^{n} I_j \subset I_k \subset \sum_{j=1}^{m} I_j$.

II.3.2. Idéaux et divisibilité dans un anneau commutatif intègre

Dans tout ce qui suit A est un anneau commutatif et intègre.

Définition 14

Soit $(a, b) \in A^2$. On dit que a divise b s'il existe $c \in A$ tel que $b = ca$. On dit aussi b est un multiple de a ou a est un diviseur de b.

Définition 15

Si $(a, b) \in A^2$ tel que $b = \varepsilon a$ et ε inversible on dit que a et b sont associés.

Remarque Pour tout $a, b, c \in A$ on a :

1. $a|a$
2. $a|b$ et $b|c \Rightarrow a|c$
3. $a|b$ et $b|a \Rightarrow a$ et b sont associés.

Proposition 23

Soit $(a, b) \in A^2$. On a : $a|b \Leftrightarrow bA \subset aA$

Preuve:

Si $a|b$ Soit $x \in bA$, alors $\exists y \in A, x = by$, or $\exists c \in Ab = ca$, donc $x = by = cay = az$ avec $z = cy \in A$. Réciproquement, Si $bA \subset aA$ alors comme $b \in bA$, on a $b \in aA$, donc $\exists c \in A, b = ac$ et $a|b$.

II.4. Le cas $A = \mathbb{Z}$ ou $A = \mathbb{K}[X]$, où $\mathbb{K}$ est un sous-corps de $\mathbb{C}$

Dans tout ce qui suit, A désigne l'un des anneaux commutatifs intègres $\mathbb{Z}$ ou $\mathbb{K}[X]$, où $\mathbb{K}$ est un sous-corps de $\mathbb{C}$.

II.4.1. Division euclidienne dans A

Théorème 1

1. Pour tout $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, il existe un et un seule couple $(q, r) \in \mathbb{Z}^2$ tel que :
$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$
C'est la division euclidienne de a par b. On dit que q est le quotient et r le reste dans la division euclidienne de a par b.
2. Pour tout $(P, B) \in \mathbb{K}[X]^2$ tel que $B \neq 0$, il existe un et un seule couple (Q, R) de polynômes tel que :
$$\begin{cases} P = BQ + R \\ \deg(R) < \deg(B) \end{cases}$$
C'est la division euclidienne de P par B.

Remarque Si $a = bq + r$ est la division euclidienne de a par b dans l'anneau A, alors on donne les apelations suivantes :

1. a est le dividende.
2. b est le diviseur : il doit être non nul.
3. q est le quotient.
4. r est le reste : il vérifie $r < s(b)$ avec $s(b) = |b|$ dans le cas de $A = \mathbb{Z}$ et $s(b) = \deg(b)$ dans le cas de $A = \mathbb{K}[X]$.

II.4.2. Les idéaux de A

Proposition 24

Tout idéal de A est de la forme aA avec $a \in A$.
Précisément :

1. Pour $A = \mathbb{Z}$: Tout idéal $\mathscr{I}$ de $\mathbb{Z}$ il existe un et un seule entier naturel n tel que $\mathscr{I} = n\mathbb{Z}$.
2. Pour $A = \mathbb{K}[X]$: Pour tout idéal non nul $\mathscr{I}$ de $\mathbb{K}[X]$, il existe un et un seule polynôme unitaire P tel que $\mathscr{I} = P\mathbb{K}[X]$

Remarque Si $\mathscr{I}$ est un ideal de A, quand on parlera de l'unique générateur a de A alors $a = 0$ si $\mathscr{I}$ est nul et l'unique $n \in \mathbb{N}^*$ tel que $\mathscr{I} = n\mathbb{Z}$ si $\mathscr{I}$ est non nul et $A = \mathbb{Z}$ et a l'unique polynôme unitaire P tel que $\mathscr{I} = P\mathbb{K}[X]$ si $A = \mathbb{K}[X]$.

II.4.3. p.g.c.d. , p.p.c.m. dans A

Définition 16

Soit $(a,b) \in A^2$ tel que $a \neq 0$ et $b \neq 0$. L'unique générateur δ de l'ideal $aA + bA$ s'appelle le plus grand diviseur de a et b. L'unique générateur μ de l'idéal $aA \cap bA$ s'appelle le plus petit multiple commun de a et b.

Notation : On note $\delta = a \wedge b$ et $\mu = a \vee b$

Remarques On note les remarques suivantes :

1. On peut généraliser pour plusieurs éléments non nuls $a_1, \cdots, a_m$ de A. On a :

$$(a_1 \wedge \cdots \wedge a_m)A = \sum_{k=1}^{m} a_k A$$

et

$$(a_1 \vee \cdots \vee a_m)A = \bigcap_{k=1}^{m} a_k A$$

2. Si $a, b \in \mathbb{Z}^*$ alors :

$$a|b \Leftrightarrow a \wedge b = |a| \Leftrightarrow a \vee b = |b|.$$

3. Pour tout polynôme non nul P, on note :

$$\widetilde{P} = (\mathrm{cd}(P))^{-1} P.$$

Si $P, Q \in \mathbb{K}[X]\backslash\{0\}$, alors

$$P|Q \Leftrightarrow P \wedge Q = \widetilde{P} \Leftrightarrow P \vee Q = \widetilde{Q}.$$

II.4.4. Algorithme d'Eucilde

Proposition 25

Soit $(a,b,\alpha,\beta) \in A^4$. Si $a = \alpha b + \beta$, alors $a \wedge b = b \wedge \beta$

Preuve:

On va démontrer que $a\mathbb{Z}+bZ = b\mathbb{Z}+\beta\mathbb{Z}$. Soit $x = au+bv \in a\mathbb{Z}+b\mathbb{Z}$, alors $x = u(\alpha b+\beta)+bv = (\alpha u + v)b + u\beta$, donc $x \in b\mathbb{Z} + \beta\mathbb{Z}$. Soit $x = bu + \beta v \in b\mathbb{Z} + \beta\mathbb{Z}$, alors $x = bu + v(a - \alpha b) = va + (u - \alpha v)b$, donc $x \in a\mathbb{Z} + b\mathbb{Z}$, d'où l'égalité ensembliste établie et par suite la proposition 25

Proposition 26

Soit $(a,b) \in \mathbb{Z}^2$ tel que $ab \neq 0$, alors $a \wedge b$ est le dernier reste non nul dans les divisions euclidiennes successives de a par b.

Proposition 27

Soit $(P,Q) \in \mathbb{K}[X]^2$ tel que $PQ \neq 0$, alors $P \wedge Q$ est le dernier reste non nul, normalisé dans les divisions euclidiennes successives de A par Q.

II.4.5. Identité de Bezout, lemme de Gauss

Proposition 28

Soit $(a,b) \in A^2$, alors

$$a \wedge b = 1 \Leftrightarrow \exists (u,v) \in A^2, \quad ua + vb = 1$$

Remarques On peut généraliser : $a_1 \wedge \cdots \wedge a_m = 1 \Leftrightarrow \exists (u_1, \cdots, u_m) \in A^m, \quad \sum_{k=1}^{m} u_k a_k = 1$

Proposition 29

Soit $(a,b,c) \in A^3$. On a : $\begin{cases} a|bc \\ a \wedge b = 1 \end{cases} \Rightarrow a|c$

II.4.6. Irréductibles de A

Définition 17

Un élément a de A est irréductible si a est non inversible et :

$$\forall b \in A, \quad b|a \Rightarrow b \text{ inversible ou } b \text{ et } a \text{ sont associés}$$

Ainsi un irréductible de A est un élément non inversible a de A dont les seules diviseurs sont de la forme ε ou εa avec $\varepsilon \in A^\times$. Autrement dit l'ensemble des diviseurs de a est $D_a = A^\times \cup A^\times a$.

Proposition 30

Les irréductibles de $\mathbb{Z}$ sont les nombres premiers.

Preuve:

Si p est premier alors p n'est pas inversible car $p \neq 1$ et $p \neq -1$, par ailleurs les diviseurs de p sont les éléments de $\{1, -1, p, -p\} = \mathbb{Z}^\times \cup p\mathbb{Z}^\times$.
Réciproquement si p est un entier non inversible dont les seuls diviseurs sont $-1, 1, p$ et $-p$ alors par définition, p est premier.

Proposition 31

Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les trinômes de la forme aX^2+bX+c tel que $(a,b,c) \in \mathbb{R}^3$ et $\begin{cases} a \neq 0 \\ b^2 - 4ac < 0 \end{cases}$.

Preuve:

Voir cours de M.P.S.I.

On note $\mathbb{P}$ l'ensemble des nombres entiers naturels premiers.

Théorème 2

Pour tout nombre entier relatif x non inversible et non nul il existe un unique $s \in \mathbb{N}^*$, un unique $\varepsilon \in \{-1, 1\}$, un unique $(\alpha_1, \cdots, \alpha_s) \in (\mathbb{N}^*)^s$ et un unique $(p_1, \cdots, p_s) \in \mathbb{P}^s$ tel que :

$$\begin{cases} p_1 < \cdots < p_s \\ x = \varepsilon \displaystyle\prod_{k=1}^{s} p_k^{\alpha_k} \end{cases}$$

Théorème 3

Pour tout polynôme non nul et non inversible $Q \in \mathbb{K}[X]$, il existe un unique $\varepsilon \in \mathbb{K}^*$, un unique $s \in \mathbb{N}^*$, un unique $(\alpha_1, \cdots, \alpha_s) \in (\mathbb{N}^*)^s$, et, à une permutation près, un unique $(P_1, \cdots, P_s) \in \mathbb{K}[X]^s$ tel que :

$$\begin{cases} \forall k \in [\![1, s]\!], \quad P_k \text{ est unitaire irréductible} \\ Q = \varepsilon \displaystyle\prod_{k=1}^{s} P_k^{\alpha_k} \end{cases}$$

III. $\mathbb{Z}/n\mathbb{Z}$: Compléments

III.1. L'anneau $\mathbb{Z}/n\mathbb{Z}$

On rappelle que $\mathbb{Z}/n\mathbb{Z}$ muni des lois $+$ et $\times$ tel que :

$$\forall k, \ell \in \mathbb{Z}, \quad \begin{cases} \overline{k} + \overline{\ell} = \overline{k+\ell} \\ \overline{k} \times \overline{\ell} = \overline{k+\ell} \end{cases}$$

est un anneau commutatif non intègre en général.

Proposition 32

$\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est un corps.

III.2. Le groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

III.2.1. Inversibles de $\mathbb{Z}/n\mathbb{Z}$

Proposition 33

Le groupe des inversible de $\mathbb{Z}/n\mathbb{Z}$ est :

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{k}/k \in [\![1, n]\!]/k \wedge n = 1\}$$

Ainsi le groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ coincide avec l'ensemble des générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$.

Preuve:

Si $k \in \mathbb{Z}$ tel que $\overline{k}$ est inversible, alors il existe $k' \in \mathbb{Z}$ tel que $\overline{kk'} = \overline{1}$, donc $kk' \equiv 1$ modulo n donc il existe $k'' \in \mathbb{Z}$ tel que $kk' - 1 = k''n$ donc $uk + vk = 1$ avec $(u, v) = (k, -k')$

Remarque On a $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement si $k \wedge n = 1$, non seulement pour tout $k \in [\![1, n]\!]$, mais pour tout $k \in \mathbb{Z}$. En effet, si r est le reste dans la division euclidienne de k par n on a $k \wedge n = r \wedge n$ et $\overline{k} = \overline{r}$.

III.2.2. Théorème d'Euler

Corollaire 3

Pour tout $n \in \mathbb{N}^*$ et tout $k \in \mathbb{Z}$, on a :

$$k \wedge n = 1 \Rightarrow k^{\varphi(n)} \equiv 1 \quad [n]$$

Preuve:

Soit r le reste de k dans la division euclidienne par n alors $r \wedge n = 1$ et $\overline{r}$ dans le groupe des inversibles dont le cardinal est $\varphi(n)$, donc $\overline{r}^{\varphi(n)} = \overline{1}$, comme $\overline{r} = \overline{k}$, le résultat en découle.

Corollaire 4

Si p est premier alors :

1. Pour tout $k \in \mathbb{Z}$ tel que p ne divise pas k on a $k^{p-1} \equiv 1\ [p]$
2. Pour tout entier k on a $k^p \equiv k \quad [p]$

III.2.3. Lemme des restes chinois

Théorème 4

Si m et n sont des entiers naturels non nuls premiers entre eux alors les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes.

Preuve:

Pour tout $x \in \mathbb{Z}$, on note $\overline{x}$, $\tilde{x}$ et $\widehat{x}$ les classes de x modulo m,n et mn respectivement. Soit $f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tel que $f(\widehat{x}) = (\overline{x}, \tilde{x})$ pour tout $x \in \mathbb{Z}$.

Tout d'abord, f est bien définie car si $x \equiv x'\ [mn]$ alors $\begin{cases} x \equiv y\ [m] \\ x \equiv y\ [n] \end{cases}$.

Ensuite f est un morphisme d'anneau car :

- $f(\widehat{1}) = (\overline{1}, \tilde{1})$.
- pour tout $x, y \in \mathbb{Z}$, on a :

$$f(\widehat{x} + \widehat{y}) = f(\widehat{x+y}) = (\overline{x+y}, \widetilde{x+y}) = (\overline{x} + \overline{y}, \tilde{x} + \tilde{y}) = (\overline{x}, \tilde{x}) + (\overline{y}, \tilde{y}) = f(\widehat{x}) + f(\widehat{y})$$

- Pour tout $x, y \in \mathbb{Z}$, on a :

$$f(\widehat{x} \times \widehat{y}) = f(\widehat{x \times y}) = (\overline{x \times y}, \widetilde{x \times y}) = (\overline{x} \times \overline{y}, \tilde{x} \times \tilde{y}) = (\overline{x}, \tilde{x}) \times (\overline{y}, \tilde{y}) = f(\widehat{x}) \times f(\widehat{y})$$

f est injectif car si pour $x \in \mathbb{Z}$, $f(\widehat{x}) = \widehat{0}$ alors $(\overline{x}, \tilde{x}) = (\overline{0}, \tilde{0})$ donc $m|x$ et $n|x$ et comme $m \wedge n = 1$ alors $mn|x$ et par suite $\widehat{x} = \widehat{0}$, donc $\ker f = \{\widehat{0}\}$, et f est injectif ; et comme les

ensembles $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont finis de même cardinal, à savoir mn, l'application f est bijective et c'est donc un isomorphisme.

Corollaire 5

Soit $m, n \in \mathbb{N}$ non nuls tel que $m \wedge n = 1$. Pour tout $(a, b) \in \mathbb{Z}^2$, le système :

$$(1) \quad \begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases}$$

admet des solutions. Si x_0 est une solution alors l'ensemble des solutions est $\mathscr{S} = x_0 + mn\mathbb{Z}$.

Preuve:

x est une solution du système (1) si et seulement si $f(\widehat{x}) = (\overline{a}, \tilde{b})$, et comme f est surjective , le système admet une solution au moins (f surjective).
Si x_0 et x sont des solutions de (1), alors $\widehat{x - x_0} \in \ker f$, et comme f est injective cela veut dire que $\widehat{x - x_0} = \widehat{0}$ donc $mn|(x - x_0)$.

Remarques On peut faire les remarques importantes suivantes :

1. Une méthode pratique pour trouver une solution du système (1) : Comme $m \wedge n = 1$ alors il existe $(u, v) \in \mathbb{Z}^2$ tel que $mu + nv = 1$. Si on pose $x_0 = bmu + anv$ alors x_0 est une solution de (1).
2. On peut généraliser : Soit $n_1, \cdots, n_s$ une famille d'entiers naturels deux à deux premiers entre eux (avec $s \geq 2$). Posons $n = \prod_{k=1}^{s} n_k$. et pour tout $k \in [\![1, s]\!]$, posons $n'_k = \dfrac{n}{n_k}$. On voit que $n_k \wedge n'_k = 1$,pour tout $k \in [\![1, s]\!]$. Par le lemme de Bezout il existe $u_k, u'_k \in \mathbb{Z}$ tel que : $u_k n_k + u'_k n'_k = 1$ Posons $\varepsilon_k = u'_k n'_k$ alors

$$\begin{cases} \varepsilon_k \equiv 1\ [n_k] \\ \varepsilon_j \equiv 0\ [n_k], \forall j \in [\![1, s]\!], j \neq k \end{cases}$$

de sorte que si on pose $x_0 = \sum_{j=1}^{s} \varepsilon_j a_j$ alors x_0 est une solution du système :

$$x \equiv a_k\ [n_k], \forall k \in [\![1, s]\!]$$

III.2.4. Conséquence : l'indicatrice d'Euler est multiplicative.

Proposition 34

Si $m, n \in \mathbb{N}^*$ tel que $m \wedge n = 1$ alors

$$\varphi(mn) = \varphi(m)\varphi(n)$$

On dit que la fonction φ est multiplicative.

Preuve:

C'est une conséquence immédiate du théorème 4, puisque le groupe des inversibles d'un anneau produit est le produit des groupes des inversibles des anneaux associés. Donc $(\mathbb{Z}/m\mathbb{Z}\times \mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$; par passage aux cardinaux, on a $\varphi(mn) = \varphi(m)\varphi(n)$.

III.2.5. Résumé des propriétés del'indicatrice d'Euler

Pour tout $n \in \mathbb{N}^*$, on note $\varphi(n) = \text{card}(\mathbb{Z}/n\mathbb{Z})^\times$. L'application φ s'appelle l'indicatrice d'Euler. Elle possède les propriétés suivantes :

1. Pour tout $n \in \mathbb{N}^*$, $\varphi(n)$ est le nombre des générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$.
2. Pour tout $n \in \mathbb{N}^*$, $\varphi(n)$ est le nombre des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
3. Pour tout entier naturel premier p, on a : $\varphi(p) = p - 1$.
4. Pour tout entier naturel premier p, et tout entier naturel non nul α, on a :
$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$
5. Si $n \in \mathbb{N}$ tel que $n = \prod_{k=1}^{s} p_k^{\alpha_k}$ avec $s \in \mathbb{N}^*$, $\alpha_1, \cdots, \alpha_s \in \mathbb{N}^*$ et $p_1, \cdots, p_s$ des nombres entiers naturels premiers deux à deux distincts alors :
$$\varphi(n) = n \prod_{k=1}^{s} \left(1 - \frac{1}{p_k}\right)$$

IV. Structure d'algèbre

IV.1. Définitions

Soit $\mathbb{K}$ un corps.

Définition 18

On appelle $\mathbb{K}-$algèbre un quadruple $(\mathscr{A},+,\times,.)$ tel que :

(1) $(\mathscr{A},+,\times)$ est un anneau.

(2) $(\mathscr{A},+,.)$ est un $\mathbb{K}-$espace vectoriel.

(3) $\forall(\alpha\in\mathbb{K})(\forall(x,y)\in\mathscr{A}^2)\quad \alpha.(x\times y)=x\times(\alpha.y)=(\alpha.x)\times y.$

Remarques On retient les remarques suivantes :

1. Si on ajoute :
   (4) $\times$ est commutative,
   on parle d'algèbre commutative.
2. Notons que si $(\mathscr{A},+,\times,.)$ est une algèbre alors $\times$ admet un élément neutre $1_{\mathscr{A}}$.
3. Si $(\mathscr{A},+,\times,.)$ est une $\mathbb{K}-$algèbre alors pour tous $x,y\in\mathscr{A}$ et tous $\alpha,\beta\in\mathbb{K}$, on a
$$(\alpha\beta).(x\times y)=(\alpha.x)\times(\beta.y)=x\times((\alpha\beta).y)=((\alpha.(\beta.x))\times y=...$$

Exemples :

1. Si $(\mathbb{K},+,\times)$ est un corps alors $(\mathbb{K},+,\times,.)$ est une $\mathbb{K}-$algèbre.
2. Si X est un ensemble non vide et $\mathscr{A}$ est une $\mathbb{K}-$algèbre alors $(\mathscr{A}^X,+,\times,.)$ est une $\mathbb{K}-$algèbre, avec $f+g(x)=f(x)+g(x)$; $f\times g(x)=f(x)\times g(x)$ et $(\alpha.f)(x)=\alpha.f(x)$, pour tout $x,y\in X$ et $\alpha\in\mathbb{K}$.
3. $(\mathbb{K}[X],+,\times,.)$ est une $\mathbb{K}-$algèbre commutative.
4. $(\mathcal{L}(E),+,\circ,.)$ et $(\mathcal{M}_n(\mathbb{K}),+,\times,.)$ sont des $\mathbb{K}-$algèbres.

IV.2. Sous-algèbre

Définition 19

Soit $\mathscr{A}$ une algèbre. On appelle sous-algèbre de $\mathscr{A}$ toute partie $\mathscr{A}'$ de $\mathscr{A}$ tel que :

(1) $\mathscr{A}'$ est un sous-anneau de l'anneau $\mathscr{A}$.

(2) $\mathscr{A}'$ est un sous-espace vectoriel de l'espace vectoriel $\mathscr{A}$.

Remarque Si $\mathscr{A}'$ est une sous-algèbre de $\mathscr{A}$ alors $\mathscr{A}'$ est stables par toutes les lois de $\mathscr{A}$ et $(\mathscr{A}',+,\times,.)$ est une $\mathbb{K}-$algèbre.

Proposition 35

Pour que $\mathscr{A}'$ soit uns sous-algèbre de $\mathscr{A}$, il suffit que :

1. $1_{\mathscr{A}}\in\mathscr{A}'$
2. $\forall\lambda\in\mathbb{K},\forall(x,y)\in\mathscr{A}'^2,\quad x+\lambda y\in\mathscr{A}'$
3. $\forall(x,y)\in\mathscr{A}'^2,\quad xy\in\mathscr{A}'$

IV.3. Morphisme d'algèbre

Définition 20

On appelle morphisme d'une algèbre $\mathscr{A}, +, \times, .)$ vers une algèbre $\mathscr{A}', +, \times, .)$ toute application $f : \mathscr{A} \to \mathscr{A}'$ tel que :

1. f est un morphisme d'espace vectoriels de $\mathscr{A}$ vers $\mathscr{A}'$
2. f est un morphisme d'anneaux de $\mathscr{A}$ vers $\mathscr{A}'$.

Proposition 36

Pour que f soit un morphisme d'algèbre de $\mathscr{A}$ vers $\mathscr{A}'$ il faut et il suffit que :

1. $f(1_{\mathscr{A}}) = 1_{\mathscr{A}'}$
2. $\forall(\lambda, x, y) \in \mathbb{K} \times \mathscr{A} \times \mathscr{A}, \quad f(x + \lambda y) = f(x) + \lambda f(y)$.
3. $\forall(x, y) \in \mathscr{A}^2 \quad f(xy) = f(x)f(y)$.

Proposition 37

Soit $f : \mathscr{A} \to \mathscr{A}'$ un morphisme d'algèbres de l'algèbre $\mathscr{A}$ vers l'algèbre $\mathscr{A}'$; alors $f(\mathscr{A})$ est une sous-algèbre de $\mathscr{A}'$. Si de plus $\mathscr{A}$ est commutative, il en est de même de $f(\mathscr{A})$.