Université de Rennes
Mathématiques
L3 Maths, parcours MI

Groupes et actions de groupes

Version en construction et non relue du 9 décembre 2025

Ce document, encore en phase de construction, est une introduction à l'étude des groupes et des actions de groupes.

Programme

Groupes, sous-groupes : définitions et exemples : $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Z}/n\mathbf{Z}$ (approche constructive), $\mathbf{K}^*$ ($\mathbf{K}$ corps), groupes des permutations (définition), $\mathbf{GL}_n$ (définition), Groupe diédral. Sous-groupes de $\mathbf{Z}$, sous-groupes fermés de $\mathbf{R}$, exemples de sous-groupes de $\mathbf{GL}_n$. Groupe produit (direct).
Morphismes, noyau, image. Théorème de Lagrange.
Rappels sur les relations d'équivalence et quotients d'ensembles.
Sous-groupes normaux, quotients dont propriété universelle et théorème d'isomorphisme. Sous-groupes d'indice 2.
Exemples. Groupes cyclique, théorème chinois. Groupes des permutations (étude détaillée), théorème de Cayley.
Actions de groupes, orbites, stabilisateurs, points fixes. Exemples. Formules des classes, théorème de Cauchy. Exemples d'application à la théorie des groupes, à l'algèbre linéaire et à la géométrie.

Bibliographie

• J. Calais, Éléments de théorie des groupes, PUF, 2014
• J. Deserti, Groupes et géométrie (cours et exercices)
• E. Ramis, C. Deschamps, J. Odoux, Cours de mathématiques spéciales, Masson, 1981
• F. Ulmer, Théorie des groupes, Ellipses, 2021
• Wikipedia

1 Lois, magmas

Définition 1 Soit E et F deux ensembles. Une application de $F \times E$ dans E est appelée loi de composition sur E (ou loi). Si $E = F$ il s'agit d'une loi de composition interne sur E (ou loi interne). Si $E \neq F$ il s'agit d'une loi de composition externe sur E à scalaires dans F (ou loi externe).

Exemples 1 L'addition et la multiplication dans $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$ sont des lois de composition internes. Il en est de même de l'addition dans l'ensemble des applications d'un ensemble X à valeurs dans un de ces ensemble de nombres. Si X est un ensemble alors la composition interne des applications de X dans X est une loi de composition sur l'ensemble $E = X^X$ des applications de X dans X. La somme de matrices (m,n) à m lignes et n colonnes à coefficients dans $\mathbf{R}$ (dans $\mathbf{Z}$, dans $\mathbf{Q}$, dans $\mathbf{C}$ ou plus généralement dans un anneau ou un corps) est une loi de composition interne sur cet ensemble. Le

produit de matrices carrées (n,n) à coefficients dans $\mathbf{R}$ (dans $\mathbf{Z}$, dans $\mathbf{Q}$, dans $\mathbf{C}$ ou plus généralement dans un anneau ou un corps) est une loi de composition interne sur cet ensemble. En revanche, si E est un $\mathbf{R}$-espace vectoriel (un $\mathbf{Q}$-espace vectoriel, un $\mathbf{C}$-espace vectoriel) la multiplication par un réel n'est pas une loi de composition interne mais une loi de composition externe.

Définition 2 Un magma est un couple $(E,\top)$ formé d'un ensemble et d'une loi de composition interne sur cet ensemble. On dit aussi que l'ensemble E est muni de la loi $\top$.

Exemples 2 Les couples $(\{0\},+)$, $(\mathbf{N},+)$, $(\mathbf{Z},+)$, $(\mathbf{Q},+)$, $(\mathbf{R},+)$ ou $(\mathbf{C},+)$ sont des magmas. Si $(E,\top)$ est un magma et X un ensemble alors $(X^E,\top')$ est un magma si la loi $\top'$ dans est définie par $(f\top' g)(x) = f(x)\top g(x)$ si $f,g \in X^E$ et $x \in X$. L'ensemble M_{mn} des matrices à m lignes et n colonnes à coefficients dans un de ces ensembles de nombres (ou plus généralement dans un magma $(E,\top)$) muni de la loi addition de matrices ainsi que l'ensemble M_n des matrices carrées (n,n) à coefficients dans un de ces ensembles de nombres (ou plus généralement dans un magma $(E,\top)$) et muni de la loi produit de matrices sont des magmas. Les couples $(\{0\},\times)$, $(\{1\},\times)$, $(\{-1,1\},\times)$, $(\mathbf{N},\times)$, $(\mathbf{Z},\times)$, $(\mathbf{Q},\times)$, $(\mathbf{R},\times)$ ou $(\mathbf{C},\times)$ sont des magmas. Le couple $(\mathbf{U},\times)$ où $\mathbf{U}$ désigne le cercle des complexes de module 1 est un magma. Le couple $(X^X,\circ)$ des applications d'un ensemble X dans lui même muni de la loi de composition des applications est un magma. Si $\lambda \in [1,+\infty)$ alors le couple $([\lambda,+\infty),\times)$ est un magma. Le couple $(\{2^n, n \in \mathbf{N}\},\times)$ est un magma.

Remarque 1 Si $(E,\top)$ est un magma et si $a \in E$ et $b \in E$ alors on note indifféremment $a\top b$ ou ab l'image $\top(a,b)$ du couple (a,b) par $\top$.

Définitions 3 Soit $(E,\top)$ et $(F,\perp)$ deux magmas. Une application $f : E \to F$ est un morphisme (de magmas) si pour tout $a \in E$ et tout $b \in E$ on a $f(a\top b) = f(a)\perp f(b)$. C'est un endomorphisme si $E = F$. C'est un isomorphisme si elle est bijective, un épimorphisme si elle est surjective, un monomorphisme si elle est injective. C'est un automorphisme si c'est à la fois un endomorphisme et un isomorphisme. L'application qui à $z \in \mathbf{C}$ associe $z^2 \in \mathbf{C}$ n'est pas un endomorphisme du magma $(\mathbf{C},+)$ ni du magma $(\mathbf{C},\times)$. En revanche l'application qui à $z \in \mathbf{C}$ de module 1 associe z^2 également de module 1 est un endomorphisme du magma $(\mathbf{U},\times)$.

Exemples 3 L'application qui à $n \in \mathbf{N}$ associe $2n$ est un endomorphisme de $(\mathbf{N},+)$ mais pas un automorphisme. L'application qui à $(x,y) \in \mathbf{R}^2$ associe $z = x+iy \in \mathbf{C}$ est un isomorphisme de $(\mathbf{R}^2,+)$ dans $(\mathbf{C},+)$. L'application qui à $n \in \mathbf{N}$ associe 2^n est un morphisme de $(\mathbf{N},+)$ dans $(\mathbf{N},\times)$ mais pas un isomorphisme.

Définition 4 Soit $(E,\top)$ un magma. La loi de composition interne $\top$ est dite associative si, pour tout $(a,b,c) \in E^3$, $a(bc) = (ab)c$. Le magma $(E,\top)$ est alors dit associatif.

Remarque 2 Les parenthèses ne sont pas nécessaires dans un magma associatif. Si $(E,\top)$ est un magma associatif $a(bc) = (ab)c$ s'écrit abc et de façon plus générale l'écriture $a_1 \cdots a_n$ n'est pas ambiguë.

Définition 5 Soit $(E,\top)$ un magma associatif. Si $a \in E$ on définit par récurrence sur $n \in \mathbf{N}^*$ a^n de la façon suivante : $a^1 = a$ et si $n \in \mathbf{N}^*$ alors $a^{n+1} = a(a^n)$.

Proposition 1 Soit $(E,\top)$ un magma associatif. Si $a \in E$ et $n \in \mathbf{N}^*$ alors $a^{n+1} = (a^n)a$.

Proposition 2 Soit $(E,\top)$ un magma associatif. Si $a \in E$ et $(n,m) \in \mathbf{N}^* \times \mathbf{N}^*$ alors $a^{m+n} = a^m a^n$ et $(a^m)^n = a^{mn}$.

Définition 6 Soit $(E,\top)$ un magma. Un élément neutre est un élément $e \in E$ tel que, pour tout $a \in E$,

$ea = ae = a$.

Remarque 3 Un magma $(E, \top)$ possède au plus un neutre.

Remarque 4 Si $(E, \top)$ est un magma associatif possédant un élément neutre e alors pour tout $a \in E$ il existe au plus un élément $b \in E$ qui est inverse de a pour $\top$. Lorsqu'il existe, l'unique inverse d'un élément a de E est souvent noté a^{-1}.

Définition 7 Si $(E, \top)$ est un magma associatif qui admet un élément neutre e alors on pose $a^0 = e$ quel que soit $a \in E$.

Proposition 3 Soit $(E, \top)$ un magma associatif qui possède un élément neutre e. Si $a \in E$ et $(n, m) \in \mathbf{N}^2$ alors $a^{m+n} = a^m a^n$ et $(a^m)^n = a^{mn}$.

Définition 8 Soit $(E, \top)$ un magma possédant un élément neutre e et $(a, b) \in E^2$. L'élément b est dit inverse de a si $ab = ba = e$.

Définition 9 Soit $(E, \top)$ un magma possédant un élément neutre e. Un élément $a \in E$ est dit inversible s'il existe un élément $b \in E$ qui est inverse de a.

Définition 10 Si $(E, \top)$ est un magma associatif qui admet un élément neutre e, si a est un élément inversible de E et si $n \in \mathbf{N}$ alors on pose $a^{-n} = (a^{-1})^n$.

Proposition 4 Soit $(E, \top)$ un magma associatif qui possède un élément neutre e. Si a est un élément inversible de E et $(n, m) \in \mathbf{Z}^2$ alors $a^{m+n} = a^m a^n$ et $(a^m)^n = a^{mn}$.

Définition 11 Soit $(E, \top)$ un magma associatif qui possède un élément neutre e et $a \in E$. S'il existe un plus petit entier naturel non nul n tel que $a^n = e$ cet entier est appelé ordre de a. Si $a^n \neq e$ quel que soit $n \in \mathbf{N}^*$ alors a est dit d'ordre infini.

Proposition 5 Soit $(E, \top)$ un magma associatif qui possède un élément neutre e, $a \in E$ et $n \in \mathbf{N}^*$. Si a est d'ordre n alors a est inversible d'inverse a^{n-1}.

Définition 12 Deux éléments a et b d'un magma $(E, \top)$ sont dits permutables si $ab = ba$ c'est à dire s'ils commutent, ce qui revient à dire que a commute avec g ou encore que g commute avec a.

Proposition 6 Si a et b sont deux éléments permutables d'un magma associatif et si $n \in \mathbf{N}^*$ alors $(ab)^n = a^n b^n$.

Définition 13 Soit $(E, \top)$ un magma. La loi de composition interne $\top$ est dite commutative si, pour tout $(a, b) \in E^3$, $ab = ba$, c'est à dire si les éléments sont deux à deux permutables. Le magma $(E, \top)$ est alors dit commutatif.

Exemples 4 Les couples $(\{0\}, +)$, $(\mathbf{N}, +)$, $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$ ou $(\mathbf{C}, +)$ sont des magmas associatifs et commutatifs. Si $(E, \top)$ est un magma (associatif, commutatif) et X un ensemble alors $(X^E, \top')$ est un magma (associatif, commutatif) si la loi $\top'$ dans est définie par $(f \top' g)(x) = f(x) \top g(x)$ si $f, g \in X^E$ et $x \in X$. L'ensemble M_{mn} des matrices à m lignes et n colonnes à coefficients dans un de ces ensembles de nombres muni (ou plus généralement dans un magma $(E, \top)$ associatif et commutatif) de la loi addition de matrices est un magma associatif et commutatif et l'ensemble M_n des matrices carrées (n, n) à coefficients dans un de ces ensembles de nombres (ou plus généralement dans un magma $(E, \top)$ associatif et commutatif) et muni de la loi produit de matrices est un magma associatif mais généralement non commutatif. Les couples $(\{0\}, \times)$, $(\{1\}, \times)$, $(\{-1, 1\}, \times)$, $(\mathbf{N}, \times)$, $(\mathbf{Z}, \times)$, $(\mathbf{Q}, \times)$, $(\mathbf{R}, \times)$ ou $(\mathbf{C}, \times)$ sont des magmas associatifs et commutatifs. Le couple $(X^X, \circ)$ des

applications d'un ensemble X dans lui même muni de la loi de composition des applications est un magma associatif et généralement non commutatif.

Remarque 5 Plusieurs notations sont couramment utilisées pour désigner une loi. Parmi les plus courantes il y a $\top$, $\perp$, $*$, $\circ$, $\cdot$ (notation multiplicative), . , $+$ (notation additive plutôt réservée aux lois commutatives).

Définition 14 Soit E un ensemble, $\top$ et $\perp$ deux lois sur E. La loi $\perp$ est dite distributive par rapport à la loi $\top$ si, pour tout $(a,b,c) \in E^3$, $a\perp(b\top c) = (a\perp b)\top(a\perp c)$ et $(a\top b)\perp c) = (a\perp c)\top(b\perp c)$.

Exemples 5 Si E est égal à $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$, la multiplication est distributive par rapport à l'addition. Si E est l'ensemble des matrices carrées (n,n) à coefficients dans un de ces ensembles de nombres (ou est un anneau) alors le produit de matrices est distributif par rapport à l'addition de matrices.

2 Groupes, sous-groupes : définitions et exemples

Définition 15 Un groupe est un magma associatif $(E,\top)$, possédant un élément neutre e et tel que tout élément $a \in E$ est inversible.

Remarque 6 Si $(E,\top)$ est un groupe alors E est non vide puisqu'il existe $e \in E$ l'unique élément neutre pour $\top$.

Exemples 6 Les magmas $(\{0\},+)$, $(\mathbf{Z},+)$, $(\mathbf{Q},+)$, $(\mathbf{R},+)$ ou $(\mathbf{C},+)$, l'ensemble $\mathbf{GL}_n(\mathbf{K})$ des matrices carrées (n,n) inversibles à coefficients dans $\mathbf{K} = \mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$ (ou plus généralement dans un anneau commutatif) muni de la loi produit de matrices, $(\mathcal{S}(X),\circ)$ où $\mathcal{S}(X)$ désigne l'ensemble des bijections d'un ensemble X dans lui-même, sont des groupes. Si $(E,\top)$ est un groupe et X un ensemble alors $(X^E,\top')$ est un groupe si la loi $\top'$ dans est définie par $(f\top' g)(x) = f(x)\top g(x)$ si $f,g \in X^E$ et $x \in X$. Le magma $(\mathbf{N},+)$, le magma $(X^X,\circ)$ où X est un ensemble qui contient au moins deux éléments ne sont pas des groupes. L'ensemble des matrices carrées (n,n) inversibles à coefficients dans $\mathbf{N}$ ou $\mathbf{Z}$ muni de la loi produit de matrices n'est pas un groupe mais l'ensemble des matrices carrées (n,n) inversibles à coefficients dans $\mathbf{Z}$, $\mathbf{Q}$ ou $\mathbf{R}$ et de déterminant dans $\{-1,1\}$ muni de la loi produit de matrices est un groupe. Les magmas $(\{0\},\times)$, $(\{1\},\times)$, $(\{-1,1\},\times)$, $(\mathbf{Q}^*,\times)$, $(\mathbf{R}^*,\times)$ ou $(\mathbf{C}^*,\times)$ sont des groupes. Les magmas $(\mathbf{Q},\times)$, $(\mathbf{R},\times)$ ou $(\mathbf{C},\times)$ ne sont pas des groupes.

Proposition 7 Soit $(E,\top)$ un magma associatif qui possède un élément neutre e et $a \in E$ un élément inversible. Alors le sous-ensemble $< a >= \{a^n \mid n \in \mathbf{Z}\}$ est stable par $\top$, ce qui signifie qu'il vérifie $\top(< a >) =< a >$, la loi $\top$ induit donc sur $< a >$ une loi $\top'$ et $(< a >,\top')$ est un groupe.

Définition 16 Soit $(E,\top)$ un groupe. S'il existe $a \in E$ tel que $E =< a >= \{a^n \mid n \in \mathbf{Z}\}$ le groupe $(E,\top)$ est dit monogène et a est appelé générateur du groupe.

Exemples 7 Le groupe $(\mathbf{Z},+)$ est monogène mais pas les groupes $(\mathbf{Q},+)$, $(\mathbf{R},+)$ ou $(\mathbf{C},+)$.

Définition 17 Un groupe $(E,\top)$ est dit cyclique s'il est monogène et fini.

Exemples 8 Les groupes $(\{0\},+)$ et $(\{-1,1\},\times)$ sont cycliques.

Proposition 8 L'ensemble $\{-1,1\}^2$ muni de la loi $\top$ définie par $(a,b)\top(c,d) = (a\times b, c\times d)$ est un groupe fini qui n'est pas cyclique.

Proposition 9 Si X est un ensemble à trois éléments le groupe $(\mathcal{S}(X),\circ)$ un groupe fini qui n'est pas

cyclique.

Proposition 10 Soit $n \in \mathbf{N}^*$ et E l'ensemble $E = \{0, ..., n-1\}$. L'application $\top$ qui à $(a,b) \in E$ associe $a \top b = a+b$ si $a+b < n$ et $a+b-n$ sinon est une loi de composition interne sur E et $(E, \top)$ est un groupe commutatif et cyclique.

Définition 18 Soit $(E, \top)$ un groupe. Le cardinal de E est appelé ordre de E et il est souvent noté $\text{ord}(E)$, $|E|$ ou $\#E$.

Proposition 11 Soit $(E, \top)$ un magma associatif qui possède un élément neutre e et $a \in E$ un élément d'ordre $n \in \mathbf{N}$ fini. Alors $(< a >, \top')$ où $\top'$ est la loi induite par $\top$ sur $< a >$ est un groupe d'ordre n.

Définition 19 Un groupe commutatif, dit aussi groupe abélien, est un groupe dont la loi de composition interne est commutative.

Exemples 9 Les groupes $(\{0\}, +)$, $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$ ou $(\mathbf{C}, +)$ sont commutatifs. Les groupes des matrices carrées (n,n) inversibles à coefficients dans $\mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$ muni de la loi produit de matrices, $(\mathcal{S}(X), \circ)$ où $\mathcal{S}(X)$ désigne l'ensemble des bijections d'un ensemble X dans lui-même avec X qui possède au moins trois éléments ne sont pas commutatifs. Les groupes $(\{0\}, \times)$, $(\{1\}, \times)$, $(\{-1, 1\}, \times)$, $(\mathbf{Q}^*, \times)$, $(\mathbf{R}^*, \times)$ ou $(\mathbf{C}^*, \times)$ sont commutatifs.

Proposition 12 Soit $(E, \top)$ un magma associatif qui possède un élément neutre e et $a \in E$ un élément inversible. Alors le groupe $(< a >, \top')$ où $\top'$ est la loi induite par $\top$ sur $< a >$ est un groupe commutatif.

Remarque 7 Dans la suite, quand on considérera un groupe, on ne nomme pas toujours la loi et on pourra se contenter de nommer seulement l'ensemble. Ainsi "Soit E un groupe" signifie "Soit $(E, \top)$ un groupe". Une loi de groupe est souvent notée $\top$, $\perp$, $*$, $\cdot$ (notation multiplicative), $.$, $+$ (notation additive réservée aux groupes abéliens).

Définition 20 Soit $(E, \top)$ un groupe. Un second groupe $(E', \top')$ est un sous-groupe de $(E, \top)$ si E' est un sous ensemble de E stable par $\top$, c'est à dire si $\top(E') \subset E' \subset E$ et si la loi $\top'$ est la loi induite par $\top$ sur E'. Un sous-groupe de G qui est différent de G est appelé sous-groupe propre de G.

Notation On note $E' \leq E$ le fait que E' soit un sous-groupe du groupe E et $E' < E$ le fait que E' soit un sous-groupe propre du groupe E.

Proposition 13 Soit $(E, \top)$ un groupe. Un sous-ensemble $E' \subset E$ est un sous-groupe de E si et seulement si E' est non vide, $\top(E') \subset E'$ et l'inverse a^{-1} de tout élément de E' est dans E'.

Remarque 8 La relation être un sous-groupe est une relation d'ordre. Ainsi si $(E, \top)$ est un groupe alors c'est un sous-groupe de lui même. Si $(E', \top')$ est un sous-groupe de $(E, \top)$ et $(E, \top)$ est un sous-groupe de $(E', \top')$ alors $(E, \top) = (E', \top')$. Enfin si $(E, \top)$, $(E', \top')$ et $(E'', \top'')$ sont trois groupes tels que $(E'', \top'')$ est un sous groupe de $(E', \top')$ et $(E', \top')$ est un sous-groupes de $(E, \top)$ alors $(E'', \top'')$ est un sous-groupe de $(E, \top)$.

Exemples 10 Le groupe $(\{0\}, +)$ est un sous-groupe des groupes $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$ et $(\mathbf{C}, +)$. Le groupe $(\mathbf{Z}, +)$ est un sous-groupe du groupe $(\mathbf{Q}, +)$. Le groupe des matrices carrées (n,n) à coefficients réels et de déterminant 1 muni de la loi produit de matrices est un sous-groupe du groupe des matrices carrées (n,n) à coefficients réels de déterminant non nul. Si $(E, \top)$ est un groupe et e son neutre alors $(\{e\}, \top)$ et $(E, \top)$ sont des sous-groupes de $(E, \top)$. Si $\lambda \in G$ avec $G = \mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$ alors $(\lambda G, +)$ est un sous-groupe de $(G, +)$.

Proposition 14 Les sous-groupes de $(\mathbf{Z},+)$ sont les groupes $(n\mathbf{Z},+)$ avec $n \in \mathbf{N}$.

Remarque 9 Plutôt que d'utiliser la lettre E pour désigner un groupe (i.e. un ensemble muni d'une loi qui lui donne une structure de groupe) on préfère souvent le noter G, G', H, H', K, K'.

Définition 21 Le centre $Z(G)$ d'un groupe G est l'ensemble des éléments de G qui commutent avec tous éléments de G : $Z(G) = \{a \in G \mid \forall g \in G,\ ag = ga\}$.

Proposition 15 Soit G un groupe. Son centre $Z(G)$ est un sous-groupe : $Z(G) \leq G$.

Proposition 16 Soit G un groupe et $(H_i)_{i\in I}$ une famille non vide de sous-groupes de G. Alors l'intersection $H = \bigcap_{i\in I} H_i$ est un sous-groupe de G.

Proposition 17 Soit $(G,+)$ un sous-groupe de $(\mathbf{R},+)$. Alors G est un sous-ensemble fermé de $\mathbf{R}$ si et seulement s'il existe $\lambda \in \mathbf{R}$ tel que $G = \lambda\mathbf{R}$.

Proposition 18 Soit $(G,+)$ un sous-groupe de $(\mathbf{R},+)$. Alors G n'est pas un sous-ensemble fermé de $\mathbf{R}$ si et seulement s'il existe deux réels non nuls λ et μ appartenant à G et de rapport λ/μ irrationnel.

Proposition 19 Soit $(G,+)$ un sous-groupe de $(\mathbf{R},+)$. Alors G n'est pas un sous-ensemble fermé de $\mathbf{R}$ si et seulement si G est un sous-ensemble dense de $\mathbf{R}$.

Définitions 22 Soit $A = (a_{ij})_{\substack{i\in\{1,\dots,n\}\\ j\in\{1,\dots,n\}}} \in M_n(\mathbf{R})$ une matrice carrée (n,n) à coefficients réels. La transposée de A est la matrice $A^{tr} = (a_{ji})_{\substack{i\in\{1,\dots,n\}\\ j\in\{1,\dots,n\}}} \in M_n(\mathbf{R})$. Les coefficient a_{ii} avec $i \in \{1,\dots,n\}$ sont les coefficients diagonaux de A. La matrice A est diagonale si tous les coefficients a_{ij} avec $i \neq j$ sont nuls. Elle est triangulaire supérieure si tous les coefficients a_{ij} avec $i > j$ sont nuls. Elle est triangulaire inférieure si tous les coefficients a_{ij} avec $i < j$ sont nuls. La matrice identité I_n est la matrice $I_n = (\delta_{ij})_{\substack{i\in\{1,\dots,n\}\\ j\in\{1,\dots,n\}}}$ telle que si $(i,j) \in \{1,\dots,n\}^2$ alors $\delta_{ij} = 0$ lorsque $i \neq j$ et $\delta_{ii} = 1$. La matrice $A = (a_{ij})_{\substack{i\in\{1,\dots,n\}\\ j\in\{1,\dots,n\}}} \in M_{mn}(\mathbf{R})$ est symétrique si $a_{ij}) = a_{ji}$ quel que soit $(i,j) \in \{1,\dots,n\}^2$. Elle est antisymétrique si $a_{ij}) = -a_{ji}$ quel que soit $(i,j) \in \{1,\dots,n\}^2$. La matrice $A = (a_{ij})_{\substack{i\in\{1,\dots,n\}\\ j\in\{1,\dots,n\}}} \in M_{mn}(\mathbf{R})$ est orthogonale si elle vérifie $A \times A^{tr} = I_n$.

Remarque 10 Les ensembles de matrices triangulaires supérieures, triangulaires inférieures, diagonales, symétriques, antisymétriques sont des sous-groupe du groupe commutatif $(M_n(\mathbf{R}),+)$.

Proposition 20 L'ensemble des matrices triangulaires supérieures dont tous les coefficients diagonaux sont non nuls est un sous-groupe du groupe $\mathbf{GL}_n(\mathbf{R})$.

Proposition 21 L'ensemble des matrices triangulaires inférieures dont tous les coefficients diagonaux sont non nuls est un sous-groupe du groupe $\mathbf{GL}_n(\mathbf{R})$.

Proposition 22 L'ensemble des matrices diagonales dont tous les coefficients diagonaux sont non nuls est un sous-groupe du groupe $\mathbf{GL}_n(\mathbf{R})$.

Proposition 23 L'ensemble des matrices de déterminant strictement positif est un sous-groupe du groupe $\mathbf{GL}_n(\mathbf{R})$.

Proposition 24 L'ensemble des matrices de déterminant ± 1 est un sous-groupe du groupe $\mathbf{GL}_n(\mathbf{R})$.

Proposition 25 L'ensemble $\mathbf{SL}_n(\mathbf{R})$ des matrices de déterminant 1 est un sous-groupe du groupe

$\mathbf{GL}_n(\mathbf{R})$.

Proposition 26 L'ensemble $\mathbf{O}_n(\mathbf{R})$ des matrices orthogonales est un sous-groupe du groupe $\mathbf{GL}_n(\mathbf{R})$.

Proposition 27 L'ensemble $\mathbf{SO}_n(\mathbf{R})$ des matrices orthogonales de déterminant 1 est un sous-groupe du groupe $\mathbf{O}_n(\mathbf{R})$.

Proposition 28 Si $n \in \mathbf{N}^*$ l'ensemble des rotations planes d'angles $\frac{2k\pi}{n}, k \in \{0, ..., n-1\}$ est un sous-groupe cyclique d'ordre n de $\mathbf{SO}_2(\mathbf{R})$.

Définition 23 Si $n \in \mathbf{N}^*$, le groupe diédral D_n est le sous-groupe de $\mathbf{SO}_2(\mathbf{R})$ engendré par la rotation d'angle $\frac{2\pi}{n}$ et la symétrie orthogonale (réflexion) par rapport à l'axe Ox.

Remarque 11 Si $n \in \mathbf{N}^*$, le groupe diédral D_n est un sous-groupe non commutatif d'ordre $2n$.

Proposition 29 Si $n \in \mathbf{N}^*$ le groupe diédral D_n est isomorphe au sous-groupe des bijections de $\mathbf{C}$ dans $\mathbf{C}$ engendré par l'application $\mathbf{C}$-linéaire $z \mapsto \exp(\frac{2i\pi}{n})z$ et la conjugaison complexe $z \mapsto \overline{z}$.

Proposition 30 Si $n \in \mathbf{N}^*$, le groupe diédral D_n est l'unique groupe à isomorphisme près engendré par deux éléments s_0 et s_1 tels que s_0^2, s_1^2 et $(s_0 s_1)^n$ soient égaux au neutre.

Proposition 31 Soit q la forme quadratique définie sur $\mathbf{R}^n$. L'ensemble $\mathbf{O}_n(q)$ des matrices A laissant invariante q est un sous-groupe du groupe $\mathbf{GL}_n(\mathbf{R})$.

Proposition 32 Soit q la forme quadratique définie sur $\mathbf{R}^n$. L'ensemble $\mathbf{SO}_n(q)$ des matrices A de déterminant 1 et laissant invariante q est un sous-groupe du groupe $\mathbf{GL}_n(\mathbf{R})$.

Définition 24 Si $(G_1, \top_1)$ et $(G_2, \top_2)$ sont deux groupes. Le produit direct $(G, \top)$ de $(G_1, \top_1)$ et $(G_2, \top_2)$ est défini de la façon suivante : l'ensemble G est $G_1 \times G_2$, la loi de composition interne $\top$ est définie par $(g_1, g_2)\top(g_1', g_2') = (g_1 \top_1 g_1', g_2 \top_2 g_2')$ si $(g_1, g_2) \in G_1 \times G_2$ et $(g_1', g_2') \in G_1 \times G_2$.

Proposition 33 Si $(G_1, \top_1)$ et $(G_2, \top_2)$ sont deux groupes alors leur produit direct $(G, \top)$ est un groupe. L'ordre de G est le produit des ordres de G_1 et G_2 : $|G| = |G_1] \times |G_2|$. Le groupe $(G, \top)$ est commutatif si $(G_1, \top_1)$ et $(G_2, \top_2)$ le sont.

Définition 25 Si $(G_i, \top_i)_{i=1,...n}$ sont des groupes. Le produit direct $(G, \top)$ de $(G_1, \top_1)$ et $(G_2, \top_2)$ est défini de la façon suivante : l'ensemble G est le produit $G_1 \times \cdots \times G_n$, la loi de composition interne $\top$ est définie par $(g_1, ..., g_n)\top(g_1', ..., g_n') = (g_1 \top_1 g_1', ..., g_n \top_2 g_n')$ si $(g_1, ..., g_n) \in G_1 \times \cdots \times G_n$ et $(g_1', ..., g_n') \in G_1 \cdots \times G_n$.

Proposition 34 Si $(G_i, \top_i)_{i=1,...,n}$ sont des groupes alors leur produit direct $(G, \top)$ est un groupe. L'ordre de G est le produit des ordres des G_i, $i = 1, ..., n$: $|G| = |G_1] \times \cdots \times |G_n|$. Le groupe $(G, \top)$ est commutatif si les G_i le sont.

Proposition 35 Si $(G_i, \top_i)_{i=1,...,n}$ et $(H_i, \top_i')_{i=1,...,n}$ sont des groupes tels que pour $i = 1, ..., n$ le groupes H_i est un sous-groupe de G_i alors le produit direct $(H, \top')$ des H_i est un sous-groupe du produit direct $(G, \top)$ des G_i.

Définitions 26 Un anneau (unitaire) est un triplet $(A, \top, \perp)$ où $(A, \top)$ est un groupe commutatif de neutre noté 0, $(A, \perp)$ est un magma associatif muni d'un élément neutre noté 1 et tel que la loi $\perp$ est distributive par rapport à la loi $\top$. L'anneau est dit commutatif si $\perp$ est commutatif. Un corps est un anneau $(A, \top, \perp)$ tel que tout élément autre que 0 admet un inverse pour $\perp$.

Remarque 12 Soit $(A, \top, \perp)$ un anneau, 0 le neutre de $\top$ et 1 le neutre de $\perp$. Alors $0 \perp 1 = 1 \perp 0 = 0$

et plus généralement, si $a \in A$ alors $0 \perp a = a \perp 0 = 0$.

Exemples 11 Les triplets $(\mathbf{Z}, +, \times)$, $(\mathbf{Q}, +, \times)$, $(\mathbf{R}, +, \times)$ et $(\mathbf{C}, +, \times)$ sont des anneaux commutatifs. Ce sont même des corps commutatifs pour les trois derniers. Le triplet $(M_n(A), +, \times)$ où A est un de ces anneaux est un anneau non commutatif. L'ensemble des matrices carrées $(2,2)$ de la forme $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ avec $(a,b) \in \mathbf{R}^2$ (ou $(a,b) \in \mathbf{Q}^2$), muni des lois d'addition et de multiplication de matrices carrées, est un corps commutatif. L'ensemble des matrices carrées $(2,2)$ de la forme $\begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}$ avec $(a,b) \in \mathbf{C}^2$, muni des lois d'addition et de multiplication de matrices carrées, est un corps non commutatif. C'est le corps des quaternions.

3 Morphismes, noyau, image

Définition 27 Soit $(G, \top)$ et $(H, \perp)$ deux groupes. Une application $f : G \to H$ est un morphisme de groupes (ou homomorphisme de groupes) de G dans H si pour tout $a \in G$ et tout $b \in G$ on a $f(a \top b) = f(a) \perp f(b)$.

Définitions 28 Un morphisme de groupes d'un groupe dans lui-même est appelé endomorphisme. Un morphisme de groupes qui est bijectif est appelé isomorphisme de groupes. C'est un épimorphisme si il est surjectif, un monomorphisme si il est injectif. Un morphisme de groupes qui est à la foi un endomorphisme et un isomorphisme est appelé automorphisme.

Proposition 36 Si $f : G \to H$ est un morphisme de groupes et si G' et H' sont des sous-groupes respectivement de G et H alors l'image $f(G')$ de G' par f est un sous-groupe de H et l'image réciproque $f^{-1}(H')$ de H' par f est un sous-groupe de G.

Définitions 29 Si $f : G \to H$ l'image $\mathbf{Im}(f)$ de f est le sous-groupe $f(G)$ de H et le noyau $\mathbf{Ker}(f)$ de f est le sous groupe $f^{-1}(\{e\})$ est un sous-groupe du groupe G.

Proposition 37 Soit $f : G \to H$ un morphisme de groupes. Ce morphisme est injectif si et seulement son noyau $\mathbf{Ker}(f)$ est égal à $\{e\}$. Il est surjectif si et seulement si son image $\mathbf{Im}(f)$ est égale à H.

Proposition 38 Si $g \in G$ alors l'application $f : G \to G$ définie par $f(a) = gag^{-1}$ si $g \in G$ est un automorphisme.

Définitions 30 On appelle automorphisme intérieur d'un groupe G tout automorphisme f de G pour lequel il existe $g \in G$ tel que $f(a) = gag^{-1}$ pour tout $a \in G$. Un tel automorphisme est appelé conjugaison par a. L'élément gag^{-1} s'appelle conjugué de a par g. Un automorphisme qui n'est pas intérieur est dit extérieur.

Proposition 39 L'ensemble $Aut(G)$ des automorphismes d'un groupe G, muni de la loi de composition, est un groupe et le sous-ensemble $Int(G)$ des automorphismes intérieurs est un sous-groupe.

Exemple 12 Dans $\mathbf{C}$ l'application qui $z = x + iy$ associe son conjugué $\overline{z} = x - iy$ et qui est appelée conjugaison complexe n'est pas un automorphisme intérieur, donc n'est pas une conjugaison au sens de la théorie des groupes.

Remarque 13 Si G est un groupe commutatif il n'admet pas d'automorphisme intérieur autre que l'identité.

Définition 31 Soit G un groupe. Un sous-groupe H de G est un sous-groupe normal (ou distingué) s'il est stable par automorphisme intérieur : pour tout tout $g \in G$, $H = gHg^{-1}$, c'est à dire si pour tout $g \in G$ et pour tout $h \in H$, le conjugué ghg^{-1} appartient à H.

Notation On note $H \triangleleft G$ le fait que H soit un sous-groupe normal du groupe G.

Proposition 40 Soit G un groupe. Un sous-groupe H de G est normal si et seulement si $aH = Ha$ quel que soit $a \in G$.

Proposition 41 Le centre $Z(G)$ d'un sous-groupe est normal : $Z(G) \triangleleft G$.

Proposition 42 Le groupe $Int(G)$ des automorphismes intérieurs d'un groupe G est un sous-groupe distingué du groupe $Int(G)$ des automorphismes de G.

Proposition 43 Soit G un groupe et $(H_i)_{i\in I}$ une famille non vide de sous-groupes normaux de G. Alors l'intersection $H = \bigcap_{i\in I} Hi$ est un sous-groupe normal de G.

Proposition 44 Soit $f : G \to H$ un morphisme de groupes. Alors son noyau $\mathbf{Ker}(f)$ est un sous-groupe normal de G.

Proposition 45 Soit $f : G \to H$ un morphisme de groupes. Si G' est un sous-groupe normal de G alors $f(G')$ est un sous-groupe normal de $f(G)$.

Proposition 46 Soit $f : G \to H$ un morphisme de groupes. Si H' est un sous-groupe normal de H alors $f^{-1}(H')$ est un sous-groupe normal de G.

4 Rappels sur les relations d'équivalence et quotients d'ensembles. Théorème de Lagrange

Définition 32 Soit X un ensemble. Une relation binaire (ou relation) $\mathcal{R}$ définie sur X est un sous-ensemble du produit X^2.

Notation Si $\mathcal{R}$ est une relation définie sur un ensemble X et $(a,b) \in X^2$, plutôt que d'écrire $(a,b) \in \mathcal{R}$ on écrit $a\mathcal{R}b$.

Remarque 14 Soit $\mathcal{R}$ une relation définie sur un ensemble X et $(a,b) \in X^2$. On dit que a est en relation avec b si $a\mathcal{R}b$.

Définitions 33 Soit X un ensemble et $\mathcal{R}$ une relation définie sur X :
- la relation $\mathcal{R}$ est dite réflexive si, quel que soit $a \in X$, $a\mathcal{R}a$;
- la relation $\mathcal{R}$ est dite symétrique si, quel que soit $(a,b \in X^2$, $b\mathcal{R}a$ dès que $a\mathcal{R}b$;
- la relation $\mathcal{R}$ est dite antisymétrique si, quel que soit $(a,b) \in X^2$, $a = b$ dès que $a\mathcal{R}b$ et $b\mathcal{R}a$;
- la relation $\mathcal{R}$ est dite transitive si, quel que soit $(a,b,c) \in X^3$, $a\mathcal{R}c$ dès que $a\mathcal{R}b$ et $b\mathcal{R}c$.

Définitions 34 Soit X un ensemble et $\mathcal{R}$ une relation définie sur X. C'est une relation d'ordre si elle est réflexive, antisymétrique et transitive. C'est une relation d'équivalence si elle est réflexive, symétrique et transitive.

Définition 35 Si $\mathcal{R}$ est une relation d'équivalence définie sur un ensemble X et si $a \in X$ alors le sous-ensemble $[a] = \{b \in X \mid a\mathcal{R}b\}$ formé des $b \in X$ avec lesquels a est en relation est appelé classe

d'équivalence de a.

Notation Si $\mathcal{R}$ est une relation d'équivalence définie sur un ensemble X et si $a \in X$ alors la classe d'équivalence de a pour cette relation est souvent notée $[a]$, $\overline{a}$, $[a]_{\mathcal{R}}$ ou encore $\overline{a}^{\mathcal{R}}$.

Définition 36 Une partition d'un ensemble X est un sous-ensemble $\mathcal{P}$ de l'ensemble $\mathcal{P}(X)$ des parties de X dont les éléments sont des sous-ensembles de X non vides, deux à deux disjoints et dont la réunion est égale à X.

Exemples 13 L'ensemble vide $\emptyset$ est l'unique partition de l'ensemble vide $\emptyset$. Si $X = \{0,1,2,3,4,5\}$, l'ensemble dont les éléments sont les paires $\{0,3\}$, $\{1,4\}$ et $\{2,5\}$ forme une partition de X. Si $X = \mathbf{N}$, l'ensemble dont les éléments sont le sous-ensemble $\{2k \mid k \in \mathbf{N}\}$ des entiers naturels pairs et le sous-ensemble $\{2k+1 \mid k \in \mathbf{N}\}$ des entiers naturels impairs est une partition de X. Si X est un ensemble et si $Y \subset X$ alors $\{Y \mid X \setminus Y\}$ est une partition de X si et seulement si Y est différent de X et du vide.

Proposition 47 Si $\mathcal{R}$ est une relation d'équivalence définie sur un ensemble X et si $(a,b) \in X$ alors $[a] = [b]$ ou $[a] \cap [b] = \emptyset$.

Corollaire 1 Si $\mathcal{R}$ est une relation d'équivalence définie sur un ensemble X alors l'ensemble des classes d'équivalence forme une partition de X.

Définition 37 Si $\mathcal{R}$ est une relation d'équivalence définie sur un ensemble X alors la partition de X en classes d'équivalence induite par cette relation est appelée ensemble quotient de X par $\mathcal{R}$ est est notée $X/\mathcal{R}$.

Définition 38 Si $\mathcal{R}$ est une relation d'équivalence définie sur un ensemble X alors cette relation défini par une application appelée projection p de X dans $X/\mathcal{R}$ en posant $p(a) = [a]$ quel que soit $a \in X$.

Proposition 48 Soit $\mathcal{R}$ une relation d'équivalence définie sur un ensemble X et p la projection de X sur $X/\mathcal{R}$ ainsi définie. Alors, pour toute application $f : X \to F$ qui vérifie $f(a) = f(b)$ quel que soit $(a,b) \in X^2$ tel que $a\mathcal{R}b$, il existe une unique application $f_{\mathcal{R}} : X/\mathcal{R} \to F$ telle que $f = f_{\mathcal{R}} \circ p$.

Définition 39 Soit $(E, \top)$ un magma et $\mathcal{R}$ une relation d'équivalence définie sur E. La loi $\top$ est dite compatible avec la relation d'équivalence $\mathcal{R}$ si, quel que soit $(a,b,c,d) \in E^4$, $(a \top b)\mathcal{R}(c \top d)$ dès que $a\mathcal{R}c$ et $b\mathcal{R}d$.

Proposition 49 Soit $(E, \top)$ un magma et $\mathcal{R}$ une relation d'équivalence définie sur E. La loi $\top$ est compatible avec la relation d'équivalence $\mathcal{R}$ si et seulement si, pour tout quadruplet $(a,b,c,d) \in E^4$, $[a \top b] = [c \top d]$ dès que $[a] = [c]$ et $[b] = [d]$.

Corollaire 2 Soit $(E, \top)$ un magma et $\mathcal{R}$ une relation d'équivalence définie sur E. Si la loi $\top$ est compatible avec la relation d'équivalence $\mathcal{R}$ alors il existe une unique loi $\top_{\mathcal{R}}$ définie sur $E/\mathcal{R}$ telle que $[a]\top_{\mathcal{R}}[b] = [a \top b]$ quel que soit $(a,b) \in E^2$. Réciproquement, s'il existe une loi $\top_{\mathcal{R}}$ définie sur $X/\mathcal{R}$ telle que $[a]\top_{\mathcal{R}}[b] = [a \top b]$ quel que soit $(a,b) \in E^2$ alors la loi $\top$ est compatible avec la relation d'équivalence $\mathcal{R}$.

Proposition 50 Soit $(E, \top)$ un magma et $\mathcal{R}$ une relation d'équivalence définie sur E. Si la loi $\top$ est compatible avec la relation d'équivalence $\mathcal{R}$ alors l'application qui à $a \in E$ associe sa classe $[a]$ est bien définie et c'est un morphisme de magmas de $(E, \top)$ dans $(E/\mathcal{R}, \top_{\mathcal{R}})$.

Proposition 51 Soit $(E, \top)$ un magma et $\mathcal{R}$ une relation d'équivalence définie sur E. La loi $\top$ est supposée compatible avec la relation d'équivalence $\mathcal{R}$. Si $\top$ est associative (respectivement commutative) alors $\top_{\mathcal{R}}$ aussi. Si la loi $\top$ possède un élément neutre e alors $[e]$ est un neutre pour $\top_{\mathcal{R}}$. Si de

plus $a \in E$ est inversible d'inverse b alors $[a]$ est inversible d'inverse $[b]$.

Définition 40 Si G un groupe et H un sous-groupe de G on définit les relations ${}_H\mathcal{R}$ et $\mathcal{R}_H$ suivantes :
- un couple $(a,b) \in G$ vérifie $a\,{}_H\mathcal{R}\,b$ s'il existe $h \in H$ tel que $a = bh$;
- un couple $(a,b) \in G$ vérifie $a\,\mathcal{R}_H\,b$ s'il existe $h \in H$ tel que $a = hb$.

Proposition 52 Soit G un groupe, H un sous-groupe de G et $(a,b) \in G$. Alors $a\,{}_H\mathcal{R}\,b$ si et seulement si $b^{-1}a \in H$ et $a\,\mathcal{R}_H\,b$ si et seulement si $ab^{-1} \in H$

Proposition 53 Si G un groupe et H un sous-groupe de G alors les relations ${}_H\mathcal{R}$ et $\mathcal{R}_H$ sont des relations d'équivalence. Les classes de ${}_H\mathcal{R}$ sont les sous-ensembles $aH = \{ah \mid h \in H\}$ avec $a \in G$ et les classes de $\mathcal{R}_H$ sont les sous-ensembles $Ha = \{ha \mid h \in H\}$ avec $a \in G$. Si $a \in G$ les applications de H dans aH et Ha qui à $h \in H$ associent ah et ha sont des bijections.

Définition 41 Si G un groupe et H un sous-groupe de G alors les classes d'équivalence de la relation ${}_H\mathcal{R}$ s'appellent classes à gauche et celles de $\mathcal{R}_H$ s'appellent classes à droite.

Remarque 15 Soit G un groupe et H un sous-groupe de G. Alors, pour tout $(a,b) \in G^2$, $b \in aH$ si et seulement si $b^{-1} \in Ha^{-1}$. Ainsi pour tout $(a,b) \in G^2$, $aH = bH$ si et seulement si $Ha^{-1} = Hb^{-1}$. Par conséquent l'application ϕ de $G/{}_H\mathcal{R}$ dans $G/\mathcal{R}_H$ définie par $\phi(aH) = [Ha^{-1}]$ est bien définie puisque si $aH = bH$ alors $Ha^{-1} = Hb^{-1}$.

Proposition 54 Soit G un groupe et H un sous-groupe de G.l'application ϕ de $G/{}_H\mathcal{R}$ dans $G/\mathcal{R}_H$ définie par $\phi([a]_{{}_H\mathcal{R}}) = [a^{-1}]_{\mathcal{R}_H}$ est bijective.

Remarque 16 Une conséquence de cette proposition est que si G un groupe et H un sous-groupe de G alors le nombre de classes d'équivalence de la relation ${}_H\mathcal{R}$ et égal au nombre de classes d'équivalence de la relation $\mathcal{R}_H$. Ce nombre est appelé indice de H dans G.

Théorème 1 (Théorème de Lagrange) Pour tout groupe fini G et tout sous-groupe H de G, l'ordre de H divise celui de G : $|H|$ divise $|G|$. De plus les nombres de classes à gauche et à droite sont tous les deux égaux au quotient $\frac{|G|}{|H|}$.

Corollaire 3 Pour tout groupe fini G et tout élément g de G, l'ordre de g divise celui de G.

Proposition 55 Si G un groupe et H un sous-groupe de G alors les relations ${}_H\mathcal{R}$ et $\mathcal{R}_H$ coïncident c'est à dire $aH = Ha$ quel que soit $a \in G$ si et seulement si H est un sous-groupe-normal de G.

5 Sous-groupes normaux, quotients dont propriété universelle et théorème d'isomorphisme. Sous-groupes d'indice 2

Proposition 56 Soit $(G, \top)$ un groupe et $\mathcal{R}$ une relation d'équivalence. La loi $\top$ est compatible avec la relation $\mathcal{R}$ si et seulement si la classe $[e]$ de l'élément neutre est un sous-groupe normal et alors la relation $\mathcal{R}$ et les relations d'équivalence ${}_H\mathcal{R}$ et $\mathcal{R}_H$ coïncident.

Corollaire 4 Soit $(G, \top)$ un groupe et H un sous-groupe. La loi $\top$ est compatible avec la relation d'équivalence ${}_H\mathcal{R}$, respectivement la relation $\mathcal{R}_H$, si et seulement si H est un sous-groupe normal. Dans ce cas, et seulement dans ce cas, les relations ${}_H\mathcal{R}$ et $\mathcal{R}_H$ coïncident.

Proposition 57 Soit $(G, \top)$ un groupe, H un sous-groupe normal et $\mathcal{R}$ la relation d'équivalence définie

par H ($\mathcal{R} =_H \mathcal{R} = \mathcal{R}_H$). Alors l'ensemble $G/\mathcal{R}$, noté G/H, muni de la loi $\top_{\mathcal{R}}$ est un groupe appelé groupe quotient de G par H. L'application qui à $a \in G$ associe sa classe aH (qui est égale à Ha) est un morphisme de groupes appelé morphisme canonique. Son noyau est le sous-groupe normal H.

Corollaire 5 Soit $(G, \top)$ un groupe. Un sous-groupe H de G est normal si et seulement si c'est le noyau d'un morphisme de groupes.

Théorème 2 (Premier théorème d'isomorphisme) Soit $f : G \to H$ un morphisme de groupes. Alors on définit un isomorphisme ϕ de groupes du groupe quotient $G/\mathbf{Ker}(f)$ dans le groupe $\mathbf{Im}(f)$ en posant $\phi(a\mathbf{Ker}(f)) = f(a)$ si $a \in G$.

Proposition 58 Soit $(G, \top)$ un groupe et H un sous-groupe. Si H est d'indice 2 alors il est normal.

Proposition 59 Le groupe $Int(G)$ des automorphismes intérieurs d'un groupe G est isomorphe au groupe quotient $G/Z(G)$ de G par son centre $Z(G)$.

Théorème 3 (Deuxième théorème d'isomorphisme) Soit G un groupe, H un sous-groupe normal et K un sous-groupe. Alors HK est un sous-groupe de G, $H \cap K$ est un sous-groupe normal de K, H est un sous-groupe normal de HK et les groupes quotients $K/(H \cap K)$ et HK/H sont isomorphes.

Théorème 4 (Troisième théorème d'isomorphisme) Soit G un groupe et H et K des sous-groupes normaux tels que $H \subset K$. Alors les groupes quotients G/K et $(G/H)/(K/H)$ sont isomorphes.

6 Exemples. Groupes cyclique, théorème chinois. Groupes commutatifs finis. Théorème de Kronecker

Proposition 60 Soit $n \in \mathbf{N}^*$. Les générateurs de $\mathbf{Z}/n\mathbf{Z}$ sont les classes $\overline{q}$ avec $q \in \mathbf{N}$ compris entre 1 et n et premier avec n

Définition 42 La fonction indicatrice d'Euler est la fonction ϕ de $\mathbf{N}^*$ dans $\mathbf{N}^*$ qui à tout $n \in \mathbf{N}^*$ associe le nombre de générateurs de $\mathbf{Z}/n\mathbf{Z}$ c'est à dire le nombre d'entiers compris entre 1 et n et premiers avec n.

Proposition 61 La fonction indicatrice d'Euler ϕ vérifié la propriété suivante : si $(n,m) \in (\mathbf{N}^*)^2$ sont tels que n et m soient premiers entre eux alors $\phi(mn) = \phi(m) \times \phi(n)$

Proposition 62 Si $p_1, ..., p_k$ sont des nombres premiers tous différents, si $(d_1, ..., d_k) \in (\mathbf{N}^*)^k$ et si $n = p_1^{d_1} \cdot ... \cdot p_k^{d_k}$ alors

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot ... \cdot \left(1 - \frac{1}{p_k}\right)$$

où ϕ désigne la fonction indicatrice d'Euler.

Théorème 5 (Théorème des restes chinois) Soit $m_1, ..., m_k$ des entiers naturels non nuls et deux à deux premiers entre eux. Alors l'application de $\mathbf{Z}/m_1 \cdot ... \cdot m_k\mathbf{Z}$ dans $\mathbf{Z}/m_1\mathbf{Z} \times ... \times \mathbf{Z}/m_k\mathbf{Z}$ qui, si $n \in \mathbf{N}$, à sa classe dans $\mathbf{Z}/m_1 \cdot ... \cdot m_k\mathbf{Z}$, associe le k u-plet formé de ses classes dans $\mathbf{Z}/m_1\mathbf{Z}, ..., \mathbf{Z}/m_k\mathbf{Z}$ est un isomorphisme de groupes.

Définition 43 L'exposant d'un groupe G de neutre e est, lorsqu'il existe, le plus petit entier naturel non nul d tel $g^d = e$ pour tout $g \in G$. Sinon G est d'exposant infini.

Proposition 63 Lorsqu'il est fini, l'exposant d'un groupe G est le ppcm des ordres de tous ses éléments.

Proposition 64 Si G est un groupe fini alors son exposant est fini et divise son ordre.

Proposition 65 Soit G un groupe et $a,b \in G$ deux éléments différents du neutre qui commutent. Si a est d'ordre $p \in \mathbf{N}$ et b est d'ordre $q \in \mathbf{N}$ il existe $\alpha,\beta \in \mathbf{N}^*$ tel que $a^\alpha b^\beta$ est d'ordre le ppcm de p et q.

Corollaire 6 Soit G un groupe commutatif d'ordre fini. Il existe alors un élément $g \in G$ dont l'ordre est l'exposant de G. L'ordre de cet élément est un multiple de l'ordre de tout élément de G.

Remarque 17 Si G est un groupe commutatif d'ordre fini alors, d'après ce corollaire, son exposant est égal au maximum des ordres des éléments de G. Ce n'est pas toujours vrai lorsque G n'est pas commutatif. Par exemple l'exposant du groupe $\mathcal{S}_3$ des permutations de $\{1,2,3\}$ est égal à son ordre, c'est à dire 6 mais les éléments de $\mathcal{S}_3$ sont d'ordre 1, 2 ou 3 et aucun élément n'est d'ordre 6.

Théorème 6 (Théorème de Kronecker) Soit G un groupe commutatif d'ordre fini. Alors il existe une unique suite finie d'entiers naturels non nuls $n_1,...,n_d$ telle que $n_d|n_{d-1},...,n_2|n_1$ et telle que G soit isomorphe à $\mathbf{Z}/n_1\mathbf{Z} \times ... \times \mathbf{Z}/n_d\mathbf{Z}$.

7 Groupes des permutations, théorème de Cayley

Définitions 44 Soit E un ensemble. Une bijection de E dans E est appelée permutation de E. Le groupe symétrique de E est le groupe des permutations de E, c'est à dire l'ensemble $\mathcal{S}(E)$ des permutations de E muni de la loi de composition des applications. Si $n \in \mathbf{N}^*$ note $\mathcal{S}_n$ le groupe symétrique de $\{1,...,n\}$.

Définition 45 Soit E un ensemble. Le support d'une permutation $g \in \mathcal{S}(E)$ est le sous-ensemble de E formés des $x \in E$ tels que $g(x) \neq x$.

Notation Soit E un ensemble et $g \in \mathcal{S}(E)$. Si le support de g est inclus dans un ensemble fini $\{a_1,...,a_d\}$ et si b_i désigne $g(a_i)$ lorsque $i = 1,...,d$ alors g peut être notée $\begin{pmatrix} a_1 & \cdots & a_d \\ b_1 & \cdots & b_d \end{pmatrix}$.

Proposition 66 Soit E un ensemble. Deux permutations $g,h \in \mathcal{S}(E)$ qui ont des supports disjoints commutent.

Proposition 67 Soit E et F deux ensembles. Les groupes $\mathcal{S}(E)$ et $\mathcal{S}(F)$ sont isomorphes si et seulement si E et F ont même cardinal.

Théorème 7 (Théorème de Cayley) Tout groupe G est isomorphe à un sous-groupe du groupe symétrique $\mathcal{S}(G)$ des permutations de G. En particulier, si G est un groupe fini d'ordre n, il est isomorphe à un sous-groupe de $\mathcal{S}_n$.

Définition 46 Soit $n \in \mathbf{N}^*$. Un élément g de $\mathcal{S}_n$ est un cycle (une permutation circulaire) s'il existe $l \in \{1,...,n\}$ et $a \in \{1,...,n\}$ tels que $a,...,g^{l-1}(a)$ sont tous différents, $g^l(a) = a$ et si $b \in \{1,...,n\} \setminus \{a,...,g^{l-1}(a)\}$ alors $g(b) = b$. L'entier l s'appelle la longueur du cycle. Un cycle de longueur l est appelé l-cycle.

Proposition 68 Soit $n \in \mathbf{N}^*$ et $g \in \mathcal{S}_n$ un cycle. Son ordre est égal à sa longueur.

Proposition 69 Soit $n \in \mathbf{N}^*$, $l \in \{1,...,n\}$ et $g \in \mathcal{S}_n$ un cycle de longueur l. Le support $S(g)$ de g est l'ensemble des $k \in \{1,...,n\}$ tels que $g(k) \neq k$. C'est un ensemble à l éléments.

Proposition 70 Soit $n \in \mathbf{N}^*$, $l \in \{1,...,n\}$ et $(a_0,...,a_{l-1}) \in \{1,...,n\}^l$ un l-uplet de termes tous différents. Alors il existe un unique l-cycle g de $\mathcal{S}_n$ tel que si $g(a_k) = a_{k+1}$ si $k \in \{0,...,l-2\}$ et $g(a_{l-1}) = a_0$. Son support est $\{a_0,...,a_{l-1}\}$.

Notation Soit $n \in \mathbf{N}^*$, $l \in \{1,...,n\}$ et $(a_0,...,a_{l-1}) \in \{1,...,n\}^l$ un l-uplet de termes tous différents. Alors l'unique l-cycle g de $\mathcal{S}_n$ tel que si $g(a_k) = a_{k+1}$ si $k \in \{0,...,l-2\}$ et $g(a_{l-1}) = a_0$ est noté $(a_0...a_{l-1})$.

Proposition 71 Soit $n \in \mathbf{N}^*$, $l \in \{1,...,n\}$, g un l-cycle de $\mathcal{S}_n$, $a \in \{1,...,n\}$ tel que $g(a) \neq a$ alors le l-uplet $(a...g^{l-1}(a))$ caractérise g. De plus $b \in \{1,...,n\}$ est tel que le l-uplet $(b...g^{l-1})$ caractérise g alors il existe $k \in \{0,...,l-1\}$ tel que $b = g^k(a)$ ou $a = g^k(b)$.

Proposition 72 Soit $n \in \mathbf{N}^*$, $l,l' \in \{1,...,n\}$, g un l-cycle de $\mathcal{S}_n$ et g' un l'-cycle de $\mathcal{S}_n$. Si les supports de g et g' sont disjoints alors $gg' = g'g$.

Proposition 73 Soit $n \in \mathbf{N}^*$, $l,l' \in \{1,...,n\}$, g un l-cycle de $\mathcal{S}_n$ et g' un l'-cycle de $\mathcal{S}_n$. Alors g et g' sont conjugués si et seulement si $l = l'$.

Définition 47 Un 2-cycle est appelé transposition.

Proposition 74 Si $n \in \mathbf{N}$ et $n \geq 2$ alors $(ij) = (1i)(1j)(1i)$ quels que soient $i,j \in \{2,...,n\}$.

Corollaire 7 Si $n \in \mathbf{N}$ et $n \geq 2$ alors les transpositions $(1,k), k \in \{2,...,n\}$ engendrent $\mathcal{S}_n$.

Proposition 75 Si $n \in \mathbf{N}$ et $n \geq 3$ alors

$$(1k) = (2...n)^{k-2}(12)(2...n)^{2-k}$$

quel que soit $k \in \{3,...,n\}$.

Corollaire 8 Si $n \in \mathbf{N}$ et $n \geq 3$ alors (12) et $(2...n)$ engendrent $\mathcal{S}_n$.

Proposition 76 Soit $n \in \mathbf{N}^*$. Si $g \in \mathcal{S}_n$ alors il existe $d \leq n-1$ et des transpositions $g_1,...,g_d$ vérifiant

$$g = g_1 \circ ... \circ g_d.$$

Proposition 77 Soit $n \in \mathbf{N}^*$. Si $g \in \mathcal{S}_n$ n'est pas l'identité alors il existe $d \leq \frac{n}{2}$ et des cycles à supports deux à deux disjoints $g_1,...,g_d$ vérifiant

$$g = g_1 \circ ... \circ g_d.$$

Cette décomposition est unique à l'ordre près : si $d' \leq \frac{n}{2}$ et $g'_1,...,g'_{d'}$ sont des cycles à supports deux à deux disjoints tels que $g = g'_1 \circ ... \circ g'_{d'}$ alors $d' = d$ et $\{g'_1,...,g'_{d'}\} = \{g_1,..,g_d\}$.

Proposition 78 Soit $n \in \mathbf{N}^*$, $d,d' \in \{1,...,n\}$ et $g = g_1 \circ ... \circ g_d, g' = g'_1 \circ ... \circ g'_{d'} \in \mathcal{S}_n$ avec $g_1,...,g_d$ des cycles à supports deux à deux disjoints et $g'_1,...,g'_{d'}$ des cycles à supports deux à deux disjoints. Alors g et g' sont conjugués si et seulement si $d = d'$ et, quitte à réindexer, pour tout $i \in \{1,...,d\}$ g_i et g'_i ont même longueur.

Proposition 79 Soit $n \in \mathbf{N}^*$, $d \in \{1,...,n\}$ et $g \in \mathcal{S}_n$. On suppose que $g = g_1 \circ ... \circ g_d$ avec $g_1,...,g_d$ des cycles à supports deux à deux disjoints. Alors l'ordre de g est le $ppcm$ des longueurs, donc des ordres, de $g_1,...,g_d$.

Définition 48 Soit $n \in \mathbf{N}^*$. La signature $\varepsilon(g)$ d'une permutation $g \in \mathcal{S}_n$ est le nombre

$$\varepsilon(g) = \prod_{\substack{(i,j)\in\{1,\ldots,n\}^2 \\ i<j}} \frac{g(i)-g(j)}{i-j}.$$

Proposition 80 Si $n \in \mathbf{N}^*$ et $g \in \mathcal{S}_n$ est une transposition (un 2-cycle) alors $\varepsilon(g) = -1$.

Proposition 81 Si $n \in \mathbf{N}^*$ et $g, h \in \mathcal{S}_n$ alors $\varepsilon(gh) = \varepsilon(g)\varepsilon(h)$.

Proposition 82 Soit $n \in \mathbf{N}^*$, $d \in \{1, \ldots, n\}$ et $g \in \mathcal{S}_n$. On suppose que $g = g_1 \circ \ldots \circ g_d$ avec $g_1, \ldots, g_d$ des cycles à supports deux à deux disjoints et de longueurs $l_1, \ldots, l_d$. Alors la signature $\varepsilon(g)$ de g vérifie

$$\varepsilon(g) = (-1)^{l_1+\ldots+l_d}(-1)^d.$$

Proposition 83 Soit $n \in \mathbf{N}^*$, $d \in \{1, \ldots, n\}$ et $g \in \mathcal{S}_n$. On suppose que $g = g_1 \circ \ldots \circ g_d$ avec $g_1, \ldots, g_d$ des transpositions. Alors la signature $\varepsilon(g)$ de g vérifie $\varepsilon(g) = (-1)^d$.

Proposition 84 Si $n \in \mathbf{N}$ avec $n \geq 2$ alors la signature est un morphisme surjectif (un épimorphisme) du groupe $\mathcal{S}_n$ dans le groupe multiplicatif $(\{-1, 1\}, \times)$.

Définition 49 Si $n \in \mathbf{N}$ avec $n \geq 2$ alors le groupe alterné $\mathcal{A}_n$ est le noyau de l'épimorphisme signature. Il est formé de l'ensemble des permutations $g \in \mathcal{S}_n$ de signature 1.

Proposition 85 Si $n \in \mathbf{N}$ avec $n \geq 2$ alors le groupe alterné $\mathcal{A}_n$ est un sous-groupe distingué de $\mathcal{S}_n$.

Proposition 86 Si $n \in \mathbf{N}$ avec $n \geq 3$ alors le groupe alterné $\mathcal{A}_n$ est engendré par les 3-cycles.

8 Actions de groupes, orbites, stabilisateurs, points fixes. Formules des classes, théorème de Cauchy

Définition 50 Soit G un groupe, e son neutre et X un ensemble non vide. Une action de G sur X est une application $\phi : G \times X \to X$ qui vérifie les conditions suivantes :
- $\phi(g_1, \phi(g_2, x)) = \phi(g_1 \cdot g_2, x)$ si $(g_1, g_2) \in G^2$ et $x \in X$;
- $\phi(e, x) = x$ quel que soit $x \in X$.

Remarque 18 Si ϕ est une action d'un groupe G sur un ensemble non vide X alors $\phi(g, x)$ est parfois noté $g \cdot x$.

Définition 51 Si ϕ est une action d'un groupe G sur un ensemble non vide X. On dit que $x \in X$ est un point fixe de g si $g \cdot x = x$.

Définition 52 Si ϕ est une action d'un groupe G sur un ensemble non vide X et si $x \in X$ on appelle orbite de x sous l'action ϕ de G le sous-ensemble $\omega(x) = \{\phi(g, x) \mid g \in G\} = \{g \cdot x \mid g \in G\}$ de X.

Définition 53 Si ϕ est une action d'un groupe G sur un ensemble non vide X et si $x \in X$ on appelle stabilisateur de x le sous-ensemble $\mathrm{St}(x) = \{g \in G \mid g \cdot x = x\}$.

Proposition 87 Si ϕ est une action d'un groupe G sur un ensemble non vide X et si $x \in X$ alors le stabilisateur $\mathrm{St}(x)$ de x est un sous-groupe de G.

Proposition 88 (Formule des classes) Soit G un groupe fini agissant sur un ensemble fini E et $x \in E$ un élément. Alors le cardinal $|\omega(x)|$ de l'orbite de x est égal à l'indice dans G de $\mathrm{St}(x)$, le stabilisateur de x :

$$|\omega(x)| = \frac{|G|}{|\mathrm{St}(x)|}.$$

Définition 54 Si ϕ est une action d'un groupe G sur un ensemble non vide X et si $g \in G$, un point fixe sous l'action de g est un élément $x \in X$ tel que $g(x) = x$ et on note $\mathrm{Fix}(g)$ le sous-ensemble $\mathrm{Fix}(g) = \{x \in X | g(x) = x\}$.

Proposition 89 (Formule de Burnside) Soit G un groupe fini agissant sur un ensemble fini E et Ω l'ensemble des orbites de cette action. Alors

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|.$$

Théorème 8 (Théorème de Cauchy) Soit G un groupe fini d'ordre n et p un nombre premier qui divise n. Alors il existe au moins un élément de G d'ordre p.

Définition 55 Soit ϕ une action d'un groupe G sur un ensemble non vide X. Cette action est dite libre si $g(x) \neq x$ quels que soient $g \in G \setminus \{e\}$ et $x \in X$. Elle est dite transitive s'il existe $g \in G$ tel que $g(x) = y$ quels que soient $x, y \in X$. Elle est dite simplement transitive si elle est libre et transitive : quels que soient $x, y \in X$ il existe un et un seul $g \in G$ tel que $g(x) = y$. Enfin, l'action ϕ est fidèle si quel que soit $g \in G \setminus \{e\}$ il existe au moins un $x \in X$ tel que $g(x) \neq x$.

9 Exemples d'application à la théorie des groupes, à l'algèbre linéaire et à la géométrie

Définition 56 Soit $(K, +, \times)$ un corps commutatif, $n \in \mathbf{N}^*$ et $M_n(K)$ l'ensemble des matrices carrées (n, n) à coefficients dans K. La somme et le produit de deux matrices sont définis de la façon suivante : si $P = (p_{ij})_{(i,j) \in \{1,\ldots,n\}^2} \in M_n(K)$ et $Q = (q_{ij})_{(i,j) \in \{1,\ldots,n\}^2} \in M_n(K)$ alors la somme $P + Q$ est la matrice $S = (s_{ij})_{(i,j) \in \{1,\ldots,n\}^2}$ telle que $s_{ij} = p_{ij} + q_{ij}$ si $(i, j) \in \{1, \ldots, n\}^2$ et le produit $P \times Q$ est la matrice $R = (r_{ij})_{(i,j) \in \{1,\ldots,n\}^2}$ telle que que $r_{ij} = \sum_{k=1}^{n} p_{ik} q_{kj}$ si $(i, j) \in \{1, \ldots, n\}^2$.

Proposition 90 Soit $(K, +, \times)$ un corps commutatif, $n \in \mathbf{N}^*$ et $M_n(K)$ l'ensemble des matrices carrées (n, n) à coefficients dans K. Alors $(M_n(K), +, \times)$ est un anneau.

Définition 57 Soit $(K, +, \times)$ un corps commutatif, $n \in \mathbf{N}^*$ et $M_n(K)$ l'ensemble des matrices carrées (n, n) à coefficients dans K. Le déterminant $|P|$ d'une matrice carrée $P = (p_{ij})_{(i,j) \in \{1,\ldots,n\}^2} \in M_n(K)$ est

$$|P| = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} p_{i\sigma(i)}.$$

Remarque 19 Le déterminant de la matrice identité de $M_n(K)$ vaut 1.

Proposition 91 Soit $(K, +, \times)$ un corps commutatif, $n \in \mathbf{N}^*$ et $M_n(K)$ l'ensemble des matrices carrées (n, n) à coefficients dans K. Soit également $P' = (p'_{ij})_{(i,j) \in \{1,\ldots,n\}^2}$ la matrice des cofacteurs de P : si

$(i,j) \in \{1,...,n\}^2$ alors p'_{ij} est le déterminant de la matrice obtenue à partir de P en remplaçant les coefficients de la ligne i et de la colonne j par 0 sauf le coefficient à l'intersection de cette ligne et de cette colonne qui est remplacé par 1. Alors $P \times P'^t = |P| I_n$ où P'^t est la transposée de P' et I_n la matrice identité.

Proposition 92 Soit $(K,+,\times)$ un corps commutatif, $n \in \mathbf{N}^*$ et $M_n(K)$ l'ensemble des matrices carrées (n,n) à coefficients dans K. L'application déterminant $|\ | : (M_n(K),\times) \to (K,\times)$ est un morphisme : si $P,Q \in M_n(K)$ alors $|P \times Q| = |P| \times |Q|$.

Théorème 9 Un sous-groupe fini de $\mathbf{SO}_3$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ ou à D_n, $n \in \mathbf{Z}^*$, à $\mathcal{A}_4$, à $\mathcal{S}_4$ ou à $\mathcal{A}_5$.

Théorème 10 Soit F un corps commutatif fini. Le groupe multiplicatif de F est cyclique.

Table des matières