كلية العلوم و التقنيات فاس
Faculté des Sciences et Techniques de Fès

جامعة سيدي محمد بن عبد الله
Université Sidi Mohamed Ben Abdellah

Licence Sciences et Techniques (LST)

MATHEMATIQUES ET APPLICATIONS

MEMOIRE DE FIN D'ETUDES

Pour l'obtention du Diplôme de Licence Sciences et Techniques

Exemples de groupes symétriques et d'anneaux classiques

Présenté par :

- **Nom : Radji Bassira**

Encadré par :

- **Encadrant : Pr Najib Mahdou**
- **Co-Encadrant : Pr Adam Anebri**

Soutenu le 08 juillet 2021 devant le jury composé de :

- **Pr Najib Mahdou**
- **Pr Adam Anebri**
- **Pr Abdelmajid Hilali**
- **Pr Lahcen Oukhtite**

Stage effectué à Faculté des sciences et technique de Fès

Année Universitaire 2020/2021

FACULTE DES SCIENCES ET TECHNIQUES FES – SAISS
B.P. 2202 – Route d'Imouzzer – FES
212 (0)5 35 61 16 86 – Fax : 212 (0)5 35 60 82 14
Site web : http://www.fst-usmba.ac.ma

UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH
FACULTÉ DES SCIENCES ET TECHNIQUES,
FES, MAROC

DÉPARTEMENT DE MATHÉMATIQUES

LICENCE MATHÉMATIQUES ET APPLICATIONS

EXEMPLES DE GROUPES SYMÉTRIQUES ET D'ANNEAUX CLASSIQUES

réalisé par : RADJI BASSIRA
dirigé par : Pr. NAJIB MAHDOU

Table des matières

REMERCIEMENTS

J'aimerais tout d'abord exprimer ma profonde gratitude à toute l'équipe pédagogique de la Faculté des Sciences et Techniques de Fès, à tous les professeurs responsables de la filière Mathématiques et Applications et à tous les enseignants auprès de qui j'ai beaucoup appris, qui ont su me donner le meilleur d'eux et qui ont participé de près ou de loin à ma réussite.

Je ne pourrai entamer ce document sans adresser mes sincères remerciements à l'endroit de mon encadrant professeur N. Mahdou pour sa disponibilité, son soutien et ses encouragements qui ont rendu le document ci-présent possible et faisable.
Mes remerciements vont également à l'endroit des membres de jury plus précisément Messieurs A. Anebri, A. Hilali et L. Oukhtite.

Je n'oublie pas également de faire un clin d'œil à ma famille, mes amis qui me portent dans leur cœur et qui aujourd'hui constituent pour moi une source intarissable de bénédictions, de soutien au travers de leurs conseils, leur écoute et surtout leur présence dans tous les domaines de ma vie, ce qui me donne la force d'avancer et de me surpasser. Merci à tous.

DÉDICACES

Je dédie ce modeste travail
À ma mère, la prunelle de mes yeux, celle qui m'a arrosé de tendresse et d'espoirs et m'a béni par dessus tout par ces prières.
À mon père qui m'a appris le sens du travail acharné.
À Monsieur Shabane Akélé pour son amour, son soutien et ses encouragements.
À Monsieur wobenekou Romaric pour tout ce qu'il a fait pour moi et je passe par là pour lui exprimer ma profonde gratitude.
À tous ceux qui ont contribuer de prés ou de loin à la réussite de mes études et à la femme que je suis aujourd'hui.
À tous ceux que j'aime.

Introduction :

Dans le premier chapitre de ce document, nous allons nous intéresser à l'étude des groupes symétriques et y présenter quelques exemples. Il sera donc utile pour nous de connaitre leur histoire, leur origine et surtout leur importance.
Rencontré dans bien de situations mathématiques dès qu'il est besoin de permuter des éléments d'un ensemble fini, l'ensemble S_n a vu sa structure étudiée et nommée (le terme "groupe" fut choisi à cette occasion) par E. Galois en 1832 dans son étude sur la résolution des équations algébriques.
La grande diversité de ses sous-groupes le place au cœur de l'étude des groupes. Il permet notamment d'apporter un éclairage nouveau sur les isométries conservant les polyèdres réguliers (solides de Platon) et son sous-groupe A_n participa à la classification des groupes simples non commutatifs à la fin du 20^e siècle.

Dans la seconde partie, il sera question des anneaux classiques. En mathématiques, la théorie des anneaux porte sur l'étude de structures algébriques qui imitent et étendent les entiers relatifs appelés anneaux. Cette étude s'intéresse notamment à la classification de ces structures, leurs représentations et leurs propriétés. Développée à partir de la fin du 19^e siècle notamment sous l'impulsion de E. Noether, la théorie des anneaux s'est trouvée être fondamentale pour le développement des mathématiques au 20^e siècle au travers de la géométrie algébrique et la théorie des nombres notamment et continue de jouer un rôle central non seulement en mathématiques mais aussi en physique.
Si les anneaux sont nombreux, rares sont ceux disposant des propriétés communes aux exemples les plus simples. L'approche consistant à étudier une question uniquement sous l'angle des propriétés spécifiques d'une structure d'anneau particulière s'est révélée fructueuse. E. Noether choisit donc un nombre plus limité de propriétés vérifiées par certains anneaux et démontre de nombreux résultats sur ceux-ci. D'où la notion d'anneaux classiques.

Chapitre 1

Exemples de Groupes symétriques

1.1 Rappels : Notion de groupes

Avant d'entamer cette partie, nous nous permettons de rappeler néanmoins la définition d'un groupe.

On dit qu'un ensemble muni d'une loi de composition interne (G,T) est un groupe si les axiomes suivants sont vérifiés :
i) La loi T est associative.
ii) Il existe un élément neutre.
iii) Tout élément est symétrisable.

1.2 Groupe symétrique

Soit E un ensemble quelconque. On munit l'ensemble $S(E)$ des bijections de E sur E de la composition des applications. On sait que la composition est associative et que l'application identique est l'élément neutre, comme toute bijection admet une bijection réciproque alors tout élément de $S(E)$ est inversible. Donc $S(E)$ est un groupe pour la composition des applications qu'on appelle groupe symétrique de E.

Théorème 1

Le groupe S_n est fini et l'ordre de S_n qu'on note $|S_n| = n!$.

Dans la suite, on prend $E := \{1, 2, ..., n\}$ et on note $S(E)$ par S_n et un élément de S_n sera dit une permutation.

1.2.1 Représentation d'une permutation

Soit σ une permutation de S_n. On représente σ par une matrice :

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$$

où la première ligne représente l'ensemble de départ, et la seconde ligne l'ensemble d'arrivée. Les éléments de la seconde ligne étant les images des éléments de la première ligne par σ.

L'élément neutre I_d est représenté par :

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix}.$$

1.2.2 Support d'une permutation

Définition 1.2.1

Soit σ un élément de S_n. On appelle support de σ et on note $Supp(\sigma)$, l'ensemble :

$$Supp(\sigma) = \{1 \leq i \leq n / \sigma(i) \neq i\}.$$

Exemple :

Soit

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 4 \end{pmatrix}$$

alors on a :

$$Supp(\sigma) = \{2, 3\}.$$

Proposition 1.2.2
Si deux éléments de S_n ont leurs supports disjoints alors ils commutent.

Remarque 1.2.3
La réciproque de la proposition 1.2.2 est fausse. Par exemple, les permutations $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *et* $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ *commutent et elles ont le même support qui est l'ensemble* $\{1, 2, 3\}$.

1.2.3 Cycles et transpositions

Définition 1.2.4
Soit $p \geq 2$. Un cycle de longueur p est une permutation σ telle qu'il existe $a_1, a_2, ...a_n \in [|1, n|]$, distincts deux à deux de sorte que :
$\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\sigma(a_3) = a_4$,....., $\sigma(a_p) = a_1$. Et pour tout $k \in [|1, n|] \setminus \{a_1, a_2, .., a_n\}$, $\sigma(k) = k$.

Remarque 1.2.5
Le support d'un cycle $\sigma = (x_1, x_2, ..., x_r)$ est $\{x_1, x_2, ..., x_r\}$.

Proposition 1.2.6
Si σ est un cycle de longueur p alors le support de σ est de cardinal p et σ est d'ordre p.

Définition 1.2.7

Soit r un entier naturel compris entre 2 et n.

On appelle cycle d'ordre r (ou r-cycle), toute permutation $\sigma \in S_n$ qui permute circulairement r éléments de $\{1, ..., n\}$ et laisse fixe les autres, c'est à dire qu'il existe une partie $\{x_1, ..., x_r\}$ de $\{1, ..., n\}$ telle que :

$$\begin{cases} \forall k \in \{1, ..., r-1\}, \sigma(x_k) = x_{k+1}, \\ \sigma(x_r) = x_1, \\ \forall x \in E - \{x_1, ..., x_r\}, \sigma(x) = x. \end{cases}$$

On notera :

$$\sigma = (x_1, ..., x_r)$$

un tel cycle et $\{x_1, ..., x_r\}$ est le support de σ.

Exemple

Dans S_6, la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 3 & 6 \end{pmatrix}$ est un $3-cycle$. On le note $(2, 5, 3)$ (ou $(5, 3, 2)$ ou $(3, 2, 5)$).

Remarque 1.2.8

L'inverse d'un r-cycle est un r-cycle de même support. Précisément, on a :

$$(x_1, x_2, ..., x_r)^{-1} = (x_r, x_{r-1}, ..., x_1).$$

Définition 1.2.9

Soient $i, j \in [|1, n|]$ distincts. La transposition sur i et j, notée τ_{ij} est la permutation τ définie par :

$$\begin{cases} \tau(i) = j, \\ \tau(j) = i, \\ \forall k \in [|1, n|] \backslash \{i, j\}, \tau(k) = k. \end{cases}$$

Proposition 1.2.10

Une transposition τ est d'ordre 2 dans le groupe S_n c'est-à-dire $\tau \neq Id$ et $\tau^2 = Id$. On a donc $\tau^{-1} = \tau$.

Remarque 1.2.11

Une transposition est d'ordre 2 mais toute permutation d'ordre 2 n'est pas forcément

une transposition. Par exemple soit :

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}$$

une permutation. L'ordre de θ est égal à 2 ($\theta^2 = Id$) mais θ n'est pas une transposition.

1.2.4 Décomposition d'une permutation

Théorème 2

Toute permutation $\sigma \in S_n - \{Id\}$ se décompose en produit de cycles deux à deux disjoints. Cette décomposition est unique à l'ordre près des facteurs.
Si $\sigma = \gamma_1 ... \gamma_p$ est une telle décomposition, on a alors la partition :

$$Supp(\sigma) = \bigcup_{k=1}^{p} Supp(\gamma_k)$$

et :

$$\theta(\sigma) = ppcm(\theta(\gamma_1), ..., \theta(\gamma_p)).$$

Une telle décomposition s'obtient en prenant, dans le cas où il n'est pas fixe, les images de 1 par σ, σ^2, ..., jusqu'au moment où on retombe sur 1 (l'orbite de 1), puis on recommence avec le plus petit entier dans $\{1, ..., n\} - Orb_\sigma(1)$ qui n'est pas fixe et ainsi de suite.

Définition 1.2.12
Soit $\sigma \in S_n$. On appelle $\sigma -$ orbite de $i \in \{1, ..., n\}$ ou bien orbite de i suivant σ l'ensemble :

$$\Omega_\sigma(i) = \{\sigma^k(i) | k \in \mathbb{N}\}.$$

1.2.5 Système de générateurs de S_n

Théorème 3

Toute permutation $\sigma \in S_n - \{Id\}$ se décompose en produit de transpositions, c'est-à-dire que le groupe S_n est engendré par des transpositions.

Proposition 1.2.13
S_n est engendré par les $n-1$ transpositions $(1,k)$ où $2 \leq k \leq n$.

1.2.6 Signature et ordre d'une permutation

Définition 1.2.14
L'homomorphisme de groupes $\epsilon : S_n \to \{\pm 1\}$ défini par $\epsilon(\tau) = -1$ pour toute transposition τ, est appelé la signature.

Définition 1.2.15
On appelle ordre d'une permutation σ, le plus petit entier naturel non nul k tel que $\sigma^k = Id$.

$A_5 = ker(\epsilon)$ est l'ensemble des permutations paires de $\{1,2,3,4,5\}$.

Définition 1.2.16
L'ensemble $A_n := ker(\epsilon)$ qui est un sous-groupe distingué de S_n est dit le groupe alterné de S_n.

1.3 EXEMPLES

Exemple 1.1

Soient σ et θ les permutations suivantes :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 8 & 3 & 6 & 5 & 4 & 7 & 2 \end{pmatrix}$$

et

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 2 & 5 & 4 & 1 & 6 & 3 & 8 \end{pmatrix}.$$

1) Déterminer les supports de σ et θ.

2) Que peut-on dire de $\sigma \circ \theta$ et $\theta \circ \sigma$?

3) Calculer $\sigma \circ \theta$.

4) Exprimer chacune des deux permutations σ et θ sous forme d'un produit de cycles à supports disjoints.

5) Trouver l'inverse et l'ordre de chacune des permutations σ et θ.

6) Trouver les signatures $\epsilon(\sigma)$ et $\epsilon(\theta)$.

Solution 1.1

1) On sait que le support d'une permutation est l'ensemble noté :

$$Supp(\sigma) = \{1 \leq i \leq 8 / \sigma(i) \neq i\}.$$

Donc

$$Supp(\sigma) = \{2, 4, 6, 8\},$$

et

$$Supp(\theta) = \{1, 3, 5, 7\}.$$

2) On remarque que :

$$Supp(\sigma) \cap Supp(\theta) = \emptyset.$$

C'est-à-dire que leurs supports sont disjoints, on en conclut alors que σ et θ commutent, c'est-à-dire que $\sigma \circ \theta = \theta \circ \sigma$.

3) Calculons $\sigma \circ \theta$. On a :

$$\begin{aligned}\sigma \circ \theta(1) &= \sigma(\theta(1)) \\ &= \sigma(7) \\ &= 7. \\ \sigma \circ \theta(2) &= \sigma(\theta(2)) \\ &= \sigma(2) \\ &= 8.\end{aligned}$$

$$\begin{aligned}\sigma \circ \theta(3) &= \sigma(\theta(3)) \\ &= \sigma(5) \\ &= 5. \\ \sigma \circ \theta(4) &= \sigma(\theta(4)) \\ &= \sigma(4) \\ &= 6.\end{aligned}$$

$$\begin{aligned}\sigma \circ \theta(5) &= \sigma(\theta(5)) \\ &= \sigma(1) \\ &= 1. \\ \sigma \circ \theta(6) &= \sigma(\theta(6)) \\ &= \sigma(6) \\ &= 4.\end{aligned}$$

$$\begin{aligned}\sigma \circ \theta(7) &= \sigma(\theta(7)) \\ &= \sigma(3) \\ &= 3.\end{aligned}$$

$$\begin{aligned}\sigma \circ \theta(8) &= \sigma(\theta(8)) \\ &= \sigma(8) \\ &= 2.\end{aligned}$$

Donc :

$$\sigma \circ \theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 8 & 5 & 6 & 1 & 4 & 3 & 2 \end{pmatrix}.$$

4) Cherchons la décomposition de chacune des permutations σ et θ en produit de cycles à supports disjoints. On a $\sigma = (2,8) \circ (4,6)$ et $\theta = (1,7,3,5)$.

5) Cherchons d'abord l'inverse de chacune des permutations σ et θ.
Si $\alpha = (i,j)$ est une transposition, alors son ordre est égal à 2 donc $\alpha^2 = Id$ et on a $\alpha^{-1} = \alpha$. Donc :

$$\begin{aligned}\sigma^{-1} &= ((2,8) \circ (4,6)))^{-1} \\ &= (4,6)^{-1} \circ (2,8)^{-1}.\end{aligned}$$

Or $(2,8)$ et $(4,6)$ sont des transpositions donc $(4,6)^{-1} = (4,6)$ et $(2,6)^{-1} = (2,6)$.
D'où $\sigma^{-1} = (4,6) \circ (2,6)$.
On sait que l'inverse d'un r-cycle est tel que :

$$(x_1, x_2, ..., x_r)^{-1} = (x_r, x_{r-1}, ..., x_1).$$

On a alors :

$$\begin{aligned}\theta^{-1} &= (1,7,3,5)^{-1} \\ &= (5,3,7,1).\end{aligned}$$

Cherchons l'ordre des permutations σ et θ. On a $\sigma^k = (2,8)^k \circ (4,6)^k$.
Si k est un multiple de 2 alors $(2,8)^k = Id$ et $(4,6)^k = Id$, donc $\sigma^k = Id$ si et seulement si 2 divise k. D'où l'ordre de σ noté $|\sigma| = 2$.
D'autre part, $\theta^k = (1,7,3,5)^k$. Si k est un multiple de 4 alors $\theta^k = Id$. D'où l'ordre de θ est égal à 4.

6) Cherchons la signature des permutations σ et θ. On a :

$$\begin{aligned}\epsilon(\sigma) &= \epsilon((2,8)\circ(4,6)) \\ &= \epsilon(2,8)\times\epsilon(4,6).\end{aligned}$$

Or on sait que la signature d'une transposition est égale à-1. On a alors :

$$\begin{aligned}\epsilon(\sigma) &= (-1)\times(-1) \\ &= 1.\end{aligned}$$

Si σ est une décomposition de la permutation σ en produit de p transpositions alors $\epsilon(\sigma) = (-1)^p$. Or, un cycle d'ordre p se décompose en $p-1$ transpositions. Ainsi $\epsilon(\sigma) = (-1)^{p-1}$.
On a alors :

$$\begin{aligned}\epsilon(\theta) &= \epsilon(1,7,3,5) \\ &= (-1)^{4-1} \\ &= (-1)^3 \\ &= -1.\end{aligned}$$

Exemple 1.2

1) Soit

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 8 & 6 & 4 & 1 & 3 & 7 \end{pmatrix} \in S_8.$$

Exprimer σ en produit de cycles à supports disjoints.
2) Calculer l'ordre et la signature de σ.

Solution 1.2

1) La décomposition de σ en produit de cycles à supports disjoints est :

$$\sigma = (1,2,5,4,6)\circ(3,8,7).$$

2) Cherchons l'ordre de σ. On a :

$$\begin{aligned}\sigma^k &= ((1,2,5,4,6)\circ(3,8,7))^k \\ &= (1,2,5,4,6)^k \circ (3,8,7)^k.\end{aligned}$$

Si k est un multiple de 5, alors $(1,2,5,4,6)^k = Id$. Si k est un multiple de 3, alors $(3,8,7))^k = Id$. D'où $\sigma^k = Id$ si et seulement si 5 divise k et 3 divise k. D'où on a :

$$\begin{aligned}|\sigma| &= ppcm(3,5) \\ &= 3\times 5 \\ &= 15.\end{aligned}$$

D'où l'ordre de σ est égale à 15.
Cherchons la Signature de σ. On a :

$$\begin{aligned}\epsilon(\sigma) &= \epsilon(1,2,5,4,6)\times\epsilon(3,8,7) \\ &= (-1)^{5-1}\times(-1)^{3-1} \\ &= 1\times 1 \\ &= 1.\end{aligned}$$

D'où la signature de σ est égal à 1.

Exemple 1.3

Soit

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}.$$

1) Exprimer σ sous forme de cycles à supports disjoints et calculer son ordre et sa signature.

2) Déterminer $<\sigma>$ le sous groupe engendré par σ.

3) Déterminer $<\sigma> \cap A_5$.

Solution 1.3

1) La décomposition sous forme de produit de cycles à supports disjoints de σ est :

$$\sigma = (1,5,3) \circ (2,4).$$

Cherchons l'ordre de σ.
On a $\sigma^k = (1,5,3)^k \circ (2,4)^k$. Or l'ordre de (2,4) est égal à 2 *car c'est une transposition.* Si k est un multiple de 3 alors $(1,5,3)^k = Id$ donc $\sigma^k = Id$ si et seulement si $k = ppcm(2,3) = 6$. D'où l'ordre de σ est égal à 6.
Cherchons sa signature. On a :

$$\begin{aligned} \epsilon(\sigma) &= \epsilon(1,5,3) \times \epsilon(2,4) \\ &= (-1)^{3-1} \times (-1) \\ &= -1. \end{aligned}$$

2) Le sous-groupe engendré par σ est :

$$< \sigma >= \{Id, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}$$

car $\sigma^6 = Id$.

3) On note que A_5 est le sous-groupe distingué propre de S_5.
$A_5 = ker(\epsilon)$, c'est l'ensemble des permutations paires de $\{1,2,3,4,5\}$ donc $A_5 = \{Id, \sigma^2, \sigma^4\}$. D'où $< \sigma > \cap A_5 = \{Id, \sigma^2, \sigma^4\}$.

Exemple 1.4

Soient σ et $\rho \in S_5$ tels que :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}$$

et

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}.$$

1) Calculer les puissances successives de chacune des permutations σ et ρ puis déterminer l'ordre de chacune.

2 Calculer les puissances successives puis déterminer l'ordre de $\sigma\rho$ et de $\rho\sigma$.

3) Calculer les puissances successives puis déterminer l'ordre de $\sigma\rho^{-1}$ et de $\rho\sigma^{-1}$.

Solution 1.4

1) Calculons les puissances successives et déterminons l'ordre de σ.
Calculons $\sigma^2 = \sigma \circ \sigma$. On a :

$$\begin{aligned} \sigma \circ \sigma(1) &= \sigma(3) \\ &= 2. \\ \sigma \circ \sigma(2) &= \sigma(4) \\ &= 5. \end{aligned}$$

$$\begin{aligned} \sigma \circ \sigma(3) &= \sigma(2) \\ &= 4. \\ \sigma \circ \sigma(4) &= \sigma(5) \\ &= 1. \end{aligned}$$

$$\begin{aligned} \sigma \circ \sigma(5) &= \sigma(1) \\ &= 3. \end{aligned}$$

D'où

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}.$$

Calculons $\sigma^3 = \sigma^2 \circ \sigma$. On a :

$$\begin{aligned}\sigma^2 \circ \sigma(1) &= \sigma^2(3)\\ &= 4.\\ \sigma^2 \circ \sigma(2) &= \sigma^2(4)\\ &= 1.\end{aligned}$$

$$\begin{aligned}\sigma^2 \circ \sigma(3) &= \sigma^2(2)\\ &= 5.\\ \sigma^2 \circ \sigma(4) &= \sigma^2(5)\\ &= 3.\end{aligned}$$

$$\begin{aligned}\sigma^2 \circ \sigma(5) &= \sigma^2(1)\\ &= 2.\end{aligned}$$

D'où

$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix}.$$

Calculons $\sigma^4 = \sigma^3 \circ \sigma$. On a :

$$\begin{aligned}\sigma^3 \circ \sigma(1) &= \sigma^3(3)\\ &= 5.\\ \sigma^3 \circ \sigma(2) &= \sigma^3(4)\\ &= 3.\end{aligned}$$

$$\begin{aligned}\sigma^3 \circ \sigma(3) &= \sigma^3(2)\\ &= 1.\\ \sigma^3 \circ \sigma(4) &= \sigma^3(5)\\ &= 2.\end{aligned}$$

$$\begin{aligned}\sigma^3 \circ \sigma(5) &= \sigma^3(1)\\ &= 4.\end{aligned}$$

D'où

$$\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}.$$

Calculons maintenant $\sigma^5 = \sigma^4 \circ \sigma$. On a :

$$\begin{aligned}\sigma^4 \circ \sigma(1) &= \sigma^4(3)\\ &= 1.\\ \sigma^3 \circ \sigma(2) &= \sigma^3(4)\\ &= 2.\end{aligned}$$

$$\begin{aligned}\sigma^3 \circ \sigma(3) &= \sigma^3(2)\\ &= 3.\\ \sigma^3 \circ \sigma(4) &= \sigma^3(5)\\ &= 4.\end{aligned}$$

$$\begin{aligned}\sigma^3 \circ \sigma(5) &= \sigma^3(1)\\ &= 5.\end{aligned}$$

D'où

$$\sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = Id.$$

On en déduit que l'ordre de σ est égal à 5.
Calculons à présent les puissances successives de ρ et déterminons son l'ordre.
Commençons par calculer $\rho^2 = \rho \circ \rho$. On a :

$$\begin{aligned} \rho \circ \rho(1) &= \rho(5) \\ &= 3. \\ \rho \circ \rho(2) &= \rho(4) \\ &= 2. \end{aligned}$$

$$\begin{aligned} \rho \circ \rho(3) &= \rho(1) \\ &= 5. \\ \rho \circ \rho(4) &= \rho(2) \\ &= 4. \end{aligned}$$

$$\begin{aligned} \rho \circ \rho(5) &= \rho(3) \\ &= 1. \end{aligned}$$

D'où

$$\rho^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}.$$

Calculons ensuite $\rho^3 = \rho^2 \circ \rho$. On a :

$$\begin{aligned} \rho^2 \circ \rho(1) &= \rho^2(5) \\ &= 1. \\ \rho^2 \circ \rho(2) &= \rho^2(4) \\ &= 4. \end{aligned}$$

$$\begin{aligned}\rho^2 \circ \rho(3) &= \rho^2(1)\\ &= 3.\\ \rho^2 \circ \rho(4) &= \rho^2(2)\\ &= 2.\end{aligned}$$

$$\begin{aligned}\rho^2 \circ \rho(5) &= \rho^2(3)\\ &= 5.\end{aligned}$$

D'où

$$\rho^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}.$$

Ensuite, $\rho^4 = \rho^3 \circ \rho$. On a :

$$\begin{aligned}\rho^3 \circ \rho(1) &= \rho^3(5)\\ &= 5.\\ \rho^3 \circ \rho(2) &= \rho^3(4)\\ &= 2.\end{aligned}$$

$$\begin{aligned}\rho^3 \circ \rho(3) &= \rho^3(1)\\ &= 1.\\ \rho^3 \circ \rho(4) &= \rho^3(2)\\ &= 4.\end{aligned}$$

$$\begin{aligned}\rho^3 \circ \rho(5) &= \rho^3(3)\\ &= 3.\end{aligned}$$

D'où

$$\rho^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}.$$

Maintenant calculons $\rho^5 = \rho^4 \circ \rho$. On a :

$$\begin{aligned}\rho^4 \circ \rho(1) &= \rho^4(5)\\ &= 3.\\ \rho^4 \circ \rho(2) &= \rho^4(4)\\ &= 4.\end{aligned}$$

$$\begin{aligned}\rho^4 \circ \rho(3) &= \rho^4(1)\\ &= 5.\\ \rho^4 \circ \rho(4) &= \rho^4(2)\\ &= 2.\end{aligned}$$

$$\begin{aligned}\rho^4 \circ \rho(5) &= \rho^4(3)\\ &= 1.\end{aligned}$$

D'où

$$\rho^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}.$$

Enfin, calculons $\rho^6 = \rho^5 \circ \rho$. On a :

$$\begin{aligned}\rho^5 \circ \rho(1) &= \rho^5(5)\\ &= 1.\\ \rho^5 \circ \rho(2) &= \rho^5(4)\\ &= 2.\end{aligned}$$

$$\begin{aligned}\rho^5 \circ \rho(3) &= \rho^5(1)\\ &= 3.\\ \rho^5 \circ \rho(4) &= \rho^5(2)\\ &= 4.\end{aligned}$$

$$\begin{aligned}\rho^5 \circ \rho(5) &= \rho^5(3)\\ &= 5.\end{aligned}$$

D'où on a :

$$\rho^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = Id.$$

On en déduit que l'ordre de ρ est égal à 6.

2) Calculons les puissances successives puis déterminons l'ordre de $\sigma\rho$, $\rho\sigma$.

On a :

$$\begin{aligned}\sigma\rho(1) &= \sigma(5)\\ &= 1.\\ \sigma\rho(2) &= \sigma(4)\\ &= 5.\end{aligned}$$

$$\begin{aligned}\sigma\rho(3) &= \sigma(1)\\ &= 3.\\ \sigma\rho(4) &= \sigma(2)\\ &= 4.\end{aligned}$$

$$\begin{aligned}\sigma\rho(5) &= \sigma(3)\\ &= 2.\end{aligned}$$

Donc on a :

$$\sigma\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}.$$

Puisque $(\sigma\rho)^2 = \sigma\rho \circ \sigma\rho$, alors on a :

$$\begin{aligned} \sigma\rho \circ \sigma\rho(1) &= \sigma\rho(1) \\ &= 1. \\ \sigma\rho \circ \sigma\rho(2) &= \sigma\rho(5) \\ &= 2. \end{aligned}$$

$$\begin{aligned} \sigma\rho \circ \sigma\rho(3) &= \sigma\rho(3) \\ &= 3. \\ \sigma\rho \circ \sigma\rho(4) &= \sigma\rho(4) \\ &= 4. \end{aligned}$$

$$\begin{aligned} \sigma\rho \circ \sigma\rho(5) &= \sigma\rho(2) \\ &= 5. \end{aligned}$$

Donc $(\sigma\rho)^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix} = Id$. On en conclut que l'ordre de $\sigma\rho$ est égal à 2. Ensuite, on a :

$$\begin{aligned} \rho\sigma(1) &= \rho(3) \\ &= 1. \\ \rho\sigma(2) &= \rho(4) \\ &= 2. \end{aligned}$$

$$\begin{aligned}\rho\sigma(3) &= \rho(2)\\ &= 4.\\ \rho\sigma(4) &= \rho(5)\\ &= 3.\end{aligned}$$

$$\begin{aligned}\rho\sigma(5) &= \rho(1)\\ &= 5.\end{aligned}$$

D'où on a :

$$\rho\sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 4 & 3 & 5\end{pmatrix}.$$

Par ailleurs, $(\rho\sigma)^2$ donne :

$$\begin{aligned}\rho\sigma \circ \rho\sigma(1) &= \rho\sigma(1)\\ &= 1.\\ \rho\sigma \circ \rho\sigma(2) &= \rho\sigma(2)\\ &= 2.\end{aligned}$$

$$\begin{aligned}\rho\sigma \circ \rho\sigma(3) &= \rho\sigma(4)\\ &= 3.\\ \rho\sigma \circ \rho\sigma(4) &= \rho\sigma(3)\\ &= 4.\end{aligned}$$

$$\begin{aligned}\rho\sigma \circ \rho\sigma(5) &= \rho\sigma(5)\\ &= 5.\end{aligned}$$

Donc $(\rho\sigma)^2 = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 5 & 3 & 4 & 2\end{pmatrix} = Id$. Il en résulte que l'ordre de $\rho\sigma$ est égal à 2.

3) Calculons les puissances successives puis déterminons l'ordre de $\sigma\rho^{-1}$ et de $\rho\sigma^{-1}$. Puisque $\rho^6 = Id$, alors on a :

$$\begin{aligned}\rho^5 \circ \rho &= \rho \circ \rho^5 \\ &= Id,\end{aligned}$$

donc $\rho^{-1} = \rho^5$. Par suite, on a :

$$\begin{aligned}\sigma\rho^{-1} &= \sigma \circ \rho^{-1} \\ &= \sigma \circ \rho^5.\end{aligned}$$

Ce qui donne :

$$\begin{aligned}\sigma \circ \rho^5(1) &= \sigma(3) \\ &= 2. \\ \sigma \circ \rho^5(2) &= \sigma(4) \\ &= 5.\end{aligned}$$

$$\begin{aligned}\sigma \circ \rho^5(3) &= \sigma(5) \\ &= 1. \\ \sigma \circ \rho^5(4) &= \sigma(2) \\ &= 4.\end{aligned}$$

$$\begin{aligned}\sigma \circ \rho^5(5) &= \sigma(1) \\ &= 3.\end{aligned}$$

Donc :

$$\sigma\rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}.$$

On a $(\sigma\rho^{-1})^2 = \sigma\rho^{-1} \circ \sigma\rho^{-1}$. Donc il s'en suit que :

$$\begin{aligned}\sigma\rho^{-1} \circ \sigma\rho^{-1}(1) &= \sigma\rho^{-1}(2)\\ &= 5.\\ \sigma\rho^{-1} \circ \sigma\rho^{-1}(2) &= \sigma\rho^{-1}(5)\\ &= 3.\\ \sigma\rho^{-1} \circ \sigma\rho^{-1}(3) &= \sigma\rho^{-1}(1)\\ &= 2.\\ \sigma\rho^{-1} \circ \sigma\rho^{-1}(4) &= \sigma\rho^{-1}(4)\\ &= 4.\\ \sigma\rho^{-1} \circ \sigma\rho^{-1}(5) &= \sigma\rho^{-1}(3)\\ &= 1.\end{aligned}$$

Par conséquent, $(\sigma\rho^{-1})^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$.
$(\sigma\rho^{-1})^2 = (1,5) \circ (2,3)$. On remarque que $(\sigma\rho^{-1})^2$ est une permutation qui permute à la fois 2,3 et 1,5 donc $((\sigma\rho^{-1})^2)^2 = Id$ implique que $(\sigma\rho^{-1})^4 = Id$. D'où l'ordre de $\sigma\rho^{-1}$ est égal à 4.

Le fait que $\sigma^5 = Id$ montre que $\sigma \circ \sigma^4 = Id$ et que $\sigma^{-1} = \sigma^4$. En outre, on a $\rho\sigma^{-1} = \rho \circ \sigma^4$. Dès lors, on a :

$$\begin{aligned}\rho \circ \sigma^4(1) &= \rho(5)\\ &= 3.\\ \rho \circ \sigma^4(2) &= \rho(3)\\ &= 1.\\ \rho \circ \sigma^4(3) &= \rho(1)\\ &= 5.\\ \rho \circ \sigma^4(4) &= \rho(2)\\ &= 4.\\ \rho \circ \sigma^4(5) &= \rho(4)\\ &= 2.\end{aligned}$$

D'où :

$$\rho\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}.$$

On constate que :

$$\begin{aligned}(\rho\sigma^{-1})^{-1} &= (\sigma^{-1})^{-1}\rho^{-1} \\ &= \sigma\rho^{-1}.\end{aligned}$$

On en déduit que $\rho\sigma^{-1}$ et $\sigma\rho^{-1}$ ont le même ordre. D'où l'ordre de $\rho\sigma^{-1}$ est égal à 4.

Exemple 1.5

Démontrer que A_n est engendré par les cycles de longueur 3 (pour $n \geq 3$).

Solution 1.5

On sait que les éléments de A_n sont des produits pairs de transpositions. Montrons qu'un produit de 2 transpositions est un produit de cycles de longueur 3.
Soient i, j, k, 3 éléments deux à deux distincts de $\{1, 2, ..., n\}$. $\tau_{ik} \circ \tau_{ij}$ est le cycle $i \to j$, $j \to k$, $k \to i$, ce qui implique qu'un $3 - cycle$ est pair et le produit de 2 transpositions dont les supports ont en commun un singleton est un $3 - cycle$.
Étudions le produit de 2 transpositions à supports disjoints. Soient i, j, k, l, 4 éléments distincts deux à deux de $\{1, 2, ..., n\}$. On a :

$$\begin{aligned}\tau_{ij} \circ \tau_{kl} &= (jikl)(ijlk) \\ &= (jkil)(ljik).\end{aligned}$$

Donc $\tau_{ij} \circ \tau_{kl}$ est bien un produit de 3-cycle. D'où A_n est engendré par les cycles de longueur 3 (pour $n \geq 3$).

Chapitre 2

Exemples d'anneaux classiques

Avant de commencer cette partie, nous jugeons important de rappeler de manière brève la notion d'anneaux.

2.1 Rappels : Notion d'anneaux

Définition 2.1.1
On appelle anneau la donnée d'un ensemble A muni de deux lois de composition internes, une addition et une multiplication telles que :
i) A est un groupe commutatif pour l'addition.
ii) La multiplication est associative.
iii) La multiplication est distributive par rapport à l'addition, c'est à dire que pour tous $x, y, z \in A$, on a : $x(y+z) = xy + xz$ et $(y+z)x = yx + zx$.

Si en outre, la multiplication est commutative, on dit que A est un anneau commutatif.
Si A possède un élément neutre pour la multiplication, on note 1 cet élément unité et on dit que A est un anneau unitaire.

2.1.1 Notion d'idéaux premiers et maximaux

La notion d'idéal joue un rôle central dans la théorie des anneaux. On a la caractérisation suivante :

Théorème 4

Soient A un anneau commutatif unitaire et P un idéal de A.
1. P est premier si et seulement s'il vérifie l'une des conditions équivalentes suivantes :
i) A/P est intègre.
ii) Pour tous a, b $\in P$, $ab \in P$ implique que $a \in P$ ou $b \in P$.
2. P est maximal si et seulement si A/P est un corps.

Remarque 2.1.2
Tout idéal de A différent de $\{0\}$ et de A est dit un idéal propre de A.

2.1.2 Morphisme d'anneaux

Définition 2.1.3
Soient A et B deux anneaux. Une application $\rho : A \to B$ est un morphisme si :

1. $\rho(a+b) = \rho(a) + \rho(b)$ *pour tous* $a, b \in A$,
2. $\rho(ab) = \rho(a)\rho(b)$,
3. $\rho(1_A) = 1_B$.

2.1.3 Noyau et Image d'un morphisme d'anneaux

Soient A et B deux anneaux. Soit $\rho : A \to B$ est un morphisme d'anneaux.

Définition 2.1.4

1. *On appelle noyau d'un morphisme d'anneaux ρ l'ensemble noté $ker(\rho)$ tel que $ker(\rho) = \{a \in A; \rho\ (a) = 0\}$.*
2. *On appelle image d'un morphisme d'anneaux ρ l'ensemble noté $Im(\rho)$ tel que $Im(\rho) = \{\rho(a); a \in A\}$.*

Un morphisme bijectif est appelé un isomorphisme.
Un endomorphisme est un morphisme de l'anneau vers lui-même.
Un automorphisme est un endomorphisme bijectif.

Théorème 5

1. Un morphisme d'anneaux ρ est injectif si et seulement si son noyau $(ker(\rho))$ est nul.
2. Un morphisme d'anneaux $\rho : A \to B$ est surjectif si et seulement si $Im(\rho) = B$.

Remarque 2.1.5
Le noyau d'un morphisme d'anneau est un idéal.

2.2 Anneau Noethérien

On considère les anneaux de cette partie commutatifs et unitaires.

Pour définir les anneaux Noethériens, on commence par la caractérisation suivante :

Théorème 6

Soit A un anneau. Les assertions suivantes sont équivalentes :

1. Toute suite croissante d'idéaux de A est stationnaire.
2. Tout idéal de A est de type fini.

Définition 2.2.1
On dit qu'un anneau A est Noethérien s'il vérifie les conditions équivalentes du Théorème précédent.

Concernant la Noethérianité des anneaux de polynômes, on a le Théorème important suivant :

Théorème 7 (Théorème de Hilbert)

Soient A un anneau Noethérien et X une indéterminée sur A. Alors $A[X]$ est Noethérien.

Remarque 2.2.2
Si A est Noethérien, alors l'anneau $A[[X]]$ des séries formelles à coefficients dans A est Noethérien.

Du Théorème de Hilbert, on déduit le corollaire suivant :

Corollaire 2.2.3
Soient A un anneau Noethérien et $X_1, ..., X_n$ des indéterminées sur A. Alors $A[X_1, ..., X_n]$ est un anneau Noethérien.

On a la caractérisation importante suivante des anneaux Noethériens par le biais de leurs idéaux premiers :

Théorème 8

Un anneau A est Noethérien si et seulement si tout idéal premier de A est de type fini.

Proposition 2.2.4
Tout anneau quotient d'un anneau Noethérien est Noethérien.

On a la proposition suivante :

Proposition 2.2.5
Soit A un anneau fini, A est intègre si et seulement si A est un corps.

2.3 Anneau local

Théorème 9

Un anneau A est dit local si et seulement si les éléments non inversibles de A forment un unique idéal (qui sera alors l'idéal maximal de A).

Exemple :

- Tout corps commutatif est un anneau local, d'idéal maximal (0).
- Pour tout corps commutatif K, l'anneau $K[[X_1, \ldots, X_n]]$ des séries formelles à coefficients dans K et à n variables est un anneau local dont l'idéal maximal est engendré par $X_1, \ldots, X_n$.

On a la proposition suivante :

Proposition 2.3.1
Dans un anneau local, tout idéal inversible est principal.

2.4 Anneau principal

Définition 2.4.1

1. *Un anneau A est dit principal si tout idéal de A est principal, c'est à dire que pour tout idéal I de A, on a $I =< a >$ pour un certain $a \in I$.*
2. *Un anneau principal et intègre est dit un domaine principal.*

On a la caractérisation suivante :

Théorème 10

Un anneau intègre A est principal si et seulement si tout idéal premier non nul de A est maximal.

2.5 Anneau euclidien

Définition 2.5.1
Soit A un anneau commutatif et intègre. On dit que A est euclidien s'il existe une application $v : A - \{0\} \longrightarrow \mathbb{N}$ telle que pour tous $a, b \in A - \{0\}$, il existe $q, r \in A$ tels que $a = bq + r$ et $r = 0$ ou $v(r) < v(b)$.

Exemple : L'anneau $\mathbb{Z}$, muni de la division euclidienne usuelle est euclidien : application $v : \mathbb{Z} \longrightarrow \mathbb{N}$ est la valeur absolue.

Proposition 2.5.2
Tout anneau euclidien A est principal.

2.6 EXEMPLES

Exemple 2.1

Soit A un anneau commutatif.
1) Si $A[X]$ est Noethérien, A est-il nécessairement Noethérien ?

2) Si $A[X]$ est un domaine principal, que peut-on dire de A ?

Solution 2.1

1) On sait que tout anneau quotient d'un anneau Noethérien est Noethérien. Puisque $A \cong A[X]/ < X >$ et $A[X]$ est Noethérien, alors A est Noethérien.

2) Supposons que $A[X]$ est un domaine principal.
Alors $A[X]$ est intègre, ce qui prouve que A l'est aussi *(car A est contenu dans $A[X]$)*. Par conséquent $A[X]/ < X > \cong A$ est intègre. Ce qui revient à dire que $< X >$ est un idéal premier de $A[X]$. Or dans un anneau principal, tout idéal premier non nul est maximal. Donc $< X >$ est un idéal maximal de $A[X]$, ce qui veut dire que $A[X]/ < X >$ est un corps. D'où A est un corps.

Exemple 2.2

Soit A un anneau commutatif.
1) Pour $a \in A$ et I un idéal de A, montrer que si les idéaux $I+ < a >$ et $(I : a) := \{x \in A, ax \in I\}$ sont de type fini, alors I l'est.

2) Montrer que A est Noethérien si et seulement si tous ses idéaux premiers sont de type fini.
Indication : Considérer un idéal maximal parmi ceux qui ne sont pas de type fini.

Solution 2.2

1) Soit A un anneau commutatif. Supposons que $I+ < a >$ est de type fini. Soient $z_1, z_2, ...z_n$ des générateurs de $I+ < a >$. On peut alors écrire $z_i = x_i + aa_i$ avec $x_i \in I$ et $a_i \in A$. Supposons maintenant que $(I : a) := \{x \in A, ax \in I\}$ est de type fini. Soient $y_1, y_2, ...y_n$ des générateurs de $(I : a)$. On a $ay_i \in I$. Montrons que $I = (x_1, ...x_n, ay_1, ...ay_n)$.
Procédons par la double inclusion.
On a $(x_1, ...x_n, ay_1, ...ay_n) \subset I$ *car* $ay_i \in I$. Montrons alors que $I \subset (x_1, ...x_n, ay_1, ...ay_n)$.
Soit $u \in I$. On a $u \in I+ < a >$ et donc $u = \sum_i u_i x_i + ta$ *(avec $t \in A$)* ce qui im-

plique que $ta = (u - \sum_i u_i x_i) \in I$. Par suite, $t \in (I : a)$, ce qui équivaut à dire que $t = \sum_j t_j y_j$ où $t_j \in A$. On obtient alors :

$$\begin{aligned} u &= \sum_i u_i x_i + \sum_j t_j y_j a \\ &= \sum_i u_i x_i + \sum_j t_j (y_j a), \end{aligned}$$

ce qui implique que $u \subset (x_1, ...x_n, ay_1, ...ay_n)$. D'où $I = (x_1, ...x_n, ay_1, ...ay_n)$. On conclut que si $I + < a >$ et $(I : a)$ sont de types finis alors I est également de type fini.

2) Par définition, si A est Noethérien, tous ses idéaux *(en particulier ses idéaux premiers)* sont de type fini. Inversement, supposons que les idéaux premiers de A sont de type fini et montrons que A est Noethérien. Soit F l'ensemble des idéaux de A qui ne sont pas de type fini. Montrons que $F = \emptyset$. Supposons que $F \neq \emptyset$. Si (I_n) est une suite croissante d'idéaux qui ne sont pas de type fini, alors $I = \cup I_n$ n'est pas de type fini. L'ensemble F étant ordonné par l'inclusion et étant inductif, il existe un ou plusieurs élément(s) maximal(aux) dans l'ensemble F d'après le lemme de Zorn. Rappelons que le lemme de Zorn stipule que si un ensemble ordonné est tel que toute chaine ou sous-ensemble totalement ordonné possède un majorant alors il possède un élément maximal. Soit I un tel élément maximal de F ($I \in F$), il n'est pas de type fini donc n'est pas premier. *On sait que I est premier si pour tous a, b $\in I$, $ab \in I$ implique que $a \in I$ ou $b \in I$*. Le complémentaire de cette définition nous donne I n'est pas premier implique qu'il existe $a, b \notin I$ tel que $ab \in I$. On a alors $I \subset I + < a >$, donc $I + < a >$ est de type fini. De plus $I \subset (I : a)$ et $b \in (I : a)$ (car pour tout $b \in A$, $ab \in I$), $b \notin I$ ce qui implique que $I \subsetneq (I : a)$ et $(I : a)$ est de type fini. D'après la question 1), on peut dire que I est de type fini. Ce qui est une contradiction. Donc $F = \emptyset$, c'est-à-dire que tous les idéaux de A sont de type fini. D'où A est Noethérien.

Exemple 2.3

Soit A un anneau local dont l'idéal maximal m est principal, engendré par a.
1) Montrer que $u \in A$ est inversible si et seulement si $u \notin m$.

2) Supposons que $\cap_{n>0} m^n = 0$.
a) Montrer que tout $x \in A$ non nul s'écrit sous la forme $x = ua^n$ avec $u \in A$ et $n \in \mathbb{N}$ et que cette écriture est unique si A est intègre.
b) Montrer que tout idéal I est de la forme $< a^n >$. En conclure que A est Noethérien et même principal s'il est intègre.
c) Montrer que l'anneau des séries formelles $\mathbb{Q}[[X]] := \{f = \sum_{n\in\mathbb{N}} a_n X^n\}$ est Noethérien.

3) Supposons maintenant que A est Noethérien.
a) Montrer que si I est un idéal tel que $m.I = I$, alors $I = 0$. On pourra raisonner par l'absurde sur un ensemble minimal $x_1, ...x_n$ de générateurs de I et écrire que $x_n \in m.I$ pour aboutir à une contradiction.
b) Montrer que $\cap_{n>0} m^n = 0$.

Solution 2.3

Soit A un anneau local dont l'idéal maximal m est principal, engendré par a.
1) Le fait que A est local implique que les éléments non inversibles de A forment un unique idéal qui sera l'idéal maximal de A. Si $u \in A$ est inversible, il ne peut appartenir à m (sinon m=A, car tout idéal qui contient un élément inversible est égal à tout l'anneau entier), donc $u \notin A$.
Par contre, si $u \in A$ n'est pas inversible, il existe alors un idéal maximal contenant u. Compte tenu de l'unicité de l'idéal maximal m, on en déduit que $u \in m$. D'où $u \in A$ est inversible si et seulement si $u \notin m$.

2) Supposons que $\cap_{n>0}\ m^n = 0$.
a) Soit $x \in A$ non nul. $\cap_{n>0}\ m^n = 0$ implique qu'il y a un $k \in \mathbb{N}$ tel que $x \notin m^k$. Soit $n \in \mathbb{N}$ le plus grand entier tel que $x \in m^n$. Le fait que $x \in m^n$ implique que $x = ua^n$ et $u \notin m$ (car sinon $x \in m^{n+1}$). Ainsi d'après 1), u est inversible, ce qui signifie que pour tout $x \in A$, on a toujours une écriture sous la forme $x = ua^n$.
Prouvons l'unicité de cette écriture lorsque A est intègre.
Supposons que A est intègre. Soient deux écritures de x telles que $x = ua^n$ et

$x = va^m$ avec $u, v \in A$. Supposons par exemple que $m \geq n$. On a :

$$\begin{aligned} x &= ua^n \\ &= va^m, \end{aligned}$$

ce qui implique que $u = va^{m-n}$. Et comme u est inversible, ceci impose nécessairement $m = n$ puis $u = v$. D'où l'unicité de l'écriture lorsque A est intègre.

b) Soit I un idéal. Pour tout $x \in I$, définissons n_x le plus grand entier tel que $x \in m^{n_x}$. Soit $n = min\ \{n_x / x \in I\}$. Si $x \in I$, alors $x = ua^{n_x}$ avec u inversible et $n_x \geq n$. On a : $x = ua^{n_x - n}a^n$, ce qui implique que $x \in < a^n >$. Ainsi $I \subset < a^n >$.
Comme $n = min\ \{n_x / x \in I\}$, il existe forcément un $x \in I$ tel que $n_x = n$. Ainsi $x = ua^n$ où u est inversible. L'idéal I contient donc $< a^n >$. On en déduit que $I =< a^n >$. On vient donc de voir que tout idéal de A est principal c'est-à-dire engendré par a donc tout idéal de A est de type fini. On déduit que A est Noethérien. Si de plus A est intègre, alors A sera principal.

c) Montrons d'abord que l'idéal $< X >$ est l'unique idéal maximal de $\mathbb{Q}[[X]]$.
Puisque X n'est pas inversible (sinon l'idéal $< X >$ sera égal à tout l'anneau $\mathbb{Q}[[X]]$), c'est au moins un idéal propre. Il suffit de prouver que son complémentaire ne contient que des éléments inversibles, c'est-à-dire que toute série formelle à terme constant non nul est inversible.
Écrivons une telle série formelle sous la forme :

$$\begin{aligned} f &= a(1 + a_1X + ...a_nX^n + ..) \\ &= a(1 + n(X)), \end{aligned}$$

alors $g = a^{-1}(1 - n(X) + n(X)^2 - ..... + (-1)^n n(X)^n + ...)$ est une série formelle bien définie. Plus précisément, on a $g = a^{-1}(1 + \sum_{d \geq 1} b_d X^d)$ avec b_d le coefficient de x^d dans le polynôme $\sum_{i=1}^{d} (-1)^i n(X)^i$. On remarque que $\cap_{n \in \mathbb{N}} < X >^n = 0$ car c'est l'ensemble des séries formelles dont tous les coefficients sont nuls.
Pour pouvoir appliquer le résultat de la question 2), il suffit de montrer que $\mathbb{Q}[[X]]$ est intègre. Pour cela, il suffit de montrer que X n'est pas un diviseur de 0, ce qui est clair puisque la multiplication par X revient à décaler les coefficients d'un degré.

3) On suppose que A est Noethérien
a) Soit I un idéal tel que $m.I = I$ et soit $(x_1, ..., x_n)$ un ensemble minimal de générateurs de I. Puisque $I = m.I$, alors $x_n \in mI$ c'est-à-dire qu'on peut écrire un x_n quelconque sous la forme : $x_n = m_1x_1 + ... + m_nx_n$ avec $m_i \in m =< a >$. Il s'en suit que $x_n - m_nx_n = m_1x_1 + ... + m_{n-1}x_{n-1}$ ce qui implique que $(1 - m_n)x_n = m_1x_1 + ... + m_{n-1}x_{n-1}$. Or $1 - m_n \notin m$ donc d'après la question 1), $1 - m_n$ est inversible. On a $x_n = (1 - m_n)^{-1}m_1x_1 + ... + (1 - m_n)^{-1}m_{n-1}x_{n-1}$. Si a est son inverse, alors $x_n = am_1x_1 + ... + am_{n-1}x_{n-1}$, cela implique que I est engendré par $(x_1, ..., x_{n-1})$, ce qui contredit la minimalité de la famille $(x_1, ...x_n)$.

b) Soit $I = \cap_{n>0}m^n$. Alors on a :

$$\begin{aligned} m.I &= \cap_{n>0}m^{n+1} \\ &= \cap_{n>0}m^n m \\ &= I, \end{aligned}$$

donc d'après la question précédente $I = 0$. D'où $\cap_{n>0}m^n = 0$.

Exemple 2.4

Soit $\rho : A \longrightarrow A$ un morphisme d'anneaux.
1) On suppose que A est Noethérien, montrer qu'il existe un entier $n \geq 1$ tel que $ker(\rho^n) = ker(\rho^{n+1})$. En déduire que l'application $\rho : Im(\rho^n) \longrightarrow Im(\rho^{n+1})$ est injective.

2) Montrer que si ρ est surjective et A est Noethérien, alors elle est bijective.

3) Montrer qu'on ne peut remplacer dans la question précédente l'hypothèse "surjective" par "injective".

4) Montrons que l'on ne peut se passer de l'hypothèse Noethérien (considérer par exemple $A = k[X_1, ...X_n, ...]$ un anneau de polynômes à une infinité de variables et ρ convenable).

Solution 2.4

1) Considérons la suite des noyaux $(ker(\rho^n))_{n\in\mathbb{N}}$. C'est une suite croissante d'idéaux de A (car $ker(\rho)$ est un idéal de A), où $ker(\rho^n) = \{x \in A, \rho^n(x) = 0\}$.
En effet, si $x \in ker(\rho^n)$ alors on a :

$$\begin{aligned}\rho^{n+1}(x) &= \rho(\rho^n(x)) \\ &= \rho(0) \\ &= 0.\end{aligned}$$

Dès lors on a $ker(\rho^n) \subseteq ker(\rho^{n+1})$.
Comme A est Noethérien, cette suite croissante d'idéaux est stationnaire (d'après la définition d'un anneau Noethérien) donc il existe $n_0 \in \mathbb{N}$ tel que pour tout $n \geq n_0$, on ait $ker(\rho^n) = ker(\rho^{n_0})$. Considérons l'application $\rho : Im(\rho^{n_0}) \longrightarrow Im(\rho^{n_0+1})$ dont le noyau est $ker(\rho) \cap Im(\rho^{n_0})$. Or on a :
$ker(\rho) \cap Im(\rho^{n_0}) = \{x \in Im(\rho^{n_0}),\ \rho(x) = 0\}$. Dès lors $x \in ker(\rho) \cap Im(\rho^{n_0})$ implique :

$$\begin{cases} x \in ker(\rho) \\ x \in Im(\rho^{n_0}). \end{cases}$$

Ce qui implique que $x = \rho^{n_0}(y)$ et $\rho(x) = 0$. On a alors :

$$\begin{aligned}\rho(x) &= \rho(\rho^{n_0}(y)) \\ &= \rho^{n_0+1}(y) \\ &= 0.\end{aligned}$$

Ceci implique que $y \in ker(\rho^{n_0+1}) = ker(\rho^{n_0})$, d'après la première question. Donc $y \in ker(\rho^{n_0})$ implique $\rho^{n_0}(y) = 0$. Ainsi, $x = \rho^{n_0}(y) = 0$, on déduit que l'application est injective. D'où $\rho : Im(\rho^n) \longrightarrow Im(\rho^{n+1})$ est injective.

2) Si on suppose que ρ est surjective alors on voit que ρ^{n_0} et ρ^{n_0+1} sont aussi surjectives et l'application $\rho : Im(\rho^n) \longrightarrow Im(\rho^{n+1})$ devient $\rho : A \longrightarrow A$. Elle est injective d'après ce qui précède et comme elle est surjective par hypothèse alors elle est bijective.

3) Prenons $A = K[X]$ et le morphisme de $k-$algèbre dans lui-même défini par $X \mapsto X^2$. Il est injectif évidement (car $\phi : K \longrightarrow A$ est injectif si $A \neq \{0\}$) mais

n'est pas surjectif car X n'est pas dans l'image. Donc on ne peut pas remplacer l'hypothèse "surjective" par "injective"dans la question 2).

4) Considérons $A = k[X_1, ...X_n, ...]$ un anneau de polynômes à une infinité de variables et définissons le morphisme de $k-$ algèbre, $\rho : A \longrightarrow A$ par l'image des générateurs $\rho(X_1) = 0$ et $\rho(X_{i+1}) = X_i$ pour $i \geq 1$. On remarque que tous les X_i pour $i \geq 1$ sont dans l'image de ρ donc ρ est surjectif alors que X_1 est dans le noyau de ρ (car $\rho(X_1) = 0$). On conclut donc que ρ n'est pas injectif car son noyau n'est pas nul (contient X_1). Donc on ne peut pas se passer de l'hypothèse Noethérien dans la question 2).

Exemple 2.5

Soit R un anneau euclidien.
1) Montrer qu'il existe $x \in R$, non inversible tel que $R^\times \cup \{0\} \longrightarrow R/(x)$ soit surjective.

2) Soit $A = \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$. Déterminer $A^\times$ et montrer que A n'est pas euclidien.

3) Soit $x \in \mathbb{C}$. On veut montrer qu'il existe $q \in A$ tel que $|x - q| < 1$ ou $|2x - q| < 1$. On pose $x = u + iv$ avec $u, v \in \mathbb{R}$.
a) Se ramener au cas où $v \in [0, \frac{\sqrt{19}}{4}]$.
b) Montrer que si $v \in [0, \frac{\sqrt{3}}{2}]$, il existe $q \in \mathbb{Z}$ tel que $|x - q| < 1$.
c) Montrer que si $v \in [\frac{\sqrt{3}}{2}, \frac{\sqrt{19}}{4}]$ alors $\frac{\sqrt{19}}{2} - 2v \in [0, \frac{\sqrt{3}}{2}]$. En déduire $q \in A$ tel que $|2x - q| < 1$.

4) Soient $a, b \in A\backslash\{0\}$. Montrer qu'il existe $q, r \in A$ tels que $r = 0$ ou $|r| < |b|$ et qui vérifient, soit $a = bq + r$ ou $2a = bq + r$.

5) Montrons que ¡2¿ est un idéal maximal de A (on pourra soit écrire la table de multiplication de $A/ < 2 >$, soit vérifier que X^2+X+5 est un polynôme irréductible de $\mathbb{Z}/ < 2 > [X]$).

6) Soit I un idéal de A et $b \in I - \{0\}$ minimisant $|b|$. Montrer que $2I \subset < b > \subset I$.

7) Montrer que A est principal.

Solution 2.5

Soit R un anneau euclidien.
1) Soit $x \in R - (R^\times \cup \{0\})$ tel que $v(x)$ soit minimal.
Le fait que R est euclidien implique qu'il existe $v : R - \{0\} \longrightarrow \mathbb{N}$ telle que pour tous $a, b \in R - \{0\}$, il existe $q, r \in R$ tels que $a = bq + r$ et $r = 0$ ou $v(r) < v(b)$. Si $y \in R$ alors il existe $q, r \in R$ tel que $y = qx + r$ (et donc $\bar{y} = \bar{r}$) et $v(r) < v(x)$, donc $r \in R^\times - \{0\}$. Donc $\bar{y}$ est l'image de r par l'application $R^\times \cup \{0\} \longrightarrow R/(x)$. D'où l'application $R^\times \cup \{0\} \longrightarrow R/(x)$ est surjective.

2) Soit $A = \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$. On sait que z est inversible si et seulement si $N(z) = 1$. Mais si $z = a + b(\frac{1+i\sqrt{19}}{2})$, on a :

$$\begin{aligned} N(z) &= z\bar{z} \\ &= (a + \frac{b}{2})^2 + 19\frac{b^2}{4}. \end{aligned}$$

On a alors $N(z) \geq 19\frac{b^2}{4} > 1$ dès que $b \neq 0$. D'où $A^\times = \{-1, 1\}$.
Soit maintenant $x \in A$ non inversible tel que $A^\times \cup \{0\} \longrightarrow A/ < x >$ est surjective. Si $y \in A$ alors x divise y, $y + 1$ ou $y - 1$, donc $N(x)$ divise $N(y)$, $N(y + 1)$ ou $N(y - 1)$. En prenant $y = 2$, on obtient $N(x)$ divise

$$\begin{aligned} N(y) &= N(2) \\ &= 4 \end{aligned}$$

ou $N(x)$ divise

$$\begin{aligned} N(y + 1) &= N(2 + 1) \\ &= N(3) \\ &= 9 \end{aligned}$$

ou $N(x)$ divise

$$\begin{aligned} N(y - 1) &= N(2 - 1) \\ &= N(1) \\ &= 1. \end{aligned}$$

Tout cela revient à dire que $N(x)$ divise 1, 4 ou 9. Or $1, 4$ et 9 sont premiers entre eux donc $N(x) = 1$. On conclut alors que x est inversible. D'après la question 1), A n'est pas euclidien.

3) Soit $x \in \mathbb{C}$. On veut montrer qu'il existe $q \in A$ tel que $|x - q| < 1$ ou $|2x - q| < 1$. On pose $x = u + iv$ avec $u, v \in \mathbb{R}$

a) Soit $n \in \mathbb{Z}$ tel que $|\frac{4v}{\sqrt{19}} - n| \leq \frac{1}{2}$. Soit $x' = x - n\frac{1+i\sqrt{19}}{2}$. Résolvons le problème pour x'. Posons $x' = u' + iv'$. On a $v' \in [\frac{-\sqrt{19}}{4}, \frac{\sqrt{19}}{4}]$. Si $v' \geq 0$, alors on s'est ramené au cas voulu sinon, on remplace x' par $-x'$.

b) Soit $q \in \mathbb{Z}$ tel que $|u - q| \leq \frac{1}{2}$. On a :

$$\begin{aligned} |x - q|^2 &= |u + iv - q|^2 \\ &= |u - q|^2 + |v|^2 \\ &< (\frac{1}{2})^2 + (\frac{\sqrt{3}}{2})^2 \\ &< \frac{1}{4} + \frac{3}{4} \\ &= 1, \end{aligned}$$

(car $v \in [0, \frac{\sqrt{3}}{2}]$). D'où il existe $q \in \mathbb{Z}$ tel que $|x - q| < 1$ si $v \in [0, \frac{\sqrt{3}}{2}]$.

c) Comme $v \leq \frac{\sqrt{19}}{4}$, $v - \frac{\sqrt{19}}{4} \leq 0$ donc $2v - \frac{\sqrt{19}}{2} \leq 0$, ce qui donne $\frac{\sqrt{19}}{2} - 2v \geq 0$. Pour l'autre inégalité, On a $\frac{\sqrt{3}}{2} \leq v$, $3\frac{\sqrt{3}}{2} \leq 3v$ ce qui implique que $3\frac{\sqrt{3}}{2} \leq 3\frac{\sqrt{19}}{4}$ (car $v \leq \frac{\sqrt{19}}{4}$). On remarque que $3\frac{\sqrt{3}}{2} \geq \frac{\sqrt{19}}{2}$. Du coup $\frac{1+i\sqrt{19}}{2} - 2x$ vérifie la condition de la question 1), c'est-à-dire que $\frac{1+i\sqrt{19}}{2} - 2x \in [0, \frac{\sqrt{3}}{2}]$. D'où il existe $\gamma \in \mathbb{Z}$ tel que $|\frac{1+i\sqrt{19}}{2} - 2x - \gamma| < 1$, ce qui équivaut à $|2x - (\frac{1+i\sqrt{19}}{2} - \gamma| < 1$. Il suffit de poser $q = \frac{1+i\sqrt{19}}{2} - \gamma$.

4) Soient $a, b \in A\backslash\{0\}$. Appliquons la question 3) à $x = \frac{a}{b}$ et posons :

$$\begin{aligned} r &= b(x - q) \\ &= b(x - q) \\ &= b(\frac{a}{b} - q) \\ &= a - bq, \end{aligned}$$

ce qui implique que $a = bq + r$, ou posons :

$$\begin{aligned} r &= b(2x - q) \\ &= b(2\frac{a}{b} - q) \\ &= 2a - bq, \end{aligned}$$

ce qui implique que $2a = bq + r$ en fonction des cas.

5) Montrons que $< 2 >$ est un idéal maximal de A.
On remarque que le nombre $\frac{-1+i\sqrt{19}}{2}$ est une racine de X^2+X+5, d'où un morphisme surjectif $f : \mathbb{Z}[X]/(X^2 + X + 5) \longrightarrow \mathbb{Z}[\ \frac{1+i\sqrt{19}}{2}]$ envoyant X sur $\frac{1+i\sqrt{19}}{2}$. Comme les deux sont les $\mathbb{Z}$-modules libres de rang 2, et que f envoie la base $(1, X)$ sur la base $(1, \frac{1+i\sqrt{19}}{2})$, c'est un isomorphisme. En effet, un module libre est un module qui possède une base B, c'est-à-dire un sous-ensemble tel que tout élément de ce module s'écrive de façon unique comme combinaison linéaire finie d'éléments de B. On parle du rang du module libre sur un anneau dans le cas où l'anneau est commutatif ou Noethérien.
Si $M \longrightarrow N$ est une application linéaire surjective entre deux modules libres de même rang fini, alors c'est un isomorphisme.
Montrons alors que $A/ < 2 >= \mathbb{Z}[X]/(X^2 + X + 5, 2) = \mathbb{F}_2\ [X]/(X^2 + X + 5)$ est un corps. Soit $P = X^2 + X + 5$. Le degré de P est égal à 2 et on remarque qu'il n'y a pas de racines de P dans $\mathbb{F}_2$. On conclut donc que P est irréductible sur $\mathbb{F}_2$, d'où $A/ < 2 >= \mathbb{Z}[X]/(X^2 + X + 5, 2) = \mathbb{F}_2\ [X]/(X^2 + X + 5)$ est un corps. D'où $< 2 >$ est un idéal maximal de A.

6) Soit I un idéal de A et $b \in I - \{0\}$ minimisant $|b|$. Remarquons que $|z|^2 \in \mathbb{N}$ donc il existe bien $b \in I - \{0\}$ minimisant $|b|^2$. Comme $b \in I$ alors $< b > \subset I$. Si $a \in I$, on applique 3) : si $a = bq + r$ alors $r = a - bq \in I$ (car $a, b \in I$) et par minimalité de $|b|$, $r = 0$ donc $a - bq = 0$ implique $a \in < b >$ et par conséquent $2a \in < b >$ alors $< 2a > \subset < b >$ par le même argument. D'où $2I \subset < b > \subset I$.

7) Montrons que A est principal. Soit I un idéal de A, on a $2I \subset < b > \subset I$. Or d'après la question 5), $< 2b >$ est maximal parmi les idéaux de A contenus dans $< b >$ (car la multiplication par b induit une bijection croissante des idéaux de A vers les idéaux contenant b). Il s'en suit que $2I =< b >$ ou $< 2b >$ est principal. Comme A est intègre, I est principal aussi.

Conclusion :

En somme, ce document ici présent essaie de donner une idée générale sur les groupes symétriques, de donner leurs origine, structures, représentations et les propriétés qui leur sont rattachées suivis de quelques exemples. Il tente également de donner un aperçu sur les anneaux classiques et d'en traiter quelques exemples. Cependant, nous admettons que plusieurs autres aspects d'anneaux classiques n'ont pas été abordés dans ce document mais il donne néanmoins l'essentiel les concernant.

Toutefois, la question qu'un esprit plus objectif se posera à la suite de tout ce qui précède est la suivante "qu'elle est l'application concrète des groupes symétriques ou des anneaux classiques dans la vie de tous les jours ?"

Bibliographie

[1] C. JOULAIN, Séminaire Dubreil. Algèbre et théorie des nombres, tome 15, no 2 (1961-1962), exp. no 14.

[2] J. Calais, Élément de théorie des anneaux-anneaux commutatifs-niveau L3, Éditions Ellipses, 2006.

[3] N. Mahdou, Cours et Exercices corrigés de structures, Faculté des Sciences et Techniques de Fès, Université sidi Mohamed Ben Abdellah, Fès, Maroc.