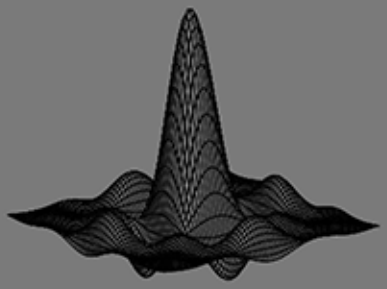
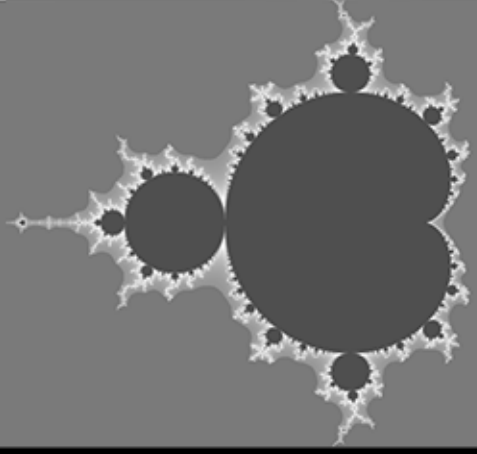




Algèbre 1

Nicolas Bouffard

Hiver 2017

Université de Saint-Boniface
Une éducation supérieure depuis 1818

Dernière mise à jour :
3 mars 2018 à 21:26

Table des matières

Première partie

La théorie des groupes

Chapitre 1

Les groupes

1.1 Les structures algébriques

Les origines de l'algèbre remonte à un ouvrage écrit en arabe du 9e siècle : abrégé du calcul par la restauration et la comparaison du mathématicien persan Al-Khwarizmi. Le terme arabe pour restauration (al-jabr) est ce qui donnera naissance au mot algèbre.

Au début, l'algèbre était l'étude de la résolution des équations contenant une ou des inconnus. Pour parvenir à trouver une solution, on doit étudier les différentes propriétés des opérations. On peut penser entre autre à la commutativité, l'associativité, la distributivité, l'existence d'inverse, etc.

L'étude des systèmes d'équations linéaires mêne naturellement à l'étude de l'algèbre linéaire et en particulier à l'étude des vecteurs et des matrices. Les variables ne sont plus seulement de simple quantité, mais bien une quantité ayant une direction. Cette idée est particulièrement utile entre autre en physique et en ingénierie.

La recherche des zéros d'un polynôme est plus compliqué. La solution de certaine équation quadratique était déjà connu des babylonniens il y a 4000 ans. Il fallu cependant attendre au 16e siècle avant qu'une méthode soit connu pour trouver les racines d'un équation cubique. Curieusement, même lorsque les racines sont réelles, dans certain cas il est nécessaire d'extraire des racines carrés de nombres négatifs, ce qui éventuellement donna naissance aux nombres complexes. Peu de temps après que la solution de l'équation cubique soit connu, l'équation de degré 4 le fut à son tour. La question de trouver une solution générale pour l'équation de degré 5 ce révéla cependant encore plus difficile. Au 19e siècle, Abel donna la première démonstration qu'il est impossible de résoudre par radicaux l'équation générale de degré 5. Quelques années plus tard, Galois en donna une seconde démonstration. Les idées de Galois étaient particulièrement révolutionnaire, et ce n'est qu'après sa mort que ses idées furent pleinement reconnu. L'idée de génie de Galois fut d'étudier les permutations des racines d'un polynôme et faire une correspondance avec certaine extension de l'ensemble des nombres rationnels. En language moderne, ces ce qui a donné naissance à l'étude des groupes et des corps, deux des trois structures qui joueront un rôle clé dans notre cours.

À partir de Galois, l'étude de l'algèbre sera complètement transformé. L'objet d'étude de l'algèbre ne sera plus réservé au méthode de résolution d'équations algébrique, mais deviendra plutôt l'étude des structures ayant certaines propriétés algébriques. Plutôt que de regarder comment des propriétés comme la commutativité, l'associativité, la distributivité, etc, peuvent jouer un rôle dans la résolution des équations, l'algèbre s'intéressera plutôt à étudier tout les objets pour lesquels l'opération définie sur cet objet a certaine propriétés.

Cette idée d'abstraction a été appliquer dans vos cours d'algèbre linéaire lorsque vous avez introduit le concept d'espace vectoriel. Lorsqu'un résultat est démontrer pour un espace vectoriel quelconque, le résultat sera alors valide pour $\mathbb{R}^n$, $\mathbb{C}^n$, les espaces de polynômes et aussi pour les espaces de matrices. Cette abstraction permet aussi dans certain cas d'obtenir des démonstrations qui sont beaucoup plus claire, lorsqu'un language approprié est utilisé. Les espaces vectoriels restent cependant relativement complexes. Dix axiomes sont nécessaire pour les définir, et ce sans compter les axiomes requis pour définir les nombres réels ou complexes qui sont nécessaire dans la définition d'un espace vectoriel.

Dans ce cours, nous allons concentrer notre étude sur trois structures : Les groupes, les anneaux et

les corps. Il s'agit de structure plus faible que celle d'espace vectoriel, dans le sens que beaucoup moins d'axiome sont nécessaire pour les définir. Par contre, ces structures sont aussi particulièrement courante en mathématiques. Ces ce qui rend leur étude particulièrement importante pour un mathématicien. Ces trois structures ne sont certainement pas les seuls qui mérite d'être étudiés dans des cours d'algèbre moderne, une omission notable est la structure de module, qui apparait dans des cours d'algèbre plus avancé, et qui généralise la notion d'espace vectoriel.

1.2 Les groupes

Nous allons maintenant introduire la première structure importante que nous allons rencontrer dans notre cours : La structure de groupe.

Definition 1.2.1. Un groupe $(G, *)$ est un ensemble G muni d'une opération $* : G \times G \to G$ et pour laquelle :

1. L'opération $*$ est associative, c'est à dire que $a * (b * c) = (a * b) * c$ pour tout $a, b, c \in G$.
2. L'opération $*$ possède un élément neutre, c'est à dire qu'il existe un élément $e \in G$ tel que $g * e = e * g = g$ pour tout $g \in G$.
3. L'opération $*$ possède des inverse, c'est à dire que pour tout $g \in G$, il existe $g^{-1} \in G$ tel que $g * g^{-1} = g^{-1} * g = e$.

Notez que bien que notre point de départ soit la notion de groupe, il existe aussi des structures plus faible (i.e. avec moins d'axiome). Un semigroupe est un ensemble muni d'une opération qui est associative. Un monoide est un ensemble muni d'une opération qui est associative et qui possède un élément neutre. Il est donc facile de remarquer que tous les groupes sont des monoides, et tout les monoides sont des semigroupes. Bien que les semigroupes et monoides possède une théorie intéressante, la structure de groupe possède une théorie beaucoup plus riche, est beaucoup plus facilement applicable, et en conséquence joue un rôle beaucoup plus important dans l'étude de l'algèbre moderne. Ces pour cette raison que nous allons concentrer notre étude sur la structure de groupe.

Definition 1.2.2. Un groupe $(G, *)$, alors on dit que

1. $(G, *)$ est abélien (ou commutatif) si l'opération $*$ est commutative, c'est à dire que $g * h = h * g$ pour tout $g, h \in G$.
2. $(G, *)$ est fini s'il contient seulement un nombre fini d'élément. Autrement, on dit que le groupe est infini.

Lorsqu'il n'y a pas de risque de confusion, on parlera souvent du groupe G, plutôt que $(G, *)$, mais il faut se rappeler que ceci est en fait un abus de langage. Un groupe ne peut exister sans qu'une opération soit sprécifié. De plus, le symbol $*$ est utilisé ici pour faire référence à un opération quelconque. Dans la plupart des exemple concret, on représentera notre opération par des symboles comme $+$ pour l'addition ou $\times$ pour la multiplication.

Exemple 1.2.1. Voici quelques exemples de groupes :

1. Les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ muni de l'opération d'addition forment des groupes abéliens. Notez cependant que l'ensemble $\mathbb{N}$ muni de l'addition ne forme pas un groupe, car même si on considère le zéro comme étant dans l'ensemble, la structure sera associative et possèdera un élément neutre, mais autre que 0, aucun élément ne sera inversible. En effet, dans $\mathbb{N}$ l'équation $1 + x = 0$ ne possède pas de solution.
2. Les ensembles $\mathbb{Q}\backslash\{0\}$, $\mathbb{R}\backslash\{0\}$ et $\mathbb{C}\backslash\{0\}$ muni de l'opération de multiplication forment des groupes abéliens. Notez cependant que les ensembles $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ muni de la multiplication ne forme pas des groupes car dans chacun des cas, l'élément 0 ne possède pas d'inverse. En effet, l'équation $0x = 1$ ne possède aucune solution dans aucun de ces trois ensembles.
3. L'ensemble des matrices réelles de dimension $n \times n$ inversible muni de la multiplication de matrices forme un groupe qui n'est pas abélien.

Definition 1.2.3. Si $(G, *)$ est un groupe, alors on appelle l'ordre du groupe, dénoté $|G|$, le nombre d'élément dans l'ensemble G. De plus, on appelle l'ordre d'un élément $g \in G$ le plus petit entre $n > 0$ tel que $g^n = e$ où $g^n = \underbrace{g * g * ... * g}_{n \text{ fois}}$.

Remarquez que les exemples précédents sont tous des groupes d'ordre infinie. Il existe aussi plusieurs groupes d'ordre fini. Lorsque l'ordre du groupe est relativement petit, il est commun de les décrire à l'aide d'une table de multiplication comme si dessous :

*	0	1
0	0	1
1	1	0

Ce groupe porte le nom de groupe cyclique d'ordre 2. Il est souvent dénoté par $\mathbb{Z}_2$ ou C_2. On remarque qu'il s'agit d'un groupe d'ordre deux possédant un élément d'ordre 1, et un élément d'ordre 2. Il est facile (par essaies et erreurs) de se convaincre qu'il s'agit en fait du seul groupe d'ordre 2 dans le sens que tout les autres groupes d'ordre 2 auront une table de multiplication identique, sauf possiblement pour le nom des éléments. On dira alors que tous les groupes d'ordre deux sont isomorphiques. La notion de groupes isomorphiques sera étudié plus en détail plus tard dans le cours.

Dans le reste de cette section, nous allons maintenant regarder quelques propriétés élémentaires des groupes, puis le reste du chapitre consistera essentiellement à l'étude de quelques familles concrètes de groupes qui jouent un rôle particulièrement important dans l'étude de la théorie des groupes.

Théorème 1.2.1. Si $(G, *)$ est un groupe, alors

1. L'identité est unique, c'est à dire que si $e, f \in G$ sont tel que $e * x = x * e = x, \ \forall x \in G$ et $f * x = x * f = x, \ \forall x \in G$, alors on a que $e = f$.
2. Pour chaque $x \in G$, il existe un unique élément $x^{-1} \in G$ tel que $x * x^{-1} = x^{-1} * x = e$.
3. Si $x, y, z \in G$ sont tel que $x * y = x * z$, alors $y = z$.
4. Si $x, y, z \in G$ sont tel que $y * x = z * x$, alors $y = z$.

Démonstration.

1. Supposons que G est un groupe, et e, f des identités pour le groupe. Alors par définition d'un identité on a : $e * f = f$ et $e * f = e$. On obtient donc $e = f$. L'identité est donc unique.
2. Supposons que $x \in G$ possède deux inverses, disons y et z. On a donc :

$$x * y = y * x = e \qquad \text{et} \qquad x * z = z * x = e$$

   En combinant ces deux équations, on obtient donc :

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

   L'inverse est donc unique.
3. Supposons que $x, y, z \in G$ sont tel que $x * y = x * z$, alors en multipliant des deux côtés par x^{-1} on obtient :

$$x^{-1} * (x * y) = x^{-1} * (x * z)$$
$$(x^{-1} * x) * y = (x^{-1} * x) * z$$
$$e * y = e * z$$
$$x = y$$

4. La démonstration est pratiquement identique à la précédente et vous est laissé en exercice.

□

Definition 1.2.4. Si $(G, *)$ est un groupe et S un sous-ensemble de G, alors on dit que S est générateur de G si tout les éléments de G peuvent être écrit à partir des éléments de S. On écrira alors $G = \langle S \rangle$ pour signifier que S est générateur de G. Si G est un groupe pour lequel il existe $g \in G$ tel que $G = \langle g \rangle$, alors on dit que G est cyclique (Certain auteur parle plutôt de groupe monogène).

Exemple 1.2.2. Considérez le groupe définie à partir de la table de multiplication suivante :

$*$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Ce groupe porte le nom de $\mathbb{Z}_5$. Il n'est pas nécessaire pour le moment de vérifier qu'il s'agit d'un groupe, car ce sera fait un peut plus loin dans le chapitre. Par contre, on remarque que :

$$1^1 = 1, \quad 1^2 = 1 * 1 = 2, \quad 1^3 = 1 * 1 * 1 = 2 * 1 = 3, \quad 1^4 = 1 * 1 * 1 * 1 = 2 * 2 = 4, \quad 1^5 = 1 * 1 * 1 * 1 * 1 = 0$$

On peut donc remarquer que tout les éléments du groupe $\mathbb{Z}_5$ peuvent s'écrire à partir de l'élément 1. On peut donc affirmer que 1 est générateur du groupe, et écrire $\mathbb{Z}_5 = \langle 1 \rangle$.

Ici, on doit faire une remarque importante. Bien que 1 soit bien générateur du groupe $\mathbb{Z}_5$, il n'y a aucun moyen de retrouver le groupe $\mathbb{Z}_5$ à partir de l'élément 1 sans avoir d'information sur l'opération. il est donc souvent plus pratique de décrire un groupe à partir de générateurs et de relation. Dans le cas de $\mathbb{Z}_5$, on pourra par exemple écrire :

$$\mathbb{Z}_5 = \langle 1 : 1^5 = 0 \rangle$$

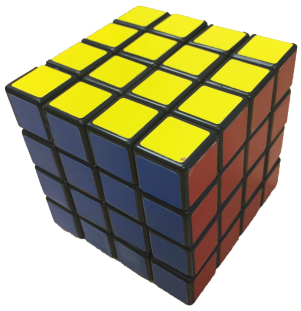
Cette description est en fait suffisante pour retrouver le groupe $\mathbb{Z}_5$.

Exemple 1.2.3. Considérez le groupe définie à partir de la table de multiplication suivante :

$*$	0	1	2	3
0	0	1	2	3
1	1	0	4	2
2	2	3	0	1
3	3	2	1	0

Ce groupe porte le nom de groupe de Klein. On le dénote habituellement par V_4. Dans ce cas, on a besoin de deux éléments pour générer le groupe au complet. On peut par exemple écrire $V_4 = \langle 1, 2 \rangle$. En particulier, on remarque que le groupe V_4 n'est pas cyclique.

Exemple 1.2.4. Un autre exemple de groupe particulièrement intéressant pour les amateurs de puzzle est celui former par l'ensemble de toutes les transformations d'un cube Rubik. Ce groupe est cependant particulièrement difficile à étudier et nous ne démontrera pas pour le moment qu'il s'agit bien d'un groupe.



1.3 Les groupes symétriques S_n et les groupes alternés A_n

L'une des familles de groupes les plus importantes est la famille des groupes symétriques. Mais avant de définir cette famille de groupe, nous aurons besoin de rappeler rapidement la notion de fonction bijective, ce que nous allons faire immédiatement.

Definition 1.3.1. Si A et B sont des ensembles, et $f : A \to B$ une fonction, alors on dit que :

1. f est une fonction injective si pour tout $x, y \in A$ tel que $f(x) = f(y)$, alors $x = y$.
2. f est une fonction surjective si pour tout $y \in B$, il existe $x \in a$ tel que $f(x) = y$.
3. f est une fonction bijective si f est injective et surjective.

Le groupe de symétrique de n éléments est dénoté par S_n. Il s'agit de l'ensemble de toutes les permutations sur un ensemble de n éléments, c'est à dire l'ensemble de toutes les fonctions bijectives sur un ensemble de n éléments. Par exemple, sur un ensemble de 3 éléments on aura les permutations suivantes :

$$\alpha : (1\ 2\ 3) \to (1\ 2\ 3)$$

$$\beta : (1\ 2\ 3) \to (2\ 1\ 3)$$

$$\gamma : (1\ 2\ 3) \to (1\ 3\ 2)$$

$$\delta : (1\ 2\ 3) \to (3\ 2\ 1)$$

$$\epsilon : (1\ 2\ 3) \to (2\ 3\ 1)$$

$$\zeta : (1\ 2\ 3) \to (3\ 1\ 2)$$

Le groupe S_3 contient donc 6 éléments, c'est à dire qu'il s'agit d'un groupe d'ordre 6. On dénote habituellement une permutation sous forme de matrice ayant deux lignes. La première correspondant aux éléments de départ, i.e. les nombres de 1 à n, et la seconde ligne indiquant à quels positions l'éléments au dessus de lui se retrouve après la permutation. Par exemple, la permutation β dans l'exemple ci-dessus s'écrit sous la forme :

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Cette notation reste cependant lourde, et il est commun de la simplifier sous forme de décomposition en cycle. On pourra alors réécrire la permutation β sous la forme (12), ce qui signifie que l'élément en première position se retrouve en deuxième position, et l'élément en deuxième position se retrouve en première position. Les termes qui sont omit de la décomposition en cycle restant à la même position. La permutation ϵ s'écrira donc : (132).

Nous avons parler du groupe symétrique, mais nous n'avons toujours pas détaillé quel est l'opération sur ce groupe. Il s'agit tout simplement de la composition des permutations (ou si vous préférer la composition des fonctions). Cette opération peut s'écrire sous la forme $\circ$, mais il est aussi courant d'ignorer complètement le symbol au même titre que sur les nombres réels, on écrit habituellement xy à la place de $x \times y$. En se référent toujours au groupe S_3, on peut essayer d'effectuer l'opération $\gamma \circ \zeta$. On aura donc :

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

On a donc $\gamma \circ \zeta = \beta$. Remarquez que comme pour les fonctions, les permutations sont évalué de droite à gauche. De plus, même si on utilise des matrices pour représenté des permutations, la composition des permutations n'a rien à avoir avoir le produit des matrices. À partir de maintenant nous allons donc éviter d'utiliser le terme matrice lorsque nous parlons de permutation. Remarquez que nous aurions pu écrire la même opération sous forme de décomposition en cycle et écrire plutôt $(23)(132) = (12)$, ce qui aurait été exactement la même chose. Nous sommes maintenant prêt à démontrer que les groupes symétriques sont bel et bien des groupes.

Théorème 1.3.1. L'ensemble des permutations sur un ensemble de n éléments muni de l'opération de composition forme un groupe appelé groupe de permutation et dénoté par S_n. De plus, l'ordre du groupe S_n est $n!$.

Démonstration. Il s'agit de démontrer que les trois axiomes d'un groupe sont satisfaites. L'existence d'un élément neutre et l'existence d'inverse sont évidentes à partir de la définition. La seule difficulté repose sur la démonstration de l'associativité. Pour ce faire, il s'agit de remarquer qu'une permutation n'est en fait rien d'autre qu'une fonction $f : A \to A$ où A est un ensemble de n éléments. Comme la composition de fonctions est associative, on a donc que l'ensemble des permutations muni de l'opération de composition est associative. Finalement, le fait que l'ordre du groupe soit $n!$ est une simple conséquence du principe du produit en combinatoire. □

Théorème 1.3.2. Le groupe S_n est abélien si et seulement si n égale 1 ou 2.

Démonstration. Il est facile de voir que si $n = 1$ ou $n = 2$ le groupe S_n est abélien. Nous allons donc démontrer que si $n \geq 3$, alors le groupe n'est pas abélien. Pour ce faire, il s'agit de remarquer que :

$$(12)(123) = (23) \qquad \text{et} \qquad (123)(12) = (13)$$

Comme ces permutations font partie de S_n pour tout $n \geq 3$, S_n n'est donc pas abélien si $n \geq 3$. □

Une transposition est une permutation de la forme (ab). Ce type de permutation joue un rôle particulièrement important du au fait que toutes les permutations peuvent s'écrire comme composition de transposition. Par exemple, dans le groupe S_4, on peut écrire :

$$(1234) = (14)(13)(12)$$

La décomposition d'une permutation sous forme de transposition n'est certainement pas unique, par contre sa parité est bien définie. On dit qu'un permutation est pair, si elle peut s'écrire sous forme de composition d'un nombre pair de transposition. On dit qu'elle est impair si elle peut s'écrire sous forme d'un nombre impair de transposition. L'ensemble de toutes les permutations paires d'un ensemble de n éléments porte le nombre de groupe alterné de n éléments et est dénoté par A_n.

Théorème 1.3.3. Si $n \in \mathbb{N}$, alors l'ensemble de toutes les permutations paires sur un ensemble de n éléments muni de la loi de composition forme un groupe appellé groupe alterné et est dénoté par A_n. L'ordre de ce groupe est $\dfrac{n!}{2}$.

Exemple 1.3.1. On veut trouver les différents éléments du groupe A_3. En se basant sur la notation utilisé au début de la section pour les éléments de S_3, on a donc :

$$\begin{array}{lll} \alpha = id & \gamma = (23) & \epsilon = (123) = (13)(12) \\ \beta = (12) & \delta = (13) & \zeta = (132) = (12)(13) \end{array}$$

Les éléments de A_3 sont donc : $\{id, (123), (132)\}$.

1.4 Les groupes modulos $\mathbb{Z}_n$ et $\mathbb{Z}_n^\times$

Nous allons maintenant étudier deux autres familles de groupes, celles des nombres modulos avec l'addition, puis la multiplication. On peut imaginer les nombres modulos comme un horloge. Après le nombre 12, on revient à 1. Donc s'il est 10h, alors 4h plus tard il sera 2h. C'est à dire que $10 + 4 = 2$. Le fait qu'il y est 12 valeurs sur un horloge n'est en fait qu'un cas particulier. En mathématiques, il est tout à fait possible d'étudier un horloge ayant 3, 18 ou même 3000 valeurs différentes. Nous allons maintenant définir formellement ce que sont les nombres modulos. Pour ce faire, nous avons besoin de définir les concepts de relation d'ordre partiel, de relation d'équivalence, et de divisibilité. C'est ce que nous allons faire immédiatement.

Definition 1.4.1. Si S est un ensemble, alors une relation d'équivalence $\sim$ sur l'ensemble S comme étant une relation qui satisfait les trois propriétés suivantes :

1. Réflexive, c'est à dire que $x \sim x$ pour tout $x \in S$.
2. Symétrique, c'est à dire que $x \sim y$ si et seulement si $y \sim x$.
3. Transitive, c'est à dire que $x \sim y$ et $y \sim z$, alors $x \sim z$.

Les relations d'équivalence servent à généralisé l'idée d'égalité que l'on retrouve sur les ensembles de nombres (i.e. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$), ainsi que l'idée d'égalité que l'on retrouve dans la théorie des ensembles par exemple. Dans l'exemple de l'horloge, les relations d'équivalence nous permettent d'exprimer l'idée que 1 et 13 ce retrouve à la même position, et donc que dans un certain sens, ils sont identiques.

Definition 1.4.2. Si S est un ensemble, alors une relation d'ordre partielle $\preceq$ sur l'ensemble S est une relation qui satisfait les trois propriétés suivantes :

1. Réflexive, c'est à dire que $x \preceq x$ pour tout $x \in S$.
2. Antisymétrique, c'est à dire que si $a \preceq b$ et $b \preceq a$, alors $a = b$.
3. Transitive, c'est à dire que $x \preceq y$ et $y \preceq z$, alors $x \preceq z$.

Les relations d'ordre partielles nous permettent de généralisé l'idée de plus petit ou égal ($\leq$) et plus grand ou égal ($\geq$) que l'on retrouve sur les ensembles de nombres, ainsi que l'idée d'inclusion $\subseteq$ que l'on retrouve en théorie des ensembles. Il est important de comparer les notions définition d'une relation d'équivalence et celle d'une relation d'ordre partielle. Les deux définitions se ressemblent beaucoup, et en fait 2 des 3 propriétés sont identiques. Ils jouent cependant un rôle très différent dans la théorie.

Definition 1.4.3. Si $a, b \in \mathbb{Z}$, alors on dit que a divise b si et seulement si il existe $k \in \mathbb{Z}$ tel que $ak = b$. Dans ce cas, on écrit $a|b$.

Théorème 1.4.1. La relation de divisibilité $|$ sur l'ensemble des nombres naturels (différent de zéro) est une relation d'ordre partielle.

Démonstration. On doit montrer que la divisibilité est réflexive, antisymétrique et transitive.

1. Prenons $x \in \mathbb{N}$, alors $x = 1x$, ce qui signifie que $x|x$. La relation est donc réflexive.
2. Prenons $x, y \in \mathbb{N}$, et supposons que $x|y$ et $y|x$. Par définition de la divisibilité, il existe donc des entiers m, n tel que $x = my$ et $y = nx$. En combinant ces deux égalités, on a donc : $x = my = m(nx) = (mn)x$. Comme $x \neq 0$, on peut donc simplifier, ce qui nous donne $1 = mn$. Comme m, n sont supposé entier, les seuls possibilités sont $m = n = \pm 1$. On a donc $x = \pm y$. De plus, comme x et y sont tous deux positifs (il s'agit de nombres naturels), alors $x = y$. La relation est donc antisymétrique.
3. Prenons $x, y, z \in \mathbb{N}$, et supposons que $x|y$ et $y|z$. Il existe donc des entiers m, n tel que $y = mx$ et $z = ny$. En combinant ces deux égalités, on obtient $z = ny = n(mx) = (nm)x$. Par définition de la divisibilité, on a donc $x|z$. La relation est donc transitive.

Comme la relation est symétrique, antisymétrique et transitive, on peut donc conclure qu'il s'agit bien d'une relation d'ordre partielle. □

Remarquer que la divisibilité n'est pas une relation d'ordre partielle sur l'ensemble des entiers. En particulier, on remarque que la relation ne serait pas réflexive, car $0 \nmid 0$.

Definition 1.4.4. Si $n \in \mathbb{N}, n \geq 2$, alors on définit la relation $\equiv_n$ comme étant :

$$a \equiv_n b \quad \Leftrightarrow \quad n|(b-a)$$

Habituellement, lorsque le n est clair selon le contexte, on écrira tout simplement $\equiv$ plutôt que $\equiv_n$.

Théorème 1.4.2. Si $n \in \mathbb{N}, n \geq 2$, alors la relation $\equiv_n$ sur l'ensemble des nombres entiers est une relation d'équivalence.

Démonstration. Fixons $n \in \mathbb{N}, n \geq 2$. On doit montrer que la relation $\equiv_n$ est réflexive, symétrique et transitive.

1. Prenons $x \in \mathbb{Z}$, alors $n|(x-x)$, donc $x \equiv x$. La relation est donc réflexive.
2. Prenons $x, y \in \mathbb{Z}$, et supposons que $x \equiv y$. Alors par définition, $n|(x-y)$, c'est à dire qu'il existe $k \in \mathbb{Z}$ tel que $nk = x - y$. en multipliant des deux côtés par -1, on obtient que $n(-k) = y - x$, ce qui nous donne $n|(y-x)$. Par définition on a donc $y \equiv x$, ce qui signifie que la relation est symétrique.
3. Prenons $x, y, z \in \mathbb{Z}$, et supposons que $x \equiv y$ et $y \equiv z$. Par définition, on a donc $n|(y-x)$ et $n|(z-y)$. Il existe donc des entiers a et b tel que $na = y - x$ et $nb = z - y$. En additionnant ces deux égalités, on obtient donc : $n(a+b) = z-x$, ce qui nous donne $n|(z-x)$, et donc $z \equiv x$. La relation est donc transitive.

Comme la relation est réflexive, symétrique et transitive, on peut donc conclure qu'il s'agit d'une relation d'équivalence. □

Considérons maintenant l'ensemble $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, ..., \overline{n-1}\}$, où $\overline{x} = \{y \in \mathbb{Z} : x \equiv y\}$. On peut alors définir les deux opérations suivantes :

$$\overline{x} + \overline{y} = \overline{x+y}$$

$$\overline{x} \cdot \overline{y} = \overline{xy}$$

Il est important ici de réaliser que les symboles x et y représentent des entiers, alors que les symboles $\overline{x}$ et $\overline{y}$ représentent des ensembles. En particulier, lorsque nous avons écrit $\overline{x} + \overline{y} = \overline{x+y}$, le premier symbol $+$ représente une opération que nous souhaitons définir sur l'ensemble $\mathbb{Z}_n$, alors que le second symbol $+$ est tout simplement l'addition habituelle sur les nombres entiers. Il faut maintenant démontrer que les opérations $+$ et $\cdot$ que nous avons définie sur $\mathbb{Z}_n$ sont bien définies.

Théorème 1.4.3. Les opérations d'addition et de multiplications sur l'ensemble $\mathbb{Z}_n$ sont bien définie, c'est à dire que si $\overline{a} = \overline{c}$ et $\overline{b} = \overline{d}$, alors on a :

1. $\overline{a} + \overline{b} = \overline{c} + \overline{d}$
2. $\overline{a} \cdot \overline{b} = \overline{c} \cdot \overline{d}$

Démonstration. Supposons que a, b, c, d sont des entiers tel que $a \equiv c$ et $b \equiv d$, alors on a :

$$n|(c-a) \quad \text{et} \quad n|(d-b)$$

Il existe donc des entiers k_1 et k_2 tel que :

$$nk_1 = c - a \quad \text{et} \quad nk_2 = d - b$$

Ce qui nous donne :

$$(c+d) - (a+b) = (c-a) + (d-b) = nk_1 + nk_2 = n(k_1 + k_2)$$

On a donc $n|[(c+d)-(a+b)]$, c'est à dire $a+b \equiv c+d$. Donc la relation d'équivalence est compatible avec l'addition. De plus, on a aussi :

$$(cd)-(ab) = cd-cb+cb-ab = c(d-b)+b(c-a) = cnk_2+bnk_1 = n(ck_2+bk_1)$$

On obtient donc $n|(cd-ab)$, c'est à dire $ab \equiv cd$. Donc la relation d'équivalence est compatible avec la multiplication. □

Théorème 1.4.4. L'ensemble $(\mathbb{Z}_n, +)$ forme un groupe abélien pour tout $n \geq 2$.

Démonstration. Il s'agit d'une conséquence directe du fait que $(\mathbb{Z}, +)$ est un groupe abélien et que l'addition est compatible avec la relation d'équivalence. □

La question de former un groupe avec l'opération de multiplication est plus délicate. Il nous faut développer la théorie du plus grand diviseur, ainsi que la fonction ϕ d'Euler. Considérons l'ensemble $\mathbb{Z}_6$. Nous savons déjà qu'avec l'addition il s'agit d'un groupe abélien, mais cette fois nous somme intéressé à l'opération de multiplication. En voici la table de multiplication :

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

On remarque immédiatement que l'identité doit être 1, mais qu'il ne peut pas s'agir d'un groupe, car certain élément ne sont pas inversible. En effet, pour que chaque élément soit inversible, nous devrions avoir un 1 sur chacune des lignes. De plus, comme l'identité est unique, il doit y avoir exactement un 1 sur chaque ligne. Ceci élimine immédiatement les éléments 0, 2, 3 et 4. Il ne nous reste donc plus que deux éléments : 1 et 5. On obtient donc la table de multiplication suivante :

×	1	5
1	1	5
5	5	1

Nous allons appeler ce nous groupe $(\mathbb{Z}_6^\times, \times)$. Remarquez aussi qu'à l'exception du nom des éléments et du symbol utilisé pour l'opération, on remarque alors qu'il s'agit exactement de la même table de multiplication que pour le groupe $(\mathbb{Z}_2, +)$. Les groupes $\mathbb{Z}_6^\times$ et $\mathbb{Z}_2$ sont donc isomorphiques.

Bien que la méthode que nous venons d'employé à l'aide des tables de multiplications puissent être pratique pour de petites valeurs de n, ils nous faut maintenant développer un cadre plus théorique pour définir et étudier les groupes modulos multiplicatif, sans devoir à chaque fois en dessiner la table de multiplication. Ceci peut être accomplie par l'intermédiaire du plus grand commun diviseur, ainsi que de la fonction ϕ d'Euler.

Definition 1.4.5. Si a et b sont des entiers, alors on appelle plus grand commun diviseur (PGCD) le plus grand entier d tel que $d|a$ et $d|b$. On dénote le PGCD de a et b par (a, b).

Théorème 1.4.5. **(Théorème de Bézout)** Si a et b sont des entiers, alors il existe des entiers x et y tel que

$$ax + by = (a, b)$$

Démonstration. Considérons l'ensemble $S = \{ax + by : ax + by > 0 \text{ et } x, y \in \mathbb{Z}\}$. Comme il s'agit d'un sous-ensemble de nombre naturel, S possède un plus petit élément. Disons $\min(S) = d = ax_1 + by_1$. Supposons que $d \nmid a$, dans ce cas, par la division euclidienne, on peut écrire $a = qd + r$ avec $0 < r < d$. On obtient donc :

$$r = a - qd = a - q(ax_1 + by_1) = a(1 - qx_1) + b(-qy_1) \in S$$

Ce qui est une contradiction, car r est plus petit que le minimum de S. On doit donc avoir $d|a$. De la même façon, on obtient $b|d$. Donc d est un diviseur commun de a et b. Il ne nous reste plus qu'à montrer qu'il s'agit du plus grand. Pour ce faire, supposons que e est aussi un diviseur commun de a et b. Comme $e|a$ et $e|b$, on a donc $e|(ax_1 + by_1)$, ce qui signifie que $e|d$, et donc $e \leq d$. d est donc la plus grand commun diviseur de a et b. On a donc trouver une solution à l'équation : $ax_1 + by_1 = d = (a, b)$. □

Théorème 1.4.6. **(Lemme d'Euclide)** Les deux énoncés suivant sont vrai :

1. Si a, b, x, y sont des entiers tel que $ax + by = 1$ alors $(a, b) = 1$.
2. Si p est un nombre premier, et a, b des entiers tels que $p|ab$, alors $p|a$ ou $p|b$.

Démonstration.

1. Supposons que $d = (a, b)$, alors par définition, $d|a$ et $d|b$. Il existe donc des entiers k_1 et k_2 tel que $dk_1 = a$ et $dk_2 = b$, ce qui nous donne :

   $$ax + by = 1 \quad \Rightarrow \quad dk_1x + dk_2y = 1 \quad \Rightarrow \quad d(k_1x + k_2y) = 1$$

   Ce qui nous permet d'affirmer que $d|1$. Comme les seuls diviseurs de 1 sont 1 et -1, et que le PGCD doit être un entier positif, on peut donc conclure que $(a, b) = 1$.
2. Si $p|a$, alors nous avons terminé. On va donc supposer $p \nmid a$. Dans ce cas, comme p est un nombre premier, on doit avoir $(a, p) = 1$. Par la première partie, il existe donc des entiers x et y tel que $ax + py = 1$. En multipliant cette équation par b, on obtient donc $abx + bpy = b$. De plus, comme $p|ab$, il existe un entier k tel que $pk = ab$, ce qui nous permet d'obtenir $pkx + bpy = b$, et donc $p(kx + by) = b$, ce qui signifie que $p|b$. On peut donc conclure que si p est un nombre premier tel que $p|ab$, alors $p|a$ ou $p|b$.

□

Si n est un entier positif, nous somme maintenant intéressé à savoir quel élément de $\mathbb{Z}_n$ sont inversible par rapport à l'opération de multiplication. Pour ce faire, prenons $a \in \mathbb{Z}_n$ et supposons que a est inversible, c'est à dire qu'il existe un élément $b \in \mathbb{Z}_n$ tel que $ab = 1 \pmod{n}$. On doit donc avoir $n|(ab - 1)$ et donc il existe un entier k tel que $nk = ab - 1$. En réarrangeant les termes, on obtient $ab + n(-k) = 1$. Par le théorème précédent, on doit donc avoir $(a, n) = 1$. Donc dans $\mathbb{Z}_n$, pour qu'un élément $a \in \mathbb{Z}_n$ puisse avoir une chance d'être inversible, il est nécessaire d'avoir $(a, n) = 1$. Nous allons voir très bientôt que cette condition est en fait sufisante.

À partir du critère que nous venons d'établir, on est amené à définir une fonction importante de la théorie des nombres, et directement relié à notre étude des groupes modulos multiplicatif. Il s'agit de la fonction ϕ d'Euler :

$$\phi(n) = \#\{x : 1 \leq x < n : (x, n) = 1\}$$

De plus, on définit l'ensemble $\mathbb{Z}_n^\times = \{x \in \mathbb{Z}_n : (x, n) = 1\}$. Nous voulons maintenant démontrer que cet ensemble, muni de l'opération de multiplication forme un groupe.

Théorème 1.4.7. $(\mathbb{Z}_n^\times, \times)$ est un groupe abélien d'ordre $\phi(n)$. Ce groupe porte le nom de groupe modulo multiplicatif.

Démonstration. On doit commencer par démontrer que le produit de deux nombres de $\mathbb{Z}_n^\times$ est aussi dans cette ensemble. Pour ce faire, prenons $a, b \in \mathbb{Z}_n^\times$. Dans ce cas, par définition, $(a, n) = (b, n) = 1$. Maintenant, supposons que $d = (ab, n)$. Si $d > 1$, alors il existe un nombre premier p tel que $p|d$. Comme $d|ab$ et $d|n$, alors on doit aussi avoir $p|ab$ et $p|n$. Par le lemme d'Euclide, comme p est un nombre premier, on doit avoir $p|a$ ou $p|b$. Sans perte de généralité, supposons que $p|a$. On a donc obtenu $p|a$ et $p|n$, ce qui est une contradiction car par hypothèse $(a, n) = 1$ et p est un diviseur commun supérieur à 2. Il ne peut donc pas y avoir de nombre premier qui divise d, ce qui signifie que $d = 1$. On peut donc conclure que si $a, b \in \mathbb{Z}_n^\times$, alors $ab \in \mathbb{Z}_n^\times$. Maintenant, il est facile de voir que la multiplication dans $\mathbb{Z}_n^\times$ est associative, commutative, et qu'il existe un élément neutre (le nombre 1). Il nous reste donc seulement à démontrer l'existence d'inverse. Prenons $a \in \mathbb{Z}_n^\times$, alors comme $(a, n) = 1$, il existe des entiers b et x tel que $ab + xn = 1$, mais en simplifiant le tout modulo n, on obtient $ab = 1 \pmod{n}$, et donc a est inversible. Ceci confirme que $(\mathbb{Z}_n^\times, \times)$ est bien un groupe. De plus, en regardant sa définition, on remarque immédiatement qu'il est d'ordre $\phi(n)$. □

Voici un tableau donnant la valeur de $\phi(n)$, et en conséquent l'ordre du groupe $(\mathbb{Z}_n^\times, \times)$, pour de petite valeur de n.

n	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	2	2	4	2	6	4	6	4	10	4

Il existe une formule simple pour calculer $\phi(n)$. Par le théorème fondamental de l'arithmétique, on peut décomposer n sous la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ où les p_i sont des nombres premiers distincts. Dans ce cas, on a la formule suivante :

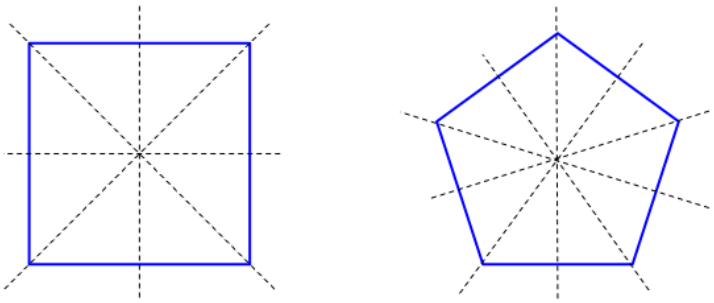
$$\phi(n) = n \prod_{p_i | n} \left(1 - \frac{1}{p_i}\right)$$

Cette formule sera démontré beaucoup plus loin dans le cours lorsque nous traiterons du théorème du reste chinois.

1.5 Les groupes dihédraux D_n

Une autre classe de groupe particulièrement importante, cette fois en géométrie, est la classe des groupes dihédraux D_{2n} [1]. D_{2n} est définie comme étant l'ensemble des symétries d'un polygone régulier à n côtés muni de l'opération de composition. Ici, on définit une symétrie comme étant une transformation rigide du plan, qui transforme le polygone sur lui même, donc une transformation pour laquelle l'image est identique au polygone d'origine. On remarque facilement qu'un polygone régulier à n côtés possède $2n$ symétries, c'est à dire n rotations, et n réflexions.

FIGURE 1.1 – Réflexions du carré et du pentagone régulier



1. Notez que la notation D_{2n} n'est pas tout à fait standard, en fait certain auteur préfère écrire tout simplement D_n pour le même groupe. Il faut donc faire très attention car la différence de notation peut porter à confusion. Dans ces notes, nous allons suivre la notation de [2].

Le groupe D_{2n} est plus facilement représenté en terme de générateur. Ici, deux générateurs sont suffisant, l'un représentant une rotation de $\frac{360}{n}$ degré (le r), et l'autre l'une des réflexions (le s). Il est facile de voir que le r doit être un élément d'ordre n, alors que le s doit être d'ordre 2. On obtient donc la représentation suivante :

$$D_{2n} = \langle r, s : r^n = s^2 = e, srs = r^{-1} \rangle$$

1.6 Le groupe de Klein V_4 et le groupe des quaternions Q_8

Nous avons vu pour le moment plusieurs famille de groupes importantes. Existe-t-il d'autre groupes qui ne font pas parti de ces familles ? La réponse est évidement oui, autrement un cours de théorie des groupes serait beaucoup trop facile. On est donc amener à chercher s'il existe d'autre groupe d'ordre 1, 2, 3, etc. En procédant de cette manière, le premier groupe que nous rencontrons qui ne fait parti d'aucune des familles que nous avons étudié jusqu'à présent est le groupe de Klein. Il s'agit d'un groupe d'ordre 4 que l'on dénote habituellement par V_4. Nous avons déjà rencontré ce groupe en tout début de chapitre, mais nous avons tout de même inclut sa table de multiplication ci-dessous. Ce groupe possède 3 éléments d'ordre 2, et un élément d'ordre 1 (l'identité). Il est aussi facile de voir que ce groupe est commutatif, car sa table de multiplication est symétrique. On peut l'écrire à partir de ses générateurs sous la forme suivante :

$$V_4 = \langle a, b : a^2 = b^2 = e \text{ et } ab = ba \rangle$$

Bien que pour le moment ce groupe ne fasse partie d'aucune des familles importantes que nous avons vu jusqu'à présent, avant la fin du chapitre nous allons voir qu'il est tout de même possible de l'obtenir à partir du groupe $\mathbb{Z}_2$ en utilisant la notion de produit direct.

L'étude du produit direct en fin de chapitre nous permettra de construire plusieurs nouveaux groupes. En continuant notre recherche de groupes ne faisant pas partie des familles que nous avons vu jusqu'à présent, et cette fois en excluant les groupes qui peuvent être obtenu à l'aide du produit direct, l'exemple suivant que l'on rencontre est le groupe de quaternion Q_8. Il s'agit d'un groupe non-commutatif d'ordre 8. Bien que ce groupe apparaisse naturellement lorsque l'on cherche à étendre les nombres complexes à un ensemble plus grand, au même titre que nous pouvons étendre les nombres réels au nombres complexes, sont intérêt pour nous sera essentiellement basé sur le fait qu'il s'agit du plus petit groupe ne faisant pas partie de nos grandes familles et qui ne peut pas être obtenu à partir de celles-ci. il pourra donc nous servir occasionellement de contre exemple.

Groupe de Klein (V_4)

*	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Groupe des quaternions (Q_8)

*	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

1.7 Les groupes de matrices $GL(n)$ et $SL(n)$

Dans cette section, nous voulons étudier deux autres familles de groupes particulièrement importantes : $GL(n)$ et $SL(n)$. Dans les deux cas, il s'agit d'ensemble de matrice, et donc une connaissance de l'algèbre linéaire est nécessaire. Nous allons donc commencer par rappeler certaine notion importante concernant les matrices, en commençant par les matrices 2×2 pour lesquels les définitions et démonstrations sont plus facile.

On dénote par $M_{2\times2}(\mathbb{R})$ l'ensemble de toute les matrices 2×2, c'est à dire

$$M_{2\times2}(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{R} \right\}$$

Sur cette ensemble, on définit les opérations d'additions et de multiplication suivante :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

L'opération d'addition n'est pas particulièrement intéressant pour nous dans le contexte de la théorie des groupes. En effet, l'ensemble des matrices muni de l'addition nous donne une structure qui est essentiellement équivalente à celle de $\mathbb{R}^4$. Nous allons donc nous concentrer sur la multiplication. Commençons par montrer que la multiplication est associativitive.

$$\begin{aligned}
\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right]\begin{pmatrix} i & j \\ k & l \end{pmatrix} &= \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}\begin{pmatrix} i & j \\ k & l \end{pmatrix} \\
&= \begin{pmatrix} aei+bgi+afk+bhk & aej+bgj+afl+bhl \\ cei+dgi+cfk+dhk & cej+dgj+cfl+dhl \end{pmatrix} \\
&= \begin{pmatrix} a(ei+fk)+b(gi+hk) & a(ej+fl)+b(gj+hl) \\ c(ei+fk)+d(gi+hk) & c(ej+fl)+d(gj+hl) \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} ei+fk & ej+fl \\ gi+hk & gj+hl \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\left[\begin{pmatrix} e & f \\ g & h \end{pmatrix}\begin{pmatrix} i & j \\ k & l \end{pmatrix}\right]
\end{aligned}$$

Donc la multiplication est bien associative. Nous allons maintenant chercher l'identité. On doit donc identifier des valeurs de e,f,g,h de sorte que :

$$\begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Dans ce cas, on obtient $e=1, f=0, g=0$ et $h=1$. De sorte qu'on peut facilement identifier l'identité comme étant :

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

La prochaine étape consiste à chercher l'inverse d'une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, pour ce faire, on doit trouver e,f,g,h tel que :

$$\begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Ce qui nous amène à résoudre les deux systèmes d'équations linéaires suivant :

$$\begin{cases} ae+bg=1 \\ ce+dg=0 \end{cases} \qquad \begin{cases} af+bh=0 \\ cf+dh=1 \end{cases}$$

Il est alors relativement facile de trouver les solutions suivante :

$$e = \frac{d}{ad-bc}, \quad f = \frac{-b}{ad-bc}, \quad g = \frac{-c}{ad-bc}, \quad h = \frac{a}{ad-bc}$$

En particulier, on remarque que pour qu'une solution existe, il est nécessaire que $ad-bc \neq 0$. On obtient donc :

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \Rightarrow \quad A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \quad \text{si } ad-bc \neq 0$$

La quantité $ad - bc$ est particulièrement importante en algèbre linéaire et porte un nom : Le déterminant. Nous devons maintenant regarder ce qui ce passe avec le déterminant lorsque l'on multiplie deux matrices. Prenons les deux matrices suivantes :

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ et } B = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \qquad \Rightarrow \qquad AB = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

En considérant les déterminants, on obtient donc :

$$\begin{aligned} \det(AB) &= (ae+bg)(cf+dh) - (af+bh)(ce+dg) \\ &= acef + adeh + bcfg + bdgh - acef - adfg - bceh - bdgh \\ &= adeh + bcfg - adfg - bceh \\ &= ad(eh-fg) + bc(fg-eh) \\ &= ad(eh-fg) - bc(eh-fg) \\ &= (ad-bc)(eh-fg) \\ &= \det(A)\det(B) \end{aligned}$$

Au vue de ce qu'on a montré, on est amener à faire les deux définitions suivantes :

$$GL(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{R}, ad-bc \neq 0 \right\}$$

$$SL(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{R}, ad-bc = 1 \right\}$$

Ces deux ensembles forment des groupes avec la multiplication des matrices. Ce que nous venons de faire peut se généralisé aux matrices $n \times n$, la difficulté dans ce cas est la nécessité de travailler avec des sommes.

Considérons l'ensemble $M_{n\times n}(\mathbb{R})$ de toutes les matrices $n \times n$. Si $A \in M_{2\times 2}(\mathbb{R})$, alors A aura la forme suivante :

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}$$

Remarquez la notation. Nous utilisons une lettre majuscule pour dénoté une matrice, et la lettre en minuscule correspondante pour dénoté les différent éléments. De plus, les indices sont utiliser pour indiquer la position de l'élément dans la matrice. Par exemple, on écrira a_{ij} pour dénoté l'élément de la matrice A qui se trouve sur la i-ième ligne et j-ième colonne. Maintenant, si A et B sont des éléments de $M_{n\times n}(\mathbb{R})$, alors on définie la multiplication comme suit :

$$C = AB \qquad \text{avec} \qquad c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

Les difficultés arrivent lorsque vient le temps de définir le déterminant et l'inverse d'une matrice. Le déterminant se définie réccursivement. Si A est une matrice $n \times n$ avec $n \geq 3$, alors on définit le mineur de A à la position ij, dénoté $M_{ij}(A)$, comme étant le déterminant de la matrice obtenu en enlevant la i-ième ligne et j-ième colonne de la matrice A. De plus, on définit le cofacteur de la matrice A à la position ij, dénoté $C_{ij}(A)$ comme étant $C_{ij}(A) = (-1)^{ij} M_{ij}(A)$. Ceci nous permet de définir le déterminant de A :

$$\det(A) = \sum_{k=1}^{n} a_{1k} C_{1k}(A)$$

Dans ce cas, on peut démontrer que A est inversible si et seulement si $\det(A) \neq 0$, et dans ce cas, l'inverse est donné par la formule suivante :

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} C_{11}(A) & C_{21}(A) & C_{31}(A) & \dots & C_{n1}(A) \\ C_{12}(A) & C_{22}(A) & C_{32}(A) & \dots & C_{n2}(A) \\ C_{13}(A) & C_{23}(A) & C_{33}(A) & \dots & C_{n3}(A) \\ \vdots & \vdots & \vdots & & \vdots \\ C_{1n}(A) & C_{2n}(A) & C_{3n}(A) & \dots & C_{nn}(A) \end{pmatrix}$$

La démonstration qu'il s'agit bien de l'inverse d'une matrice est technique et vous est laissé en exercice. Ce qui est important est que les propriétés que nous avons démontré pour les matrices 2×2 sont aussi valide pour les matrices $n \times n$, ce qui nous permet d'obtenir le théorème suivant :

Théorème 1.7.1. Si n est un entier supérieur ou égal à 2, alors les deux ensembles ci-dessous muni de la multiplication des matrices forment des groupes (non commutatif).

$$GL(n) = \{A \in M_{n\times n}(\mathbb{R}) : \det(A) \neq 0\}$$

$$SL(n) = \{A \in M_{n\times n}(\mathbb{R}) : \det(A) = 1\}$$

1.8 Le produit direct

Nous allons maintenant voir une construction importante nous permettant de construire un nouveau groupe à partir de deux groupes donnés. Il s'agit du produit direct.

Definition 1.8.1. Si $(G, *)$ et $(H, \cdot)$ sont des groupes, alors on définit le produit direct $G \times H$ comme étant l'ensemble :

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

Menu de l'opération $\circ$ définie par :

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 * g_2, h_1 \cdot h_2)$$

Théorème 1.8.1. Si $(G, *)$ et $(H, \cdot)$ sont des groupes, alors l'opération $\circ$ définie ci-dessus sur l'ensemble $G \times H$ est bien définie, et $(G \times H, \circ)$ forme un groupe. De plus, si G et H sont abélien, alors $G \times H$ est aussi abélien.

Démonstration. Pour montrer qu'il s'agit bien d'un groupe, on doit montrer que $\circ$ est associative, qu'il existe un élément neutre, et que chaque élément possède un inverse.

1. Prenons $(g_1, h_1), (g_2, h_2)$ et (g_3, h_3) dans $G \times H$. On a donc :

$$\begin{aligned}
[(g_1, h_1) \circ (g_2, h_2)] \circ (g_3, h_3) &= (g_1 * g_2, h_1 \cdot h_2) \circ (g_3, h_3) \\
&= ((g_1 * g_2) * g_3, (h_1 \cdot h_2) \cdot h_3) \\
&= (g_1 * (g_2 * g_3), h_1 \cdot (h_2 \cdot h_3)) \\
&= (g_1, h_1) \circ (g_2 * g_3, h_2 \cdot h_3) \\
&= (g_1, h_1) \circ [(g_2, h_2) \circ (g_3, h_3)]
\end{aligned}$$

   On peut donc affirmer que $\circ$ est associative.

2. Supposons que e_G est l'identité du groupe G et e_H est l'identité du groupe H. On veut montrer que (e_G, e_H) est l'identité de $G \times H$. Pour ce faire, prenons $(g, h) \in G \times H$, on a donc :

$$(e_G, e_H) \circ (g, h) = (e_G * g, e_H \cdot h) = (g, h)$$

$$(g, h) \circ (e_G, e_H) = (g * e_G, h \cdot e_H) = (g, h)$$

3. On veut maintenant démontrer l'existence d'inverse. Prenons $(g, h) \in G \times H$, on veut montrer que (g^{-1}, h^{-1}) est son inverse.

$$(g, h) \circ (g^{-1}, h^{-1}) = (g * g^{-1}, h \cdot h^{-1}) = (e_G, e_H)$$

$$(g^{-1}, h^{-1}) \circ (g, h) = (g^{-1} * g, h^{-1} \cdot h) = (e_G, e_H)$$

Ce qui confirme qu'il s'agit bien de l'inverse de (g, h). Tout les éléments de $G \times H$ sont donc bien inversible.

On peut donc affirmer que $(G \times H, \circ)$ est bien un groupe. □

Exemple 1.8.1. On veut construire la table de multiplication du groupe $\mathbb{Z}_2 \times \mathbb{Z}_4$. Pour ce faire, remarquons que les éléments de ce groupe ont la forme (a, b) avec $a \in \mathbb{Z}_2$ et $b \in \mathbb{Z}_4$. De plus, si (a, b) et (c, d) sont dans le groupe, alors le product est $(a, b) * (c, d) = (ac, bd)$ où le produit ac est calculé dans $\mathbb{Z}_2$ et le produit bd est calculé dans le groupe $\mathbb{Z}_4$. On a donc la table suivante :

Le groupe $\mathbb{Z}_2 \times \mathbb{Z}_4$

$*$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,0)$
$(0,2)$	$(0,2)$	$(0,3)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,3)$	$(1,0)$	$(1,1)$
$(0,3)$	$(0,3)$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,3)$	$(1,0)$	$(1,1)$	$(1,2)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,0)$
$(1,2)$	$(1,2)$	$(1,3)$	$(1,0)$	$(1,1)$	$(0,2)$	$(0,3)$	$(0,0)$	$(0,1)$
$(1,3)$	$(1,3)$	$(1,0)$	$(1,1)$	$(1,2)$	$(0,3)$	$(0,0)$	$(0,1)$	$(0,2)$

Exemple 1.8.2. Dans le groupe $S_3 \times D_8$, quel est l'ordre de l'élément (σ, s). Pour ce faire, nous devons calculer les différente puissance jusqu'à ce qu'on obtienne l'identité :

$(\sigma, s)^1 = (\sigma, s) \neq (e, e)$
$(\sigma, s)^2 = (\sigma^2, s^2) = (\sigma^2, e) \neq (e, e)$
$(\sigma, s)^3 = (\sigma^3, s) = (e, s) \neq (e, e)$
$(\sigma, s)^4 = (\sigma, s^2) = (\sigma, e) \neq (e, e)$
$(\sigma, s)^5 = (\sigma^2, s) = (\sigma^2, s) \neq (e, e)$
$(\sigma, s)^6 = (\sigma^3, s^2) = (e, e)$

L'ordre de l'élément (σ, s) est donc 6.

1.9 Remarques sur la notation

Nous avons vu qu'un groupe est un ensemble G muni d'un opération $*$. Il s'agit donc d'un couple $(G, *)$, pour lequel l'ensemble et l'opération sont indissociable. Bien qu'il soit courant de faire référence au groupe G, ceci n'est qu'un abus de langage, car sans savoir quelle est l'opération, il n'est pas possible d'affirmer que G soit un groupe. Par contre, cet abus reste très pratique pour simplifier l'écrire, et nous allons continuer à utiliser cette notation jusqu'à la fin du cours.

Lorsque deux groupes ou plus interviennent dans un problème, le symbol utilisé pour leur opération respective est particulièrement important. Par contre, lorsque un seul groupe intervient dans un problème, le symbol utilisé n'est pas vraiment important, car il n'y a pas de risque de confusion. Un groupe possède une seule opération. Le plus souvent, nous allons donc utiliser ce que l'on appelle la notation multiplicative. C'est à dire, si G est un groupe, nous allons traiter l'opération comme une multiplication et écrire ab à la place de $a * b$. De la même manière, on écrit a^n pour signifier $\underbrace{aaa...a}_{n \text{ fois}}$.

Il existe cependant une autre notation couramment utilisé : La notation additive. Cette dernière est cependant réservé aux groupes abéliens, parfois justement pour mettre l'emphase sur le fait que l'opération est commutative. Donc si G est un groupe abélien, on peut écrire $a + b$ à la place de $a * b$. Dans ce cas, on écrira na pour signifier $\underbrace{a + a + a + ... + a}_{n \text{ fois}}$.

Notez qu'il n'est cependant pas permis dans le même problème, d'utiliser en même temps la notation additive et multiplicative pour un même groupe. Notez aussi que comme un groupe ne possède qu'une seule opération, il n'y a normalement pas de confusion possible.

Chapitre 2

Les sous-groupes

2.1 Introduction

Dans ce chapitre, nous somme maintenant intéressé à étudier le concept de sous-groupe. L'idée étant qu'un groupe, en toute généralité, peut être particulièrement difficile à étudier. Il est donc souvent plus facile d'étudier une structure plus petite et qui est comprise dans notre groupe. Il s'agit d'une idée récurrente en mathématiques, et en particulier c'est ce qui a été fait en algèbre linéaire lorsque vous avez étudier les sous-espaces vectoriels. Le but de ce chapitre est d'établir le théorème de Lagrange, l'un des théorèmes les plus important de la théorie des groupes. Il nous permettra d'obtenir de très nombreuses informations sur nos groupes.

Definition 2.1.1. On dit que H est un sous-groupe d'un groupe G si H est un sous-ensemble de G qui est aussi un groupe. Dans ce cas, on écrit $H \leq G$.

Exemple 2.1.1. Si G est un groupe quelconque, alors $\{e\} \leq G$ et $G \leq G$.

Les sous-groupes d'un groupe symétrique joue un rôle important dans la théorie et portent un nom particulier : Les groupes de permutations. Historiquement, les premiers groupes à avoir été étudiés était les groupes de permutations, et ce avant même que la définition moderne d'un groupe voie le jour.

Théorème 2.1.1. Si G est un groupe, et H un sous-ensemble non-vide de G, alors H est un sous-groupe si et seulement si

$$xy^{-1} \in H, \quad \forall x, y \in H$$

Démonstration. Supposons que G est un groupe, et H un sous-ensemble de G tel que

$$xy^{-1} \in H, \quad \forall x, y \in H$$

On doit montrer que si H satisfait les trois axiomes d'un groupe.

1. L'opération sur H est nécessairement associative, car l'opération est la même que celle sur G.
2. Comme H est non-vide, on peut choisir un $x \in H$, alors $xx^{-1} = e \in H$. Donc l'identité est bien dans H.
3. Si $x \in H$, comme l'identité e est aussi dans H, alors on doit avoir $ex^{-1} = x^{-1} \in H$. Donc les inverses sont bien dans H.

On peut donc conclure que H est bien un groupe, et donc un sous-groupe de G. D'un autre côté, tout les groupes doivent satisfaire $xy^{-1} \in H, \forall x, y \in H$ par définition, ce qui complète la démonstration. □

Definition 2.1.2. Si $S = \{g_1, g_2, ...g_k\}$ sont des éléments d'un groupe G, alors on définit le sous-groupe généré par les éléments de S comme étant le plus petit groupe contenant les éléments de S. On le dénote par $\langle S \rangle$ ou bien $\langle g_1, g_2, ...g_k \rangle$.

Exemple 2.1.2. Si G est un groupe, et H, K sont des sous-groupes de G, alors $H \cap K$ est aussi un sous-groupe de G.

Exemple 2.1.3. Si G et H sont des groupes, alors $G \times \{e_H\}$ et $\{e_G\} \times H$ sont des sous-groupes de $G \times H$. Nous allons faire la démonstration pour $G \times \{e_H\}$ et laisser l'autre en exercice. Prenons (g_1, e_H) et (g_2, e_H) dans $G \times \{e_H\}$. Alors, on a :

$$(g_1, e_H)(g_2, e_H)^{-1} = (g_1, e_H)(g_2^{-1}, e_H^{-1}) = (g_1, e_H)(g_2^{-1}, e_H) = (g_1 g_2^{-1}, e_H)$$

Comme G est un groupe, alors $g_1 g_2^{-1} \in G$. On a donc $(g_1 g_2^{-1}, e_H) \in G \times \{e_H\}$, ce qui confirme que $G \times \{e_H\}$ est bien un sous-groupe de $G \times H$.

Exemple 2.1.4. Pour tout entier k, alors $k\mathbb{Z} = \{kn : n \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$.

Exemple 2.1.5. Si H est un sous-groupe de $\mathbb{Z}$, alors il existe un $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$. Pour le montrer, considérons l'ensemble $K = \{x \in H : x > 0\}$. Comme il s'agit d'un sous-ensemble non vide de nombre naturel, par la propriété du bon ordre il existe un plus petit élément. Posons $k = \min(K)$. Il est facile de voir que comme H est un groupe et $k \in H$, alors $k\mathbb{Z} \subseteq H$. Supposons que $H \neq k\mathbb{Z}$, alors il existe un $a \in H \backslash k\mathbb{Z}$. Comme H est un groupe additif, $-a$ doit aussi être dans H, et ne peut pas non plus être dans $k\mathbb{Z}$. Donc sans perte de généralité, on peut supposer $a > 0$. Par le théorème de Bézout, il existe donc des entiers x et y tel que $ax + ky = (a, k)$. Comme H est un groupe et $a, k \in H$, on a donc que $(a, k) \in K$. Comme par hypothèse $k \nmid a$, on doit donc avoir $(a, k) < k$, ce qui contredit l'hypothèse que k était le minimum de K. On doit donc avoir $H = k\mathbb{Z}$.

Exemple 2.1.6. Dans le groupe $GL(2)$, considérons les éléments $a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $b = \begin{pmatrix} 0 & 1/2 \\ 2 & 0 \end{pmatrix}$. Quel est l'ordre des groupes $\langle a \rangle$, $\langle b \rangle$ et $\langle a, b \rangle$? Comme $a^2 = b^2 = I$, où I dénote la matrice identité, il est facile de voir que $\langle a \rangle$ et $\langle b \rangle$ sont tous deux des sous-groupes d'ordre 2. Par contre, les choses ce complique légèrement pour le sous-groupe $\langle a, b \rangle$.

$$ab = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1/2 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

Comme ab est une matrice diagonale, il est donc facile de calculer sa puissance, on a donc :

$$(ab)^k = \begin{pmatrix} 2^k & 0 \\ 0 & 1/2^k \end{pmatrix}$$

Maintenant, comme pour toutes les valeurs de k on a $(ab)^k \in \langle a, b \rangle$, on obtient donc que ce sous-groupe est d'ordre infinie.

Exemple 2.1.7. Dans le groupe S_n, on définit $\tau = (12)$ et $\sigma = (1234...n)$. Si $H \leq S_n$ et H contient τ et σ, on veut montrer que $H = S_n$. Pour ce faire, commençons par remarquer que pour tout $k \in \{1, 2, 3, ...n-1\}$ on a :

$$\sigma^{k-1} \tau (\sigma^{-1})^{k-1} = (k \ (k+1))$$

Comme H est un groupe, on a donc que toutes les transpositions de la forme $(k \ (k+1))$ sont dans H. Maintenant, remarquons que :

$$((k-1) \ k)(1 \ (k-1))((k-1) \ k) = (1 \ k)$$

Par induction, on obtient donc que toutes les transpositions de la forme $(1 \ k)$ sont dans H. De plus, il n'est pas très difficile de remarquer que

$$(1 \ b)(1 \ a)(1 \ b) = (a \ b)$$

Donc comme toute les transpositions de la forme $(1 \ k)$ sont dans H, on doit avoir que toute les transpositions sont dans H. Finalement, comme toutes les permutations de S_n peuvent s'écrire comme produit de transposition, on doit donc avoir que $H = S_n$.

Exemple 2.1.8. En procédant de manière similaire à ce que nous avons fait dans l'exemple précédent, on peut montrer que si $H \leq S_n$ et H contient les éléments $\tau = (123)$ et $\sigma = (1234...n)$, alors $H = A_n$ ou $H = S_n$. En particulier, dans S_n on a que $A_n = \langle \sigma, \tau \rangle$.

2.2 Centralisateur, normalisateur et le centre d'un groupe

Si G est un groupe, nous allons maintenant nous intéressé à certain sous-groupe important de G qui reviendront fréquemment durant toute notre étude de la théorie des groupes. Il s'agit du stabilisateur, du normalisateur et du centre du groupe.

Definition 2.2.1. Si G est un groupe, alors on définit le centre du groupe , dénoté $Z(G)$ comme étant l'ensemble :

$$Z(G) = \{x \in G : xy = yx, \forall y \in G\}$$

Le centre d'un groupe est donc l'ensemble des éléments qui commutent avec tous les éléments du groupe. En particulier, pour n'importe quel groupe G, l'identité doit être dans $Z(G)$ ce qui fait que le centre ne peut pas être vide.

Théorème 2.2.1. Pour tout groupe G, le centre $Z(G)$ est un sous-groupe abélien de G.

Démonstration. Supposons que $x \in Z(G)$ et $g \in G$, alors on a :

$$\begin{aligned}
xg &= gx && \text{par définition du centre}\\
xgx^{-1} &= gxx^{-1} && \text{en multipliant à droite des deux côtés par } x^{-1}\\
xgx^{-1} &= g && \text{en simplifiant}\\
x^{-1}xgx^{-1} &= x^{-1}g && \text{en multipliant à gauche des deux côtés par } x^{-1}\\
gx^{-1} &= x^{-1}g && \text{en simplifiant}
\end{aligned}$$

Comme g est un élément quelconque du groupe G, on peut donc conclure que $x^{-1} \in Z(G)$. Maintenant si on prend $x, y \in Z(G)$ et $g \in G$, alors on obtient :

$$xy^{-1}g = xgy^{-1} = gxy{-}1$$

On peut donc conclure que $xy^{-1} \in Z(G)$, ce qui démontre que $Z(G)$ est bien un sous-groupe de G. Finalement, il est évident par définition que $Z(G)$ doit être abélien, ce qui complète la démonstration. □

Exemple 2.2.1. Si G est un groupe abélien, alors $Z(G) = G$.

Exemple 2.2.2. On veut trouver le centre du groupe $GL(2)$. Si $A \in Z(GL(2))$, alors A doit commuter avec tout les éléments de $GL(2)$. En particulier, A doit commuter avec les matrices $\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$ et $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$. On doit donc avoir :

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix} \Rightarrow \begin{pmatrix}a+b & b\\ c+d & d\end{pmatrix} = \begin{pmatrix}a & b\\ a+c & b+d\end{pmatrix} \Rightarrow \begin{cases} b = 0\\ a = d\end{cases}$$

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix} \Rightarrow \begin{pmatrix}a & a+b\\ c & c+d\end{pmatrix} = \begin{pmatrix}a+c & b+d\\ c & d\end{pmatrix} \Rightarrow \begin{cases} c = 0\\ a = d\end{cases}$$

Donc les seuls candidats possible pour le centre sont de la forme $\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}$ avec $a \neq 0$. Nous allons maintenant montrer que toutes les matrices de cette forme sont bien dans le centre. On a donc :

$$\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}\begin{pmatrix}x & y\\ z & w\end{pmatrix} = \begin{pmatrix}ax & ay\\ az & aw\end{pmatrix} = \begin{pmatrix}x & y\\ z & w\end{pmatrix}\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}$$

Ce qui nous donne :

$$Z(GL(2)) = \left\{\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}, a \neq 0\right\}$$

Plus généralement, si A est un sous-ensemble d'un groupe G, on peut s'intéresser à l'ensemble des éléments de G qui commutent avec avec tous les éléments de A. C'est ce qu'on appelle le centralisateur.

Definition 2.2.2. Si A est un sous-ensemble d'un groupe G, alors on définit le centralisateur $C_G(A)$ comme étant :

$$C_G(A) = \{x \in G : xa = ax, \forall a \in A\}$$

De plus, si $a \in G$, alors on écrit $C_G(a)$ plutôt que $C_G(\{a\})$.

De la définition précédente, on remarque facilement que si G est un groupe, alors $C_G(G) = Z(G)$.

Théorème 2.2.2. Si A est un sous-ensemble d'un groupe G, alors $C_G(A)$ est un sous-groupe de G et

$$C_G(A) = \bigcap_{a \in A} C_G(a)$$

Démonstration. Supposons que G est un groupe, et A un sous-ensemble de G. Premièrement, remarquons qu'il est évident que l'ensemble $C_G(A)$, car l'identité commute avec tous les éléments de G, et donc en particulier ceux que A. Prenons $x, y \in C_G(A)$, alors on a :

$$\begin{aligned}
ya = ay, \quad & \forall a \in A && \text{par définition de l'ensemble } C_G(A) \\
y^{-1}ya = y^{-1}ay, \quad & \forall a \in A && \text{en multipliant à gauche par } y^{-1} \\
a = y^{-1}ay, \quad & \forall a \in A && \text{en simplifiant} \\
ay^{-1} = y^{-1}ayy^{-1}, \quad & \forall a \in A && \text{en multipliant à droite par } y^{-1} \\
ay^{-1} = y^{-1}a, \quad & \forall a \in A && \text{en simplifiant}
\end{aligned}$$

On remarque donc que $y^{-1} \in C_G(A)$, ce qui nous permet d'écrire :

$$(xy^{-1})a = x(y^{-1}a) = x(ay^{-1}) = (xa)y^{-1} = (ax)y^{-1} = a(xy^{-1}), \quad \forall a \in A$$

On peut donc conclure que $xy^{-1} \in C_G(A)$, et donc $C_G(A)$ est bien un sous-groupe de G. Finalement, par définition des ensembles $C_G(A)$ et $C_G(a)$, l'égalité ci-dessous est évidente :

$$C_G(A) = \bigcap_{a \in A} C_G(a)$$

□

Definition 2.2.3. Si A est un sous-ensemble d'un groupe G, alors on définit le normalisateur $N_G(A)$ comme étant :

$$N_G(A) = \{g \in G : gAg^{-1} = A\} = \{g \in G : gA = Ag\}$$

Notez que bien que la notion de normalisateur et de centralisateur se ressemblent beaucoup, elles sont bel et bien différente. Dans la définition du normalisateur, on ne suppose absoluement pas que $x \in N_G(A)$ commute avec chacun des éléments de A, mais plutôt que pour chaque $a \in A$, il existe un $b \in A$ tel que $xa = bx$ et vice versa. Donc x commute avec l'ensemble A, mais pas nécessairement avec chacun de ses éléments individuellement.

Théorème 2.2.3. Si A est un sous-ensemble d'un groupe G, alors $N_G(A)$ est un sous-groupe de G.

Démonstration. Supposons que G est un groupe, et A un sous-ensemble de G. Il est facile de voir que dans ce cas, l'identité e se trouve dans $N_G(A)$ car il commute avec tous les éléments de G. En particulier, on peut

affirmer que $N_G(A)$ n'est pas vide. Supposons que $y \in N_G(A)$, et prenons $a \in A$, il existe donc un $b \in A$ tel que $ay = yb$, ce qui nous donne :

$$ay = yb \quad \Rightarrow \quad ayy^{-1} = yby^{-1} \quad \Rightarrow \quad a = yby^{-1} \quad \Rightarrow \quad y^{-1}a = y^{-1}yby^{-1} \quad \Rightarrow \quad y^{-1}a = by^{-1} \subseteq Ay^{-1}$$

On a donc que $y^{-1}A \subseteq Ay^{-1}$. L'autre inclusion ce faire de manière très semblable et vous est laissé en exercice. On peut donc affirmer que si $y \in N_G(A)$, alors $y^{-1} \in N_G(A)$. Maintenant, supposons que $x, y \in N_G(A)$, et prenons $a \in A$. Il existe donc un $b \in A$ tel que $y^{-1}a = by^{-1}$. De plus, il existe un $c \in A$ tel que $xb = cx$. On obtient donc :

$$(xy^{-1})a = x(y^{-1}a) = x(by^{-1}) = (xb)y^{-1} = (cx)y^{-1} = c(xy^{-1}) \subseteq A(xy^{-1})$$

On peut donc affirmer que $xy^{-1}A \subseteq A(xy^{-1})$. L'autre inclusion est très semblable et vous est laissé en exercice. On a donc obtenu que $(xy^{-1})A = A(xy^{-1})$, et donc $xy^{-1} \in N_G(A)$. On peut donc affirmer que $N_G(A)$ est bien un sous-groupe de G. □

Théorème 2.2.4. Si A est un sous-ensemble de G, alors $C_G(A) \leq N_G(A)$

Démonstration. Si G est un groupe et A un sous-ensemble de G, alors il est facile de voir que $C_G(A)$ est un sous-ensemble de $N_G(A)$ par leur définition respective. Maintenant comme nous savons que $C_G(A)$ forme un groupe, il doit donc s'agir d'un sous-groupe de $N_G(A)$. □

2.3 Le théorème de Lagrange

Nous allons maintenant regarder l'un des théorèmes les plus important de la théorie des groupes. il s'agit du théorème de Lagrange qui nous permet d'obtenir des informations sur l'ordre des sous-groupes d'un groupe. Avant d'énoncer le théorème, nous allons cependant introduire la notion de classe à gauche d'un groupe.

Definition 2.3.1. Si G est un groupe, H un sous-groupe de G, et $x \in G$, alors on définit la classe à gauche xH comme étant :

$$xH = \{xh : h \in H\}$$

De la même manière, on peut définir la classe à droite Hx comme étant :

$$Hx = \{hx : h \in H\}$$

Théorème 2.3.1. Si G est un groupe et H un sous-groupe de G, alors l'ensemble des classes à gauche partitionne G. C'est à dire que si $x, y \in G$, alors $xH = yH$ ou $xH \cap yH = \varnothing$. De plus :

$$G = \bigcup_{x \in G} xH$$

Démonstration. Supposons que G est un groupe, et H un sous-groupe de G. Prenons $x, y \in G$ et supposons que $g \in xH \cap yH \neq \varnothing$. Prenons $xh_1 \in xH$. On veut montrer que $xh_1 \in yH$. Pour ce faire, il suffit de remarquer que comme $g \in xH \cap yH$, alors il existe $a, b \in H$ tel que $g = xa = yb$, donc $x = yba^{-1}$. On obtient donc :

$$xh_1 = (yba^{-1})h_1 = y(ba^{-1}h_1) = yh_2 \quad \text{où} \quad h_2 = ba^{-1}h_1$$

Comme H est un groupe et $a, b, h_1 \in H$, on a donc que $h_2 \in H$, ce qui signifie que $xh_1 = yh_2 \in yH$. Donc si $xH \cap yH \neq \varnothing$, alors $xH = yH$. Maintenant, pour la seconde partie du théorème, il suffit de remarquer que comme $e \in H$, alors pour tout $g \in G$, on a $g \in gH$. Ce qui nous donne :

$$G = \bigcup_{x \in G} xH$$

□

Théorème 2.3.2. **(Théorème de Lagrange)** Si G est un groupe fini et H un sous-groupe de G, alors

$$|H| \Big| |G|$$

Démonstration. Si G est un groupe et H un sous-groupe de G, alors on sait déjà que les classes à gauche de H partitionne G en classe disjointe. Nous allons maintenant essayer de montrer que toutes ces classes contiennent le même nombre d'élément. Pour ce faire, prenons $x \in G$ et définissons la fonction

$$f : H \to xH$$

$$f(h) = xh$$

Remarquez qu'il ne s'agit pas en général d'un homomorphisme. On veut montrer que la fonction f est bijective, pour ce faire, commençons par montrer qu'elle est injective. Supposons que $g, h \in H$ sont tel que $f(g) = f(h)$, alors on a :

$$f(g) = f(h) \quad \Rightarrow \quad xg = xh \quad \Rightarrow \quad x^{-1}xg = x^{-1}xh \quad \Rightarrow \quad g = h$$

donc la fonction est bien injective. On veut maintenant montrer qu'elle est surjective. Pour ce faire, prenons $h \in xH$, en posant $g = x^{-1}h$, alors on obtient :

$$f(g) = f(x^{-1}h) = xx^{-1}h = h$$

La fonction est donc surjective. Comme f est un bijection entre H et xH, on peut donc conclure que ces deux ensembles contiennent le même nombre d'élément. Finalement, comme le x est arbitraire, on peut donc conclure que chacune des classes à gauche contient le même nombre d'élément. Comme G est l'union de classe à gauche disjointe, le nombre d'élément de G est donc un multiple du nombre d'élément de H, ce qui nous donne le résultat. □

Corollaire 2.3.1. Si G est un groupe et $x \in G$, alors l'ordre de l'élément x divise l'ordre du groupe G.

Démonstration. Si G est un groupe et $x \in G$, alors posons $H = \langle x \rangle$, c'est à dire que H est le sous-groupe de G engendré par x. Dans ce cas, il est facile de voir que l'ordre de H égal l'ordre de l'élément x. Par le théorème de Lagrange, l'ordre de H divise l'ordre de G, ce qui signifie que l'ordre de x divise l'ordre de G. □

Corollaire 2.3.2. Si G est un groupe d'ordre p, où p est un nombre premier, alors les seuls sous-groupes de G sont $\{e\}$ et G.

Démonstration. Si G est un groupe d'ordre p où p est un nombre premier. Par le corollaire précédent, si $x \in G$, alors l'ordre de x doit diviser p. Comme p est premier, l'ordre de x doit donc être 1 ou p. Comme e est le seul élément d'ordre 1, si $x \neq e$ on doit donc que l'ordre de x est p. On a donc $\langle x \rangle = G$. Comme ceci est le cas pour tout $x \neq e$. On peut donc conclure que les seuls sous groupe de G sont $\{e\}$ et G. □

Nous allons maintenant voir deux autres applications du théorème de Lagrange. Il s'agit du théorème d'Euler, et du petit théorème de Fermat. C'est deux théorèmes jouent un rôle particulièrement important en théorie des nombres, et en particulier dans les applications à la cryptographie. La cryptographie RSA [1], l'une des plus répondu en particulier sur internet, n'est en fait rien d'autre qu'une application des ces deux théorèmes.

Corollaire 2.3.3. **(Théorème d'Euler)** Si $a, n \in \mathbb{N}$ sont des nombres copremier (c'est à dire leur PGCD est 1), avec $n \geq 2$, alors :

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Démonstration. Supposons que $n \in \mathbb{Z}$, $n \geq 2$, et considérons le groupe $G = \mathbb{Z}_n^\times$. Nous avons déjà vu que l'ordre de ce groupe est $\phi(n)$. Posons $H = \langle a \rangle$, donc H est clairement un sous-groupe de G, et par le théorème de Lagrange, on peut affirmer que $|H| \Big| |G|$. Il existe donc un entier k tel que $k|H| = \phi(n)$. Maintenant, comme l'ordre du groupe H n'est rien d'ordre que l'ordre de l'élément a, on a donc :

$$a^{\phi(n)} = a^{k|H|} = \left(a^{|H|}\right)^k = 1^k = 1$$

□

Corollaire 2.3.4. **(Petit théorème de Fermat)** Si p est un nombre premier, et $a \in \mathbb{N}$ est un nombre tel que $a \nmid p$, alors :

$$a^{p-1} \equiv 1 \pmod{p}$$

Démonstration. La démonstration est essentiellement identique à celle du théorème d'Euler une fois qu'on a remarquer que si p est un nombre premier, alors $\phi(p) = p - 1$. □

2.4 Treillis des sous-groupes

Pour compléter ce chapitre, nous allons introduire la notion de treillis des sous-groupes d'un groupe. Il s'agit tout simplement d'une manière graphique de représenter l'ensemble de tous les sous-groupes d'un groupe donné. Pour le moment, il ne nous manque encore beaucoup de théorie, et donc il est difficile de pouvoir être complètement certain que nos schémas sont vraiment complet.

Exemple 2.4.1. Pour le groupe $(\mathbb{Z}_2, +)$, on a le treillis suivant :

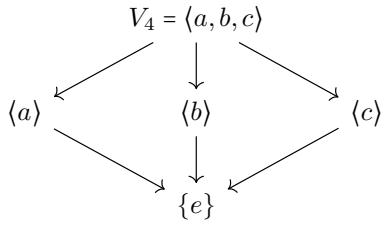
$$\begin{array}{c} \mathbb{Z}_2 = \langle 1 \rangle \\ \downarrow \\ \{0\} = \langle 0 \rangle \end{array}$$

Exemple 2.4.2. Pour le groupe $(\mathbb{Z}_4, +)$, on a le treillis suivant :

$$\begin{array}{c} \mathbb{Z}_4 = \langle 1 \rangle = \langle 3 \rangle \\ \downarrow \\ \langle 2 \rangle \\ \downarrow \\ \{0\} = \langle 0 \rangle \end{array}$$

1. La cryptographie RSA est une méthode de cryptage à clé publique basé sur la très grande difficulté à factoriser un grand nombre comme produit de nombres premiers. Elle a été décrite pour la première fois en 1977 au MIT par Ron Rivest, Adi Shamir, et Leonard Adleman. L'acronyme RSA est basé sur l'initiale de leur nom de famille.

Exemple 2.4.3. Pour le groupe de Klein V_4, on a le treillis suivant :



Remarquez que $\mathbb{Z}_4$ et V_4 sont tous les deux des groupes d'ordre 4. Par contre, on remarque que leur treillis de sous-groupes sont différents, et donc ces deux groupes, dans un certain sens, doivent être différent.

Chapitre 3

Les homomorphismes

3.1 Introduction

Dans ce chapitre, nous somme maintenant intéressé à introduire une notion de fonctions entre deux groupes. Pour être intéressante, cette notion de fonction doit être compatible avec les opérations qui sont définie sur notre groupe. C'est ce qui nous amène à parler d'homomorphisme de groupe que nous allons définir immédiatement.

Definition 3.1.1. Si G et H sont des groupes, alors on appelle homomorphisme une fonction $\phi : G \to H$ telle que

$$\phi(xy) = \phi(x)\phi(y), \quad \forall x, y \in G$$

De plus, si ϕ est aussi inversible, alors on dit que ϕ est un isomorphime, et on dit que G et H sont isomorphique. Dans ce cas, on écrit $G \cong H$.

Remarquez qu'un homomorphisme en théorie des groupes joue un rôle similaire à celui des applications linéaires en algèbre linéaire. La notion de groupe isomorphique signifie que les deux groupes sont essentiellement identique. Notez aussi que la notion d'homomorphisme dépend du type de structure qui nous intéresse. Lorsque nous étudierons les anneaux et les corps, il nous faudra donner une nouvelle définition d'homomorphisme qui sera approprié pour ces structures.

Théorème 3.1.1. Si G et H sont des groupes et $\phi : G \to H$ est un homomorphisme, alors :

1. $\phi(e) = e$
2. $\phi(x^{-1}) = [\phi(x)]^{-1}$ pour tout $x \in G$.
3. Pour tout $k \in \mathbb{N}$, alors $\phi(x^k) = [\phi(x)]^k$ pour tout $x \in G$.

Démonstration.

1. Par définition d'un homomorphisme, on sait que $\phi(e) = \phi(e^2) = \phi(e)\phi(e)$, maintenant, en multipliant par l'inverse de $\phi(e)$ de chaque côté, on obtient

   $$\phi(e)[\phi(e)]^{-1} = \phi(e)\phi(e)[\phi(e)]^{-1}$$

   Puis en simplifiant on obtient le résultat : $e = \phi(e)$.
2. Prenons $x \in G$, alors par définition de l'inverse et d'un homomorphisme on a :

   $$e = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$$

   On peut donc conclure que $[\phi(x)]^{-1} = \phi(x^{-1})$.

3. Prenons $x \in G$ et $k \in \mathbb{N}$, alors on a :

$$\phi(x^k) = \phi(xx...x) = \phi(x)\phi(x)...\phi(x) = [\phi(x)]^k$$

□

Exemple 3.1.1. Si G et H sont des groupes, alors on peut définir deux homomorphismes canoniques sur le produit direct $G \times H$:

$$\pi_G : G \times H \to G, \qquad \pi_G(g,h) = g$$
$$\pi_H : G \times H \to H, \qquad \pi_H(g,h) = h$$

Pour le démontrer, il suffit d'appliquer directement la définition. On a donc :

$$\pi_G\Big((g_1,h_1)(g_2,h_2)\Big) = \pi_G(g_1g_2, h_1h_2) = g_1g_2 = \pi_G(g_1,h_1)\pi_G(g_2,h_2)$$

$$\pi_H\Big((g_1,h_1)(g_2,h_2)\Big) = \pi_H(g_1g_2, h_1h_2) = h_1h_2 = \pi_H(g_1,h_1)\pi_H(g_2,h_2)$$

Lorsque nous avons introduit la notion de groupe symétrique, nous avons définie les notions de fonctions injectives, surjectives et bijectives. Étant donné qu'un homomorphisme est en particulier une fonction, ces notions s'appliquent donc aux homomorphismes, et dans ce cas un vocabulaire particulier est utilisé.

Definition 3.1.2. Si G et H sont des groupes et $\phi : G \to H$ est un homomorphisme, alors on dit que :

1. ϕ est un monomorphisme si ϕ est injective.
2. ϕ est un épimorphisme si ϕ est surjective.
3. ϕ est un isomorphisme si ϕ est bijective.

Dans le cas ou ϕ est un homomorphisme d'un groupe vers lui même, disons $\phi : G \to G$, alors on dit que ϕ est un endomorphisme. Finalement, un endomorphisme bijectif est appellé un automorphisme.

En particulier, c'est la notion d'isomorphisme qui va nous permettre de déterminer si deux groupes sont identiques ou non. Cette notion sera étudié en détail un peu plus loin dans le chapitre. La notion d'automorphisme de groupe pour sa part est fondamental dans la théorie de Galois sur l'étude de la résolution des équations par radicaux.

Exemple 3.1.2. Si G et H sont des groupes, alors les homomorphismes canoniques $\pi_G : G \times H \to G$ et $\pi_H : G \times H \to H$ sont tous deux des épimorphismes (i.e. des homomorphismes surjectifs).

Exemple 3.1.3. On veut déterminer tous les homomorphismes $\phi : \mathbb{Z}_6 \to S_3$. Pour ce faire, commençons par nous rappeler la définition de ces deux groupes en termes de générateurs et de relations. On a donc :

$$\mathbb{Z}_6 = \langle 1 : 6(1) = 0 \rangle \qquad \text{et} \qquad S_3 = \langle \sigma, \tau : \sigma^3 = \tau^2 = e, \tau\sigma = \sigma^2\tau \rangle$$

Remarquez qu'ici, pour le groupe $\mathbb{Z}_6$ nous avons utilisé la notion additive. Étant donné que ce groupe est cyclique, il est suffisant de connaitre la valeur de $\phi(1)$ pour pouvoir calculer toutes les autres valeurs de ϕ. En effet, par définition d'un homomorphisme, nous avons $\phi(k) = \phi(k(1)) = [\phi(1)]^k$. Maintenant, comme $6(1) = 0$ dans le groupe $\mathbb{Z}_6$, pour que ϕ soit bien définie nous devons avoir $e = \phi(0) = \phi(6(1)) = [\phi(1)]^6$. Comme les éléments de S_3 sont d'ordre $1, 2$ et 3, toutes les valeurs de $\phi(1)$ sont donc possible. Nous avons donc 6 homomorphismes entre $\mathbb{Z}_6$ et S_3.

$\phi_1(0) = e$	$\phi_2(0) = e$	$\phi_3(0) = e$	$\phi_4(0) = e$	$\phi_5(0) = e$	$\phi_6(0) = e$
$\phi_1(1) = e$	$\phi_2(1) = \tau$	$\phi_3(1) = \sigma$	$\phi_4(1) = \sigma^2$	$\phi_5(1) = \sigma\tau$	$\phi_6(1) = \sigma^2\tau$
$\phi_1(2) = e$	$\phi_2(2) = e$	$\phi_3(2) = \sigma^2$	$\phi_4(2) = \sigma$	$\phi_5(2) = e$	$\phi_6(2) = e$
$\phi_1(3) = e$	$\phi_2(3) = \tau$	$\phi_3(3) = e$	$\phi_4(3) = e$	$\phi_5(3) = \sigma\tau$	$\phi_6(3) = \sigma^2\tau$
$\phi_1(4) = e$	$\phi_2(4) = e$	$\phi_3(4) = \sigma$	$\phi_4(4) = \sigma^2$	$\phi_5(4) = e$	$\phi_6(4) = e$
$\phi_1(5) = e$	$\phi_2(5) = \tau$	$\phi_3(5) = \sigma^2$	$\phi_4(5) = \sigma$	$\phi_5(5) = \sigma\tau$	$\phi_6(5) = \sigma^2\tau$

Remarquez qu'aucun des homomorphismes ci-dessous ne sont injectif ou surjectif. Il n'y a donc aucun monomorphisme ou épimorphisme entre $\mathbb{Z}_6$ et S_3.

Exemple 3.1.4. On veut déterminer tous les homomorphismes $\phi : S_3 \to \mathbb{Z}_6$. L'idée est similaire à l'exemple précédent, mais cette fois, il nous faut connaitre la valeur de $\phi(\tau)$ et $\phi(\sigma)$ pour pouvoir déterminer les autres valeurs de ϕ. Pour pouvoir déterminer les contraintes, nous allons déterminer l'ordre de chacun des éléments de ces deux groupes.

Groupe S_3

Élément	Ordre
e	1
τ	2
σ	3
σ^2	3
$\sigma\tau$	2
$\sigma^2\tau$	2

Groupe $\mathbb{Z}_6$

Élément	Ordre
0	1
1	6
2	3
3	2
4	3
5	6

Comme $0 = \phi(e) = \phi(\tau^2) = [\phi(\tau)]^2$, on doit donc avoir que $\phi(\tau)$ est un élément d'ordre 1 ou 2. Les seules possibilités pour $\phi(\tau)$ sont donc 0 ou 3. Maintenant, nous avons aussi $0 = \phi(e) = \phi(\sigma^3) = [\phi(\sigma)]^3$, donc $\phi(\sigma)$ est un élément d'ordre 1 ou 3. Les seules possibilité pour $\phi(\sigma)$ sont donc $1, 2$ ou 4. Finalement, en utilisant la relation $\tau\sigma = \sigma^2\tau$, nous avons :

$$\begin{aligned}
&\phi(\tau\sigma) = \phi(\sigma^2\tau)\\
&\phi(\tau) + \phi(\sigma) = 2\phi(\sigma) + \phi(\tau)\\
&\phi(\tau) + \phi(\sigma) = \phi(\tau) + 2\phi(\sigma)\\
&\phi(\sigma) = 2\phi(\sigma)\\
&\phi(\sigma) + 0 = \phi(\sigma) + \phi(\sigma)\\
&0 = \phi(\sigma)
\end{aligned}$$

Donc la seule valeur possible pour $\phi(\sigma)$ est 0. On obtient donc qu'il existe seulement deux homomorphismes entre S_3 et $\mathbb{Z}_6$:

$$\begin{aligned}
&\phi_1(e) = 0 \qquad \phi_2(e) = 0\\
&\phi_1(\tau) = 0 \qquad \phi_2(\tau) = 3\\
&\phi_1(\sigma) = 0 \qquad \phi_2(\sigma) = 0\\
&\phi_1(\sigma^2) = 0 \qquad \phi_2(\sigma^2) = 3\\
&\phi_1(\sigma\tau) = 0 \qquad \phi_2(\sigma\tau) = 0\\
&\phi_1(\sigma^2\tau) = 0 \qquad \phi_2(\sigma^2\tau) = 3
\end{aligned}$$

Comme pour l'exemple précédent, on remarque qu'il n'y a aucun monomorphisme ou épimorphisme entre S_3 et $\mathbb{Z}_6$.

Théorème 3.1.2. Si G est un groupe, alors l'ensemble de tout les automorphismes de G muni de l'opération de composition forme un groupe dénoté $Aut(G)$.

Démonstration. Supposons que ψ, ϕ et η sont des éléments de $Aut(G)$, comme il s'agit en particulier de fonctions bijectives, alors on doit nécessairement avoir $(\psi \circ \phi) \circ \eta = \psi \circ (\phi \circ \eta)$, l'opération est donc associative. Maintenant, considérons la fonction $e : G \to G$ définie par $e(x) = x, \forall x \in G$. Cette fonction est clairement un homomorphisme bijectif, et donc $e \in Aut(G)$. De plus, il est facile de voir que $(e \circ \phi)(x) = (\phi \circ e)(x) = \phi(x), \forall \phi \in Aut(G)$ et $\forall x \in G$. Il s'agit donc d'un élément neutre. Finalement, si $\phi \in Aut(G)$, comme il s'agit en particulier d'une fonction bijective, elle doit être inversible, et sont inverse doit être bijectif. Il

suffit maintenant de montrer qu'il s'agit d'un homomorphisme. Prenons $x, y \in G$, alors il existe des éléments $z, w \in G$ tel que $\phi(z) = x$ et $\phi(w) = y$. On obtient donc :

$$\phi(zw) = \phi(z)\phi(w) = xy$$

$$\phi^{-1}(xy) = \phi^{-1}(\phi(zw)) = zw = \phi^{-1}(x)\phi^{-1}(y)$$

Il s'agit donc bien d'un homormorphisme. Donc tout les éléments $\phi \in Aut(G)$ possède un inverse $\phi^{-1} \in Aut(G)$. On peut donc conclure que $Aut(G)$ est bien un groupe. □

3.2 Noyau et image

Definition 3.2.1. Si G et H sont des groupes, et $\phi : G \to H$ est un homomorphisme, alors on définit le noyau de ϕ, dénoté $ker(\phi)$ comme étant

$$ker(\phi) = \{x \in G : \phi(x) = e\}$$

De plus, on définit l'image de ϕ, dénoté $Im(\phi)$, comme étant :

$$Im(\phi) = \{\phi(x) : x \in G\}$$

Théorème 3.2.1. Si G et H sont des groupes, et $\phi : G \to H$ un homomorphisme, alors $\ker(\phi)$ est un sous-groupe de G et $Im(\phi)$ est un sous-groupe de H.

Démonstration. Supposons que G et H sont des groupes, et $\phi : G \to H$ un homomorphisme. Nous allons commencer par montrer que $\ker(\phi)$ est un sous-groupe de G. Pour ce faire, prenons $x, y \in \ker(\phi)$. On a donc :

$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)[\phi(y)]^{-1} = ee^{-1} = e$$

Donc $xy^{-1} \in \ker(\phi)$. $\ker(\phi)$ est donc un sous-groupe de G. Nous allons maintenant montrer que $\mathrm{Im}(\phi)$ est un sous-groupe de H. Pour ce faire, prenons $x, y \in \mathrm{Im}(\phi)$. Il existe donc $z, w \in G$ tel que $\phi(z) = x$ et $\phi(w) = y$. On a donc :

$$\phi(zw^{-1}) = \phi(z)[\phi(w)]^{-1} = xy^{-1}$$

On a donc que $xy^{-1} \in \mathrm{Im}(\phi)$, ce qui nous permet de conclure que $\mathrm{Im}(\phi)$ est un sous-groupe de H. □

Théorème 3.2.2. Si G et H sont des groupes et $\phi : G \to H$ est un homomorphisme, alors ϕ est injective si et seulement si $\ker(\phi) = \{e\}$.

Démonstration.
($\Rightarrow$) Comme ϕ est un homomorphisme, alors $\phi(e) = e$. Maintenant, supposons que ϕ est injective, et prenons $x \in \ker(\phi)$. Donc par définition du noyau, on a $\phi(x) = \phi(e) = e$, donc par injectivité $x = e$. On peut donc conclure que $\ker(\phi) = \{e\}$.
($\Leftarrow$) Supposons maintenant que $\ker(\phi) = \{e\}$ et prenons $x, y \in G$ tel que $\phi(x) = \phi(y)$. En multipliant des deux côtés par $[\phi(y)]^{-1}$ on obtient donc :

$$\begin{aligned} \phi(x)[\phi(y)]^{-1} &= \phi(y)[\phi(y)]^{-1} \\ \phi(x)\phi(y^{-1}) &= e \\ \phi(xy^{-1}) &= e \end{aligned}$$

On a donc $xy^{-1} \in \ker(\phi)$ et donc $xy^{-1} = e$. En multipliant des deux côtés par y, on obtient donc $x = y$, c'est à dire ϕ est injective. □

Exemple 3.2.1. Dans l'exemple 3.1.4, nous avons déterminé qu'il y a exactement deux homomorphsimes entre S_3 et $\mathbb{Z}_6$. Nous voulons maintenant identifié quel est le noyau et l'image de ces deux homomorphismes.

$$\begin{array}{ll} \phi_1(e) = 0 & \phi_2(e) = 0 \\ \phi_1(\tau) = 0 & \phi_2(\tau) = 3 \\ \phi_1(\sigma) = 0 & \phi_2(\sigma) = 0 \\ \phi_1(\sigma^2) = 0 & \phi_2(\sigma^2) = 3 \\ \phi_1(\sigma\tau) = 0 & \phi_2(\sigma\tau) = 0 \\ \phi_1(\sigma^2\tau) = 0 & \phi_2(\sigma^2\tau) = 3 \\ \\ \ker(\phi_1) = S_3 & \ker(\phi_2) = \{e, \sigma, \sigma^2\} \\ \mathrm{Im}(\phi_1) = \{0\} & \mathrm{Im}(\phi_2) = \{0, 3\} \end{array}$$

Pour le premier homomorphisme, on remarque que $\ker(\phi_1) = S_3 \leq S_3$ et $\mathrm{Im}(\phi_1) = \{0\} \leq \mathbb{Z}_6$. De plus, le fait qu'il ne s'agit pas d'un monomorphisme est confirmer par le fait que $\ker(\phi_1) \neq \{e\}$. Dans le cas du deuxième homomorphisme, on remarque que $\ker(\phi_2) = \{e, \sigma, \sigma^2\} \leq S_3$ et $\mathrm{Im}(\phi_2) = \{0, 3\} \leq \mathbb{Z}_6$. De plus, à nouveau nous avons que $\ker(\phi_2) \neq \{e\}$, ce qui confirme qu'il ne s'agit pas d'un monomorphisme.

Exemple 3.2.2. Nous voulons déterminer tous les homomorphismes $\phi : \mathbb{Z}_5 \to S_3$. Comme $\mathbb{Z}_5$ est un groupe d'ordre premier, les seules sous-groupes de $\mathbb{Z}_5$ sont lui-même et $\{0\}$. De plus, nous savons que si ϕ est un homomorphisme, alors $\ker(\phi)$ est un sous-groupe de $\mathbb{Z}_5$. Comme l'ordre des éléments de S_3 sont $1, 2$ et 3, on doit nécessairement avoir $\phi(0) = [\phi(1)]^2 = \phi(2)$ ou $\phi(0) = [\phi(1)]^3 = \phi(3)$, l'homomorphisme ne peut pas être injectif. Donc $\ker(\phi) \neq \{0\}$, ce qui signifie que $\ker(\phi) = \mathbb{Z}_5$. Le seul homomorphisme entre $\mathbb{Z}_5$ et S_3 est donc $\phi(x) = e$ pour tout $x \in \mathbb{Z}_5$.

Exemple 3.2.3. Nous voulons trouver tous les homomorphismes $\phi : S_3 \to \mathbb{Z}_5$. Cette fois, nous allons travailler avec l'image de ϕ. Par le théorème de Lagrange, nous savons que $\mathrm{Im}(\phi)$ est soit $\{0\}$ ou $\mathbb{Z}_5$. Si $\mathrm{Im}(\phi) = \mathbb{Z}_5$, alors il existe $x \in S_3$ tel que $\phi(x) = 1$. Comme tout les éléments de S_3 sont d'ordre $1, 2$ ou 3, on doit donc avoir $0 = \phi(x^2) = [\phi(x)]^2 = 2$ ou $0 = \phi(x^3) = [\phi(x)]^3 = 3$. Comme aucune de ces deux options n'a de sens, la seule option est donc $\mathrm{Im}(\phi) = \{0\}$, c'est à dire $\phi(x) = 0$ pour tout $x \in S_3$.

3.3 Les groupes isomorphiques

Definition 3.3.1. Si G et H sont des groupes, alors on dit qu'ils sont isomorphiques, et on écrit $G \cong H$, s'il existe un isomorphisme $\phi : G \to H$.

Théorème 3.3.1. Si G et H sont des groupes isomorphiques, alors :

1. G et H ont le même nombre d'élément, c'est à dire que l'ordre de G égal l'ordre de H.
2. Si $g \in G$ est un élément d'ordre k, alors $\phi(g)$ est aussi un élément d'ordre k.
3. G est est abélien si et seulement si H est abélien.

Démonstration.

1. Si ϕ est un isomorphisme, alors en particulier ϕ est une fonction bijective. G et H doivent donc avoir la même cardinalité.
2. Supposons que $g \in G$ est un élément d'ordre k, alors $[\phi(g)]^k = \phi(g^k) = \phi(e_G) = e_H$. Maintenant, supposons que $m < k$ est un nombre naturel tel que $[\phi(g)]^m = e_H$, alors on a $[\phi(g)]^m = \phi(g^m) = e_H$, on doit donc avoir $g^m \in \ker(\phi)$. Maintenant, comme ϕ est injective, le théorème de la section précédente nous affirme que $g^m = e_G$. On a donc une contradiction, car l'ordre de g est par hypothèse k, et $m < k$. On peut donc conclure que si l'ordre de g est k, alors l'ordre de $\phi(g)$ est aussi k.
3. Exercice.

□

Dans cette section, nous allons maintenant chercher à classer les groupes finis. Le but est de déterminer tous les groupes finis qui ne sont pas isomorphiques. Cette question étant particulièrement complexe, nous allons donc nous concentrer sur certain cas particulier, et sur les groupes d'ordre relativement petit.

Exemple 3.3.1. Si G est un groupe cyclique d'ordre $n \in \mathbb{N}$, alors G est isomorphique à $(\mathbb{Z}_n, +)$. Pour le montrer, il suffit de remarquer que comme G est cyclique, il existe un élément $x \in G$ qui est d'ordre n. On peut donc écrire :

$$G = \langle x \rangle = \{1, x, x^2, x^3, x^4, ..., x^{n-1}\}$$

Remarquer que les éléments $1, x, x^2, ..., x^{n-1}$ sont tous distinct, car autrement, on aurait $k_1, k_2 \in \mathbb{N}$, $k_1 < k_2 < n$ tel que $x^{k_1} = x^{k_2}$, ce qui nous donne en simplifiant $e = x^{k_1 - k_2}$. Comme $k_1 - k_2 < n$, ceci contredit le fait que l'ordre de x est n. On obtient donc l'isomorphisme suivant :

$$\phi : G \to \mathbb{Z}_n$$

$$\phi(x^k) = k, \quad \forall k \in \{0, 1, 2, ..., n-1\}$$

Ce qui signifie que $G \cong \mathbb{Z}_n$.

Exemple 3.3.2. Si p est un nombre premier, et G est un groupe d'ordre p, alors G est isomorphique à $\mathbb{Z}_p$. Pour le montrer, il suffit de remarquer que par le théorème de Lagrange, tous les éléments de G sont soit d'ordre 1 ou d'ordre p. Comme l'identité est le seul élément d'ordre 1, il doit donc exister un élément $x \in G$ qui est d'ordre p. Le groupe G doit donc être cyclique. Par l'exemple précédent, on doit donc avoir $G \cong \mathbb{Z}_p$.

Exemple 3.3.3. Si G est un groupe d'ordre 4, alors G est isomorphique à $\mathbb{Z}_4$ ou V_4. Pour le démontrer, supposons premièrement que G contient un élément d'ordre 4. Dans ce cas, G est cyclique et $G \cong \mathbb{Z}_4$. Maintenant, supposons que G ne contient pas d'élément d'ordre 4. Dans ce cas, tout les éléments de G sont soit d'ordre 1 ou d'ordre 2. Comme le seul élément d'ordre 1 est l'identité e, on obtient donc que G contient 3 éléments d'ordre 2. Supposons donc que $G = \{e, a, b, c\}$ avec $a^2 = b^2 = c^2 = e$. Supposons que $x, y \in \{a, b, c\}$ et $x \neq y$, alors on a :

1. Si $xy = x$, alors $x^{-1}xy = x^{-1}x$ et donc $y = e$, ce qui est une contradiction.
2. Si $xy = y$, alors $xyy^{-1} = yy^{-1}$ et donc $x = e$, ce qui est une contradiction.
3. Si $xy = e$, alors y est l'inverse de x, mais comme x est d'ordre 2, on doit donc avoir $x = y$, ce qui est une contradiction.

À partir de ceci, on peut construire la table de multiplication du groupe G.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

En remarquant que $c = ab$, il est donc facile de voir qu'il s'agit exactement de la même table de multiplication que nous avons déjà donné pour V_4. On a donc l'isomorphisme $\phi : G \to V_4$, $\phi(x) = x$. On peut donc affirmer que $G \cong V_4$.

Chapitre 4

Les groupes quotients

4.1 Les groupes normaux

Lorsque nous avons introduit le théorème de Lagrange, nous avons commencer par discuter du concept de classe à gauche qui nous a permis de partitionner un groupe G en différente classe d'équivalence. La question est maintenant de savoir dans quel cas l'ensemble des classes à gauche forme un groupe ? C'est le théorème suivant qui va nous permettre de répondre à la question, et en même temps va nous permettre de définir le concept de groupes quotient dans la section suivante.

Théorème 4.1.1. Si G est un groupe et N un sous-groupe de G, alors les énoncés suivants sont équivalent :

1. $xN = Nx$ pour tout $x \in G$
2. $xnx^{-1} \in N$ pour tout $x \in G$ et pour tout $n \in N$.
3. L'opération $(xN) * (yN) = (xy)N$ sur les classes à gauche de N dans G est bien définie.

Démonstration.
(1) ⇒ (2) : Supposons que $xN = Nx$ pour tout $x \in G$. Donc si on prend $x \in G$ et $n \in N$, il existe un élément $n_2 \in N$ tel que $xn = n_2x$, ce qui nous donne :

$$xnx^{-1} = (xn)x^{-1} = (n_2x)x^{-1} = n_2(xx^{-1}) = n_2 \in N$$

(2) ⇒ (1) : Fixons $x \in G$. On veut montrer que $xN \subseteq Nx$ et $Nx \subseteq xN$. Pour la première inclusion, prenons $n \in N$, par hypothèse on a donc $xnx^{-1} \in N$. Il existe donc $n_2 \in N$ tel que $xnx^{-1} = n_2$, ce qui nous donne $xn = n_2x \in Nx$, c'est à dire $xN \subseteq Nx$. Maintenant pour l'autre inclusion, prenons à nouveau $n \in N$, alors par hypothèse on a $x^{-1}n(x^{-1})^{-1} = x^{-1}nx \in N$. Il existe donc un $n_2 \in N$ tel que $x^{-1}nx = n_2$, ce qui nous donne $nx = xn_2 \in xN$. On a donc l'inclusion $Nx \subseteq xN$. Finalement, comme nous avons démontrer les deux inclusions, on peut donc affirmer que $xN = Nx$ pour tout $x \in G$.
(1) ⇒ (3) : Supposons que $x_1, x_2, y_1, y_2 \in G$ sont tel que :

$$x_1N = x_2N \quad \text{et} \quad y_1N = y_2N$$

et supposons que $n_1 \in N$. On peut donc trouver des éléments $n_2, n_3, n_4, n_5 \in N$ tel que :

$$\begin{aligned} y_1n_1 &= y_2n_2 && \text{car} && y_1N = y_2N \\ y_2n_2 &= n_3y_2 && \text{car} && y_2N = Ny_2 \\ x_1n_3 &= x_2n_4 && \text{car} && x_1N = x_2N \\ n_4y_2 &= y_2n_5 && \text{car} && Ny_2 = y_2N \end{aligned}$$

En combinant toutes ces égalités, on obtient donc :

$$x_1y_1n_1 = x_1y_2n_2 = x_1n_3y_2 = x_2n_4y_2 = x_2y_2n_5 \in x_2y_2N$$

On a donc l'inclusion $x_1y_1N \subseteq x_2y_2N$. De la même manière, on peut obtenir l'inclusion inverse, ce qui nous permet donc d'affirmer que $x_1y_1N = x_2y_2N$. L'opération est donc bien définie.
(3) ⇒ (2) : Supposons que l'opération est bien définie, c'est à dire que si $x_1N = x_2N$ et $y_1N = y_2N$, alors on a $x_1y_1N = x_2y_2N$. En particulier, si $x \in G$ et $n \in N \subseteq G$, on a $eN = nN$ et $x^{-1}N = x^{-1}N$, ce qui nous donne :

$$ex^{-1}N = nx^{-1}N$$

Il existe donc $n_2, n_3 \in N$ tel que :

$$x^{-1}n_2 = nx^{-1}n_3 \quad \Rightarrow \quad n_2 = xnx^{-1}n_3 \quad \Rightarrow \quad xnx^{-1} = n_2n_3^{-1} \in N$$

□

Definition 4.1.1. Si G est un groupe, et N est un sous-groupe de G, alors on dit que N est un sous-groupe normal (ou sous-groupe distingué) si N satisfait l'une des propriétés équivalentes du théorème précédent. Dans ce cas, on écrit $N \trianglelefteq G$.

Théorème 4.1.2. Si A est un sous-ensemble d'un groupe G, alors $C_G(A) \trianglelefteq N_G(A)$

Démonstration. Nous savons déjà que $C_G(A)$ est un sous-groupe de $N_G(A)$, il est donc suffisant de démontrer la normalité. Prenons $x \in N_G(A)$, $n \in C_G(A)$ et $a \in A$. Par définition de $N_G(A)$, il existe donc a_2 tel que $ax = xa_2$. En réarrangeant les termes, on obtient donc $x^{-1}a = a_2x^{-1}$, ce qui nous donne :

$$xnx^{-1}a = xna_2x^{-1} = xa_2nx^{-1} = axnx^{-1}$$

Donc $xnx^{-1} \in C_G(A)$, c'est à dire que $C_G(A)$ est un sous-groupe normal de $N_G(A)$. □

Au chapitre 2, lorsque nous avons étudié la notion de sous-groupe, nous avons introduit la notion de normalisateur d'un ensemble sans pour autant justifier le nom de normalisateur. Notez que ce nom nous vient en fait de la notion de sous-groupe normal, et plus précisément du théorème suivant que nous ne démontrerons pas pour le moment.

Théorème 4.1.3. Si H est un sous-groupe d'un groupe G, alors le plus grand sous-groupe de G pour lequel H est un sous-groupe normal est $N_G(H)$.

4.2 Les groupes quotients

Dans la section précédente, nous avons vu que si G est un groupe, et N un sous-groupe normal de G, alors on peut définir un opération sur l'ensemble des classe à gauche. En fait, nous avons vu que cet opération est bien définie si et seulement si N est normal. Dans cette section, nous voulons aller un peu plus loin et montrer que cet opération donne une structure de groupe à l'ensemble des classes à gauche. Ce groupe est particulièrement important, et porte le nom de groupe quotient.

Théorème 4.2.1. Si G est un groupe et N un sous-groupe normal de G, alors l'ensemble des classes à gauche de N dans G muni de l'opération $(xN) * (yN) = (xy)N$ forme un groupe.

Démonstration. Comme N est par hypothèse un sous groupe normal de G, alors nous savons déjà que l'opération est bien définie. Il ne nous reste donc qu'à démontrer que l'opération est associative, possède un élément neutre, et que chaque classe à gauche possède un inverse. Prenons xN, yN et zN des classes à gauche, alors on a :

$$[(xN) * (yN)] * (zN) = [(xy)N] * (zN) = ((xy)z)N = (x(yz))N = (xN) * [(yz)N] = (xN) * [(yN) * (zN)]$$

l'opération est donc associative. Nous allons maintenant montrer que si e est l'identité du groupe G, alors eN est un identité pour les classes à gauche. Pour ce faire, prenons xN une classe à gauche, alors on a :

$$(eN) * (xN) = (ex)N = xN \quad \text{et} \quad (xN) * (eN) = (xe)N = xN$$

Il s'agit donc bien d'un identité. Finalement, si xN est une classe à gauche, on veut montrer que $x^{-1}N$ en est son inverse. On a donc :

$$(xN) * (x^{-1}N) = (xx^{-1}N) = eN \quad \text{et} \quad (x^{-1}N) * (xN) = (x^{-1}x)N = eN$$

Toutes les classes à gauche sont donc inverse. On peut donc conclure que l'ensemble des classes à gauche muni de l'opération $*$ forme un groupe. □

Si N est un sous-groupe normal d'un groupe G, alors dans la section précédente nous avons déjà vu que l'ensemble des classes à gauche de N dans G forme un groupe. Ce groupe est particulièrement important en théorie des groupes, et est appelé groupe quotient. On le dénote par G/N.

Definition 4.2.1. Si G est un groupe, et N un sous-groupe normal de G, alors on dit que $x \sim y$ si et seulement si il existe un élément $n \in N$ tel que $xny^{-1} \in N$.

Théorème 4.2.2. L'opération $\sim$ que nous venons de définir est une relation d'équivalence sur G. L'ensemble de ces classes d'équivalence forme un groupe appelé groupe quotient et est dénoté par G/N.

Démonstration. Pour démontrer qu'il s'agit d'une relation d'équivalence, on doit démontrer que la relation est réflexive, symétrique et transitive. Commeçons par démontrer qu'elle est réflexive. Pour ce faire, prenons $x \in G$. Comme l'identité e doit être dans le sous-groupe N, on a donc $xex^{-1} = e \in N$, et donc $x \sim x$. La relation est donc réflexive. Maintenant, pour montrer que la relation est symétrique, prenons $x, y \in G$ tel que $x \sim y$. Il existe donc n_1 et n_2 dans N tel que $xn_1y^{-1} = n_2$. En prenant l'inverse, on obtient : $n_2^{-1} = (xn_1y^{-1})^{-1} = yn_1^{-1}x^{-1}$. Comme n_1^{-1} et n_2^{-1} doivent être dans N, on obtient donc $y \sim x$. La relation est donc symétrique. Il ne nous reste plus qu'à démontrer que la relation est transitive. Pour ce faire, prenons $x, y, z \in G$ tel que $x \sim y$ et $y \sim z$. Il existe donc $n_1, n_2 \in N$ tel que $xn_1y^{-1} \in N$ et $yn_2z^{-1} \in N$. On obtient donc :

$$\underbrace{xn_1y^{-1}}_{\in N}\underbrace{yn_2z^{-1}}_{\in N} = xn_1n_2z^{-1} \in N$$

Ce qui nous permet d'affirmer que $x \sim z$. La relation est donc transitive. On peut donc conclure qu'il s'agit bien d'une relation d'équivalence. Maintenant, en remarquant que les différentes classes d'équivalence sont en fait les classes à gauche, le théorème précédent nous permet d'affirmer que les classes d'équivalence forment bien un groupe. □

Exemple 4.2.1. Si on considère le groupe $G = (\mathbb{Z}, +)$ et le sous-groupe $N = 2\mathbb{Z}$, alors N est un sous-groupe normal de G, et dans ce cas $G/N = \mathbb{Z}/2\mathbb{Z}$ est isomorphique à $\mathbb{Z}_2$.

On peut généraliser l'exemple précédent sous la forme suivante.

Exemple 4.2.2. Si on considère le groupe $G = (\mathbb{Z}, +)$ et le sous-groupe $N = k\mathbb{Z}$, où k est un nombre naturel supérieur ou égal à 2, alors N est un sous-groupe normal de G, et dans ce cas $G/N = \mathbb{Z}/k\mathbb{Z}$ est isomorphique à $\mathbb{Z}_k$.

Un exemple important de sous-groupe normal est donné par le noyau d'un homomorphisme. En effet, le noyau d'un homomorphisme est toujours un sous-groupe normal. En fait, tout les sous-groupes normal peuvent s'écrire comme le noyau d'un homomorphisme. C'est ce que nous affirme le théorème suivant.

Théorème 4.2.3. Si G est un groupe et N un sous-groupe de G, alors les énoncés suivants sont équivalent :

1. N est un sous-groupe normal
2. Il existe un homomorphisme ϕ tel que $\ker(\phi) = N$.

Démonstration.
($\Rightarrow$) Supposons que G est un groupe, et N un sous-groupe normal, alors nous avons vu que G/N est un groupe. Définissons la fonction suivante :

$$\phi : G \to G/N$$
$$\phi(g) = gN$$

alors comme N est normal, la fonction ϕ est un homomorphisme. Pour le vérifier, il suffit de remarquer que :

$$\phi(g_1)f(g_2) = g_1Ng_2N = g_1g_2NN = g_1g_2N = \phi(g_1g_2)$$

De plus, on remarque que le noyau de ϕ est donné par l'ensemble des $g \in G$ tel que $f(g) = gN \subseteq N$. Dans ce cas, il existe $n_1, n_2 \in N$ tel que $gn_1 = n_2$ ce qui implique que $g = n_2n_1^{-1} \in N$, donc $\ker(\phi) = N$.
($\Leftarrow$) Supposons que $\phi : G \to H$ est un homomorphisme tel que $\ker(\phi) = N$. Prenons $x \in G$ et $n \in N$, alors on a : $\phi(n) = e$, ce qui nous permet d'obtenir :

$$\phi(xnx^{-1}) = \phi(x)\phi(n)[\phi(x)]^{-1} = \phi(x)[\phi(x)]^{-1} = e$$

On peut donc affirmer que $xnx^{-1} \in N$, ce qui signifie que N est un sous-groupe normal de G. □

4.3 Le théorème de Cauchy pour les groupes abéliens

Nous allons maintenant illustrer comment obtenir des informations sur un groupe G à partir d'un sous-groupe normal N de G, et du groupe quotient G/N. Le théorème de Cauchy ci-dessous est valide pour tout les groupes finis, mais nous allons nous contenter d'énoncer le théorème et de le démontrer seulement pour les groupes abéliens. Mais avant, nous avons besoin d'un lemme :

Lemme 4.3.1. *Si G est un groupe et y un élément de G d'ordre fini et différent de l'identité. Alors pour tout entier $n > 1$, alors $|y^n| = \dfrac{|y|}{(n, |y|)}$.*

Démonstration. Supposons que $|y| = a$ et $|y^n| = b$, et supposons aussi que $(n, a) = d$. Il existe donc des entiers s, t tel que $ds = n$ et $dt = a$. De plus, il est facile de voir que dans ce cas on doit avoir $(s, t) = \left(\dfrac{n}{d}, \dfrac{a}{d}\right) = 1$. Notre but est de montrer que $b = t$. Pour ce faire, remarquons premièrement que :

$$(y^n)^t = y^{nt} = y^{dst} = y^{as} = (y^a)^s = e^s = e$$

Par le théorème de Lagrange, l'ordre de l'élément y^n doit diviser t, c'est à dire $b|t$. D'un autre côté, nous avons aussi :

$$y^{nb} = (y^n)^b = e$$

Par le théorème de Lagrange on a donc que l'ordre de y doit diviser nb, c'est à dire $a|nb$, ce qui nous donne $dt|dsb$ et en simplifiant $t|sb$. Maintenant, comme $(s, t) = 1$, le lemme d'Euclide nous permet d'obtenir $t|b$. Nous avons donc obtenu $b|t$ et $t|b$. Comme il s'agit d'entier positif, on doit donc avoir $b = t$. On peut donc conclure que :

$$|y^n| = t = \frac{a}{d} = \frac{|y|}{(n, |y|)}$$

□

Théorème 4.3.1. **(Théorème de Cauchy)** Si G est un groupe abélien d'ordre fini et p un nombre premier tel que p divise l'ordre du groupe G, alors G contient au moins un élément d'ordre p.

Démonstration. Remarquons premièrement que si l'ordre du groupe G est $1, 2$ ou 3, alors il est évident que le résultat est vrai. Nous allons donc procéder par induction. Nous savons déjà que le résultat est vrai pour les groupes de petit ordre. Supposons que le résultat est vrai pour tout les groupes d'ordre (strictement) plus petit que l'ordre de G et prenons $x \in G$ avec $x \neq e$. Donc nécessairement, l'ordre de x doit être plus grande que 1. Supposons que $|x| = n$ et posons $N = \langle x \rangle$. Donc N est un sous groupe normal de G d'ordre n. Par le théorème de Lagrange, nous avons :

$$|G| = |N| \ |G/N|$$

Donc si p divise $|G|$, on doit avoir que p divise $|N|$ ou p divise $|G/N|$. Nous allons donc traiter séparément les deux cas.

1. Supposons que $p \Big| |N|$, alors il existe un élément $y \in N$ qui est d'ordre p. En particulier, cet élément fait aussi partie de G. On a donc trouvé un élément d'ordre p dans G.
2. Supposons que p ne divise par $|N|$, alors p divise G/N. Il existe donc un élément $yN \in G/N$ qui est d'ordre p. On a donc $(yN)^p = y^p N = N$. En particulier, on doit avoir $y^p \in N$. On remarque donc que les sous-groupe $H_1 = \langle y \rangle$ et $H_2 = \langle y^p \rangle$ ne sont pas égal car $H_2 \leq N$, mais H_1 contient l'élément y qui n'est pas dans N. En particulier, l'ordre de l'élément y n'est pas égal à l'ordre de l'élément y^p. Par le lemme, nous savons que :

   $$|y^p| = \frac{|y|}{(p, |y|)}$$

   Comme $|y^p| \neq |y|$, on doit donc avoir $(p, |y|) = p$, ce qui nous donne :

   $$|y| = p|y^p| \quad \Rightarrow \quad p \Big| |y|$$

   Donc p divise l'ordre du sous-groupe $H_1 = \langle y \rangle$. Par hypothèse d'induction, il existe donc un élément $z \in H_1$ qui est d'ordre p. On a donc trouver un élément z qui est d'ordre p dans G.

□

4.4 Les groupes simples

La théorie des groupes est un sujet très vaste et plusieurs techniques existes pour étudier les groupes. Par contre, une idée qui revient souvent est d'étudier un groupe, à partir de groupe plus petit. C'est ce que nous avons fait dans un premier temps à l'aide des sous-groupes, ce qui nous a amené au théorème de Lagrange, l'un des résultats les plus important de la théorie. Une autre façon d'obtenir des informations sur un groupe G à partir de groupe plus petit est de regarder un sous-groupe normal $N \trianglelefteq G$ et son quotient G/N. Il arrive souvent que si N et G/N ont une propriété donné, alors G possède aussi cette propriété (Ce n'est cependant pas toujours vrai). C'est pour cette raison que le groupe quotient sont particulièrement important.

Cette idée nous amène à se demander s'il est possible de reconstruire un groupe G donné à partir d'un groupe normal N et de son quotient G/N. C'est ce qu'on appelle la théorie des extensions de groupe. Bien que plusieurs résultats soit connu sur cette question, le problème reste toujours ouvert et aucune théorie connu à se jour permet de le faire en toute généralité. Si ce problème vient un jour à être résolu, il sera alors possible de construire tout les groupes finis à partir d'un certain nombre de groupe plus simple, un peu sur le même principe que tout les entiers positifs peuvent être obtenu à partir des nombres premiers. En théorie des groupes, ce sont les groupes simples qui jouent ce rôle.

Definition 4.4.1. Un groupe G est simple, si les seul sous-groupe normaux de G sont $\{e\}$ et G.

On doit alors se tourner sur la question de caractériser l'ensemble de tous les groupes simples. La bonne nouvelle est que dans ce cas, la réponse complète existe et une classification complète de tout les groupes simples d'ordre fini a été complété en 2008. Il existe un total de 18 familles de groupes simples, et 26 groupes simples exceptionnels qui ne font pas partie de ces familles. Il s'agit de l'une des démonstrations les plus difficiles des mathématiques, et plus de 100 auteurs y ont contribué. La caractérisation de tous les groupes simples d'ordre finis est très loin d'être à notre porté, mais nous somme tout de même en mesure d'étudier deux familles importantes de groupes simples.

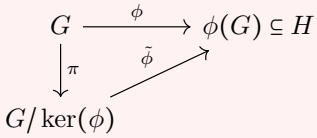
Exemple 4.4.1. Si p est un nombre premier, alors $\mathbb{Z}_p$ est un groupe simple. Ceci est une simple application du théorème de Lagrange. Comme l'ordre du groupe $\mathbb{Z}_p$ est p qui est par hypothèse un nombre premier, les seuls sous-groupes doivent être d'ordre 1 ou p, c'est à dire que les seuls sous groupes sont le groupe trivial et $\mathbb{Z}_p$. Le groupe doit donc être simple.

Exemple 4.4.2. Si $n \geq 5$, alors le groupe A_n est simple.

4.5 Les théorèmes d'isomorphimes

Nous allons maintenant compléter ce chapitre avec trois théorèmes permettant d'établir l'isomorphisme de certain groupe. Ces théorèmes joueront un rôle important dans le chapitre suivant.

Théorème 4.5.1. (Premier théorème d'isomorphisme) Si G et H sont des groupes, et $\phi : G \to H$ un homomorphisme, alors $G/\ker(\phi) \cong \mathrm{Im}(\phi)$.



Démonstration. Supposons que G et H sont des groupes, et $\phi : G \to H$ un homomorphisme. Alors $K = \ker(\phi)$ est un sous-groupe normal de G, et donc $G/\ker(\phi)$ est un groupe. Définissons la fonction :

$$\tilde{\phi} : G/\ker(\phi) \to \phi(G)$$
$$\tilde{\phi}(gK) = \phi(g)$$

Nous allons commencer par démontrer que cette fonction est bien définie. Pour ce faire, supposons que $g, h \in G$ sont tel que $gK = hK$. Il existe donc des éléments k_1, k_2 tel que $gk_1 = hk_2$, ou de manière équivalente $g = hk_2k_1^{-1}$. On obtient donc :

$$\tilde{\phi}(gK) = \phi(g) = \phi(hk_2k_1^{-1}) = \phi(h)\phi(k_2)[\phi(k_1)]^{-1} = \phi(h)ee = \phi(h) = \tilde{\phi}(hK)$$

La fonction est donc bien définie. On veut maintenant montrer qu'il s'agit d'un homomorphisme. Pour ce faire, prenons $gK, hK \in G/\ker(\phi)$, on obtient donc :

$$\tilde{\phi}(gKhK) = \tilde{\phi}(ghK) = \phi(gh) = \phi(g)\phi(h) = \tilde{\phi}(gK)\tilde{\phi}(hK)$$

Il s'agit donc bien d'un homomorphisme. Nous voulons maintenant montrer que cet homomorphisme est injectif. Pour ce faire, nous allons utiliser le théorème ? ? ?. On a donc :

$$\ker(\tilde{\phi}) = \{gK : \tilde{\phi}(gK) = e\} = \{gK : \phi(g) = e\} = \{gK : g \in \ker(\phi)\} = \{gK : g \in K\} = K$$

Comme K est l'identité du groupe $G/\ker(\phi)$, l'homomorphisme est donc injectif. Il ne nous reste plus qu'à démontrer la surjectivité. Prenons $y \in \phi(G)$, il existe donc $g \in G$ tel que $\phi(g) = y$, ce qui nous donne :

$$\tilde{\phi}(gK) = \phi(g) = y$$

ce qui confirme la surjectivité. Finalement, comme $\tilde{\phi}$ est un homomorphisme injectif et surjectif, on peut donc conclure qu'il s'agit d'un isomorphisme. □

Corollaire 4.5.1. Si G et H sont des groupes et $\phi : G \to H$ est un homomorphisme surjectif, alors $G/\ker(\phi)$ est isomorphique à H.

Démonstration. Il s'agit d'une conséquence directe du premier théorème d'isomorphisme. Si ϕ est surjectif (i.e. un épimorphisme), alors $\phi(G) = H$, donc par le théorème $G/\ker(\phi) \cong H$. □

Corollaire 4.5.2. Si G et H sont des groupes et $\phi : G \to H$ est un homomorphisme injectif (i.e. un monomorphisme), alors G est isomorphique à $\phi(G)$.

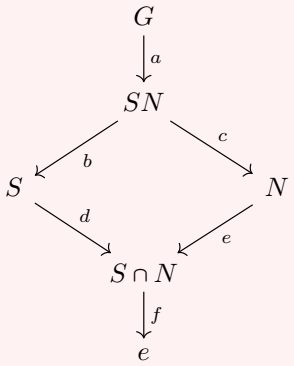
Démonstration. Il s'agit à nouveau d'une conséquence directe du premier théorème d'isomorphisme. Si ϕ est injectif, alors $\ker(\phi) = \varnothing$, donc par définition du groupe quotient on a $G/\ker(\phi) \cong G$. En appliquant le théorème, on a donc $G \cong \phi(G)$. □

Exemple 4.5.1. Si $n \in \mathbb{N}$, considérons l'homomorphisme $\phi : \mathbb{Z} \to \mathbb{Z}_n$ définie par $\phi(x) = x, \forall x \in \mathbb{Z}$. Il est facile de voir que la fonction est bien définie et qu'il s'agit bien d'un homomorphisme. De plus, l'homomorphisme est surjectif, mais n'est pas injectif car $\phi(1) = \phi(1+n)$ par exemple. Nous allons donc chercher à déterminer quel est le noyau de ϕ. Pour ce faire, on doit trouver l'ensemble des x pour lesquels $\phi(x) = 0 \in \mathbb{Z}_n$. Par la relation d'équivalence qui nous a permis de définir $\mathbb{Z}_n$, on a donc : $x = 0 \pmod{n}$ si et seulement si $n|x$, ce qui est le cas si et seulement si il existe $k \in \mathbb{Z}$ tel que $nk = x$. On a donc :

$$\ker(\phi) = \{nk : k \in \mathbb{Z}\}$$

Donc, par le corollaire, on obtient donc l'isomorphisme suivant : $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Théorème 4.5.2. **(Second théorème d'isomorphisme)** Si G est un groupe, S un sous-groupe de G, et N un sous-groupe normal de G. Alors, $(SN)/N \cong S/(S \cap N)$.



Démonstration. Il faut commencer par montrer que si S est un sous-groupe de G, et N un sous-groupe normal de G, alors SN est un sous-groupe de G pour lequel $N \trianglelefteq SN$. De plus, il faut montrer que $S \cap N \trianglelefteq S$. Cette partie est laissé en exercice. Maintenant, il s'agit de considérer l'homomorphisme suivant :

$$\phi : SN \to S/(S \cap N)$$

$$\phi(sn) = s(S \cap N)$$

Nous devons commencer par montrer que ϕ est bien définie. Pour ce faire, supposons que $s_1n_1 = s_2n_2$ avec $s_1, s_2 \in S$ et $n_1, n_2 \in N$. Alors, ont veut montrer que $\phi(s_1n_1) = \phi(s_2n_2)$. Pour ce faire, remarquons que $s_1n_1 = s_2n_2$ implique que $s_2^{-1}s_1 = n_2n_1^{-1}$, ce qui signifie que $s_2^{-1}s_1 \in S \cap N$. Posons $s_2^{-1}s_1 = x$, alors on a $s_1e = s_2x$ et donc $s_1(S \cap N) = s_2(S \cap N)$, ce qui signifie que $\phi(s_1n_1) = \phi(s_2n_2)$. La fonction est donc bien définie.

Ensuite, nous devons montrer que ϕ est bien un homomorphisme. Pour ce faire, prenons s_1n_1 et s_2n_2 dans SN. Comme N est normal dans G, on a $s_2n_1s_2^{-1} \in N$. Il existe donc un $n_3 \in N$ tel que $s_2n_2 = n_3s_2$. On a donc :

$$\phi((s_1n_1)(s_2n_2)) = \phi(s_1s_2n_3n_2) = s_1s_2(S \cap N)$$

Maintenant, comme $S \cap N$ est un groupe, $S \cap N = (S \cap N)(S \cap N)$. De plus, comme $S \cap N$ est un sous-groupe normal de S, on a donc $s_2(S \cap N) = (S \cap N)s_2$. On obtient donc :

$$\phi((s_1n_1)(s_2n_2)) = s_1(S \cap N)s_2(S \cap N) = \phi(s_1n_1)\phi(s_2n_2)$$

Il s'agit donc bien d'un homomorphisme. L'homomorphisme ϕ est clairement surjectif, par le premier théorème d'isomorphisme, on doit donc avoir :

$$SN/\ker(\phi) \cong S/(S \cap N)$$

Il ne nous reste plus à déterminer quel est le noyau de ϕ. On cherche donc l'ensemble des $sn \in SN$ tel que $\phi(sn) \in S \cap N$. Ceci sera le cas si et seulement si $s \in S \cap N$. Comme s est déjà par hypothèse dans S, il suffit donc que pour que sn soit dans le noyau que $s \in N$. On a donc $\ker(\phi) = N$. On peut donc finalement affirmer que :

$$SN/N \cong S/(S \cap N)$$

Ce qui complète la démonstration. □

Exemple 4.5.2. Prenons $a, b \in \mathbb{N}$, alors $a\mathbb{Z}, b\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$. Posons $S = a\mathbb{Z}$ et $N = b\mathbb{Z}$. Nous voulons appliquer le second théorème d'isomorphisme. Pour ce faire, remarquons que :

$$SN = a\mathbb{Z} + b\mathbb{Z} = PGCD(a,b)\mathbb{Z}$$

$$S \cap N = a\mathbb{Z} \cap b\mathbb{Z} = PPCM(a,b)\mathbb{Z}$$

Le théorème nous affirme donc :

$$\frac{PGCD(a,b)\mathbb{Z}}{b\mathbb{Z}} \cong \frac{a\mathbb{Z}}{PPCM(a,b)\mathbb{Z}}$$

Maintenant, si on compare la cardinalité de ces deux groupes, on obtient :

$$\frac{b}{PGCD(a,b)} = \frac{PPCM(a,b)}{a} \quad \Rightarrow \quad PGCD(a,b) \cdot PPCM(a,b) = ab$$

Théorème 4.5.3. **(Troisième théorème d'isomorphisme)** Si G, K et N sont des groupes tel que $N \trianglelefteq K \trianglelefteq G$, alors $(G/N)/(K/N) \cong G/K$.

Démonstration. Premièrement, remarquons que comme $N \trianglelefteq K \trianglelefteq G$, alors $N \trianglelefteq G$. Considérons l'homomorphisme suivant :

$$\phi : G/N \to G/K$$

$$\phi(gN) = gK$$

Nous allons commencer par montrer que ϕ est bien définie. Pour ce faire, supposons que $g_1, g_2 \in G$ sont tel que $g_1N = g_2N$. Comme $N \leq K$, on doit donc avoir $g_1K = g_2K$, ce qui signifie que $\phi(g_1N) = \phi(g_2N)$. La fonction ϕ est donc bien définie. Maintenant, il nous faut montrer qu'il s'agit d'un homomorphisme. Pour ce

faire, prenons $g_1N, g_2N \in G/N$. Maintenant, comme N est normal, alors $g_2N = Ng_2$, et comme K est aussi normal, alors $g_2K = Kg_2$, ce qui nous donne :

$$\phi(g_1Ng_2N) = \phi(g_1g_2NN) = \phi(g_1g_2N) = g_1g_2K = g_1Kg_2K = \phi(g_1N)\phi(g_2N)$$

Il s'agit donc bien d'un homomorphisme. Maintenant, il est facile de voir que ϕ est surjectif. Il nous faut maintenant déterminer le noyau :

$$\ker(\phi) = \{gN : g \in K\} = K/N$$

En applicant le premier théorème d'isomorphisme, on obtient donc :

$$(G/N)/(K/N) \cong G/K$$

□

Chapitre 5

Les actions de groupes

5.1 Introduction

En algèbre linéaire II, il a été montre qu'une matrice $n \times n$ n'est en fait rien d'autre qu'une application linéaire de $\mathbb{R}^n$ vers $\mathbb{R}^n$. En théorie des groupes, il y a une notion similaire, celle d'action de groupe. On peut regarder un groupe comme étant une collection de fonctions qui agit sur un ensemble, de la même manière qu'une matrice agit sur $\mathbb{R}^n$.

Definition 5.1.1. Si G est un groupe, et X est un ensemble, alors on définit un action de groupe comme étant une fonction $G \times X \to X$ telle que :

1. $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$, pour tout $g_1, g_2 \in G$ et pour tout $x \in X$.
2. $e \cdot x = x$ pour tout $x \in X$.

Exemple 5.1.1. Si $n \in \mathbb{N}, n \geq 2$, alors le groupe S_n définit un action de groupe sur un ensemble X de n éléments. Ceci n'est en fait rien autre que la définition du groupe symétrique. En effet, nous avons définit le groupe symétrique S_n comme étant l'ensemble des permutations d'un ensemble de n éléments.

Exemple 5.1.2. Si G est un groupe, alors on définit un action de G sur lui même par translation à gauche comme étant l'action suivante :

$$g \cdot x = gx, \quad \forall g, x \in G$$

notez qu'ici le point dénote l'action, alors que l'absence de symbol à droite de l'égalité représente l'opération du groupe G.

Exemple 5.1.3. Si G est un groupe, alors on définit un action de G sur lui même par conjugaison comme étant l'action suivante :

$$g \cdot x = gxg^{-1}, \quad \forall g, x \in G$$

Definition 5.1.2. Si G est un groupe qui agit sur un ensemble X, alors on définit les termes suivant :

1. Le noyau de l'action est définit par l'ensemble $\{g \in G : g \cdot x = x, \forall x \in X\}$, c'est à dire l'ensemble des éléments de G qui agisse trivialement sur X.
2. Le stabilisateur d'un élément $x \in X$ est l'ensemble $\mathcal{S}(x) = \{g \in G : g \cdot x = x\}$, c'est à dire l'ensemble des éléments de G qui garde l'élément x fixe.
3. L'orbite d'un élément $x \in X$ est l'ensemble $\mathcal{O}(x) = \{g \cdot x : g \in G\}$, c'est à dire l'ensemble des éléments qui peuvent être obtenu par l'action d'un élément de G sur x.
4. L'ensemble des points fixes d'un élément $g \in G$ est l'ensemble $Fix(g) = \{x \in X : g \cdot x = x\}$, c'est à dire l'ensemble des éléments de X qui sont fixés par l'action de g.
5. L'action est dites fidèle si le noyau de l'action contient uniquement l'identité, c'est à dire que l'intersection de tout les stabilisateurs est réduite à l'identité.
6. L'action est dites transitive si pour tout $x, y \in X$, il existe un $g \in G$ tel que $g \cdot x = y$.

Théorème 5.1.1. Si G est un groupe qui agit sur un ensemble X, alors les orbites partitionnent X en différentes classes d'équivalence. C'est à dire :

1. $X = \bigcup_{x \in X} \mathcal{O}(x)$.
2. Si $x, y \in X$, alors $\mathcal{O}(x) = \mathcal{O}(y)$ ou $\mathcal{O}(x) \cap \mathcal{O}(y) = \varnothing$.
3. La relation $x \sim y$ si et seulement si x est dans la même orbite de y est une relation d'équivalence sur X.

Démonstration.

1. Pour cette partie, il suffit de remarquer que si e est l'identité du groupe G, alors $e \cdot x = x$ pour tout $x \in X$. On a donc que $x \in \mathcal{O}(x)$ pour tout $x \in X$, ce qui signifit que l'union de tous les orbites doit contenir tout les éléments de X.
2. Supposons que $x, y \in X$ sont tel que $\mathcal{O}(x) \cap \mathcal{O}(y) \neq \varnothing$, alors il existe $z \in \mathcal{O}(x) \cap \mathcal{O}(y)$. Par définition d'un orbite, il existe donc $g_x, g_y \in G$ tel que $g_x \cdot x = z$ et $g_y \cdot y = z$. Maintenant, prenons $w \in \mathcal{O}(x)$, il existe donc un $g_w \in G$ tel que $g_w \cdot x = w$. Ceci nous permet donc d'obtenir :

   $$w = g_w \cdot x = g_w \cdot (g_x^{-1} g_y \cdot y) = (g_w g_x^{-1} g_y) \cdot y \in \mathcal{O}(y)$$

   On obtient donc $\mathcal{O}(x) \subseteq \mathcal{O}(y)$. De la même manière, on obtient l'inclusion inverse. On peut donc conclure que si $\mathcal{O}(x) \cap \mathcal{O}(y) \neq \varnothing$, alors $\mathcal{O}(x) = \mathcal{O}(y)$.
3. Cette partie est une conséquence directe de la partie précédente et vous est laissé en exercice.

□

Théorème 5.1.2. Si G est un groupe et X un ensemble, alors il existe une bijection entre les actions de G sur X et les homomorphismes de G sur $S_{|X|}$.

Démonstration. Supposons que $G \times X \to X$ est un action de groupe. Pour chaque $g \in G$, on définit $\sigma_g : X \to X$. On veut montrer que σ_g est une bijection, et donc est un élément de $S_{|X|}$. Pour ce faire, supposons que $\sigma_g(x) = \sigma_g(y)$, alors en utilisant la définition d'un action, on obtient :

$$\begin{aligned} \sigma_g(x) = \sigma_g(y) &\Rightarrow g \cdot x = g \cdot y \\ &\Rightarrow g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y) \\ &\Rightarrow (g^{-1} g) \cdot x = (g^{-1} g) \cdot y \\ &\Rightarrow e \cdot x = e \cdot y \\ &\Rightarrow x = y \end{aligned}$$

Donc la fonction σ_g est injective. Maintenant supposons que $y \in X$ et posons $x = g^{-1} \cdot y$, ce qui nous donne :

$$\sigma_g(x) = g \cdot x = g \cdot (g^{-1} \cdot y) = (g g^{-1}) \cdot y = e \cdot y = y$$

Donc la fonction σ_g est aussi surjective, ce qui confirme qu'il s'agit d'une bijection et donc $\sigma_g \in S_{|X|}$. Maintenant, définissons la fonction $\Psi : G \to S_{|X|}$ comme étant $\Psi(g) = \sigma_g$. On veut montrer qu'il s'agit d'un homomorphisme.

$$\sigma_{gh}(x) = (gh) \cdot x = g \cdot (h \cdot x) = \sigma_g(h \cdot x) = \sigma_g(\sigma_h(x)) = (\sigma_g \circ \sigma_h)(x)$$

Ce qui nous donne :

$$\Psi(gh) = \sigma_{gh} = \sigma_g \circ \sigma_h = \Psi(g) \circ \Psi(h)$$

Ce qui confirme que Ψ est bien un homomorphisme. Donc pour tout action de G sur X, on peut donc associer un élément $\Psi \in \mathrm{Hom}(G, S_{|X|})$. Pour montrer qu'il s'agit bien d'une bijection entre les actions de G sur X et les homomorphismes de G sur $S_{|X|}$, il faut maintenant montrer que le processus est réversible. Pour ce faire, prenons $\Phi \in \mathrm{Hom}(G, S_{|X|})$ et définissons

$$g \cdot x = \Phi(g)(x), \quad \forall g \in G, \forall x \in X$$

On veut montrer qu'il sagit qu'il s'agit bien d'un action de groupe. Si e est l'identité de G, alors que Φ est un homomorphisme, $\Phi(e)$ est l'identité de $S_{|X|}$. Donc pour tout $x \in X$, on a $e \cdot x = \Phi(e)(x) = x$. Maintenant, si $g, h \in G$ et $x \in X$, alors on a :

$$(gh) \cdot x = \Phi(gh)(x) = \Phi(g)\Phi(h)(x) = \Phi(g)[\Phi(h)(x)] = \Phi(g)(h \cdot x) = g \cdot (h \cdot x)$$

Donc il s'agit bien d'un action de groupe. Maintenant, remarquons que si on commence avec un action de groupe et on applique la méthode ci-dessus pour obtenir un homomorphisme entre G et $S_{|X|}$, puis en repartant de cet homomorphisme, on applique la méthode que nous venons de voir pour obtenir un action de groupe, alors cette action est la même que l'action que nous avions au départ. Il s'agit donc d'une bijection entre les actions de G sur X et les homomorphisme de G sur $S_{|X|}$. □

Théorème 5.1.3. **(formule d'orbite-stabilisateur)** Si G est un groupe et X est un ensemble, et supposons que G agit sur l'ensemble X, alors il existe une bijection entre les éléments de $\mathcal{O}(x)$ et les classes à gauche de $\mathcal{S}(x)$. En conséquence, on a l'égalité suivante :

$$|\mathcal{O}(x)| = [G : \mathcal{S}(x)]$$

Démonstration. Prenons $x \in X$, alors rappellons nous premièrement les deux définitions suivantes :

$$\mathcal{O}(x) = \{g \cdot x : g \in G\}$$

$$\mathcal{S}(x) = \{g \in G : g \cdot x = x\}$$

Et on définit la fonction suivante :

$$g \cdot x \to g\mathcal{S}(x)$$

On veut montrer qu'il s'agit d'une bijection entre les éléments de $\mathcal{O}(x)$ et les classes à gauche de $\mathcal{S}(x)$. Supposons premièrement que $g\mathcal{S}(x) = h\mathcal{S}(x)$, alors :

$$g\mathcal{S}(x) = h\mathcal{S}(x) \Rightarrow g^{-1}h \in \mathcal{S}(x) \Rightarrow g^{-1}h \cdot x = x \Rightarrow gg^{-1}h \cdot x = g \cdot x \Rightarrow h \cdot x = g \cdot x$$

La fonction est donc injective. Maintenant, d'après la définition de la fonction, il est évident qu'elle est aussi surjective. Il y a donc bien une bijection entre les éléments de $\mathcal{O}(x)$ et les classes à gauche de $\mathcal{S}(x)$. En conséquence, ces deux ensembles doivent avoir le même nombre d'élément, ce qui nous permet d'affirmer que :

$$|\mathcal{O}(x)| = [G : \mathcal{S}(x)]$$

□

5.2 Le théorème de Cayley

Le but de cette section est de développer la théorie nécessaire pour démontrer que tout les groupes finis peuvent être vu comme des sous-groupes d'un groupe de permutation. Ce théorème porte le nom de théorème de Cayley. Pour démontrer le théorème, nous allons étudier plus en détail l'action de groupe sur lui même par multiplication à gauche. Si G est un groupe, alors on définit l'action de G sur lui même par multiplication à gauche comme étant :

$$g \cdot h = gh$$

Théorème 5.2.1. L'action d'un groupe G sur lui même par multiplication à gauche est toujours transitive et fidèle.

Démonstration. Commençons par montrer que l'action est transitive. Pour ce faire, prenons $h_1, h_2 \in G$. Si on pose $g = h_2 h_1^{-1}$, alors on obtient :

$$g \cdot h_1 = gh_1 = (h_2 h_1^{-1})h_1 = h_2(h_1^{-1}h_1) = h_2 e = h_2$$

Ce qui confirme la transitivité de l'action. Maintenant, on veut montrer que l'action est fidèle, Pour ce faire, on doit trouver l'intersection de tout les stabilisateurs. Supposons que $h \in G$, alors on veut déterminer $\mathcal{S}(h)$:

$$\mathcal{S}(h) = \{g \in G : g \cdot h = h\} = \{g \in G : gh = h\} = \{g \in G : g = e\} = \{e\}$$

En conséquence, si on prend l'intersection de tous les stabilisateurs, on obtient :

$$\bigcap_{h \in G} \mathcal{S}(h) = \bigcap_{h \in G} \{e\} = \{e\}$$

L'action est donc fidèle. □

Théorème 5.2.2. **(Théorème de Cayley)** Si G est un groupe d'ordre n, alors G est isomorphique à un sous-groupe de S_n.

Démonstration. Considérons l'action de G sur lui même par multiplication à gauche. Comme nous l'avons vu dans la section précédente, cette action génère un homomorphisme $\Psi : G \to S_{|G|}$. D'après le théorème, cet homomorphisme est donné par :

$$\Psi : G \to S_{|G|}$$

$$\Psi(g) = \sigma_g$$

Où σ_g est la fonction $\sigma_g : G \to G$ définit par $\sigma_g(h) = g \cdot h = gh$. D'après le premier théorème d'isomorphisme, on a donc :

$$G/\ker(\Psi) \cong Im(\Psi) \subseteq S_{|G|}$$

Comme l'action est fidèle, on a donc $Im(\Psi) = \{e\}$, ce qui nous permet d'obtenir :

$$G \cong Im(\Psi) \subseteq S_{|G|}$$

G est donc isomorphique à un sous-groupe de S_n, où n est donné par l'ordre du groupe G. □

Remarquer que le théorème affirme qu'un groupe d'ordre n est isomorphique à un sous-groupe de S_n, mais ce n'est pas nécessaire l'isomorphisme le plus simple vers un sous-groupe d'un groupe de permutation. Par exemple, selon le théorème S_3 est un sous-groupe de S_6, ce qui n'est pas nécessairement très intéressant car S_3 est déjà un groupe de permutations.

Exemple 5.2.1. Le groupe de Klein V_4 est un groupe d'ordre 4. D'après le théorème de Cayley, V_4 est donc isomorphique à un sous-groupe de S_4. On veut déterminer quel est ce sous-groupe. Pour ce faire, on remarque que cet isomorphisme est donné par la démonstration du théorème de Cayley.

$$\Psi : V_4 \to S_4$$

$$\Psi(g) = \sigma_g$$

Maintenant, rapellons nous la table de multiplication du groupe V_4 :

$*$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Maintenant, question d'obtenir un isomorphisme qui respecte la notation numérique utilisé dans S_4, nous allons associé un nombre à chaque élément de V_4. On aura donc $e \to 1$, $a \to 2$, $b \to 3$ et $c \to 4$. Ce qui nous donne :

$$\begin{aligned} \sigma_e &= id \\ \sigma_a &= (12)(34) \\ \sigma_b &= (13)(24) \\ \sigma_{ab} &= (14)(23) \end{aligned}$$

On a donc que V_4 est isomorphique au sous-groupe de S_4 généré par :

$$\langle (12)(34), (13)(24), (14)(23) \rangle$$

5.3 L'équation de classe

Nous allons maintenant considérer l'action d'un groupe G sur lui même par conjugaison. Si $g, h \in G$, cette action est définie par :

$$g \cdot h = ghg^{-1}$$

Nous allons maintenant utiliser cette action, pour démontrer l'équation de classe, une équation particulièrement importante de la théorie des groupes.

Théorème 5.3.1. **(L'équation de classe)** Si G est un groupe fini, et $g_1, g_2, ..., g_r$ sont des éléments des différentes classe de conjugaison, alors on a l'équation suivante :

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$$

Démonstration. Premièrement, remarquons que pour chaque $g \in G$ on a $g \in \mathcal{O}(g)$, et donc tout les éléments de G font partie d'au moins une orbite, et de plus, si $\mathcal{O}(g) \cap \mathcal{O}(h) \neq \varnothing$, alors $\mathcal{O}(g) = \mathcal{O}(h)$. En particulier, on remarque donc que les différentes orbites partitionnent G. Donc si on choisit $\{g_1, g_2, g_3, ...g_k\}$ des représentants des différentes orbites de G, alors on a :

$$G = \bigcup_{i=1}^{k} \mathcal{O}(g_i) \qquad \text{et} \qquad \mathcal{O}(g_i) \cap \mathcal{O}(g_j) \text{ si } i \neq j$$

Ce qui nous permet d'obtenir :

$$|G| = \sum_{i=1}^{k} |\mathcal{O}(g_i)|$$

Maintenant, supposons que $g \in Z(G)$, alors :

$$\mathcal{O}(g) = \{g \cdot h : h \in H\} = \{hgh^{-1} : h \in G\} = \{g : h \in G\} = \{g\}$$

Donc les orbites des éléments du centre contiennent exactement un élément chaque. Donc si on suppose que $\{g_1, g_2, g_3, ..., g_k\}$ sont des représentant des différentes orbites de G, excluant les éléments qui ce trouve dans le centre du groupe, alors on obtient l'égalité suivante :

$$|G| = |Z(G)| + \sum_{i=1}^{k} |\mathcal{O}(g_i)|$$

Maintenant, comme $|\mathcal{O}(x)| = [G : \mathcal{S}(x)]$, on obtient donc :

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : \mathcal{S}(g_i)]$$

Maintenant, remarquons que :

$$\mathcal{S}(g_i) = \{g \in G : g \cdot g_i = g_i\} = \{g \in G : gg_ig^{-1} = g_i\} = \{g \in G : gg_i = g_ig\} = C_G(g_i)$$

Ce qui nous donne finalement :

$$|G| = |Z(G)| + \sum_{i=1}^{k} |G : C_G(g_i)|$$

□

Corollaire 5.3.1. Si G est un groupe d'ordre p^2 où p est un nombre premier, alors G est isomorphique à $\mathbb{Z}_{p^2}$ ou $\mathbb{Z}_p \times \mathbb{Z}_p$.

Démonstration. Supposons que $\{g_1, g_2, g_3, ..., g_k\}$ sont des représentants des différentes orbites qui ne sont pas dans le centre, alors par l'équation de classe on obtient :

$$|G| = |Z(G)| + \sum_{i=1}^{k} |G : C_G(g_i)|$$

Maintenant, comme $|G : C_G(g_i)| = \dfrac{|G|}{|C_G(g_i)|}$ et $|G| = p^2$, alors $|G : C_G(g_i)|$ doit être $1, p$ ou p^2. Maintenant, comme par hypothèse $g_i \notin Z(G)$, alors $C_G(g_i) \neq G$. Donc $|C_G(g_i)| \neq p^2$, et en conséquence $|G : C_G(g_i)| \neq 1$. On obtient donc que $p \| G : C_G(g_i)|$ pour tout i, et donc :

$$p \Big| \sum_{i=1}^{k} |G : C_G(g_i)|$$

Comme p divise aussi l'ordre du groupe G, par l'équation de classe on doit donc avoir $p|Z(G)$. Comme $Z(G)$ est un sous-groupe de G, on doit donc avoir que l'ordre de $Z(G)$ est soit p ou p^2. Il est donc facile de voir que $G/Z(G)$ est soit d'ordre 1 ou p. Dans les deux cas, $G/Z(G)$ est un groupe cyclique. Il existe donc un $x \in G$ tel que :

$$G/Z(G) = \langle xZ(G) \rangle$$

En particulier si $g, h \in G$, alors il existe $j, k \in \mathbb{N}$ et $y, z \in Z(G)$ tel que :

$$g = x^j y \qquad h = x^k z$$

Ce qui nous donne :

$$gh = x^j y x^k z = x^j x^k yz = x^k x^j yz = x^k x^j zy = x^k z x^j y = hg$$

Et donc le groupe G doit être abélien. Comme G est un groupe d'ordre p^2, alors les éléments de G doivent être d'ordre $1, p$ ou p^2. Si G contient un élément d'ordre p^2, alors nous avons déjà vu que $G \cong \mathbb{Z}_{p^2}$. Supposons donc que G ne contient pas d'élément d'ordre p^2. Donc tout les éléments de G sauf l'identité doit être d'ordre p. Fixons $x \in G \backslash \{e\}$, et prenons $y \in G \backslash \langle x \rangle$. On a donc $|\langle x \rangle| = |\langle y \rangle| = p$. De plus, comme $y \notin \langle x \rangle$ et $|\langle x, y \rangle| > |\langle x \rangle| = p$, alors $|\langle x, y \rangle| = p^2 = |G|$. On a donc que tout les éléments de G sont de la forme $x^j y^k$. Comme $\langle x \rangle \cong \langle y \rangle \cong \mathbb{Z}_p$, on obtient donc l'isomorphisme suivant :

$$\psi : \langle x \rangle \times \langle y \rangle \to \langle x, y \rangle$$

$$\phi(x^j, y^k) = x^j y^k$$

Ce qui n'est rien d'autre qu'un isomorphisme entre G et $\mathbb{Z}_p \times \mathbb{Z}_p$. □

Théorème 5.3.2. **(Théorème de Cauchy)** Si G est un groupe fini et p un nombre premier tel que $p \Big| |G|$. Alors G contient un élément d'ordre p.

Démonstration. Si G est un groupe abélien, la démonstration a déjà été faites. Nous allons donc supposer que G n'est pas abélien, et donc $Z(G) \neq G$. Nous allons à nouveau faire la démonstration par induction sur l'ordre du groupe G. Le résultat est facile à vérifier pour des groupes de petit ordre. Nous allons donc supposer que le théorème est vrai pour tout groupe d'ordre inférieur à celle de G. Supposons que $\{g_1, g_2, ..., g_k\}$ sont des représentant des différentes classe de conjugaison qui ne contiennent pas un seul élément. Comme $C_G(g_i)$ est un sous-groupe de G et l'ordre de $C_G(g_i)$ est nécessairement inférieure à celle de G, on a donc que si $p \Big| |C_G(g_i)|$, alors $C_G(g_i)$ contient un élément d'ordre p par induction, et donc G contient un élément d'ordre p. Nous allons donc supposer qu'aucune des $|C_G(g_i)|$ n'est divisible par p. Dans ce cas, on doit avoir que :

$$p \Big| \frac{|G|}{|C_G(g_i)|}, \ \forall i \quad \Rightarrow \quad p \Big| [G : C_G(g_i)], \ \forall i$$

Par l'équation de classe, nous avons :

$$|Z(G)| = |G| - \sum_{i=1}^{k} [G : C_G(g_i)]$$

Comme tout les termes de droite sont divisible par p, on doit donc avoir que $p \Big| |Z(G)|$. Par induction, $Z(G)$ contient donc un élément d'ordre p, et en conséquence, G contient un élément d'ordre p. □

5.4 Le lemme de Burnside

Nous allons maintenant nous intéressé à une application de la théorie des groupes à un problème de combinatoire, mais avant nous avons besoin de quelques résultats supplémentaires.

Théorème 5.4.1. Si G est un groupe qui agit sur un ensemble X, alors :

$$\sum_{x \in X} |\mathcal{S}(x)| = \sum_{g \in G} |Fix(g)|$$

Démonstration. Il s'agit de compter le nombre d'élément dans l'ensemble ci-dessous de deux manières différentes :

$$A = \{(g, x) \in G \times X : g \cdot x = x\}$$

On remarque facilement que les éléments de A qui commence par $g_1 \in G$ sont en fait les éléments de $Fix(g_1)$. Donc si on veut compter le nombre d'éléments de A, il suffit de calculer le nombre d'élément dans $Fig(g)$ pour tout les $g \in G$. On a donc :

$$|A| = \sum_{g \in G} |Fix(g)|$$

Ensuite, on remarque aussi que les éléments de A qui se termine par $x_1 \in X$ sont en fait les élément de $\mathcal{S}(x_1)$. Donc si on veut compter le nombre d'éléments A, il suffit de calculer le nombre d'élément dans $\mathcal{S}(x)$ pour tout les $x \in X$. On a donc :

$$|A| = \sum_{x \in X} |\mathcal{S}(x)|$$

En combinant ces deux équations, on obtient le résultat. □

Théorème 5.4.2. **(Lemme de Burnside)** Si G est un groupe qui agit sur un ensemble X, alors :

$$\text{Nombre d'orbites} = \frac{1}{|G|}\sum_{g\in G}|Fix(g)|$$

Démonstration. Par la formule d'orbite-stabilisateur, on a que :

$$|\mathcal{O}(x)| = |G : \mathcal{S}(x)| = \frac{|G|}{|\mathcal{S}(x)|}$$

Ce qui signifie en réorganisant les termes :

$$|\mathcal{S}(x)| = \frac{|G|}{|\mathcal{O}(x)|}$$

Maintenant, si on calcul la somme sur les différents $x \in X$, on obtient donc :

$$\sum_{x\in X}|\mathcal{S}(x)| = \sum_{x\in X}\frac{|G|}{|\mathcal{O}(x)|}$$

Puis, en utilisant le théorème précédent, on obtient :

$$\sum_{g\in G}|Fix(g)| = \sum_{x\in X}\frac{|G|}{|\mathcal{O}(x)|} = |G|\sum_{x\in X}\frac{1}{|\mathcal{O}(x)|}$$

Maintenant, remarquons que :

$$\sum_{x\in\mathcal{O}(x)}\frac{1}{|\mathcal{O}(x)|} = \frac{\text{Nombre d'élément dans } \mathcal{O}(x)}{|\mathcal{O}(x)|} = 1$$

Ce qui signifie que si $x_1, x_2, x_3, ..., x_k$ sont des représentants des différentes orbites de l'action, on a donc :

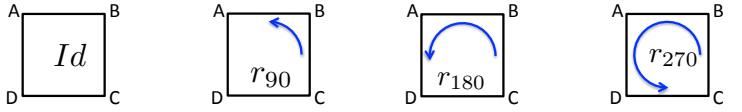
$$\sum_{x\in X}\frac{1}{|\mathcal{O}(x)|} = \sum_{x\in\mathcal{O}(x_1)}\frac{1}{|\mathcal{O}(x)|} + \sum_{x\in\mathcal{O}(x_2)}\frac{1}{|\mathcal{O}(x)|} + ... + \sum_{x\in\mathcal{O}(x_k)}\frac{1}{|\mathcal{O}(x)|} = \underbrace{1+1+...+1}_{k\text{fois}} = k = \text{Nombre d'orbites}$$

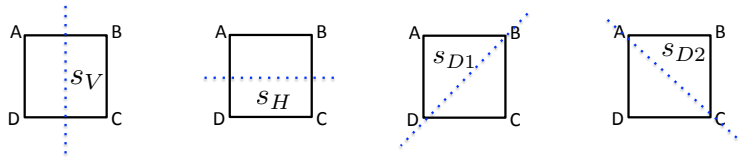
Ce qui nous donne finalement :

$$\sum_{g\in G}|Fix(g)| = \sum_{x\in X}\frac{|G|}{|\mathcal{O}(x)|} = |G|\sum_{x\in X}\frac{1}{|\mathcal{O}(x)|} = |G|\cdot\text{Nombre d'orbites}$$

□

Exemple 5.4.1. Combien de collier de 4 perles peut-on faire si on possède des perles de 5 couleurs différentes ? Pour ce faire, on remarque qu'un collier reste inchangé selon l'action des éléments du groupe D_8. La solution du problème revient donc à déterminer le nombre d'orbite différente de l'action du groupe D_8 sur nos collier. Pour appliquer le lemme de Burnside, il nous faut donc déterminer le nombre de carré avec des sommets de 5 couleurs différentes possible sont fixé selon chacun des éléments de notre groupe.





Éléments du groupe	Condition pour que le carré soit fixé	$\|Fix(g)\|$
Id	Toutes les configurations sont acceptable	625
r_{90}	Tous les sommets doivent être de même couleur	5
r_{180}	A et C doivent être de même couleur, ainsi que B et D	25
r_{270}	Tous les sommets doivent être de même couleur	5
s_V	A et B doivent être de même couleur ainsi que C et D	25
s_H	A et D doivent être de même couleur ainsi que B et C	25
s_{D1}	A et C doivent être de même couleur	125
s_{D2}	B et D doivent être de même couleur	125
Somme		960

Par le lemme de Burnside, on peut donc affirmer qu'il y a $\frac{960}{8} = 120$ colliers différents de 4 perles si 5 couleurs de perles sont disponible.

Deuxième partie

La théorie des anneaux et des corps

Chapitre 6

Les anneaux et les corps

6.1 Introduction

Dans la première partie du cours, nous avons étudier une structure algébrique comportant une seule loi de composition interne : La structure du groupe. Cette dernière est particulièrement importante, et se retrouve dans une variété de domaine, que ce soit en mathématiques ou dans les domaines d'applications. Dans la partie II, nous allons maintenant regarder des structures algébriques comportant deux lois de composition internes, communément appelé l'addition et la multiplication. Il s'agit de la structure d'anneau, et de celle de corps.

Definition 6.1.1. Un anneau $(R, +, \times)$ est un ensemble R muni de deux lois de composition interne, une addition $+$ et une multiplication $\times$ et qui satisfait les propriétés suivante :

1. $(R, +)$ est un groupe abélien
2. $\times$ est associative, c'est à dire que pour tout $a, b, c \in R$ on a $(a \times b) \times c = a \times (b \times c)$
3. La multiplication est distributive sur l'addition, c'est à dire que pour tout $a, b, c \in R$ on a $a \times (b + c) = (a \times b) + (a \times c)$ et $(a + b) \times c = (a \times c) + (b \times c)$.

Lorsqu'il n'y a pas de confusion possible, on parle de l'anneau R plutôt que de l'anneau $(R, +, \times)$. Ceci est un abut de language techniquement incorecte, mais qui est très pratique pour simplifier la notation. Notez aussi qu'il est très commun d'écrire ab à la place de $a \times b$. De plus, on dénote l'identité et l'inverse du groupe $(R, +)$ à l'aide de la notation additive. C'est à dire que l'identité de ce groupe sera dénoté par 0 et l'inverse de l'élément a sera dénoté par $-a$.

Definition 6.1.2. Si $(R, +, \times)$ est un anneau, alors on dit que :

1. R est un anneau avec identité s'il existe un élément $1 \in R$ tel que $1a = a1 = a$ pour tout $a \in R$.
2. R est un anneau commutatif si la multiplication est commutative ($ab = ba$ pour tout $a, b \in R$).
3. R est un anneau de division si R est un anneau avec identité pour lequel tout les éléments $a \in R \backslash \{0\}$ possède un inverse multiplicatif, c'est à dire que pour tout $a \in R \backslash \{0\}$, il existe $a^{-1} \in R$ tel que $aa^{-1} = 1$.
4. R est un corps si R est un anneau de division pour lequel la multiplication est commutative.

Notez que notre définition de corps et d'anneau de division n'est pas tout à fait standard. Il existe en effet un vocabulaire qui diverge entre le monde francophone et anglophone sur le sujet. Dans le texte, il a été choisi de suivre la momenclature américaine, car ces celle que vous risquer le plus de rencontrer que ce soit sur internet, dans des livres de références, des articles, ou bien dans des cours plus avancé. En France, le terme corps est habituellement utilisé pour ce que nous avons définit être un anneau de division. Les objets que nous avons appelé corps sont habituellement appelé corps commutatif en France. Il faut donc faire très attention à la définition du mot corps pour éviter des erreurs.

À partir des définitions que nous venons faire, on obtient donc les deux chaînes d'inclusion suivante :

$$\text{Corps} \subset \text{Anneaux de division} \subset \text{Anneaux avec identité} \subset \text{Anneaux}$$

Corps $\subset$ Anneaux commutatif $\subset$ Anneaux

Exemple 6.1.1. Les nombres rationnels $\mathbb{Q}$, les nombres réels $\mathbb{R}$ et les nombres complexes $\mathbb{C}$ muni des opérations habituelles d'addition et de multiplication sont des corps. De plus, l'ensemble des nombres entiers $\mathbb{Z}$ muni des opérations habituelles d'addition et de multiplication est un anneau commutatif avec identité, mais ne forme pas un anneau de division car à l'exception de ± 1, aucun élément ne possède d'inverse multiplicatif. En particulier, le nombre 2 ne possède pas d'inverse multiplicatif ($1/2$ ne fait pas partie des nombres entiers.).

Exemple 6.1.2. Les nombres modulos $\mathbb{Z}_n$ forme un anneau commutatif avec identité pour tout $n \geq 2$. Pour le voir, rappelons que sur l'ensemble des nombres entiers, on peut définir la relation d'équivalence $a \equiv_n b$ si et seulement si $n|(b-a)$. Maintenant, pour tout $a \in \mathbb{Z}$, on définit $\overline{a} = \{x \in \mathbb{Z} : x \equiv_n a\}$, puis on définit $\mathbb{Z}_n = \{\overline{a} : a \in \mathbb{Z}\}$. Ceci nous permet donc de partitionner l'ensemble des entiers en n classe d'équivalence. Sur l'ensemble $\mathbb{Z}_n$, on définit ensuite les deux opérations suivantes :

$$\overline{a} + \overline{b} = \overline{a+b}$$

$$\overline{a} \times \overline{b} = \overline{ab}$$

Nous avons déjà démontré dans la première partie du cours que ces deux opérations sont bien définie et que $(\mathbb{Z}_n, +)$ forme un groupe abélien. Nous allons maintenant démontrer que la multiplication est associative, commutative, possède un identité et finalement est distributive sur l'addition. Si $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$, alors on a

$$(\overline{a}\ \overline{b})\ \overline{c} = \overline{ab}\ \overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a}\ \overline{bc} = \overline{a}\ (\overline{b}\ \overline{c})$$

La multiplication est donc associative. Maintenant, si $\overline{a}, \overline{b} \in \mathbb{Z}_n$, alors on a aussi :

$$\overline{a}\ \overline{b} = \overline{ab} = \overline{ba} = \overline{a}\ \overline{b}$$

La multiplication est donc commutative. De plus, il est facile de voir que pour tout $\overline{a} \in \mathbb{Z}_n$, on a $\overline{1}\ \overline{a}$. La multiplication possède donc un identité. Il ne nous reste donc plus qu'à démontrer que la multiplication est distributive sur l'addition. Pour ce faire, prenons $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$, alors on a :

$$\overline{a}\ (\overline{b} + \overline{c}) = \overline{a}\ (\overline{b+c}) = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab} + \overline{ac} = (\overline{a}\ \overline{b}) + (\overline{a}\ \overline{c})$$

Notez qu'il n'est pas nécessaire de vérifier l'autre égalité car nous savons déjà que la multiplication est commutative. Nous avons donc montrer que $\mathbb{Z}_n$ forme bien un anneau commutatif avec identité.

Exemple 6.1.3. Si p est un nombre premier, alors les nombres modulos $\mathbb{Z}_p$ forment un corps. Nous avons déjà vu dans l'exemple précédent qu'il s'agit d'un anneau commutatif avec identité, il ne reste donc plus qu'à démontrer que chaque élément différent de 0 possède un inverse multiplicatif. Rappelons de la première partie du cours qu'un élément $\overline{a}$ de $\mathbb{Z}_p$ est inversible (selon la multiplication) si et seulement si $(a,p) = 1$. Comme p est premier, cette condition est toujours satisfaite si $a \notin \overline{0}$. Il s'agit donc bien d'un corps. Notez qu'il est commun de dénoter ce corps par $\mathbb{F}_n$ plutôt que $\mathbb{Z}_n$ pour différentier le corps du groupe modulo.

Exemple 6.1.4. Si R est un anneau commutatif avec identité, alors on définit $R[x]$ comme étant l'ensemble de tous les polynômes de la forme

$$a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0, \quad a_i \in R, \forall i \in \{0, ..., n\}$$

C'est à dire l'ensemble des polynômes à coefficient dans l'anneau R. Notez qu'ici nous considérons l'ensemble de tous les polynômes, peut importe leur degré. Par contre, par définition, le degré d'un polynôme doit être un entier positif. Il nous faut maintenant définir un addition et une multiplication sur les polynômes. Ces deux opérations se définisse comme pour les polynômes à coefficient réels. On aura donc :

$$\left(\sum_{k=0}^{n_1} a_k x^k\right) + \left(\sum_{k=0}^{n_2} b_k x^k\right) = \sum_{k=0}^{\max\{n_1,n_2\}} (a_k + b_k) x^k$$

$$\left(\sum_{k=0}^{n_1} a_k x^k\right)\left(\sum_{k=0}^{n_2} b_k x^k\right) = \sum_{k=0}^{n_1+n_2} c_k x^k, \quad \text{où } c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

Nous voulons maintenant montrer qu'avec cet addition et multiplication, l'ensemble $R[x]$ est un anneau commutatif avec identité. Il n'est pas très difficile de remarquer que $(R[x], +)$ est un groupe abélien, nous allons donc nous concentrer sur les propriétés de la multiplication. Pour l'associativité, on a donc :

$$\left[\left(\sum_{k=0}^{n_1} a_k x^k\right)\left(\sum_{k=0}^{n_2} b_k x^k\right)\right]\left(\sum_{k=0}^{n_3} c_k x^k\right) = \left(\sum_{k=0}^{n_1+n_2}\left(\sum_{j=0}^{k} a_j b_{k-j}\right)x^k\right)\left(\sum_{k=0}^{n_3} c_k x^k\right) = \sum_{k=0}^{n_1+n_2+n_3}\left(\sum_{i=0}^{k}\left(\sum_{j=0}^{i} a_j b_{i-j}\right)c_{k-i}\right)x^k$$

$$= \sum_{k=0}^{n_1+n_2+n_3}\sum_{i=0}^{k}\sum_{j=0}^{i} a_j b_{i-j} c_{k-i} x^k = \sum_{k=0}^{n_1+n_2+n_3}\sum_{j=0}^{k}\sum_{i=j}^{k} a_j b_{i-j} c_{k-i} x^k = \sum_{k=0}^{n_1+n_2+n_3}\left(\sum_{j=0}^{k} a_j\left(\sum_{i=j}^{k} b_{i-j} c_{k-i}\right)\right)x^k$$

$$= \sum_{k=0}^{n_1+n_2+n_3}\left(\sum_{j=0}^{k} a_j\left(\sum_{i=0}^{k-j} b_i c_{(k-j)-i}\right)\right)x^k = \left(\sum_{k=0}^{n_1} a_k x^k\right)\left(\sum_{k=0}^{n_2+n_3}\left(\sum_{i=0}^{k} b_i c_{k-i}\right)x^k\right) = \left(\sum_{k=0}^{n_1} a_k x^k\right)\left[\left(\sum_{k=0}^{n_2} b_k x^k\right)\left(\sum_{k=0}^{n_3} c_k x^k\right)\right]$$

Notez que la partie la plus difficile de la démonstration de l'associativité de la multiplication est lorsque nous avons changé l'ordre des sommes. Vous devriez y porter une attention particulière et vous convaincre qu'il n'y a pas d'erreur. Maintenant, pour la commutativité, on a :

$$\left(\sum_{k=0}^{n_1} a_k x^k\right)\left(\sum_{k=0}^{n_2} b_k x^k\right) = \sum_{k=0}^{n_1+n_2}\left(\sum_{j=0}^{k} a_j b_{k-j}\right)x^k = \sum_{k=0}^{n_1+n_2}\left(\sum_{j=0}^{k} b_{k-j} a_j\right)x^k = \sum_{k=0}^{n_1+n_2}\left(\sum_{j=0}^{k} b_j a_{k-j}\right)x^k = \left(\sum_{k=0}^{n_1} b_k x^k\right)\left(\sum_{k=0}^{n_2} a_k x^k\right)$$

Notez qu'ici la commutativité de l'anneau R était essentielle pour démontrer la commutativité de $R[x]$. Maintenant, pour l'identité, il est facile de voir que l'identité de R est le même que l'identité de $R[x]$. Il ne nous reste donc plus qu'à démontrer la distributivité de la multiplication sur l'addition.

$$\left(\sum_{k=0}^{n_1} a_k x^k + \sum_{k=0}^{n_2} b_k x^k\right)\left(\sum_{k=0}^{n_3} c_k x^k\right) = \left(\sum_{k=0}^{\max\{n_1+n_2\}} (a_k + b_k)x^k\right)\left(\sum_{k=0}^{n_3} c_k x^k\right) = \sum_{k=0}^{\max\{n_1+n_2\}+n_3}\sum_{j=0}^{k}(a_j + b_j)c_{k-j}x^k$$

$$= \sum_{k=0}^{n_1+n_3}\sum_{j=0}^{k} a_j c_{k-j} x^k + \sum_{k=0}^{n_2+n_3}\sum_{j=0}^{k} b_j c_{k-j} x^k = \left(\sum_{k=0}^{n_1} a_k x^k\right)\left(\sum_{k=0}^{n_3} c_k x^k\right) + \left(\sum_{k=0}^{n_2} b_k x^k\right)\left(\sum_{k=0}^{n_3} c_k x^k\right)$$

Par commutativité, l'autre partie de la distributivité est automatiquement satisfaite. On peut donc conclure que si R est un anneau commutatif avec identité, alors $R[x]$ est aussi un anneau commutatif avec identité.

Exemple 6.1.5. Il est possible de généraliser l'exemple précédent et considérez l'ensemble des séries formelles. Si R est un anneau commutatif avec identité, alors on définit l'ensemble $R[[x]]$ comme étant :

$$R[[x]] = \left\{\sum_{k=0}^{\infty} a_k x^k : a_k \in R, \forall k \in \mathbb{N}\right\}$$

Pour que cette ensemble devienne un anneau, il nous faut maintenant y ajouter une addition et une multiplication. Ceci est fait essentiellement de la même façon que pour les polynômes. On définit donc :

$$\left(\sum_{k=0}^{\infty} a_k x^k\right) + \left(\sum_{k=0}^{\infty} b_k x^k\right) = \sum_{k=0}^{\infty}(a_k + b_k)x^k \quad \text{et} \quad \left(\sum_{k=0}^{\infty} a_k x^k\right)\left(\sum_{k=0}^{\infty} b_k x^k\right) = \sum_{k=0}^{\infty}\left(\sum_{j=0}^{k} a_j b_{k-j}\right)x^k$$

On peut maintenant démontrer qu'il s'agit bien d'un anneau et faisant une démonstration très semblable à ce que nous avons fait pour les polynômes. Il y a cependant un point important à noter. Dans cet exemple, nous somme intéressé aux séries formelles et non aux séries numériques. Il n'y a donc pas de notion de convergence. Le x est utilisé ici comme un simple symbol, et non comme une variable.

Exemple 6.1.6. Si R est un anneau et $n \in \mathbb{N}$, alors on définit $M_n(R)$ l'ensemble de toutes les matrices $n \times n$ avec coefficient dans R. Si A_{ij} dénote l'élément qui se trouve sur la i-ème ligne et la j-ème colonnes de la matrice A, alors on définit la somme et le produit à partir des différents éléments qui compose les matrices $A + B$ et AB comme suit :

$$(A + B)_{ij} = A_{ij} + B_{ij}$$

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj}$$

Avec ces opérations, l'ensemble $M_n(R)$ devient donc un anneau.

Exemple 6.1.7. Si $G = \{g_1, g_2, ..., g_n\}$ est un groupe fini et R un anneau commutatif avec identité, alors on définit l'anneau de groupe RG comme étant l'ensemble

$$RG = \{a_1 g_1 + a_2 g_2 + ... + a_n g_n : a_i \in R, \forall i\}$$

Muni de l'addition et de la multiplication suivante :

$$(a_1 g_1 + a_2 g_2 + ... + a_n g_n) + (b_1 g_1 + b_2 g_2 + ... + b_n g_n) = (a_1 + b_1) g_1 + (a_2 + b_2) g_2 + ... + (a_n + b_n) g_n$$

$$(a_1 g_1 + a_2 g_2 + ... + a_n g_n)(b_1 g_1 + b_2 g_2 + ... + b_n g_n) = \sum_{k=0}^{n} \left(\sum_{g_i g_j = g_k} a_i b_j \right) g_k$$

Avec ces opérations, RG est un anneau. De plus, RG est commutatif si et seulement si G est un groupe abélien.

Exemple 6.1.8. Si $(R, +_r, \times_r)$ et $(S, +_s, \times_s)$ sont des anneaux, alors on peut définir l'anneau produit $R \times S$ comme étant l'ensemble

$$R \times S = \{(r, s) : r \in R \text{ et } s \in S\}$$

muni des opérations suivantes :

$$(r_1, s_1) + (r_2, s_2) = (r_1 +_r r_2, s_1 +_s s_2)$$

$$(r_1, s_1) \times (r_2, s_2) = (r_1 \times_r r_2, s_1 \times_s s_2)$$

Dans ce cas, il est facile de vérifier qu'il s'agit bien d'un anneau, et il vous est laissé en exercice de le démontrer. L'anneau $R \times S$ possède un identité si et seulement R et S possèdent tous deux un identité. L'anneau $R \times S$ est commutatif si et seulement si R et S sont commutatif. Notez cependant qu'en général, même si R et S sont des corps, la construction que nous venons faire pour obtenir l'anneau produit $R \times S$ ne permet pas en général d'obtenir un corps. Par exemple, on peut considérez le corps des nombres réels $\mathbb{R}$, et le produit $\mathbb{R} \times \mathbb{R}$ qui est un anneau, mais n'est pas un corps.

Exemple 6.1.9. L'ensemble $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ muni des opérations habituelles d'addition et de multiplication forment un corps. Notons que comme il s'agit de la même multiplication que dans les nombres réels, les propriétés de commutativité, associativité et distributivité sont automatiquement satisfaites. Il nous faut cependant vérifier que les deux opérations sont bien définies, que l'identité de chacune des deux opérations, ainsi que l'inverse additif et multiplicatif de chaque élément se trouve bien dans l'ensemble. Commençons par montrer que l'ensemble est fermé par rapport à l'addition et la multiplication. Pour ce faire, prenons $(a + b\sqrt{2})$ et $(c + d\sqrt{2})$ dans $\mathbb{Q}[\sqrt{2}]$. On obtient donc :

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

L'ensemble est donc bien fermé par rapport à nos deux opérations. Maintenant, il est facile de voir que $0+0\sqrt{2}$ et $1 + 0\sqrt{2}$ sont dans l'ensemble et correspondent bien aux identités de l'addition et de la multiplication respectivement. Ensuite, si $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, alors sont inverse est $a - b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. La seule partie un peu

plus délicate consiste à montrer que l'inverse multiplicatif d'un élément $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ tel que $(a,b) \neq (0,0)$ se trouver dans l'ensemble. Pour ce faire, remarquons que

$$\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-ab\sqrt{2}+ab\sqrt{2}-2b^2} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \left(\frac{a}{a^2-2b^2}\right) + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2}$$

On obtient donc que l'inverse multiplicatif de $a+b\sqrt{2}$ est donné par $\left(\frac{a}{a^2-2b^2}\right) + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Remarquez que ceci est vrai à la condition que $a^2-2b^2 \neq 0$, mais il n'est pas très difficile de voir que cette condition est toujours satisfaite. Ceci confirme donc qu'il s'agit bien d'un corps.

Exercice 6.1.1. Dans l'ensemble précédent, nous avons notez que $a+b\sqrt{2}$ est inversible dans $\mathbb{Q}[\sqrt{2}]$ à la condition que $a^2-2b^2 \neq 0$. Pouvez-vous expliquer pourquoi cette condition est toujours satisfaite ?

Exemple 6.1.10. Si X est un ensemble, alors on définit $\mathcal{P}(X)$ comme étant l'ensemble des sous-ensemble de X. Dans ce cas, $(\mathcal{P}(X), \triangle, \cap)$ forme un anneau commutatif. Rappelons que $\triangle$ dénote la différence symétrique, c'est à dire que $A \triangle B$ est l'ensemble des éléments qui sont dans A ou dans B, mais pas les deux en même temps. Pour ce qui est de $\cap$, il s'agit de l'intersection de deux ensembles, c'est à dire que $A \cap B$ est l'ensemble des éléments qui sont dans A et dans B. Commençons par démontrer que l'addition $(\triangle)$ est associative :

$$\begin{aligned}
A \triangle (B \triangle C) &= A \triangle ((B\backslash C) \cup (C\backslash B)) \\
&= [A\backslash((B\backslash C) \cup (C\backslash B))] \cup [((B\backslash C) \cup (C\backslash B))\backslash A] \\
&= ((A\backslash B)\backslash C) \cup (A \cap B \cap C) \cup ((B\backslash C)\backslash A) \cup ((C\backslash B)\backslash A) \\
&= ((A\backslash B)\backslash C) \cup (A \cap B \cap C) \cup ((B\backslash A)\backslash C) \cup ((C\backslash A)\backslash B) \\
&= ((A\backslash B)\backslash C) \cup ((B\backslash A)\backslash C) \cup ((C\backslash A)\backslash B) \cup (A \cap B \cap C) \\
&= (A\backslash B \cup B\backslash A)\backslash C \cup C\backslash(A\backslash B \cup B\backslash A) \\
&= (A\backslash B \cup B\backslash A) \triangle C \\
&= (A \triangle B) \triangle C
\end{aligned}$$

De plus, on remarque facilement que l'identité avec l'addition est $\varnothing$ et que si $A \subseteq \mathcal{P}(X)$, alors $A \triangle A = \varnothing$, ce qui nous permet d'affirmer que l'inverse additif de A est lui même. Il est aussi facile de voir que $\triangle$ est commutatif. Pour ce faire, remarquons que si A et B sont dans $\mathcal{P}(X)$, alors :

$$A \triangle B = A\backslash B \cup B\backslash A = B\backslash A \cup A\backslash B = B \triangle A$$

Maintenant pour la multiplication (i.e. l'opération $\cap$), il est facile de voir qu'elle est associative, et que l'ensemble X est l'identité pour cette opération. Pour montrer qu'il s'agit d'un anneau, il ne nous reste donc plus qu'à établir la distributivité. Pour ce faire, prenons A, B et C dans $\mathcal{P}(X)$, alors on a :

$$\begin{aligned}
A \cap (B \triangle C) &= A \cap (B\backslash C \cup C\backslash B) = (A \cap (B\backslash C)) \cup (A \cap (C\backslash B)) = ((A \cap B)\backslash(A \cap C)) \cup ((A \cap C)\backslash(A \cap B)) \\
&= (A \cap B) \triangle (A \cap C)
\end{aligned}$$

Ceci confirme donc qu'il s'agit bien d'un anneau commutatif avec identité.

Exercice 6.1.2. Dans l'exemple précédent, pour démontrer l'associativité de l'opération $\triangle$, nous avons utiliser les trois propriétés suivantes sur les ensembles. Si X, Y et Z sont des ensembles, alors :

1. $(X\backslash Y)\backslash Z = (X\backslash Z)\backslash Y$.
2. $(X \cup Y)\backslash Z = (X\backslash Z) \cup (Y\backslash Z)$.
3. $X\backslash(Y\backslash Z \cup Z\backslash Y) = (X\backslash Y)\backslash Z \cup (X \cap Y \cap Z)$.

Vous devriez être en mesure de démontrer ces trois propriétés. De plus, la propriété additionnelle suivante a été utilisé pour démontrer la distributivité. Vous devriez aussi être en mesure de la démontrer :

1. $(X \cap Y)\backslash(X \cap Z) = X \cap (Y\backslash Z)$.

Definition 6.1.3. Si $(R, +, \times)$ est un anneau, alors on définit les termes suivant :

1. Si R possède un identité, alors on dit qu'un élément $a \in R$ est un unité s'il existe un $b \in R$ tel que $ab = ba = 1$. Autrement dit, a est inversible. On dénote l'ensemble des unités de R par $R^\times$.
2. On dit que $a \in R\backslash\{0\}$ est un diviseur de 0, s'il existe un $b \in R\backslash\{0\}$ tel que $ab = 0$ ou $ba = 0$.

Remarque : Dans un corps, tout les éléments différent de 0 sont des unités (par définition), de plus, il n'est pas très difficile de démontrer qu'un corps ne peut pas avoir de diviseur de 0.

Exemple 6.1.11. Si R est un anneau commutatif avec identité, on veut montrer que la la série $\sum_{k=0}^{\infty} x^k$ est un unité dans l'anneau $R[[x]]$. Pour ce faire, on cherche une série $\sum_{k=0}^{\infty} a_k x^k$ telle que

$$\left(\sum_{k=0}^{\infty} a_k x^k\right)\left(\sum_{k=0}^{\infty} x^k\right) = \sum_{k=0}^{\infty}\left(\sum_{j=0}^{k} a_j\right) x^k = 1$$

On obtient donc :

$$\sum_{j=0}^{k} a_j = \begin{cases} 1 \text{ si } k = 0 \\ 0 \text{ autrement} \end{cases}$$

Il est facile de remarquer que dans ce cas on obtient $a_0 = 1$ et $a_i = 0$ si $i \geq 1$. L'inverse de la série $\sum_{k=0}^{\infty} x^k$ est donc $-x + 1$. Remarquer que ceci nous permet d'obtenir la formule familière pour la série géométrique :

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$$

Mais cette fois nous avons procédé de manière purement algébrique, sans avoir recours aux limites.

Exemple 6.1.12. Dans l'anneau $\mathbb{Z}_6$, les éléments 2 et 3 sont des diviseurs de zéro car $2 \times 3 = 0$.

Definition 6.1.4. Un anneau intègre est un anneau commutatif avec identité $1 \neq 0$ qui ne possède aucun diviseur de zéro.

Théorème 6.1.1. Voici quelques propriété des anneaux :

1. Si R est un anneau, alors $0x = x0 = 0$ pour tout $x \in R$.
2. Si R est un anneau intègre et $a, b, c \in R$, alors $a(b-c) = 0 \Leftrightarrow a = 0$ ou $b = c$.

Démonstration.

1. Comme 0 est l'identité pour l'addition, alors $0 + 0 = 0$. En application la règle de distributivité, on obtient donc :
$$0x = (0+0)x = 0x + 0x$$
Ce qui nous permet d'obtenir :
$$0 = 0x + (-0x) = (0x + 0x) + (-0x) = 0x + (0x + (-0x)) = 0x + 0 = 0x$$
On doit donc avoir $0x = 0$ pour tout $x \in R$. En appliquant la même méthode, on obtient que $x0 = 0$ pour tout $x \in R$. Cette dernière partie est laissé en exercice.
2. Supposons premièrement que $a(b-c) = 0$. Comme l'anneau est intègre, il n'y a pas de diviseur de zéro. On doit donc avoir $a = 0$ ou $b - c = 0$, autrement on aurait un diviseur de zéro. Finalement, on remarque que si $b - c = 0$, alors $b = c$, ce qui signifie que $a = 0$ ou $b = c$. Pour l'autre direction, remarquez qu'il s'agit d'une simple conséquence de la première partie du théorème.

□

Corollaire 6.1.1. Si R est un anneau intègre d'ordre fini, alors R est un corps.

Démonstration. Supposons que R est un anneau intègre d'ordre fini, et prenons $a \in R\backslash\{0\}$. On veut montrer que a est inversible. Pour ce faire, considérons la fonction $f : R \to R$ définie par $f(x) = ax$. Cette fonction est injective, pour le montrer remarquons que :

$$f(x) = f(y) \quad \Rightarrow \quad ax = ay \quad \Rightarrow \quad a(x-y) = 0 \quad \Rightarrow \quad a = 0 \text{ ou } x = y$$

Comme nous savons déjà par hypothèse que $a \neq 0$, on doit donc avoir $x = y$ ce qui démontrer l'injectivité. Maintenant, rappelons que si g est une fonction entre deux ensembles finis contenant le même nombre d'élément, alors les notions d'injectivité et de surjectivité de g sont équivalente. Comme notre fonction f se trouve exactement dans ce contexte, on peut donc affirmer que la fonction f est surjective. En particulier, il doit exister un élément $b \in R$ tel que $f(b) = ab = 1$. L'élément a est donc inversible (et $a^{-1} = b$). Comme ceci est le cas pour tout les éléments non nul de R, il doit donc s'agir d'un corps. □

6.2 Les sous-anneaux

Maintenant que nous avons définis le concept d'anneau et regardé plusieurs exemple, nous voulons nous attaquer à la notion de sous-anneaux. Nous allons procéder de la même façon que nous avons définis les notions de sous-groupes et de sous-espaces vectoriels.

Definition 6.2.1. Si R est un anneau, un sous anneau R_1 de R est un sous ensemble $R_1 \subseteq R$ pour lequel la restriction des opérations de R à R_1 transforme R_1 en un anneau.

Notez que la définition d'un sous-anneau est en fait équivalente à dire que R_1 est un sous-anneau de R si et seulement si R_1 est un sous-groupe de R qui est fermé par rapport à la multiplication. Cette seconde définition est d'ailleurs plus facile à vérifier. Il existe de très nombreux exemples de sous-anneaux.

Exemple 6.2.1. Les anneaux $\mathbb{Z}$ et $\mathbb{Q}$ sont des sous-anneaux de $\mathbb{R}$.

Dans le cas des groupes, l'étude des sous-groupes nous a amener naturellement au théorème de Lagrange, puis au concept de groupe quotient. Le problème ici est que les sous-anneaux ne sont pas tout à fait la notion que nous avons besoin pour continuer notre étude de la théorie des anneaux. Il s'agira plutôt de la notion d'idéal. Mais avant, nous allons étudier la notion d'homomorphisme qui va nous permettre d'arriver de manière plus simple à la notion d'idéal.

6.3 Les homomorphismes et les isomorphismes

Comme pour les groupes, nous avons maintenant besoin d'introduire un concept de fonction entre deux anneaux. Pour que ce concept soit intéressant, il n'est plus suffisant d'imposer qu'il soit compatible avec l'addition, il nous faut maintenant qu'il soit compatible avec les deux opérations de nos anneaux. La notion d'homomorphisme d'anneau sera donc la suivante :

Definition 6.3.1. Si R_1 et R_2 sont des anneaux, alors un homomorphisme ϕ est une fonction $\phi : R_1 \to R_2$ qui satisfait les deux propriétés suivantes :

1. $\phi(a+b) = \phi(a) + \phi(b), \quad \forall a, b \in R_1$.
2. $\phi(ab) = \phi(a)\phi(b), \quad \forall a, b \in R_1$.

Il faut faire attention ici à ne pas confondre les homomorphismes de groupe et les homomorphismes d'anneaux qui ne sont pas définie exactement de la même manière. Normalement, le contexte nous permet cependant de déterminer lequel des deux nous intéresse. À partir de cette définition, nous pouvons maintenant définir les notions de monomorphisme, d'épimorphisme et d'isomorphisme comme étant des homomorphisme injectif, surjectif et bijectif respectivement. , La notion d'isomorphisme d'anneau est la plus importante des trois et mérite d'être définie formellement.

Definition 6.3.2. Un ismomorphisme ϕ entre des anneaux R_1 et R_2 est un homomorphisme $\phi : R_1 \to R_2$ qui est bijectif. De plus, on dit que des anneaux R_1 et R_2 sont isomorphique s'il existe une isomorphisme entre R_1 et R_2.

Comme dans le cas des groupes, la notion d'isomorphisme d'anneau signifie que deux anneaux sont en tout point identique dans le contexte de la théorie des anneaux.

Definition 6.3.3. Si R_1 et R_2 sont des anneaux, et $\phi : R_1 \to R_2$ un homomorphisme, alors on définit le noyau de ϕ comme étant l'ensemble :

$$\ker(\phi) = \{x \in R_1 : \phi(x) = 0\}$$

Théorème 6.3.1. Si R_1 et R_2 sont des anneaux et $\phi : R_1 \to R_2$ un homomorphisme, alors :

1. Pour tout $r \in R$ et $x \in \ker(\phi)$ on a $rx \in \ker(\phi)$.
2. Pour tout $r \in R$ et $x \in \ker(\phi)$ on a $xr \in \ker(\phi)$.

Démonstration. Nous allons démontrer seulement la première partie, la seconde étant pratiquement identique. Supposons que $r \in R$ et $x \in \ker(\phi)$, alors on a :

$$\phi(rx) = \phi(r)\phi(x) = \phi(r)\ 0 = 0$$

Ce qui signifie que $rx \in \ker(\phi)$. □

Notez que nous avions trouvé une propriété semblable dans le contexte de la théorie des groupes, ce qui nous avait amener à définir le concept de groupe normal, puis nous a permis de développer la théorie des groupes quotient. Le même principe s'applique dans le contexte des anneaux. Le théorème précédent nous amène à définir les trois concept suivant :

Definition 6.3.4. Si R est un anneau et I un sous-groupe de R, alors on dit que :

1. I est un idéal à gauche de R si $rI \subseteq I$ pour tout $r \in R$.
2. I est un idéal à droite de R si $Ir \subseteq I$ pour tout $r \in R$.
3. I est un idéal s'il s'agit d'un idéal à gauche et d'un idéal à droite.

Rappelons que dans notre définition les ensembles rI et Ir sont définies comme étant :

$$rI = \{rx : x \in I\} \quad \text{et} \quad Ir = \{xr : x \in I\}$$

Dans le cas où l'anneau R en question est commutatif, il est facile de voir que ces trois notions coïncident et ce sera le sujet principal du chapitre suivant.

Chapitre 7

Les idéaux et les anneaux quotients

7.1 Les idéaux

Dans le chapitre précédent, nous avons introduit le concept d'idéal pour un anneau quelconque. Remarquer qu'il avait alors été nécessaire de faire la distinction entre les idéaux à gauches, les idéaux à droites et les idéaux bilatères. Dans ce chapitre, nous voulons continuer notre étude, mais cette fois en ce concentrant uniquement sur les anneaux commutatif qui sont plus facile à étudier. Rappelons donc la définition d'un idéal.

Definition 7.1.1. Si $(R, +, \times)$ est un anneau commutatif et $I \subseteq R$, alors on dit que I est un idéal de R si les deux propriétés suivantes sont satisfaites :

1. $(I, +)$ est un sous-groupe de $(R, +)$.
2. Pour tout $x \in I$ et $r \in R$ on a $rx \in I$.

Remarquez qu'ici il n'est pas nécessaire de faire la distinction entre idéal à gauche et à droite, car ces deux notions coïncide pour les anneaux commutatif.

Théorème 7.1.1. Si R est un anneau commutatif, et I_1, I_2 des idéaux de R, alors :

1. $I_1 \cap I_2$ est un idéal de R.
2. $I_1 + I_2$ est un idéal de R.

Démonstration.

1. Exercice
2. Supposons que I_1 et I_2 sont des idéaux de R. On veut commencer par montrer que la somme forme un sous groupe abélien de R. Pour ce faire, prenons $x, y \in I_1 + I_2$, alors $x = x_1 + x_2$ et $y = y_1 + y_2$ où $x_1, y_1 \in I_1$ et $x_2, y_2 \in I_2$. On veut montrer que $x + (-y)$ est aussi dans $I_1 + I_2$. On a donc :

$$x + (-y) = (x_1 + x_2) + (-y_1 - y_2) = (x_1 + (-y_1)) + (x_2 + (-y_2)) \in I_1 + I_2$$

Il s'agit donc bien d'un sous-groupe abélien de R. Il ne nous reste plus qu'à démontrer que $x(I_1 + I_2) \in (I_1 + I_2)$ pour tout $x \in R$. Pour ce faire, prenons $z_1 \in I_1$ et $z_2 \in I_2$, alors :

$$x(z_1 + z_2) = xz_1 + xz_2 \in I_1 + I_2$$

On peut donc conclure que $I_1 + I_2$ est bien un idéal de R.

□

Théorème 7.1.2. Si R est un anneau commutatif, et A est un sous-ensemble de R, alors il existe un plus petit idéal I de R qui contient l'ensemble A. De plus, cet idéal est donné par :

$$I = \bigcap_{\substack{A \subseteq J \subseteq R \\ J \text{ idéal}}} J$$

On dénote habituellement cet idéal par $I = \langle A \rangle$.

Démonstration. Il s'agit d'une conséquence du théorème précédent. Si on pose I comme étant l'intersection de tout les idéaux qui contiennent A, alors nécessairement I est aussi un idéal. De plus, il ne peut pas exister d'autre idéal plus petit qui contiennent A, car cet idéal ferait aussi partie de l'intersection. □

Théorème 7.1.3. Si R est un anneau commutatif, et I_1, I_2 des idéaux de R, alors on a l'égalité suivante :

$$\langle I_1 \cup I_2 \rangle = I_1 + I_2$$

Démonstration. Il s'agit de montrer que si K est un idéal qui contient $I_1 \cup I_2$, alors $I_1 + I_2 \subseteq K$. Pour ce faire, remarquons premièrement que $I_1 \subseteq I_1 \cup I_2$ et $I_2 \subseteq I_1 \cup I_2$. Maintenant, prenons $x \in I_1$ et $y \in I_2$. On a donc en particulier que $x, y \in I_1 \cup I_2$. Par définition d'un idéal, on doit donc avoir $x + y \in \langle I_1 \cup I_2 \rangle$. On a donc $I_1 + I_2 \subseteq \langle I_1 \cup I_2 \rangle$. Comme d'un autre côté on a $I_1 \cup I_2 \subseteq I_1 + I_2$, on peut donc conclure que $\langle I_1 \cup I_2 \rangle = I_1 + I_2$. □

Théorème 7.1.4. Un anneau commutatif R est un corps si et seulement si les seuls idéaux de R sont $\{0\}$ et lui même.

Démonstration. Dans un premier temps, supposons que R est un corps et prenons $I \subseteq R$ un idéal de R. Supposons que $I = \{0\}$, donc il existe au moins un $a \in I$ tel que $a \neq 0$. Maintenant, remarquons que $1 = a^{-1}a = a^{-1}I \subseteq I$, où la dernière inclusion vient de la définition d'un idéal. Maintenant, si on prend $x \in R$, alors $x = x1 \in xI \subseteq I$. Comme le x est un élément quelconque de R, on obtient que $I = R$, et donc les seuls idéaux de R sont $\{0\}$ et R.

Mainenant, pour l'autre direction, supposons que R est un anneau commutatif pour lequel les seuls idéaux sont $\{0\}$ et R. Prenons $a \in R$, tel que $a \neq 0$. Il est facile de voir que $I = aR$ est un idéal. Par hypothèse, comme $I \neq \{0\}$, on doit avoir $I = R$. En particulier, il doit exister un $b \in R$ tel que $ab = 1$. L'élément a est donc inversible, et $a^{-1} = b$. Tout les éléments non nul de R sont donc inversible. □

7.2 Les anneaux quotients

Nous voulons maintenant introduire une relation d'équivalence sur nos anneaux de manière similaire à ce que nous avons fait à l'aide des groupes normaux pour introduire la notion de groupe quotient. Par définition, un idéal I est en particulier un groupe abélien. Dans si on suppose notre anneau R commutatif, alors un idéal sera un sous-groupe normal. Nous allons donc procéder de manière très similaire à ce que nous avons fait pour les groupes.

Supposons donc que R est un anneau commutatif et I un idéal de R. Si $x, y \in R$, alors on dit que $x \sim y$ si et seulement si il existe $i \in I$ tel que $x + i = y$. Il est facile de montrer qu'il s'agit d'un relation d'équivalence, on est donc amené à définir la classe d'équivalence de x comme étant $\overline{x} = \{x + i : i \in I\}$, et finalement on définit

l'ensemble R/I comme étant l'ensemble des classes d'équivalence de $\sim$. Il nous faut maintenant introduire un addition et une multiplication sur cette ensemble. On définit donc :

$$\overline{x} + \overline{y} = (x + I) + (y + I) = (x + y) + I$$

$$\overline{x}\ \overline{y} = (x + I)(y + I) = xy + I$$

Il nous faut maintenant montrer qu'il s'agit bien d'un anneau. C'est ce que nous allons faire dans le théorème ci-dessous.

Théorème 7.2.1. Si R est un anneau commutatif, et I un idéal de R, alors l'ensemble $\{r + I : r \in R\}$ forme un anneau lorsque les opérations sont définie par :

1. $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$
2. $(r_1 + I)(r_2 + I) = r_1 r_2 + I$

Démonstration. Comme R est un anneau, il s'agit en particulier d'un groupe commutatif, et I est en particulier un sous-groupe normale. On remarque donc en particulier que l'addition est bien définie et R/I est un groupe commutatif. Nous allons donc nous concentrer sur la multiplication. Commençons par démontrer qu'elle est bien définie. Pour ce faire, remarquons que :

$$(r_1 + I)(r_2 + I) = r_1 r_2 + r_1 I + I r_2 + I^2 \subseteq r_1 r_2 + I$$

ou l'inclusion vient de la définition d'un idéal bilatère. Maintenant, nous voulons montrer que cet opération est associative.

$$[(r_1+I)(r_2+I)](r_3+I) = (r_1 r_2+I)(r_3+I) = (r_1 r_2)r_3+I = r_1(r_2 r_3)+I = (r_1+I)(r_2 r_3+I) = (r_1+I)[(r_2+I)(r_3+I)]$$

L'opération est donc bien associative. Nous allons maintenant montrer qu'elle est commutative.

$$(r_1 + I)(r_2 + I) = r_1 r_2 + I = r_2 r_1 + I = (r_2 + I)(r_1 + I)$$

Finalement, il ne nous reste plus qu'à démontrer la distributivité.

$$(r_1 + I)[(r_2 + I) + (r_3 + I)] = (r_1 + I)((r_2 + r_3) + I) = r_1(r_2 + r_3) + I = (r_1 r_2 + r_1 r_3) + I = (r_1 r_2 + I) + (r_1 r_3 + I)$$

On peut donc conclure qu'il s'agit bien d'un anneau commutatif. □

Definition 7.2.1. Si R est un anneau commutatif et I un idéal de R, alors on définit l'anneau quotient R/I comme étant l'anneau décrit dans le théorème précédent.

Exemple 7.2.1. Nous avons déjà remarquer que pour tout entier positif n, on a que $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$. Nous allons donc chercher à démontrer que comme dans le cas des groupes, nous avons que l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ est isomorphique à $\mathbb{Z}_n$. Pour ce faire, définissons la fonction :

$$\phi : {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \to \mathbb{Z}_n$$

$$\phi(k + n\mathbb{Z}) = k$$

Nous allons premièrement montrer que cette fonction est bien définie. Pour ce faire, remarquons que $k_1 + n\mathbb{Z} = k_2 + n\mathbb{Z}$ si et seulement si il existe des entiers s_1, s_2 tel que $k_1 + ns_1 = k_2 + ns_2$, ce qui est le cas si et seulement si $k_1 - k_2 = n(s_2 - s_1)$ ce qui est vrai si et seulement si $n|(k_1 - k_2)$, c'est à dire si $k_1 = k_2$ dans $\mathbb{Z}_n$. On a donc que si $k_1 + n\mathbb{Z} = k_2 + n\mathbb{Z}$, alors :

$$\phi(k_1 + n\mathbb{Z}) = k_1 = k_2 = \phi(k_2 + n\mathbb{Z})$$

La fonction est donc bien définie. Maintenant, nous allons montrer qu'il s'agit bien d'un homomorphisme :

$$\phi((k_1 + n\mathbb{Z}) + (k_2 + n\mathbb{Z})) = \phi(k_1 + k_2 + n\mathbb{Z}) = k_1 + k_2 = \phi(k_1 + n\mathbb{Z}) + \phi(k_2 + n\mathbb{Z})$$

$$\phi((k_1+n\mathbb{Z})(k_2+n\mathbb{Z}) = \phi(k_1k_2+n\mathbb{Z}) = k_1k_2 = \phi(k_1+n\mathbb{Z})\phi(k_2+n\mathbb{Z})$$

Il s'agit donc bien d'un homomorphisme. Il nous faut maintenant montrer qu'il est bijectif. La surjectivité étant évidente, nous allons seulement montrer l'injectivité. On a donc :

$$\phi(k_1+n\mathbb{Z}) = \phi(k_2+n\mathbb{Z}) \quad \Rightarrow \quad k_1 = k_2 \text{ dans } \mathbb{Z}_n \quad \Rightarrow \quad n|(k_1-k_2) \quad \Rightarrow \quad k_1 = k_2+ns \quad \Rightarrow \quad k_1+n\mathbb{Z} = k_2+n\mathbb{Z}$$

Il s'agit donc bien d'un isomorphisme.

Exemple 7.2.2. Les anneaux $\mathbb{Q}[x]/\langle x^2-2\rangle$ et $\mathbb{Q}(\sqrt{2})$ sont isomorphiques. Pour le voir, notez que les éléments de l'anneau $\mathbb{Q}[x]/\langle x^2-2\rangle$ sont de la forme $ax+b+\langle x^2-2\rangle$ avec $a,b \in \mathbb{Q}$. La fonction suivante est donc bien définie :

$$\phi : \mathbb{Q}[x]/\langle x^2-2\rangle \to \mathbb{Q}(\sqrt{2})$$

$$\phi(ax+b+\langle x^2-2\rangle) = a\sqrt{2}+b$$

Il nous faut montrer qu'il s'agit bien d'un homomorphisme. Pour ce faire, remarquons que si $(a_1x+b_1+\langle x^2-2\rangle)$ et $(a_2x+b_2+\langle x^2-2\rangle)$ sont dans $\mathbb{Q}[x]/\langle x^2-1\rangle$, alors on a :

$$\begin{aligned}
\phi((a_1x+b_1+\langle x^2-2\rangle)+(a_2x+b_2+\langle x^2-2\rangle)) &= \phi((a_1+a_2)x+(b_1+b_2)+\langle x^2-2\rangle) \\
&= (a_1+a_2)\sqrt{2}+(b_1+b_2) \\
&= (a_1\sqrt{2}+b_1)+(a_2\sqrt{2}+b_2) \\
&= \phi(a_1x+b_1)+\phi(a_2x+b_2)
\end{aligned}$$

$$\begin{aligned}
\phi((a_1x+b_1+\langle x^2-2\rangle)(a_2x+b_2+\langle x^2-2\rangle)) &= \phi((a_1a_2)x^2+(a_1b_2+a_2b_1)x+(b_1b_2)+\langle x^2-2\rangle) \\
&= \phi((a_1b_2+a_2b_1)x+(b_1b_2+2a_1a_2)+\langle x^2-2\rangle) \\
&= (a_1b_2+a_2b_1)\sqrt{2}+(b_1b_2+2a_1a_2) \\
&= a_1a_2(\sqrt{2})^2+a_1b_2\sqrt{2}+a_2b_1\sqrt{2}+b_1b_2 \\
&= (a_1\sqrt{2}+b_1)(a_2\sqrt{2}+b_2) \\
&= \phi(a_1x+b_1)\phi(a_2x+b_2)
\end{aligned}$$

Il s'agit donc bien d'un homomorphisme. De plus, l'injectivité et la surjectivité de ϕ sont facile à observer. Il s'agit donc d'un isomorphisme. Les anneaux $\mathbb{Q}[\sqrt{2}]/\langle x^2-2\rangle$ et $\mathbb{Q}(\sqrt{2})$ sont donc isomorphiques.

7.3 Les idéaux maximaux, premiers et principaux

Definition 7.3.1. Si R est un anneau commutatif et I un idéal de R, alors on définit les termes suivant :

1. I est maximal si les seuls idéaux contenant I sont I et R.
2. I est premier si pour tout $a,b \in R$ tel que $ab \in I$, alors a ou b est dans I.
3. I est principal si $I = \langle a\rangle$ pour un $a \in R$.

Théorème 7.3.1. Si R est un anneau commutatif, alors I est un idéal maximal si et seulement si R/I est un corps.

Démonstration. Supposons premièrement que I est un idéal maximal, et prenons $a+I \in R/I$ avec $a+I \neq 0+I$. Posons $J = \{x+ay : x \in I, y \in R\}$. Il n'est pas très difficile de montrer que J est un idéal, $I \subseteq J$ et $a \in J$.

Comme l'idéal I est maximal, on doit donc avoir $J = R$. Il existe donc $x_1 \in I$ et $y_1 \in R$ tel que $x_1 + ay_1 = 1$. Ceci nous permet donc d'obtenir :

$$(a + I)(y_1 + I) = ay_1 + I = (1 - x_1) + I = 1 + I$$

Ce qui signifie que $a + I$ est inversible dans R/I. Comme l'élément $a + I$ était n'importe quel élément non nul, on peut donc conclure que R/I est un corps.

Pour l'autre direction, supposons maintenant que R/I est un corps, et prenons J un idéal de R tel que $I \subset J$, $I \neq J$. Si on prend $a \in J \backslash I$, alors $a + I$ est inversible dans R/I. Il existe donc un élément $b + I$ tel que : $(a + I)(b + I) = 1 + I$, et donc $ab + I = 1 + I$. Il existe donc un élément $c \in I$ tel que $ab + c = 1$. Comme $ab \in J$, on obtient donc que $1 \in J$, ce qui signifie que $J = R$. On peut donc conclure que I est un idéal maximal. □

Théorème 7.3.2. Si R est un anneau commutatif, alors I est un idéal premier si et seulement si R/I est un domaine intègre.

Démonstration. Supposons que I est un idéal premier, et supposons que $(a + I), (b + I) \in R/I$ sont tel que $(a + I)(b + I) = 0 + I$. On a donc :

$$(a + I)(b + I) = ab + I = I$$

Comme I est un idéal, il s'agit en particulier d'un sous-groupe. On doit donc avoir $ab \in I$. Comme il s'agit d'un idéal premier, on doit donc avoir $a \in I$ ou $b \in I$, ce qui signifie que $a + I = I$ ou $b + I = I$. R/I est donc un domaine intègre. Maintenant, pour l'autre direction, supposons que R/I est un domaine intègre. Prenons $a, b \in R$ tel que $ab \in I$. On a donc :

$$(a + I)(b + I) = ab + I = I$$

Comme il s'agit d'un domaine intègre, on doit donc avoir $a + I = I$ ou $b + I = I$. Finalement, comme I est un idéal, il s'agit en particulier d'un sous-groupe, ce qui signifie que $a \in I$ ou $b \in I$. Il s'agit donc d'un idéal premier. □

Théorème 7.3.3. Si R est un anneau commutatif et I un idéal maximal, alors I est un idéal premier.

Démonstration. Il s'agit d'une application des deux théorèmes précédent. Supposons que R est un anneau commutatif et I un idéal maximal de R. On doit donc avoir R/I est un corps. Maintenant, comme tout les corps sont en particulier des domaines intègres, on doit donc avoir que R/I est un domaine intègre, ce qui nous permet finalement d'affirmer que I est un idéal premier. □

Les idéaux premiers sont en quelques sortes une généralisation des nombres premiers. Dans $\mathbb{Z}$, le lemme d'Euclide nous affirme que si $a, b, p \in \mathbb{Z}$ sont tel que p est premier et $p|ab$, alors $p|a$ ou $p|b$. La même idée s'applique aussi pour les idéaux premiers comme le montre l'exemple suivant :

Exemple 7.3.1. Dans l'anneau des entiers $(\mathbb{Z}, +, \times)$, tous les idéaux sont principaux, c'est à dire qu'ils ont la forme $n\mathbb{Z}$ pour un $n \in \mathbb{Z}$. Ceci est facile à voir car un idéal de $(\mathbb{Z}, +, \times)$ doit en particulier être un sous-groupe de $(\mathbb{Z}, +)$. Comme les seuls sous-groupes de $(\mathbb{Z}, +)$ ont la forme $n\mathbb{Z}$, alors tous les idéaux de l'anneau des entiers doivent avoir cette même forme.

Exemple 7.3.2. Dans l'anneau des entiers $(\mathbb{Z}, +, \times)$, un idéal I est premier si et seulement si il existe un nombre premier p tel que $I = p\mathbb{Z}$. Pour le montrer, supposons premièrement que I est un idéal premier de l'anneau de entier, alors il existe un n tel que $I = n\mathbb{Z}$. Supposons que n n'est pas un nombre premier, alors il existe $1 < a, b < n$ tel que $n = ab$. On a donc que $ab \in I$, mais ni a ou b ne sont dans I, ce qui contredit le fait que I est un idéal premier. On conclut donc que n doit être un nombre premier. Maintenant pour l'autre direction, supposons que p est un nombre premier. On veut montrer que l'idéal $p\mathbb{Z}$ est un idéal premier. Pour

ce faire, supposons que $ab \in p\mathbb{Z}$. Il existe donc un entier k tel que $ab = pk$, ce qui signifie que $p|ab$. Comme p est un nombre premier, par le lemme d'Euclide on doit avoir $p|a$ ou $p|b$. Il doit donc exister un entier k' tel que $a = pk' \subseteq p\mathbb{Z}$ ou $b = pk' \subseteq p\mathbb{Z}$. L'idéal $p\mathbb{Z}$ est donc un idéal premier.

Exemple 7.3.3. Dans l'anneau $\mathbb{Q}[x]$, l'idéal $\langle x^2 - 1\rangle$ n'est pas permier car $(x-1)(x+1) = x^2 - 1$. On peut donc déduire que l'anneau $\mathbb{Q}[x]/\langle x^2 - 1\rangle$ n'est pas un domaine intègre. Par contre, toujours dans l'anneau $\mathbb{Q}[x]$ l'idéal $\langle x^2 - 2\rangle$ est premier. Ceci est facile à voir car nous avons déjà démontré que $\mathbb{Q}[x]/\langle x^2 - 2\rangle \cong \mathbb{Q}(\sqrt{2})$ et ce dernier est un corps (donc en particulier un domaine intègre).

Definition 7.3.2. Un anneau R est un domaine d'idéaux principaux si R est un domaine intègre et si tout les idéaux de R sont principaux.

Théorème 7.3.4. Un anneau R est un corps si et seulement si $R[x]$ est un domaine d'idéaux principaux.

7.4 La caractéristique

Definition 7.4.1. Si R est un anneau, alors on définit la caractéristique de R comme étant le plus petit entier $n > 0$ (s'il existe) tel que $nx = 0$ pour tout $x \in R$. Si un tel entier n'existe pas, alors on dit que R est de caractéristique 0.

Exemple 7.4.1. La caractéristique des anneaux $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ est 0.

Exemple 7.4.2. Si $m \in \mathbb{N}$, alors la caractéristique de l'anneau $\mathbb{Z}_m$ est m.

Théorème 7.4.1. Si R est un anneau intègre, alors la caractéristique de R est soit 0 ou un nombre premier.

Démonstration. Supposons que R est un anneau intègre de caractéristique n avec $n = rs$ et $r, s \neq 1$. Par définition de la caractéristique, on a donc $0 = n \cdot 1$ ce qui nous donne :

$$0 = n \cdot 1 = (rs) \cdot 1 = r \cdot (s \cdot 1) = (r \cdot 1)(s \cdot 1)$$

Comme il s'agit d'un anneau intègre, on doit donc avoir soit $r \cdot 1$ ou $s \cdot 1$ qui est égal à 0, ce qui est une contradiction car $r, s < n$. En conséquence, si R est un anneau intègre, alors la caractéristique de R est soit 0 ou un nombre premier. □

Remarquez qu'une conséquence du théorème précédent est que l'anneau $\mathbb{Z}_m$ n'est pas intègre si m n'est pas un nombre premier. En particulier, $\mathbb{Z}_m$ n'est pas un corps si m n'est pas premier.

7.5 Le théorème du reste chinois

Le théorème du reste chinois, dans sa version d'origine, fait son apparition dans une enigme chinoise datant du 3e siècle. Il s'agit d'un problème de dénombrement, dans lequel une personne cherche à trouver le plus petit entier satisfaisant un ensemble de congruence modulo. Dans cette section, nous allons démontrer une généralisation à la théorie des anneaux qui revient à démontrer l'existence et l'unicité d'une solution au problème original, mais dans un contexte beaucoup plus général. Comme corollaire, nous allons pouvoir obtenir une démonstration de la formule pour calculer les valeurs de la fonction ϕ d'Euler que nous avons mentionné beaucoup plus tôt dans le cours.

Definition 7.5.1. Si R est un anneau commutatif et A et B des idéaux, alors A et B sont dit comaximal si $A + B = R$.

Exemple 7.5.1. Si m et n sont des entiers positifs tel que $(m, n) = 1$, alors les idéaux $m\mathbb{Z}$ et $n\mathbb{Z}$ sont comaximal dans l'anneau des entiers. Pour le voir, il s'agit d'appliquer le théorème de Bézout. Comme m, n sont copremier, il existe des entiers a, b tel que $am + bn = 1$. Donc si $z \in \mathbb{Z}$, alors $azm + bzm = z$. Maintenant, comme $azm \in m\mathbb{Z}$ et $bzn \in n\mathbb{Z}$, on obtient donc l'égalité $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$. Les deux idéaux sont donc comaximal.

Théorème 7.5.1. (Théorème du reste chinois) Si R est un anneau commutatif avec un identité et $I_1, I_2, ..., I_k$ des idéaux de R, alors l'application ci-dessous est un homomorphisme :

$$\phi : R \to R/I_1 \times R/I_2 \times ... \times R/I_k$$

$$\phi(r) = (r + I_1, r + I_2, ..., r + I_k)$$

Le noyau de cet homomorphisme est $I_1 \cap I_2 \cap ... \cap I_k = I_1 I_2 ... I_k$. De plus, si les idéaux sont deux à deux comaximal, alors l'homomorphisme est surjectif et on obtient isomorphisme suivant :

$$R/(I_1 I_2 ... I_k) = R/(I_1 \cap I_2 \cap ... \cap I_k) \cong R/I_1 \times R/I_2 \times ... \times R/I_k$$

Démonstration. La démonstration se fait par induction. Nous allons donc commencer par traiter le cas où $k = 2$. Le fait qu'il s'agit d'un homomorphisme et que son noyau est $I_1 \cap I_2$ n'est pas très difficile à voir. Nous allons donc dans un premier temps montrer que $I_1 \cap I_2 = I_1 I_2$, puis établir la surjectivité. Premièrement, par définition d'un idéal, on a $I_1 I_2 \subseteq I_1$ et $I_1 I_2 \subseteq I_2$. On a donc $I_1 I_2 \subseteq I_1 \cap I_2$. Pour l'autre inclusion, comme I_1 et I_2 sont comaximal, alors $I_1 + I_2 = R$. Il existe donc $x \in I_1$ et $y \in I_2$ tel que $x + y = 1$. Donc si $z \in I_1 \cap I_2$, alors :

$$\underbrace{xz}_{I_1 I_2} + \underbrace{yz}_{I_1 I_2} = z \in I_1 \cap I_2$$

Comme $I_1 I_2$ est un idéal de R, alors la somme $xz + yz$ est aussi dans $I_1 I_2$, c'est à dire $z \in I_1 I_2$. On a donc l'égalité $I_1 I_2 = I_1 \cap I_2$. Il nous faut maintenant établir la surjectivité. Pour ce faire, en prenant les mêmes x et y, on remarque que :

$$\phi(x) = (x + I_1, x + I_2) = (I_1, x + I_2) = (I_1, (1 - y) + I_2) = (I_1, 1 + I_2)$$

$$\phi(y) = (y + I_1, y + I_2) = (y + I_1, I_2) = ((1 - x) + I_1, I_2) = (1 + I_1, I_2)$$

Donc si on prend un élément quelconque de $R/I_1 \times R/I_2$, disons $(a + I_1, b + I_2)$, alors on a :

$$\begin{aligned} \phi(bx + ay) &= \phi(b)\phi(x) + \phi(a)\phi(y) = (b + I_1, b + I_2)(I_1, 1 + I_2) + (a + I_1, a + I_2)(1 + I_1, I_2) \\ &= (I_1, b + I_2) + (a + I_1, I_2) = (a + I_1, b + I_2) \end{aligned}$$

Par le premier théorème d'isomorphisme on a donc $R/(I_1 I_2) \cong R/I_1 \times R/I_2$. Par induction, on peut maintenant établie le résultat général, ce qui est laissé en exercice. □

Corollaire 7.5.1. Si n est un entier supérieur à 1 tel que $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, alors on a l'égalité suivante :

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Démonstration. Par l'exemple qui se trouve en début de section, nous savons que les idéaux $p_1^{\alpha_1}\mathbb{Z}, p_2^{\alpha_2}\mathbb{Z}, ..., p_k^{\alpha_k}\mathbb{Z}$ sont comaximal. Donc par le théorème du reste chinois, on obtient l'isomorphisme suivant :

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p_2^{\alpha_2}\mathbb{Z} \times ... \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$$

Ce dernier isomorphisme est un isomorphisme d'anneau, donc en particulier, si on considère seulement l'opération de multiplication, on obtient l'isomorphisme de groupe suivant :

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times ... \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times$$

Par définition, le groupe de gauche est d'ordre $\phi(n)$. Maintenant pour la partie de gauche, l'ordre du groupe produit est le produit de l'ordre de chacun des groupes. On obtient donc l'égalité :

$$\phi(n) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})...\phi(p_k^{\alpha_k})$$

Donc pour évaluer la valeur de $\phi(n)$, il est suffisant d'être capable d'évaluer la valeur de $\phi(p^\alpha)$ pour un nombre premier p. Comme tout les entiers positifs inférieur à p^α sont copremier avec lui à l'exception des multiple de p, on obtient facilement la formule :

$$\phi(p^\alpha) = p^\alpha - \frac{p^\alpha}{p} = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right)$$

Ce qui nous permet d'obtenir la formule désiré pour la valeur de ϕ. □

7.6 Corps des fractions

Nous voulons maintenant montrer que tout les anneaux intègre peuvent être étendu pour former un corps. C'est ce qu'on appelle le corps des fractions. Il s'agit essentiellement du même processus qui peut être fait pour passer des entiers $\mathbb{Z}$ pour obtenir les nombres rationnels $\mathbb{Q}$.

Théorème 7.6.1. Si R est un anneau intègre, alors R est isomorphique à un sous-anneau d'un corps.

Démonstration. Si R est un anneau intègre, alors on considère l'ensemble $R \times R\backslash\{0\}$ sur lequel on définit la relation d'équivalence suivante :

$$(a,b) \sim (c,d) \quad \Leftrightarrow \quad ad = bc$$

Puis on définit l'ensemble $F = (R \times R\backslash\{0\})/\sim$. On doit maintenant définir un addition et une multiplication sur l'ensemble F :

$$(a,b) + (c,d) = (ad + bc, bd) \quad \text{et} \quad (a,b) \times (c,d) = (ac, bd)$$

Avec ces opérations, en utilisant le fait que R est un anneau intègre, il est facile de montrer que F est un corps. Considérons maintenant l'homomorphisme suivant :

$$\phi : R \to F$$

$$\phi(x) = (x, 1)$$

On veut montrer que cet homomorphisme est injectif. Supposons que $\phi(x) = \phi(y)$, alors $(x,1) \sim (y,1)$, ce qui signifie que $x = y$. Ce qui confirme l'injectivité. On peut donc conclure que R est isomorphique à un sous-anneau du corps F. Plus précisément, R est isomorphique à $Im(\phi)$. □

Maintenant que nous avons établie l'existence du corps de fractions, il est plus pratique de changer notre notation. À la place d'écrire (a,b) il est plus commun d'écrire $\frac{a}{b}$. Dans ce cas, les opérations que nous avons définie plus haut correspondent aux opérations habituelles sur les fractions. Notez cependant qu'une fraction est habituellement regardé comme un entier sur un entier, alors qu'ici nous avons définie une fraction de manière beaucoup plus générale comme étant un élément d'un anneau, sur un élément (non nul) du même anneau.

Bibliographie

[1] Ibrahim Assem and Pierre Yves Leduc. *Cours d'algèbre : Groupes, anneaux, modules et corps.* Presse internationnales Polytechnique, 2009.

[2] David S. Dummit and Richard M. Foote. *Abstract algebra.* John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[3] Nathan Jacobson. *Basic algebra. I.* W. H. Freeman and Company, New York, second edition, 1985.

[4] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, third edition, 2002.

[5] Javad Mashreghi. *Structures algébriques.* Loze-Dion éditeur, 2014.

Index