Université Mohammed V
Faculté des Sciences
Rabat, Maroc

Polycopié du cours d'Algèbre 2

Structures algébriques, Polynômes et Fractions Rationnelle

Filière : Sciences Mathématiques Informatique et Applications (SMIA)

2020-2021

Professeur Driss Bennis

Ce polycopié contient les définitions et les résultats du cours d'algèbre 2. Les démonstrations ainsi que d'autres exemples seront donnés en cours. Ainsi, ce polycopié se veut avant tout un outil complémentaire aux cours et travaux dirigés.

Table des matières

Chapitre 1

Groupes

1.1 Vocabulaire des lois de composition interne

Dans cette section, E désigne un ensemble non vide.

- **Loi de composition interne :** Toute application $*$ de $E \times E$ dans E est appelée une **loi de composition interne** (en bref, lci), ou simplement une loi sur un ensemble E, ou encore une opération dans E.
- Pour tout $(x, y) \in E$, l'élément $*(x, y)$ sera noté $x * y$. Il sera appelé le **composé** de x par y par la loi $*$.
- On appelle **magma** tout couple $(E, *)$ où $*$ est une lci sur E.
- **Associativité :** La loi $*$ est dite **associative** si, pour tout $(x, y, z) \in E^3$,

$$(x * y) * z = x * (y * z).$$

  On dit aussi que le magma $(E, *)$ est associatif.
- **Commutativité :** La loi $*$ est dite **commutative** si, pour tout $(x, y) \in E^2$, $x * y = y * x$.
  On dit aussi que le magma $(E, *)$ est commutatif.

Les lci sont souvent notées avec l'un des symboles suivants : $*, \cdot, +, T, \perp, \times$. Cependant, le choix du symbole pour noter une loi est complètement arbitraire. C'est pour cette raison que souvent on préfère d'utiliser les notations usuelles $+$ ou . ou $\times$.

- Si on utilise $+$, la loi est appelée **addition**. On dit que la loi de E est notée **additivement**. Dans ce cas, "$x + y$" s'appelle la somme de x et de y.
- Si on utilise . ou $\times$, la loi est appelée **multiplication**. On dit que la loi de E est notée **multiplicativement**. Dans ce cas, "$x \times y = x.y$" s'appelle le produit de x et de y. Parfois, il convient d'omettre les symboles . et $\times$ (i.e., on utilise simplement xy pour désigner "$x \times y$").

Exemples 1.1.1

1. *La multiplication et l'addition usuelles sont des lci sur $\mathbb{R}$ qui sont à la fois associatives et commutatives.*

2. *L'union et l'intersection des parties d'un ensemble A sont des lci sur l'ensemble des parties de A.*
3. *En général, si on a deux magmas (E, T) et $(F, *)$, alors on peut définir un magma $(E \times F, \perp)$ tel que $(x, y) \perp (x', y') := (xTx', y * y')$ pour tous $(x, x') \in E^2$ et $(y, y') \in F^2$. De plus :*
   — *La loi $\perp$ est associative si et seulement si (E, T) et $(F, *)$ sont associatifs.*
   — *La loi $\perp$ est commutative si et seulement si (E, T) et $(F, *)$ sont commutatifs.*
4. *On considère l'ensemble $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}^*$. L'addition $+$ définie sur $\mathbb{Z}/n\mathbb{Z}$ par $\overline{a} + \overline{b} := \overline{a + b}$ pour tout $(a, b) \in \mathbb{Z}^2$, est une lci sur $\mathbb{Z}/n\mathbb{Z}$ qui est à la fois associative et commutative. De même le produit $\times$ défini sur $\mathbb{Z}/n\mathbb{Z}$ par $\overline{a} \times \overline{b} := \overline{a \times b}$ pour tout $(a, b) \in \mathbb{Z}^2$, est une lci sur $\mathbb{Z}/n\mathbb{Z}$ qui est à la fois associative et commutative.*
5. *La division (des nombres) peut être ou non une loi de composition interne selon l'ensemble de nombres considéré : Elle n'est pas une loi de composition interne dans , mais elle l'est dans $\mathbb{R}^*$ (ensemble des réels non nuls). Elle est aussi claire que la division n'est pas une loi de composition interne dans $\mathbb{Z}^*$.*
6. *La soustraction n'est pas une loi de composition interne dans $\mathbb{N}$, mais elle l'est dans $\mathbb{Z}$.*

Définition 1.1.2
Etant donné un magma fini $(E, *)$ de cardinal $n \in \mathbb{N}^*$, disons $E = \{x_1, ..., x_n\}$, on appelle ***table de Cayley*** *de $(E, *)$ (ou simplement de E) le tableau carré de n lignes et n colonnes obtenu en inscrivant à la i-ème ligne et à la j-ième colonne l'élément $x_i * x_j$ du magma E.*

Exemple 1.1.3
La table de Cayley du magma $(\mathbb{Z}/2\mathbb{Z}, \times)$ est la suivante :

$\times$	0	1
0	0	0
1	0	1

Exercice 1.1.4
1. *Dresser la table de Cayley de $(Z/4Z; +)$.*
2. *On considère le magma $(Z/2Z \times Z/2Z; +)$ définie, comme dans l'exemple 1.1.1 (4), par $(x, y) + (x', y') := (x + x', y + y')$ pour tout $(x, y, x', y') \in (\mathbb{Z}/2\mathbb{Z})^4$.*

Définition 1.1.5
Une partie non vide H d'un magma $(E, *)$ est dite ***stable*** *pour la loi de E si, pour tout $(x, y) \in H^2$, $x * y \in H$. Dans ce cas, la restriction de la loi de E à H est une loi de composition interne sur H appelée* ***la loi induite*** *sur H. Cette loi sera notée par le même symbole que celui de la loi de E.*

Exercice 1.1.6

1. *L'ensemble des matrices triangulaires supérieures à diagonale unité est stable pour le produit mais pas pour la somme.*
2. *L'ensemble $\mathbb{U}$ des nombres complexes de module 1 est stable pour le produit.*
3. *L'ensemble $\mathbb{U}_n \subset \mathbb{C}$ des racines n-ièmes de l'unité est stable pour le produit des nombres complexes.*

Définition 1.1.7 (Elément neutre)
Soit $(E, *)$ un magma. On appelle ***élément neutre*** *de $(E, *)$ tout élément $e \in E$ vérifiant $x * e = e * x = x$ pour tout $x \in E$.*

Il est claire que si $(E, *)$ est un magma commutatif, alors $e \in E$ est un élément neutre de E si seulement $x * e = x$ pour tout $x \in E$.

Exercice 1.1.8
Donner un exemple d'un magma $(E, *)$ qui admet un élément $f \in E$ vérifiant $x * f = x$ pour tout $x \in E$ sans qu'il soit un élément neutre.

Proposition 1.1.9
Si un magma admet un élément neutre, alors il est unique.

Notation. Soit E un magma admettant un élément neutre.
— Si la loi de E est notée multiplicativement, alors l'élément neutre de E est parfois noté 1_E ou simplement 1.
— Si la loi de E est notée additivement, alors l'élément neutre de E est parfois noté 0_E ou simplement 0.

Notez, qu'en général, un magma n'admet pas nécéssairement un élément neutre (donner un exemple d'un tel magma). Mais, lorsqu'il admet un élément neutre, on peut donc parler de la notion d'un élément symétrisable définie comme suit.

Définition 1.1.10 (Symétrique d'un élément)
Soit $(E, *)$ un magma admettant un élément neutre e.
Un élément x est dit ***symétrisable*** *dans E, s'il existe un élément $y \in E$ vérifiant : $x * y = y * x = e$. Dans ce cas, y est appelé un* ***symétrique*** *de x dans E.*

Il est claire que si $(E, *)$ est un magma commutatif, alors $x \in E$ est symétrisable dans E s'il existe un élément $y \in E$ vérifiant seulement l'un des égalités $x * y = e$ ou $y * x = e$.

Exercice 1.1.11
On muni $\mathbb{R}$ de loi de composition interne $*$ définie par : $\forall (x, y) \in \mathbb{R}^2$, $x * y = xy + (x^2 - 1)(y^2 - 1)$.

1. *Montrer que $\mathbb{R}$ muni de la loi $*$ admet un élément neutre que l'on déterminera.*
2. *Montrer que la loi $*$ est commutative.*

3. *Montrer que la loi $*$ n'est pas associative.*
4. *Déterminer l'ensemble S des éléments symétrisables dans $(\mathbb{R}, *)$. Et montrer qu'en particulier tout élément $a \in \mathbb{R}$ avec $|a| > 1$ admet deux symétriques.*

Pour garentir l'unicité du symétrique, on a besoin que la loi soit associative.

Définition 1.1.12
Un magma associatif $(E, *)$ admettant un élément neutre sera appelé un monoïde.

Proposition 1.1.13
Dans un monoïde, tout élément symétrisable admet un unique symétrique.

Notation. Si la loi d'un monoïde E est notée :
— multiplicativement, les éléments symétrisables seront appelés inversibles. Dans ce cas, le symétrique d'un élément inversible x sera appelé **l'inverse** de x et noté x^{-1}.
— additivement, le symétrique de x sera noté $-x$ et appelé **l'opposé** de x.

Remarque 1.1.14
Dans un monoïde $(E, *)$, tout élément symétrisable x est simplifiable ; i.e., il vérifie les deux assertions suivantes :

1. *Pour tout $(y, z) \in E^2$, $x * y = x * z \Rightarrow y = z$ (simplification à gauche).*
2. *Pour tout $(y, z) \in E^2$, $y * x = z * x \Rightarrow y = z$ (simplification à droite).*

*Un élément x de E vérifiant les assertions 1 et 2 ci-dessous est dit aussi **régulier**.*
Notez, qu'un élément régulier n'est pas nécessairement symétrisable. Par exemple, dans $(\mathbb{Z}, \times)$, tout élément non nul est simplifiable, alors que seuls 1 et -1 sont inversibles dans $(\mathbb{Z}, \times)$.

Exercice 1.1.15
On Pose $H = (\mathbb{Z}/n\mathbb{Z})\backslash\{\overline{0}\}$, où $n \in \mathbb{N}\backslash\{0, 1\}$, et on considère le monoïde $(H, \times)$.

1. *Déterminer les éléments inversibles de $(H, \times)$.*
2. *En déduire que n est premier si et seulement si tout élément de H est inversible.*
3. *Montrer qu'un élément de $(H, \times)$ est régulier si et seulement s'il est inversible.*

Exercice 1.1.16
Soit $(G, *)$ un monoïde fini.

1. *Soit $g \in G$. On considère l'application $d_g : G \to G$ définie par $d_g(x) = g*x$ pour tout $x \in G$.*
   Montrer que d_g est bijective si et seulement si g est symétrisable.
2. *On suppose que tout élément de G est régulier. Montrer que tout élément de G est symétrisable.*
3. *Montrer qu'on obtient le même résultat de la question précédente si on suppose que $(G, *)$ est seulement un magma associatif fini.*

4. *Donner un exemple d'un monoïde dont tout élément est régulier mais pas tout élément est symétrisable.*

On termine cette partie par quelques règles de calcul dans un monoïde.

Proposition 1.1.17
Soit $(E, *)$ un monoïde.

1. *Soit $(x, y) \in E^2$. Si x et y sont symétrisables de symétriques x' et y', respectivement, alors xy est symétrisable de symétrique $y'x'$.*
2. *Si un élément x de E est symétrisable, alors son symétrique est de même symétrisable de symétrique x.*

Remarque 1.1.18
La proposition ci-dessus peut être reformuler dans le cas des notations additive et multiplicative comme suit :

1. *Si la loi de E est notée multiplicativement, alors pour deux éléments inversibles x et y de E, xy est inversible et on a : $(xy)^{-1} = y^{-1}x^{-1}$.*
   Et si la loi est notée additivement, alors si x et y admettent des opposés, il en est de même de $x + y$, et on a : $-(x + y) = (-y) + (-x)$.
2. *Si la loi de E est notée multiplicativement, on écrit pour un élément inversible x : $(x^{-1})^{-1} = x$.*
   Et si la loi de E est notée additivement, on écrit pour un élément x qui admet un opposé : $-(-x) = x$.

Définition 1.1.19
Soit $(E, *)$ un monoïde d'élément neutre e.
Le composé d'un nombre fini d'éléments de E se définit par récurrence comme suit : Considérons une suite $(x_i)_i$ d'éléments de E. Pour tout entier $n \geq 2$, on écrit :

$$x_1 * \cdots * x_n * x_{n+1} := (x_1 * \cdots * x_n) * x_{n+1}.$$

En particulier, si $x = x_1 = \cdots = x_n$, alors $x_1 * \cdots * x_n$ sera noté x^{*n}.
Pour $n = 1$, on convient de poser $x^{*1} = x$.
Pour $n = 0$, on convient de poser $x^{*0} = e$.

Notation. Soit x un élément d'un monoïde $(E, *)$. Si on note la loi de E :
— multiplicativement, alors x^{*n} sera simplement noté x^n et appelé la puissance n-ième de x. On lit x exposant n ou x puissance n.
— additivement, alors x^{*n} sera simplement noté nx. Dans ce cas, nx est dit un multiple de x.

Proposition 1.1.20
Soit $(E, *)$ un monoïde. Soient $x \in E$ et n un entier naturel. Si x est symétrisable de symétrique x', alors x^{*n} est symétrisable de symétrique $(x')^{*n}$.
Si la loi est notée multiplicativement, on écrit : $(x^n)^{-1} = (x^{-1})^n$. Et si la loi est notée additivement, on écrit : $-(nx) = n(-x)$.

La proposition précédente nous permet d'étendre l'utilisation de la notation x^{*n} à tout entier relatif comme suit :

Définition 1.1.21 (Puissances généralisées)
Soient $(E, *)$ un monoïde d'élément neutre e et x un élément symétrisable de E de symétrique x'. Pour tout entier négatif $n > 0$, on pose : $x^{*n} := ((x')^{*(-n)})$.
— *Si la loi est notée multiplicativement, on écrit $x^{-n} = (x^{-1})^n = (x^n)^{-1}$.*
— *Si la loi est notée additivement, on écrit $(-n)x = n(-x) = -(nx)$.*

Il arrive des fois qu'on a $a * b = b * a$ pour deux éléments a et b d'un monoïde E sans qu'il soit nécessairement commutatif. On dit que les deux éléments a et b **commutent** si $a * b = b * a$.

Proposition 1.1.22
Soient a et b deux éléments symétrisables d'un monoïde $(E, *)$. Alors, pour tout $(p, q) \in \mathbb{Z}^2$, on a les assertions suivantes :

1. $a^{*p} * a^{*q} = a^{*(p+q)}$.
2. $(a^{*p})^{*q} = a^{*pq}$.
3. *Si a et b commutent, alors $(ab)^{*p} = a^{*p} b^{*p}$.*

1.2 Groupes et Sous-groupes

Dans la suite, sauf mention contraire, on utilisera la notation multiplicative.

Définition 1.2.1 (Groupe)
*On appelle **groupe** tout monoïde G tel que tout élément est inversible.*
*Si la loi de G est commutative, G est dit un **groupe commutatif** ou un **groupe abélien**.*
*Si G est fini, on dit que G est **d'ordre fini** et son cardinal sera noté par $|G|$ et appelé **l'ordre** de G.*

Exemple 1.2.2
1. *$(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ sont des groupes abéliens.*
2. *$(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ et $(\mathbb{Q}^*, \times)$ sont des groupes abéliens.*
3. *Pour tout $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien.*
4. *$(\mathbb{Z}^*, \times)$ n'est pas un groupe car, par exemple, 2 n'est pas inversible (en fait, seuls 1 et -1 sont inversibles).*
5. *$(\mathbb{R}, \times)$ n'est pas un groupe car, par exemple, 0 n'est pas inversible.*
6. *$(\mathbb{N}, +)$ n'est pas un groupe. En effet, aucun élément non nul n'est inversible.*
7. *Soit E un ensemble. Si on note $\mathfrak{S}(E)$ l'ensemble des bijections de E dans E, alors l'ensemble $\mathfrak{S}(E)$ muni de la comoposition des applications o est un groupe appelé **groupe symétrique** de E. En particulier, S_n est l'ensemble des permutations de $\mathbb{N}_n = \{1, 2, ..., n\}$ où $n \geq 1$. Rappelons que $Card(S_n) = n!$.*
8. *L'ensemble des isométries du plan (i.e., des applications qui préservent les distances) muni de la comoposition des applications est un groupe.*

9. *L'ensemble* $\{0,1\}$ *muni de la loi définie par la table de Cayley suivante*

$+$	0	1
0	0	1
1	1	0

est un groupe.

10. *Soit* $(G_1, ..., G_n)$ *(où* $n \in \mathbb{N}^*$*) une famille finie de groupes. On munit le produit cartésien* $G = G_1 \times \cdots \times G_n$ *de la loi suivante :* $(a_i)_i(b_i)_i = (a_i b_i)_i$ *pour tous* $(a_i)_i$ *et* $(b_i)_i$ *dans* G *(ici* $(a_i)_i$ *désigne l'élément* $(a_1, ..., a_n)$*). Alors, muni de cette loi* G *est un groupe qui est commutatif si et seulement si* G_i *est commutatif pour tout* $i \in \{1, ..., n\}$ *(à faire à titre d'exercice). Le groupe* G *est appelé le* ***groupe produit*** *des groupes* G_i*. Dans le cas où* $G_1 = \cdots = G_n = G$*, le groupe produit sera noté simplement* G^n*.*

Exercice 1.2.3
Soit $n \in \mathbb{N}^*$*. On désigne par* $(\mathbb{Z}/n\mathbb{Z})^*$ *l'ensemble* $(\mathbb{Z}/n\mathbb{Z})\backslash\{\overline{0}\}$*. Montrer que* $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ *est un groupe si et seulement si* n *est premier.*

Exercice 1.2.4
Soit G *un magma associatif vérifiant les deux assertions suivantes :*

1. $\exists\, e \in G, \forall\, x \in G, x\, e = x$ *(autrement dit,* G *possède un élément neutre à droite* e*).*
2. $\forall\, x \in G, \exists\, x' \in G, x\, x' = e$ *(autrement dit,* x *admet possède un inverse à droite* x'*).*

Montrer que G *est un groupe.*

Exercice 1.2.5
On considère l'ensemble E *des matrices carrées à coefficients réels de la forme*

$$\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}$$

tel que $x \in \mathbb{R}^*$ *et* $y \in \mathbb{R}$*, muni du produit des matrices.*

1. *Montrer que* E *est une partie stable pour le produit des matrices carrées à coefficients réels.*
2. *Déterminer tous les éléments neutres à droite de* E*.*
3. *Montrer que* E *n'admet pas d'élément neutre à gauche.*
4. *Soit* e *un élément neutre à droite. Montrer que tout élément de* E *possède un inverse à gauche pour cet élément neutre, i.e.* $\forall\, g \in E, \exists\, h \in E, hg = e$*.*

Exercice 1.2.6
Soit G *un groupe d'élément neutre* e*.*

1. *Montrer que si* G *est d'ordre pair, alors il existe un élément* $x \in G$ *tel que* $x^2 = e$*.*
2. *On suppose que, pour tout* $x \in G$*,* $x^2 = e$*. Montrer que* G *est commutatif.*

3. *Soit $n \geq 2$ un entier positif. On considère le groupe produit H^n, où H est le groupe additif $\mathbb{Z}/2\mathbb{Z}$. Montrer que le groupe H^n vérifie bien la condition de la dernière question.*

Définition 1.2.7 (Sous-groupe)
Soit H une partie d'un groupe G. On dit que H est un ***sous-groupe*** *de G si les assertions suivantes sont vérifiées :*

1. *$H \neq \emptyset$,*
2. *H est stable pour la loi de G, et*
3. *H muni de la loi induite est un groupe.*

Exemples 1.2.8

1. *Pour tout groupe G d'élément neutre e, les deux ensembles G et $\{e\}$ sont des sous-groupes de G, appelés* ***sous-groupes triviaux*** *de G.*
2. *$(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$.*
3. *$(\mathbb{Q}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.*
4. *$(2\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$.*
5. *L'ensemble des rotations du plan est un sous-groupe du groupe des isométries du plan.*

Proposition 1.2.9
Soit H un sous-groupe d'un groupe G. Alors,

1. *l'élément neutre de H est celui de G.*
2. *L'inverse d'un élément $a \in H$ dans H est celui de a dans G.*

En pratique, pour montrer qu'une partie non vide est un sous-groupe on utilise le résultat important suivant.

Théorème 1.2.10
Soit H une partie ***non vide*** *d'un groupe G. Alors, les assertions suivantes sont équivalentes :*

1. *H est un sous-groupe de G.*
2. *Les assertions suivantes sont vérifiées :*
   (a) *H est stable pour la loi de G.*
   (b) *H est stable par passage à l'inverse (i.e., pour tout $x \in H$, $x^{-1} \in H$).*
3. *Pour tout $(x, y) \in H^2$, $xy^{-1} \in H$.*

Exercice 1.2.11
Montrer que l'ensemble $\{1 + 2m/1 + 2n | n, m \in \mathbb{Z}\}$ est un sous-groupe multiplicatif de $\mathbb{Q}^*$.

Exercice 1.2.12
On munit $E = \mathbb{R}^* \times \mathbb{R}$ de la loi de composition interne $\star$ définie par
$$(a, e) \star (b, f) = (ab, af + e) \text{ pour tout } ((a, e), (b, f)) \in E^2.$$

1. *Montrer que $(E, \star)$ est un groupe non commutatif.*

2. *Soit H un sous-groupe de $(\mathbb{R}^*, \times)$. Montrer que $H \times \mathbb{R}$ est un sous-groupe de E.*

Exercice 1.2.13
Soit G un groupe. Montrer que l'ensemble $Z(G) := \{g \in G | \forall x \in G,\ gx = xg\}$ est un sous-groupe de G.

Proposition et Définition 1.2.14
*Soient G un groupe et $a \in G$. L'ensemble $\{a^n | n \in \mathbb{Z}\}$ est un sous-groupe de G appelé le sous-groupe **monogène** de G engendré par a et noté $< a >$.*
*Si, en particulier, $G = \{a^n | n \in \mathbb{Z}\}$ on dit que G est un groupe **monogène** engendré par a. Si en plus G est d'ordre fini, il sera dit **cyclique**. Dans ce cas, l'ordre de G est dit aussi l'ordre de a et noté simplement par $|a|$ (au lieu de $| < a > |$).*

Il importe de noter que si la loi de G est notée additivement, alors on écrit $< a >= \{na | n \in \mathbb{Z}\}$

Proposition 1.2.15
Les sous-groupes de $(\mathbb{Z}, +)$ sont tous monogènes de la forme $n\mathbb{Z} := \{nk | k \in \mathbb{Z}\}$ où $n \in \mathbb{N}$.

Exercice 1.2.16
Déterminer les sous-groupes de $n\mathbb{Z}$ pour un entier positif n.

Théorème 1.2.17
Soit $G =< a >$ un groupe monogène. Alors, G est d'ordre fini (i.e., G est cyclique) si et seulement s'il existe $k \in \mathbb{N}^*$ tel que $a^k = 1$.
Dans ce cas l'ordre n de a vérifie les assertions suivantes :

1. $n = \min\{k \in \mathbb{N}^* | a^k = 1\}$.
2. $G = \{1, a, a^2, ..., a^{n-1}\}$.
3. *Si $k \in \mathbb{N}^*$ vérifie $a^k = 1$ alors n divise k. Autrement dit, $\{k \in \mathbb{N} | a^k = 1\} = n\mathbb{Z}$.*

Exercice 1.2.18
1. *Montrer que l'ensemble $\{\overline{0}, \overline{9}, \overline{6}, \overline{3}\}$ est un sous-groupe de $\mathbb{Z}/12\mathbb{Z}$.*
2. *Déterminer les sous-groupes $< \overline{2} >$ et $< \overline{3} >$ du groupe multiplicatif $(\mathbb{Z}/7\mathbb{Z})^*$.*
3. *Est-ce que $< \overline{2} > \cup < \overline{6} >$ est aussi un sous-groupe de $(\mathbb{Z}/7\mathbb{Z})^*$?*

Proposition 1.2.19
Soient H et K deux sous-groupes d'un groupe G. Alors,

1. *$H \cap K$ est un sous-groupe de G*
2. *$H \cup K$ est un sous-groupe de G si et seulement si $H \subseteq K$ ou $K \subseteq H$.*

Exercice 1.2.20
Soient n et m deux entiers naturels. Déterminer l'ntersection $n\mathbb{Z} \cap m\mathbb{Z}$.

Exercice 1.2.21
Soient H et K deux sous-groupes d'un groupe G abélien. Supposons que la loi de G est notée additivement. L'ensemble $H + K := \{h + k | h \in H, k \in K\}$ est appelé la somme des sous-groupes H et K.

1. *Montrer que $H + K$ est un sous-groupe de G.*
2. *Déterminer l'ntersection $n\mathbb{Z} + m\mathbb{Z}$ où sont n et m deux entiers naturels.*

Exercice 1.2.22
Soit G un groupe fini d'élément neutre e vérifiant $x^2 = e$ pout $x \in G$. Alors, G est commutatif d'après l'exercice 1.2.6.

1. *Soient H un sous-groupe de G et $g \in G \backslash H$. On pose $gH = \{gh/h \in H\}$.*
   (a) *Montrer que $H \cup gH$ est un sous-groupe de G.*
   (b) *Montrer que $card(gH) = |H|$.*
   (c) *En déduire $|H \cup gH| = 2|H|$.*
2. *On pose $H =< a >$ pour un élément $a \in G$. On considère $g \in G \backslash H$. Déterminer $|H \cup gH|$.*
3. *Montrer que l'ordre de G est une puissance de 2.*

1.3 Morphismes de groupes

Définition 1.3.1 (Morphisme de groupes)
*Soient $(G, *)$ et (G', T) deux groupes. On appelle **morphisme de groupes** ou **homomorphisme de groupes** de G dans G' toute application $\phi : G \longrightarrow G'$ vérifiant : pour tout $(x, y) \in G^2$, $\phi(x * y) = \phi(x) T \phi(y)$.*

Lorsque les lois de G et G' sont notées multiplicativement on écrit simplement $\phi(xy) = \phi(x)\phi(y)$.

Notation et vocabulaire. Soit $\phi : G \longrightarrow G'$ un morphisme de groupes.
— L'ensemble $\phi(G)$ est appelé l'**image** de ϕ et il sera noté $Im(\phi)$.
— Si $G = G'$, alors le morphisme ϕ est appelé **endomorphisme** de G.
— Si ϕ est bijectif, il sera appelé un **isomorphisme** de groupes. Dans ce cas, on dit que G et G' sont isomorphes et on écrit $G \cong G'$.
— Si $G = G'$ et ϕ est un isomorphisme, alors ϕ est appelé un **automorphisme** de G.

Exemples 1.3.2
1. *L'application identité d'un groupe G est un automorphisme de G. Rappelons l'application identité d'un ensemble E (ou application identique de E) est l'application de E dans E, notée Id_E, définie par $\mathrm{Id}_E(x) = x$ pour tout $x \in E$.*
2. *Soit $(G, *)$ un groupe d'élément neutre e. L'application $\phi : x \mapsto e$ est un endomorphisme de G.*
3. *L'application exponentielle est un isomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}^{+*}, \times)$.*
4. *L'application logarithme est un isomorphisme de $(\mathbb{R}^{+*}, \times)$ dans $(\mathbb{R}, +)$.*

Exercice 1.3.3
Soient G un groupe et $g \in G$.

1. *Montrer que l'application $f : \mathbb{Z} \mapsto G$ définie par $f(p) = g^p$ pour tout $p \in \mathbb{Z}$, est un morphisme de groupes.*
2. *Montrer que l'application $\phi : G \longrightarrow G'$, $x \mapsto gxg^{-1}$ est un automorphisme de G. Le morphisme ϕ est appelé un* ***automorphisme intérieur****.*

Proposition 1.3.4
Pour tout morphisme de groupes $\phi : G \longrightarrow G'$, on a :

1. *$\phi(1_G) = 1_{G'}$.*
2. *Pour tout $p \in \mathbb{Z}$ et tout $x \in G$, $\phi(x^p) = \phi(x)^p$.*
   En particulier, $\phi(x^{-1}) = \phi(x)^{-1}$.
3. *Toute image directe d'un sous-groupe de G est un sous-groupe de G'.*
   En particulier, $Im(\phi)$ est un sous-groupe de G'.
4. *Toute image inverse d'un sous-groupe de G' est un sous-groupe de G.*

Proposition 1.3.5

1. *La composée de deux morphismes de groupes est un morphisme de groupes.*
2. *L'inverse d'un isomorphisme de groupes est un isomorphisme de groupes.*
3. *La relation d'isomorphisme de groupes est une relation d'équivalence.*

Théorème 1.3.6

1. *Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.*
2. *Tout groupe cyclique d'ordre n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Il est facile de noter qu'un homomorphisme de groupes $f : G \longrightarrow G'$ est surjectif si et seulement si $Im(f) = G'$ (ce qui est en fait vrai pour n'importe quelle application). Nous allons voir que dans le cas des homomorphismes de groupes, l'injectivité est peut être étudiée en utilisant aussi un ensemble particulier défini comme suit.

Définition 1.3.7 (Noyau)
Soit $f : G \longrightarrow G'$ un homomorphisme de groupes. L'ensemble $f^{-1}(\{1_{G'}\})$ est appelé le ***noyau*** *de f et noté $Ker(f)$.*

Notons, d'après la proposition 1.3.4, $Ker(f)$ est un sous-groupe de G.

Proposition 1.3.8
Soit $f : G \longrightarrow G'$ un homomorphisme de groupes. Alors, f est injectif si et seulement si $Ker(f) = \{1_G\}$.

Exercice 1.3.9

1. *Soient H et K deux groupes et f un homomorphisme de H dans K. Montrer que pour tout $a \in H$, $f(< a >) =< f(a) >$.*
2. *On considère l'application surjectif $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ (où $n \in \mathbb{N}^*$) définie par $\pi(k) = \overline{k}$ pour $k \in \mathbb{Z}$.*
   (a) *Montrer que π est un homomorphisme de groupes additifs et en déterminer le noyau.*

(b) *Montrer que l'image réciproque par π de tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est de la forme $m\mathbb{Z}$ où $m \in \mathbb{N}$ divise n.*

(c) *Déduire l'ensemble des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.*

Exercice 1.3.10

1. *Justifier que $exp : \mathbb{C} \to \mathbb{C}^*$ est un homomorphisme du groupe $(\mathbb{C}, +)$ vers $(\mathbb{C}, \times)$.*
2. *En déterminer l'image et le noyau.*

Exercice 1.3.11

On considère le groupe produit $G = \mathbb{Z} \times \mathbb{Z}$. On définit les deux applications $f : G \to \mathbb{Z}$ et $g : G \to G$ par $f(n, m) = 3n+2m$ et $g(n, m) = (2n-m, 3n-m)$.

1. *Déterminer l'image et le noyau de f.*
2. *Montrer que g est un automorphisme.*

Exercice 1.3.12

Soit G un groupe. Pour tout $g \in G$, on considère l'application

$$\begin{array}{rccc} I_g : & G & \longrightarrow & G \\ & x & \longmapsto & gxg^{-1} \end{array}$$

1. *Montrer que I_g est un automorphisme de G pour tout $g \in G$.*
2. *On considère l'application*

$$\begin{array}{rccc} I : & G & \longrightarrow & Aut(G) \\ & g & \longmapsto & I_g \end{array}$$

(a) *Montrer que I est un homomorphisme de groupes.*

(b) *Montrer que $Ker(I) = \{g \in G | \forall x \in G,\ gx = xg\}$.*

1.4 Engendrement (cas général)

Dans toute cette partie, G désigne un groupe.
Dans cette partie nous allons voir comment construire des sous-groupes à partir des parties d'un groupes. Nous parlons alors d'engendrement d'un sous-groupe à partir d'une partie d'un groupe.

Notons que la relation d'inclusion est un ordre partiel sur l'ensemble des sous-groupes d'un groupe. On montre l'existence du plus petit élément dans l'ensemble des sous-groupes contenant une partie déterminée d'un groupe. Pour cela, on a besoin du résultat suivant.

Proposition 1.4.1

Toute intersection de sous-groupes d'un groupe G est un sous-groupe de G.

Théorème et Définition 1.4.2

Soit S une partie d'un groupe G. L'intersection de tous les sous-groupes de G contenant S est le plus petit sous-groupe (au sens de l'inclusion) de G contenant S. Il sera appelé le ***sous-groupe engendré*** *par S et noté par $< S >$.*

En particulier, $< \emptyset >= \{e\} =< e >$ et $< G >= G$.

Corollaire 1.4.3
Soient S une partie d'un groupe G et H un sous-groupe de G. Alors, $< S > \subset H$ si et seulement si $S \subset H$.

Théorème 1.4.4
Soit S une partie non vide d'un groupe G. Alors,

$$< S >= \{x_1 \cdots x_n | x_i \in S \text{ ou } x_i^{-1} \in S\}$$

En particulier, si $S = \{a\}$, alors $< S >= \{a^n | n \in \mathbb{Z}\}$.

Corollaire 1.4.5
Soit $S = \{x_1, ..., x_n\}$ une partie finie non vide d'un groupe commutatif G. Alors, $< S >= \{x_1^{n_1} \cdots x_n^{n_n} | n_1, ..., n_n \in \mathbb{Z}\}$.

Soient $i, j \in \mathbb{N}_n$ où $n \geq 2$. On appelle transposition de i et de j et on note $\tau_{i,j}$ la permutation de S_n définie par : $\tau_{i,j}(i) = j$, $\tau_{i,j}(j) = i$ et $\tau_{i,j}(k) = k$ pour tout $k \in \mathbb{N}_n - \{i, j\}$.

Théorème 1.4.6
Pour tout entier $n \geq 2$, S_n est engendré par ses transpositions.

Il faut noter que le nombre de transpositions d'une décomposition d'une permutation peut varier. Cependant nous pouvons montrer que la parité de ce nombre reste la même.