Initiation à la théorie des groupes

Thomas Delzant

Prologue

Il ne s'agit ni d'un tout premier cours de théorie des groupes (les étudiants ont déjà été initiés à cette notion dans les deux premières années), ni d'un cours avancé d'introduction, pour lequel des centaines d'excellents traités sont disponibles, en particulier le livre de Hall [Ha], ou celui de Karpagalov-Merzlyakov [K-M]. Les connaissances requises sont en particulier : l'algèbre linéaire et la géométrie en particulier en dimension 2 et 3, connaissance des anneaux de congruences $\mathbb{Z}/n\mathbb{Z}$.

Les contenus des cours Algèbre S1, Algèbre S2, géométrie du plan. Algèbre S4. sont supposés acquis, et ce cours sera l'occasion de les réviser. Une connaissance de l'algèbre linéaire sur un corps fini est bien commode.

Table des matières

Chapitre 1
Généralités

1.1 Définitions et premières propriétés.

1.1.1 Axiomes et définitions

Définition 1.1. *Une loi de composition interne dans un ensemble G est une application de $G \times G$ dans G*

Autrement dit c'est une règle qui partant de deux éléments de G en construit un troisième.
On note souvent par un . ou par rien du tout cette loi $(a,b) \to a.b$ ou $(a,b) \to ab$.
Il y a des tas de lois très intéressantes à étudier dans la nature, mais dans ce cours, nous considérerons uniquement des lois de groupe.

Définition 1.2. *On dit que la loi . munit l'ensemble G d'une structure de groupe si elle satisfait les trois axiomes :*

1. *Associativité. Pour tout triplet x, y, z d'élément de G, $(x.y).z = x.(y.z)$*
2. *Elément neutre. Il existe un élément e, appelé l'élément neutre, tel que pour tout élément x de G, $x \cdot e = e \cdot x = x$*
3. *Inverse. Tout élément x admet un inverse y c'est à dire un élément y tel que $x \cdot y = y \cdot x = e$*

L'inverse, dont nous allons montrer qu'il est unique, se note souvent x^{-1}.

Définition 1.3. *Un groupe est dit commutatif -on dit aussi abélien- si sa loi satisfait :*
Pour tout couple x,y d'éléments de G $x \cdot y = y \cdot x$.

Remarque 1.4. Si la loi de composition est commutative on peut la noter additivement par un $+$ l'inverse se note $-x$, et l'élément neutre 0. Ainsi, on écrit $x - x = 0$. Pas toujours. Par exemple, si $\mathbb{K}$ est un corps (ça c'est pour ceux qui savent ce qu'est un corps), comme par exemple $\mathbb{R}$ ou $\mathbb{C}$, ou $\mathbb{F}_p$, $(\mathbb{K}^*, \times)$ est toujours noté multiplicativement.

Exemple 1.5. Groupes commutatifs.

Les groupes $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{C}^*, \times)$. sont commutatifs ; plus généralement, si $\mathbb{K}$ est un corps, $(\mathbb{K}, +)$ est un groupe abélien, ainsi que $(\mathbb{K}^*, \times)$. Si A est un anneau, $A, +$ est aussi un groupe abélien ; on note souvent A^* l'ensemble des éléments inversibles de A qui est un groupe.

Le groupe des racines $n-i$èmes de l'unité $\mathbb{U}_n = \{z \in \mathbb{C}^*, z^n = 1\}$ est noté multiplicativement.

Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est le groupe des classes d'entiers modulo n. C'est le groupe formés des éléments $\{\bar{0}, \bar{1}, ..., \overline{n-1}\}$ muni de la loi $x + y =$ le reste de la division de x modulo n. L'application $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est justement l'application qui à un entier associe le reste de la division par n.

Remarque 1.6. les groupes $\mathbb{U}_n$ et $\mathbb{Z}/n\mathbb{Z}$ sont isomorphes (voir plus tard), mais il n'y a pas d'isomorphisme naturel entre ces deux groupes, dès que $n = 3$. En fait choisir un isomorphisme entre ces deux groupes, revient à choisir une racine primitive n-ième de l'unité, et il y en a beaucoup.

Exemple 1.7. Le groupe des symétries du carré a 8 éléments, on l'appelle $\mathbb{D}_8$. Il n'est pas commutatif, il admet 4 rotations, et 4 réflexions.

Question 1. Décrire le groupe des symétries d'un polygones régulier à n cotés.

Exemple 1.8. Le groupe linéaire $\mathrm{GL}(n, \mathbb{K})$ des matrices (n, n) inversibles. Le groupe affine, le groupe des similitudes, le groupe des isométries sont des groupes de transformations.

Proposition 1.9. *Soit X un ensemble, et $S(X)$ l'ensemble des bijections de X. La composition munit $S(X)$ d'une loi de groupe. On l'appelle le groupe des permutations de X. Si X est l'ensemble à n éléments $\{1, ..., n\} \subset \mathbb{Z}$, on le note S_n, et on l'appelle « le » groupe symétrique de n lettres.*□

Remarque 1.10. Il se peut très bien que X ait n éléments mais que ce ne soit pas l'ensemble $\{1....n\}$ par exemple, X est un jeu de 52 cartes. On obtient un groupe : le groupe du battage des cartes. Il n'y a pas d'isomorphisme préféré entre ce groupe et S_{52}.

Question 2. Groupe des coupages. C'est le groupe obtenu en coupant le jeu de cartes un certain nombre de fois. Quel est il ?

La structure de groupe est une structure ; comme toujours, si il y a des structures il y a des homomorphismes.

Définition 1.11. *Une application f définie entre deux groupes G et H est un homomorphisme si elle préserve les produits $f(x \cdot y) = f(x) \cdot f(y)$.*

Avertissement 1.12. Certains auteurs -français- disent un **morphisme**, plutôt que homomorphisme. Les anglais/américains disent « homomorphism », les italiens « omomorfismo » les espagnols « homomorfismo », les allemands « Homomorphismus », ou « Gruppenhomomorphismus ». Depuis quelques années, certains français disent « morphisme » bon.

Exemple 1.13. Les homomorphismes de groupes « naturels » sont nombreux, citons :
L'application exponentielle $\exp : \mathbb{C} \to \mathbb{C}^*$.
Le logarithme népérien $\ln : \mathbb{R}_+^* \to \mathbb{R}$
Le déterminant, qui est un homomorphisme de groupes $\mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$
La réduction modulo n $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.
La partie linéaire. Si A est un espace affine et E l'espace vectoriel sous-jacent, $\mathrm{Aff}(A) \to \mathrm{Gl}(E)$ est un homomorphisme.

1.1.2 Calculs dans un groupe.

On fixe un groupe $(G, .)$

Proposition 1.14. *L'inverse d'un élément est unique.*

Démonstration. Soient y_1 et y_2 deux inverses de x. On utilise l'associativité :
$y_2 = (y_1 \cdot x) \cdot y_2 = y_1 \cdot (x \cdot y_2) = y_1$. □

Proposition 1.15. *Si x et y sont deux éléments de G, $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$*

Démonstration. $(xy)\cdot(y^{-1}x^{-1}) = ((xy)y^{-1})x^{-1} = x\cdot x^{-1} = e$ □

Définition 1.16. *Si x_1, ..., x_n sont n éléments de G, on définit* ***par récurrence*** *le produit $\Pi_{i=1}^n x_i = x_1.\Pi_{i=2}^n x_i$. On écrit aussi $\Pi_{i=1}^n x_i = (x_1\cdots x_n) = x_1\cdot(x_2\cdots x_n)$.*

Lemme 1.17. *Si $x_1, ..., x_n, ...x_{n+m}$ sont $n+m$ éléments de G, on a $(x_1\cdot\cdot x_n)(x_{n+1}\cdot x_{n+m}) = (x_1\cdots x_{n+m})$, ou $\Pi_{i=1}^{m+n} x_i = \Pi_{i=1}^n x_i \cdot \Pi_{i=n+1}^{m+n} x_i$.*

Démonstration. Par récurrence sur l'entier n. L'hypothèse de récurrence est (l'entier m est fixé).

$\mathbb{H}_{n+m}$: pour tout $(n+m)$ uplet $y_1\cdots y_{m+n}$ on a $(y_1\cdots y_n)(y_{n+1}\cdots y_{m+n}) = (y_1\cdots y_{m+n})$

Initialisation. Si $n=1$, c'est la définition de $(x_1\cdots x_m) = x_1\cdot(x_2\cdots x_m)$.
Induction. $(x_1\cdot\cdot x_n)(x_{n+1}\cdots x_{n+m+1}) = (x_1\times(x_2...x_n))(x_{n+1}...x_{m+n+1})$
$= x_1\cdot((x_2\cdots x_n).(x_{n+1}\cdots x_{m+n+1}))$
On applique l'hypothèse de récurrence $(x_2\cdot\cdots x_n).(x_{n+1}\cdot\cdots x_{m+n+1}) = (x_2\cdot\cdots x_{m+n+1})$ et la définition
$x_1\cdot(x_2\cdots x_{n+m+1}) = x_1\cdots x_{n+m+1}$. □

Le lemme précédent nous dit que **l'ordre des parenthèses importe peu**. Du coup, on les oublie :

Notation 1.18. *On note $x_1\cdots x_n$ le produit des éléments dans cet ordre ; on le note aussi $\Pi_{i=1}^n x_i$. Si x est un élément donné, x^n est $\overbrace{x.....x}^{n\text{fois}}$.*

Proposition 1.19. $(x_1\cdots x_n)^{-1} = x_n^{-1}\cdots x_1^{-1}$.

Démonstration. Par récurrence sur l'entier $n\geqslant 2$. Le cas $n=2$ (initialisation) a déjà été vu.
Pour l'étape d'induction calculons
$(x_1\cdots x_{n+1})\cdot x_{n+1}^{-1}\cdot x_n^{-1}\cdots x_1^{-1} = (x_1\cdots x_n)\cdot x_{n+1}\cdot x_{n+1}^{-1}\cdot x_n^{-1}\cdots x_1^{-1} = (x_1\cdots x_n)\cdot x_n^{-1}\cdots x_1^{-1} = e$ □

Proposition 1.20. *Pour tout x dans G, pour tous entiers n, m, on a :*
$x^{n+m} = x^n\cdot x^m$, $(x^{-1})^n = (x^n)^{-1}$

Du coup, on note $x^{-n} = (x^n)^{-1}$, et la formule $x^{n+m} = x^n\cdot x^m$ reste vraie pour n, m dans $\mathbb{Z}$.

Proposition 1.21. *Soient a, b, c trois éléments de G. Alors l'équation $axb = c$, où x est l'inconnue, admet une unique solution $x = a^{-1}cb^{-1}$.*

Démonstration. on suppose $axb = c$. On multiplie à droite par b^{-1}, il vient $ax = cb^{-1}$, à gauche par a^{-1}, il vient $x = a^{-1}cb^{-1}$ □

On peut reformuler cette proposition.

Proposition 1.22. *Si a, b sont deux éléments fixés, la multiplication à gauche (droite) par l'élément a(b) notée L_a (R_b) définie par $L_a x = ax$ ($R_b x = xb$) sont des bijections de G.*

1.1.3 Tableaux de Cayley.

Si on a un groupe fini, dont les éléments sont $a_1, ...a_n$ on dessine souvent son tableau de Cayley qui est le tableau à $n+1$ lignes et $n+1$ colonnes suivant :

Tableau d'un groupe

	a_1	a_2	a_3				a_n
a_1	a_1^2	a_1a_2	a_1a_3				a_1a_n
a_2	a_2a_1	a_2^2	a_2a_3				a_2a_1
a_3	a_3a_1	a_3a_2					a_3a_n
a_{n-1}	$a_{n-1}a_1$	$a_{n-1}a_2$	$a_{n-1}a_3$				$a_{n-1}a_n$
a_n	a_na_1	a_na_2	a_na_{13}				a_na

Sauf idée saugrenue, il est logique de mettre l'élément neutre en a_1.

Le tableau de $\mathbb{Z}/n\mathbb{Z}$

	0	1	2				$n-1$
0	0	1	2	3			$n-1$
1	1	2	3				0
2	2	3					1
3	3						2
$n-2$	$n-2$	$n-1$	0				
$n-1$	$n-1$	0	1	2			$n-2$

Proposition 1.23. *Le tableau de Cayley d'un groupe est « magique » : chaque élément du groupe apparait une fois et une seule dans chaque ligne et chaque colonne.*

Démonstration. En effet la multiplication à gauche par un élément est une bijection donc chaque ligne contient une fois et une seule chaque élément de g, et comme la multiplication à droite par un élément donné est aussi une bijection il en est de même de chaque colonne. □

Si on part d'un groupe quelconque ayant par exemple 8 éléments, on peut fabriquer un tableau magique très compliqué en appelant ces éléments avec des nombres bizarres $(3,5,7,11,13,17,19,23)$ et obtenir un tableau magique ou l'on voit ces nombres une fois et une seule dans chaque ligne et chaque colonne. Il n'est pas si facile que cela de fabriquer des tableaux magiques sans cette méthode..

Définition 1.24. *L'ordre d'un groupe fini est son cardinal. On le note par une valeur absolue* $|G|$.

Le groupe $\mathbb{Z}/n\mathbb{Z}$ a exactement n élément : il est donc bien caractérisé par son ordre.

Remarque 1.25. En théorie des groupes finis, le cardinal d'un ensemble X se note souvent $|X|$.

1.1.4 Homomorphismes.

Proposition 1.26. *Soit* $f: G \to H$ *un homomorphisme de groupe.*

1. $f(e) = e$
2. $f(x^{-1}) = f(x)^{-1}$
3. $f(x_1 \cdot \cdot x_n) = f(x_1) \cdot \cdot f(x_n)$
4. Pour tout entier $n \in \mathbb{Z}$, $f(x^n) = f(x)^n$

Avertissement 1.27. On a noté de la même façon l'élément neutre e de la source G et celui du but H. Par ailleurs, on n'a pas écrit les quantificateurs (universels) qui ont été utilisé, ainsi, la ligne 3 devrait s'écrire :

$$\forall n \in \mathbb{N}^*,\ \forall x = (x_1, ..., x_n) \in G^n\ f(\Pi_{i=1}^n x_i) = \Pi_{i=1}^n f(x_i).$$

Il n'est pas sûr que cela aide beaucoup à comprendre.

Démonstration.
1. On a $f(e)=f(e.e)=f(e).f(e)$. En simplifiant, $f(e)=e$
2. $e=f(e)=f(x.x^{-1})=f(x).f(x^{-1})$, donc $f(x^{-1})$est l'inverse de $f(x)$
3. Par récurrence sur l'entier n. L'hypothèse de récurrence étant
H_n; Pour tout entier n et tout n-uplet $x_1...x_n$ on a
Le cas $n=2$ est la définition du mot « homomorphisme ». Pour l'étape d'induction, on écrit alors $f(x_1\cdot\cdots.x_n)=f((x_1\cdots x_{n-1})\cdot x_n)=f(x_1\cdot\cdots.x_{n-1})\cdot f(x_n)=_{H_{n-1}}f(x_1)\cdot f(x_2)\cdot\cdots f(x_n)$
4 On spécialise $x_i=x$ si $n>0$, $x_i=x^{-1}$ si $n<0$.

□

Corollaire 1.28. *Si $x\in G$, l'application $\mathbb{Z}\to G$ définie par $f(n)=x^n$ est un homomorphisme.* □

Définition 1.29. *Un isomorphisme est un homomorphisme bijectif.*
Un automorphisme de G est un isomorphisme de G avec lui même.
Un endomorphisme est un homomorphisme de G dans lui même.

Proposition 1.30. *Si $\varphi: G\to H$ est un isomorphisme, son inverse est un homomorphisme.*

Démonstration. On calcule $\varphi(\varphi^{-1}(y_1)\varphi^{-1}(y_2))=y_1y_2$. Donc, comme φ est injective, $\varphi^{-1}(y_1)\varphi^{-1}(y_2)=\varphi(y_1y_2)$ □

1.1.5 Conjugaison externe et conjugaison.

Théorème 1.31. *Si X et Y sont deux ensemble et $f: X\to Y$ une bijection, alors $S(X)$ et $S(Y)$ sont isomorphes. Plus précisément par l'application $f_*: S(X)\to S(Y)$ définie par $f_*(\sigma)=f\circ\sigma\circ f^{-1}$ est un isomorphisme. Si f^{-1} est l'inverse de f, l'inverse de f^* est f^{-1*}.*

$$\begin{array}{rccc} f: & X & \to & Y \\ & \sigma\uparrow & & \downarrow\ f_*(\sigma) \\ & X & \leftarrow & Y\ : f^{-1} \end{array}$$

Démonstration. $f_*(\sigma\circ\sigma')=f\circ\sigma\circ\sigma'\circ f^{-1}=f\circ\sigma\circ f\circ f^{-1}\circ\sigma'\circ f=f_*(\sigma)\circ f_*(\sigma')$. Donc f_* est un homomorphisme.
On a $f\circ\sigma\circ f^{-1}=\tau$ si et seulement si $\sigma=f^{-1}\circ\tau\circ f$, donc $f_*(\sigma)=\tau$ si et seulement si $f_*^{-1}(\tau)=\sigma$, donc l'inverse de f_* est bien f_*^{-1}. □

Définition 1.32. *L'isomorphisme ainsi défini s'appelle la conjugaison par f. Si on veut se souvenir que les deux ensembles sont différents on ajoute le terme « externe ».*

Dans la pratique les ensembles X et Y ont des structures. Par exemple ce sont des espaces vectoriels, ou alors des espaces affines. On suppose alors que f est un isomorphisme de ces structures et alors f_* induit un isomorphisme des groupes préservant ces structures. Tout ceci est abstrait, mais trè sfacile et souvent oublié dans la littérature, donnons quelques exemples.

Exemple 1.33. Si X est un ensemble fini de cardinal n, une bijection de X et de $[\![1,.,n]\!]$ est juste une *numérotation* des éléments de X. Après cette numérotation on peut identifier $S(X)$ et S_n. Mais cette identification dépend de la numérotation choisie.

Exemple 1.34. Espaces euclidiens. Soient E, F deux espaces vectoriels euclidien, et f une isométrie bijective entre ces deux espaces. Alors l'application $O(E)\to O(F)$ définie par $f_*(l)=flf^{-1}$ est un isomorphisme. Prenons l'exemple de la dimension 3. Alors les isométries de E sont soit des réflexions par rapport à un plan, soit des rotation d'angle $\alpha\in[0,\pi]$. En fait (exercice) une réflexion de E est toujours conjuguée à une réflexion de F et des rotation d'angles α et β de E et F sont conjuguées si et seulement si $\alpha=\beta$.

Exemple 1.35. Si P_1 et P_2 sont deux plans euclidiens, C_1 et C_2 deux carrés de P_1 et P_2 il existe une similitude $f\colon P_1 \to P_2$ qui transforme C_1 en C_2. Alors la conjugaison par f induit un isomorphisme entre les groupes d'isométries des plans P_i qui conservent les carrés C_i.

Exemple 1.36. Espaces vectoriels. Soient E et F deux espaces vectoriels de dimension finie et f un isomorphisme. Alors l'application $\mathrm{GL}(E) \to \mathrm{GL}(F)$ définie par $f_*(l) = fl f^{-1}$ est un isomorphisme.

Le cas particulier ou $F = \mathbb{R}^n$ est bien connu si $f\colon E \to \mathbb{R}^n$ est un isomorphisme il existe une unique base B de E telle que $f(x)$ soit les coordonnées de x dans cette base. Alors $fl f^{-1} \in \mathrm{Gl}(\mathbb{R}^n)$ n'est autre que la matrice de l dans cette base.

Corollaire 1.37. *Si $\sigma \in S(X)$ l'application de $S(X)$ dans lui même définie par $\varphi_\sigma(x) = \sigma x \sigma^{-1}$ est un automorphisme, apppelé conjugaison par σ.*

Ce fait est très général

Proposition 1.38. *Soit G un groupe, et $\sigma \in G$. L'application $G \to G$ définie par $\varphi_\sigma(x) = \sigma x \sigma^{-1}$ est un automorphisme. On l'appelle la **conjugaison** par σ.* □

Définition 1.39. *Deux éléments x, y d'un groupe sont conjugués si il existe un troisième élément z de ce groupe tel que $y = z.x\,z^{-1}$.*

Proposition 1.40. *Être conjugué est une relation d'équivalence dont les classes d'équivalence sont appelées les classes de conjugaison.*

Démonstration. Associativité si $x = \sigma y \sigma^{-1}$ et $y = \tau z \tau^{-1}$ alors $x = (\sigma\tau) z (\sigma\tau)^{-1}$.
Symétrie si $x = \sigma y \sigma^{-1}$ et $y = \sigma^{-1} x \sigma$
Réflexivité $x = e\,x\,e$. □

Avertissement 1.41. L'un des grands faits de la théorie des groupes est que deux éléments qui sont conjugués dans un groupe ont exactement les mêmes propriétés.

Exemple 1.42. Classes de conjugaison dans $\mathrm{GL}(n, \mathbb{R})$: Deux matrices sont conjuguées si elles représentent la même application linéaire dans deux bases différentes.

Deux rotations de SO(3) sont conjuguées si et seulement si elles ont le même angle. Plus précisément si ρ est la rotation d'angle θ autour de l'axe orienté $\vec{u}$ $g\rho g^{-1}$ est la rotation de même angle autour de l'axe $g\,\vec{u}$.

Deux symétries de l'espace vectoriel E sont conjuguées si et seulement si la dimension des points fixes de l'un est la même que celle de l'autre.

Deux homothéties sont conjuguées dans le groupe affine si et seulement si elles ont le même rapport. Deux translations de vecteur non nul sont toujours conjuguées.

1.1.6 Automorphismes et automorphismes intérieurs.

Proposition 1.43. *L'ensemble des automorphismes d'un groupe G est un groupe. On le note* $\mathrm{Aut}(G)$.

Démonstration. Le point déliucat à vérifier est que l'inverse d'un automorphisme est un atormorphisme, mais on l'a déjà fait. □

Définition 1.44. *Un automorphisme φ de G est dit intérieur si il existe un élément g tel que φ soit la conjugaison par g.*

Proposition 1.45. *L'ensemble des automorphismes intérieurs est un sous groupe de* $\mathrm{Aut}(G)$ *c'est l'image de l'homomorphisme* $G \to \mathrm{Aut}(G)$ *définie par* $\psi(g) = \text{conjugaison par } g$.

Démonstration. Il s'agit de démontrer que ψ est un homomorphisme. Mais $\psi(\mathrm{gh})(x) = (gh)x(\mathrm{gh}^{-1}) = g(hxh^{-1})g^{-1} = \psi(g)(\psi(h)(x)) = (\psi(g) \circ \psi(h))(x)$. □

1.2 Sous-groupes, groupes cycliques, produits et quotients.

1.2.1 Sous-groupes.

La plupart du temps, les groupes de la nature apparaissent comme **sous-groupes**.

Définition 1.46. *Soit H un sous ensemble du groupe G. On dit que H est un sous-groupe si la loi de composition interne envoie $H \times H$ dans H et si sa restriction à H est une structure de groupe.*

Proposition 1.47. *Les propriétés sont équivalentes :*

i. H est un sous-groupe de G

ii. H contient l'élément neutre e, est stable par la loi de composition interne et par passage à l'inverse

iii. H est non vide, et pour tout couple x, y d'éléments de H, $x^{-1}y$ est un élément de H.

Notation 1.48. *On écrit $H < G$ pour signifier que H est un sous-groupe de G.*

Exemple 1.49. Le groupe des transformations affines de la doite réelle $\mathbb{R}$ $x \to ax + b$ est un **sous-groupe** du groupe des bijections de $\mathbb{R}$.

Théorème 1.50. *Les sous-groupes de $(\mathbb{Z}, +)$ sont 0, et les $n\mathbb{Z}$.*

Démonstration. Soit $G < \mathbb{Z}$ un sous groupe non réduit à 0, et soit n son plus petit élément strictement positif. Comme $n \in G$, pour tout entier q $qn \in G$ donc $n\mathbb{Z} < G$. Si $g \in G$ on écrit la division euclidienne de g par n: $g = nq + r$ avec $r \in [\![0, n-1]\!]$ Comme $r = g - q.n$, $r \in G$ et comme n est le plus petit élément de G non nul, il résulte que $r = 0$ et $g \in n\mathbb{Z}$ □

Exemple 1.51. Venant de la géométrie euclidienne.

Soit A un plan (ou un espace) affine euclidien.

Le groupe affine est le **sous-groupe** du groupe des bijections de A qui conserve la colinéation (théorème fondamental de la géométrie affine).

Définition 1.52. *Le groupe des symétries d'un objet donné est le sous-groupe du groupe des isométries conservant cet objet.*

Exemple 1.53. Le groupe des symétries du triangle isocèle est un groupe à 6 éléments. Si on note a, b, c les trois sommets il a autant d'éléments qu'il y a de permutations de ces trois éléments.

Question 3. Tient ce groupe ne dépend pas beaucoup du triangle...

Ecrire une conjugaison dans le groupe affine entre le groupe des symétries du triangle T_1 et celui du triangle T_2.

Exemple 1.54. Le groupe des translations de A est un sous groupe du groupe des transformations affines de A.

Le groupe des symétries du polygone régulier à n cotés, est un sous groupe du groupe des isométries du plan, il s'appelle le groupe diédral.

Le groupe des **similitudes** est un sous-groupe du groupe des transformation affines du plan qui conserve les angles.

Exemple 1.55. Venant de l'algèbre linéaire. Le groupe des matrices triangulaires supérieures avec des 1 sur la diagonale, le groupe $O(n)$; le groupe $\mathrm{SL}(n,\mathbb{R})$ sont des sous-groupes du groupe linéaire.

Proposition 1.56. *L'intersection de deux sous-groupes, on plus généralement d'une famille de sous-groupes est un sous-groupe.*

Proposition 1.57. *Si $\varphi: G \to H$ est un homomorphisme l'image de tout sous-groupe de G est un sous-groupe de H. L'image réciproque de tout sous groupe de H est un sous groupe de G.*

Démonstration. Image. Il s'agit de vérifier que si h_1 et h_2 sont dans $\mathrm{im}(G)$, $h_1^{-1}h_2$ l'est aussi. Pour cela choisissons deux antécédants g_1 et g_2. Alors $h_1^{-1}h_2 = \varphi(g_1^{-1}g_2)$ est bien dans l'image.

Image réciproque. Is'agit de vérifier que si g_1 et g_2 ont leur image dans le sous groupe K, $g_1^{-1}g_2$ l'est aussi. Or $\varphi(g_1^{-1}g_2) = \varphi(g_1)^{-1}\varphi(g_2)$ est bien dans K. □

Définition 1.58. *Le noyau, noté* $\ker\varphi$ *d'un homomorphisme $\varphi: G \to H$ est $\varphi^{-1}(e)$, son image* $\mathrm{im}(\varphi)$ *est $\varphi(G)$.*

Le noyau est bine un sous)groupe, comme image réciproque du sous groupe $(e\}$ de H.

Exemple. $\varphi: \mathbb{Z} \to G$ définie par $\varphi(n) = g^n$ est un homomorphisme. Son noyau est de la forme $n\mathbb{Z}$.

Proposition 1.59. *L'homomorphisme $\varphi: G \to H$ est injectif si et seulement si son noyau est réduit à $\{e\}$.*

Démonstration. On a $\varphi(g) = \varphi(h)$ si et seulemnt si $\varphi(g^{-1}h) = e$ si et seulement si $g^{-1}h \in \ker\varphi$. On démontre le résultat en passant à la contraposée.

Si φ n'est pas injective ont peut trouver deux élémnets distincts g, h dan sle noyau. Alors $g^{-1}h$ est un élément du noyau qui n'est pas e. Si le noyau n'est par réduit à $\{e\}$ il existe au moins deux élément dnt l'image par φ est e et φ n'est âs injective. □

1.2.2 Groupes cycliques (engendrés par un élément).

Définition 1.60. *Soit $g \in G$ on rappelle que $\mathbb{Z} \to G$ définie par $\varphi(n) = g^n$ est un homomorphisme. Son image s'appelle le groupe cyclique engendré par g.*

Réciproquement,

Définition 1.61. *Le plus petit entier positif (éventuellement infini) pour lequel $g^n = e$ s'appelle l'ordre de g.*

Exemple 1.62. Soit $\varphi = \mathbb{Z}/n\mathbb{Z} \to G$ un homomorphisme injectif. Posons $g = \varphi(\bar{1})$ alors $g^n = \varphi(\bar{0}) = e$ et g est d'ordre n.

Lemme 1.63. *Soit g un élément d'ordre n. Posons $\varphi: \mathbb{Z} \to G$ $\varphi(k) = g^k$. Alors* $\ker\varphi \supset n\mathbb{Z}$ *et φ passe au quotient en un homomorphisme $\bar{\varphi}: \mathbb{Z}/n\mathbb{Z} \to G$ tel que $\bar{\varphi}(\bar{1}) = g$.*

Passe au quotient veut dire que $\varphi = \bar{\varphi} \circ q$ ou $q: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est la réduction modulo n.

Démonstration. Notons que $\varphi(k+qn)=g^k.(g^n)^q=\varphi(k)$, donc si $k\equiv l(n)$ $\varphi(k)=\varphi(n)$ ce qui veut dire qu'il existe une unique application $\bar{\varphi}$ telle que $\bar{\varphi}\circ q=\varphi$. Soit $a,b\in\mathbb{Z}/n\mathbb{Z}$ et k,l tels que $\bar{k}=a$, $\bar{l}=b$, alors $\overline{k+l}=a+b$ donc $\bar{\varphi}(a+b)=g^{k+l}=g^kg^l=\bar{\varphi}(a)\bar{\varphi}(b)$ et $\bar{\varphi}$ est bien un homomorphisme. □

Théorème 1.64. *Soit $\varphi:\mathbb{Z}\to G$ définie par $\varphi(k)=g^k$.*

1. *φ est injective si et seulement si l'ordre de g est infini.*
2. *Si φ n'est pas injective, soit $n\in\mathbb{N}^*$ tel que $\ker(\varphi)=n\mathbb{Z}$. Alors φ passe au quotient en un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ et du groupe engendré par g (l'image de φ).*
3. *L'ordre de g est le cardinal du groupe engendré par φ.*

Démonstration. Si φ n'est pas injective, le noyau de φ est de la forme $n\mathbb{Z}$, pour un certain n. Montrons que sa restriction a $[\![0,n-1]\!]$ est bijective.

Surjectivité. Si $a\in\mathbb{Z}$, on écrit $a=qn+r$, avec $r\in[\![0,n-1]\!]$. Alors $\varphi(a)=\varphi(r)$ car $\varphi(n)=e$.

Injectivité si a, b sont dans $[\![0,\ n-1]\!]$ leur différence $b-a$ aussi et $\varphi(b-a)=0$ implique $b-a\in\ker(\varphi)\cap[\![0,n-1]\!]=\{0\}$ autrement dit $a=b$.

Ainsi les éléments $\varphi(0)\varphi(1),\varphi(n-1)$ sont tous distincts et forment $\varphi(\mathbb{Z})$. L'ordre de ce groupe est bien n.

Le point 1 en résulte, car si φ est injective son image est infinie. Le point 3 aussi. Pour démontrer le point 2, on a déjà vu que φ passe au quotient. L'application induite est bijective car elle est évidemment surjective (puisque φ l'est) et que les deux ensembles ont même cardinal. □

Définition 1.65. *On dit qu'un groupe est cyclique si il est engendré par un élément.*

Remarque 1.66. Certains auteurs -français uniquement- parlent de groupe *monogène* au lieu de groupe cyclique.

Remarque 1.67. Le mot cyclique n'est pas anodin. Si on considère une rotation dans le plan d'angle $\alpha\in[0,2\pi[$ on peut se demander quel est son ordre. En bien si $\frac{\alpha}{2\pi}=\frac{p}{q}$ avec p,q deux entiers premiers entre eux, cette rotation est d'ordre q. Par contre si $\frac{\alpha}{2\pi}\notin\mathbb{Q}$ cette rotation est d'ordre infini.

Exemple 1.68. Le groupe $(\mathbb{Z},+)$ est engendré par 1 (ou par -1) ; cet élément est d'ordre infini. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est engendré par la classe $\bar{1}$ et cet élément est d'ordre n.

Exemple 1.69. Le groupe $\mathbb{U}_n<\mathbb{C}^*$ des racines n-ième de l'unité est cyclique engendré par $e^{2i\pi/n}$.

Le point 3 du théorème précédent donne la classification des groupes cycliques dit que **-à isomorphisme près-** il n'y a qu'un seul groupe cyclique d'ordre n. Elle est basée sur la classification des sous-groupes de $\mathbb{Z}$ déjà vue au théorème précédent.

Proposition 1.70. *Un groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Exemple 1.71. Le groupe des coupages d'un jeu de carte est isomorphe à groupe cyclique d'ordre 52. Pourquoi ?

Les groupes cycliques ont des tas de propriétés très faciles et amusantes.

Théorème 1.72.
1. *Tout sous groupe d'un groupe cyclique est cyclique.*
2. *L'ordre d'un sous groupe d'un groupe cyclique fini divise l'ordre de ce groupe.*
3. *Si G est un groupe cyclique d'ordre n fini et si $d|n$, G contient un unique sous groupe d'ordre d*

Démonstration.

Pour faire cette démonstration nous allons utiliser les isomorphismes de G avec $\mathbb{Z}/n\mathbb{Z}$ et avec $\mathbb{U}_n$.

Si G est cyclique d'ordre infini, il est isomorphe à $\mathbb{Z}$ et les sous groupes de $\mathbb{Z}$ sont 0 et les $d\mathbb{Z}$ d'ordre 1 et ∞. Ils sont bien cycliques.

Si G est fini d'ordre n, il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$

Soit $\varphi: \mathbb{Z} \to G$ un homomorphisme de noyau $n\mathbb{Z}$, ou n est l'ordre de G, surjectif. Soit $H < G$ un sous groupe. Le groupe $\varphi^{-1}(H)$ est un sous groupe de $\mathbb{Z}$, donc de la forme $a\mathbb{Z}$. Dons $\mathbb{H}$ est l'image surjective de $a\mathbb{Z}$ (engendré par a) et est bien cyclique. De plus $H = a\mathbb{Z}/n\mathbb{Z} = a\mathbb{Z}/ad\mathbb{Z} = \mathbb{Z}/d\mathbb{Z}$, et son ordre divise bien celui de G. Ceci prouve 1 et 2.

Pour 3. Notons que soit d un diviseur de n. Le groupe $\mathbb{U}_d$ des racines $d-$ièmes de l'unité $\{z \in \mathbb{C}^* / z^d = 1\}$ est contenu dans le groupe des racines n-ièmes de l'unité, car $z^d = 1 \Rightarrow z^n = 1$. Donc $\mathbb{U}_n$ contient un sous groupe d'ordre d. Montrons qu'il est unique. Si $G < \mathbb{U}_n$ d'ordre d, comme celui-ci est cyclique (d'après 1) il est constitué d'éléments tels que $z^d = 1$ est c'est donc $\mathbb{U}_d$. □

Corollaire 1.73. *Dans un groupe cyclique d'ordre n, si d divise n il y a exactement d éléments tels que* $x^d = 1$

1.2.3 Groupes produits.

Si G_1 et G_2 sont deux groupes on fabrique le produit $G_1 \times G_2$ qui est l'ensemble des couples (g_1, g_2) muni de la loi de composition bête. Ce truc est un groupe.

Proposition 1.74. *Les applications* $G_1 \to G_1 \times G_2$ $g_1 \to (g_1, e)$ *et* $G_2 \to G_1 \times G_2$ $g_2 \to (e, g_2)$ *sont des homomorphismes injectifs.*

Les applications $G_1 \times G_2 \to G$ $(g_1, g_2) \to g_1$ *et* $G_1 \times G_2 \to G_2$ $(g_1, g_2) \to g_2$ *sont ds homomorphismes surjectifs. autrement dit les groupes* G_i *sont des quotients de* G

Grâce à cela on identifie souvent G_1 et G_2 aux sous groupes $G_1 \times \{e\}$ et $\{e\} \times G_2$ du produit.

Proposition 1.75. *Dans le produit* $G_1 \times G_2$ *tout élément de* G_1 *commute à tout élément de* G_2.

Proposition 1.76. *Soit G un groupe. Supposons que G contienne deux sous groupes* G_1 *et* G_2 *tels que*

$G_1 \cap G_2 = \{e\}$

Tout élément de G_1 *commute à tout élément de* G_2

Tout élément de G s'écrit comme produit d'un élément de G_1 *et d'un élément de* G_2

Alors l'application $G_1 \times G_2 \to G$ *définie par* $i(g_1, g_2) = g_1 g_2$ *est un isomorphisme*

Exemple 1.77. Considérons un ensemble X , et supposons que $X = X_1 \sqcup X_2$ est une partition. On peut considérer le sous-groupe de $S(X)$ formé des bijections qui conserve la partition $f(X_1) = X_1$.Alors $S(X) \asymp S(X_1) \times S(X_2)$

1.2.4 Sous-groupes normaux et groupes quotients

Soit G un groupe. On dit que le groupe H est un groupe quotient de G si on s'est donné un homomorphisme surjectif $\pi: G \to H$. On dit alors que H est le quotient de G par le noyau de π.

Exemple 1.78. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est le quotient de $\mathbb{Z}$ par $n\mathbb{Z}$.

Théorème 1.79. *Soient* $\pi_1: G \to H_1$ *et* $\pi_2: G \to H_2$ *deux quotients de G. Si les noyaux de* π_1 *et* π_2 *sont les mêmes, alors il existe un (unique) isomorphisme* $\varphi: H_1 \to H_2$ *tel que* $\pi_2 = \varphi \circ \pi_1$.

Démonstration. On fabrique d'abord une application φ/ Soit $h \in H$ et g, g' tel que $\pi_1(g) = \pi_1(g') = h$ comme $gg'^{-1} \in \ker \pi_1 = \ker \pi_2$, $\pi_2(gg'^{-1}) = e$, donc $\pi_2(g) = \pi_2(g')$. On défini alors $\varphi(h) = \pi_2(g)$. Pour vérifier que φ est un homomorphisme, notons que si $\pi_1(g) = h$ et $\pi_1(g') = h'$ alors $\pi_1(gg') = hh'$. Donc $\varphi(h.h') = \pi_2(gg') = \pi_2(g)\pi_2(g') = \varphi(h)\varphi(h')$. reste à établir la bijectivité de φ. Si $h \in \ker \varphi$ et si $\pi_1(g) = h$, alors $\pi_2(g) = e$ donc $g \in \ker \pi_2 = \ker \pi_1$ et $h = e$. Ce qui établi l'injectivité. Pour la surjectivité notons que π_2 est surjective, comme $\pi_2 = \varphi \circ \pi_1$, φ l'est aussi. □

Exemple 1.80. Nous avons déjà vu que si deux groupes cycliques ont même ordre ils sont isomorphes.

Définition 1.81. *Un sous groupe N de G est dit normal (ou distingué) si il est invariant par les conjugaisons intérieures. On note $N \lhd G$ pour signifier que N est un sous groupe normal de G*

Remarque 1.82. Beaucoup d'auteurs français disent « distingué », mais comme nous sommes le seul pays au monde qui utilise cette terminologie, elle tend à disparaître.

Théorème 1.83. *Soit $N \lhd G$ un sous groupe normal. Il existe groupe* noté G/N *et un quotient $\pi : G \to G/N$ de G dont N est le noyau. Celui-ci est unique d'après le théorème précédent.*

Démonstration. On définit H à partir de G et N comme on définit $\mathbb{Z}/n\mathbb{Z}$ à partir de $\mathbb{Z}$ et $n\mathbb{Z}$: On dit que $g \sim_N g'$ si $g.g'^{-1} \in N$. Alors les classes d'équivalence modulo N forment un groupe. Démontrons que si $g \sim_N g'$ et $h \sim_N h'$ alors $gh \sim_N g'h'$. En effet $g'h' = gnhn' = gh(h^{-1}nhn')$. La structure produit du quotient est ainsi définie, et il est facile de se convaincre qu'il s'agit bien d'une structure de groupe. □

Exemple 1.84. Exercice si g est une transformation affine de partie linéaire G, et t_u la translation de vecteur u. $gt_ug^{-1} = t_{G.(u)}$ Il en résulte que le groupe affine contient le groupe des translations comme sous groupe normal. Le quotient est le groupe linéaire. $\mathrm{Aff}(A) \to \mathrm{Gl}(E)$ est un homomorphisme surjectif dont le noyau est précisément le groupe E des translations de A.

Proposition 1.85. *Si $\varphi : G \to H$ est un homomorphisme, et si* $\ker f \supset N$ *alors f passe au quotient en un homomorphisme $\bar{\varphi} : G/N \to H$. Autrement dit si $\pi : G \to G/N$ est l'application quotient, $\bar{\varphi} \circ \pi = \varphi$*

Démonstration. Si deux élément de G sont congrus modulo N ils ont même image dans H. Il existe donc une unique application $\bar{\varphi} : G/N \to H$ telle que $\bar{\varphi} \circ \pi = \varphi$. Il est facile de se convaincre de cette application est un homomorphisme. □

Exemple 1.86. Le centre $Z(G)$ d'un groupe est l'ensemble des éléments qui commutent à tous les autres. Le centre est un sous-groupe normal. C'est le noyau de l'homomorphisme $G \to \mathrm{Aut}(G)$ qui a un élément associe la conjugaison par cet élément. Ainsi $G/Z(G)$ est un sous groupe de $\mathrm{Aut}(G)$. On l'appelle le groupe des automorphismes intérieurs.

1.2.5 Groupe engendré par une partie.

Définition 1.87. *Si G et $A \subset G$ une partie, le groupe* engendré *par A est l'intersection de tous les sous-groupes de G contenant A.*

Proposition 1.88. *Un élément g appartient au sous groupe engendré par A si et seulement si il existe un entier n, des éléments $a_1, ..., a_n$ de A et des signes $\varepsilon_1, ...\varepsilon_n$ de $\{-1, 1\}$ tel que $g = \Pi_{i=1}^n a_i^{\varepsilon_i}$*

Démonstration. Laissée au lecteur. □

Question 4. Quel est le sous groupe du groupe de permutation de l'ensemble des 52 cartes engendré par les battages?

Exemple 1.89. Le groupe **diédral** est le groupe obtenu en mettant deux miroirs l'un à coté de l'autre faisant un angle α. Si $\alpha/\pi \in \mathbb{Q}$ ce groupe est fini, et sinon, il est infini. Par exemple si on met deux miroirs à angle droit, on obtient le groupe du carré. On peut aussi le faire en dimension 3

Exemple 1.90. Le groupe engendré par les trois réflexions le long des bord d'un triangle isocèle est le groupe des isométries du pavage triangulaire standard. On l'appelle (3, 3, 3), ou groupe du kaléidoscope. Si on identifie le plan euclidien à la droite complexe $\mathbb{C}$, il conserve le réseaux triangulaire standard Λ formé des points de la forme $\mathbb{Z} + j\mathbb{Z}$. Ici les sommets du triangle isocèle sont $1, j, j^2$.

Théorème 1.91. *Le groupe du kaléidoscope est composé des translations de vecteur dans Λ des rotations d'angle $k.2\pi/6$ autour d'un sommet de Λ et des réflexions suivant une droite de Λ.* □

Remarque 1.92. L'étude des groupes engendré par des réflexions d'un espace est un sujet très important et actuel. On appelle ces groupes les groupes de Coxeter.

1.2.6 Sous-groupe invariant, abélianisé. *.

Ce paragraphe est à faire en exercice.

Un sous groupe N d'un groupe G est normal si il est invariant par toutes les conjugaisons. Comme les conjugaisons sont des automorphismes particuliers il est naturel de regarder les sous-groupes invariants par tous les automorphismes.

Définition 1.93. *Un sous groupe N d'un groupe G est dit invariant si pour tout automorphisme ψ de G, $\psi(N) = N$*

Un sous groupe invariant est donc un sous groupe normal.

Rappelons que le centre d'un groupe G, noté $Z(G)$ est défini par :
$Z(G) = \{g \in G / \forall h \in G, gh = hg\}$.

Comme la formule $gh = hg$ implique $\psi(g)\psi(h) = \psi(h)\psi(g)$, il est facile de se convaincre de la proposition suivante.

Proposition 1.94. *Le sous groupe $Z(G)$ est invariant dans G.*

Il est souvent plus facile de démontrer qu'un sous groupe est invariant plutôt que normal.

Définition 1.95. *Le groupe dérivé d'un groupe noté $[G, G]$ est le sous groupe engendré par les commutateurs $ghg^{-1}h^{-1}$.*

Comme l'image d'un commutateur par un automorphisme est un commutateur, on a :

Proposition 1.96. *Le groupe dérivé est invariant donc normal, et le quotient G^{ab}est abélien.*

Tout homomorphisme de $G \to A$ de G vers un groupe abélien contient $[G, G]$ dans son noyau et se factorise par G^{ab}. □

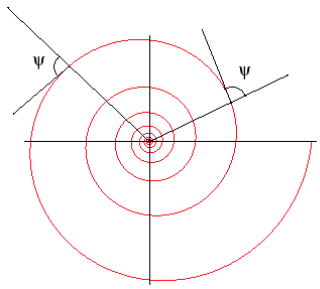
Exemple 1.97. Si $\mathbb{K}$ est un corps le groupe dérivé de $\mathrm{Aff}_1(\mathbb{K})$ est le groupe des translations, le quotient le groupe des homothéties.

1.2.7 Digression. Pavage du plan, spirale logarithmique et application exponentielle.

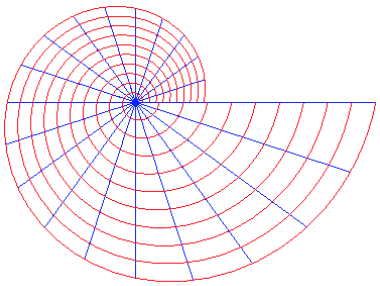
L'application exponentielle complexe est un homomorphisme de groupe $\exp: \mathbb{C} \to \mathbb{C}^*$

Cette application transforme donc la droite $x = pt, y = t$, qui est un sous-groupe de $(\mathbb{C}, +)$ en une jolie spirale qui est un sous-groupe de $\mathbb{C}^*$. $z = \exp pt. \exp(it)$. Quand on fait tourner la courbe d'un angle de 2π, on obtient la même même courbe point a point c'est comme si on avait fait une homothétie de rapport $\exp(2\pi p)$: Bernoulli trouvait ça tellement incroyable qu'il a fait graver sur cette courbe sur sa tombe avec l'explication "eadem mutata resurgo".

Ici, $z = \exp(\ln a(a)\,\theta + i\theta)$, est l'image de la droite $x = \ln(a)\,y$ du plan complexe. On voit qu'elle fait un angle constant avec les droites passant à l'origine qui sont quand à elles les images des droites horizontales : on ditq ue l'expoenetielle conserve les angles, ou est conforme.

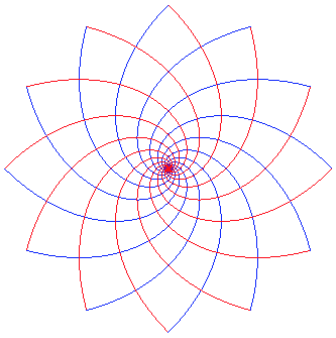


La courbe obtenue rencontre les droites passant à l'origine avec un angle constant de cotangente $1/p$. En effet, elle rencontre la droite $\mathrm{Arg}(z) = \theta$ aux points $t = \theta + 2k\pi$. En prenant le logarithme, c'est l'image de $x = py$, $y = \theta + 2k\pi$ qui font un angle constant de tangent p, et les fonctions holomorphes gardent les angles.



Si ce dessin est si joli, c'est que c'est l'image par l'application exponentielle d'un pavage du plan : les droites bleues sont les images des droites horizontales $y = y_0$, les spirales rouges des droites $y = cx + n\frac{2\pi}{6}$.

Ce dernier dessin est quand à lui l'image par l'application exponentielle de deux familles de droites orthogonales $y = ax + 2n\pi$, $y = \frac{-1}{a}x + \frac{2n\pi}{12}$. Pourquoi $\frac{2\pi}{12}$?



Ces dessins ont été pris sur le très beau site web https://mathcurve.com.

1.3 Exercices du chapitre 1

1.3.1 Définitions et premières propriétés.

Exercice 1.1. Dessiner la table de multiplication du groupe S_3 des bijections d'un ensemble à trois éléments.

Exercice 1.2. Dessiner « toutes » les tables de multiplication d'un groupe à 2,3, 4.
Ici, « toutes » veut dire à isomorphisme de groupe près.

Exercice 1.3. Rappel. Si P est un plan affine et si (A,B,C) sont trois points non alignés, ils forment un **repère affine** : tout point P du plan s'écrit d'une unique façon comme barycentre des points A,B, C :$P=xA+yB+zC$ (avec $x+y+z=1$). Démonstration les vecteurs $\overrightarrow{AB}$ et $\overrightarrow{AC}$ forment une base de l'espace vectoriel sous jacent donc $\overrightarrow{AP}=y\overrightarrow{AB}+z\overrightarrow{AC}$, soit $P=yB+zC+(1-(y+z))A=xA+yB+zC$. Une transformation affine est une transformation qui conserve les barycentre $f(xA+yB+zC)=xf(A)+yf(B)+zf(C)$

On se place dans le plan affine. Soit T un triangle (non dégénéré).
1. Montrer que le groupe des transformations **affines** qui conservent T est isomorphe au groupe des bijections de l'ensemble des trois sommets de T.
2. Soient T_1 et T_2 deux triangles, et g un transformation affine telle que $g(T_1)=T_2$. Si $G_i\subset$ Aff est le sous groupe du groupe des transformations affines qui conservent T_i, montrer que $gG_1g^{-1}=G_2$.

Exercice 1.4. Pour chacun des ensembles suivant du plan **euclidien**, déterminer l'ensemble des isométries Isom(X) le préservant, montrer que c'est un groupe et en faire le tableau de Cayley.

Triangle équilatéral, triangle isocèle non équilatéral, carré, rectangle non carré, losange non rectangle.

Si T_1 et T_2 sont deux triangles *semblables* et s une similitude entre ces deux triangles montrer que $\sigma\to s.\sigma s^{-1}$ induit un isomorphisme entre Isom(T_2) et Isom(T_1).

Exercice 1.5. On refera cet exercice en cours plus tard. Soit G un groupe fini. Démontrer que pour tout élément x, il existe deux entiers distincts tels que $x^k=x^m$, en déduire qu'il existe un entier positif n tel que $x^n=e$ et qu'il existe un entier $m\geqslant 0$ tel que $x^m=x^{-1}$.

Exercice 1.6. Si $\varphi: G\to H$ est un homomorphisme et si g est d'ordre fini n , que peut on dire de l'ordre de $\varphi(g)$?
L'ordre d'un conjugué de g est le même que celui de g.

Exercice 1.7. Soit G un groupe et Aut(G) le groupe des automorphismes de G. L'application $G\to$ Aut(G) qui à un élément g associe la conjugaison $(x\to gxg^{-1})$ est un homomorphisme.

Exercice 1.8. Soit G un groupe. On considère la relation $\sim$ définie dans G par

$$(x\sim y)\Leftrightarrow(x=y \text{ ou } x=y^{-1}).$$

Montrer que $\sim$ est une relation d'équivalence.
Montrer que tout groupe fini d'ordre pair contient un nombre impair d'éléments d'ordre 2 (et en particulier qu'il en contient au moins un).

Exercice 1.9. Soit G un groupe tel que tout élément est d'ordre 2. Montrer que G est commutatif . On note alors 0 son élément neutre, et + sa loi de groupe.
Montrer que G est muni d'une structure de $\mathbb{Z}/2\mathbb{Z}$ espace vectoriel.
Si de plus G est fini, en déduire que G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^d$, ou $d=\ln_2|G|$.
Démonter que si H est un autre groupe dont tout élément est d'ordre 2, tout homomorphisme de G vers H est $\mathbb{Z}/2\mathbb{Z}$ linéaire. En déduire le cardinal Card(Hom(G,H)). Démontrer que Aut$(G)=\mathrm{GL}_d(\mathbb{Z}/2\mathbb{Z})$

Exercice 1.10. Quels sont tous les homomorphismes de $(\mathbb{Z},+)$ dans lui même.
Soit f: $\mathbb{Q},+\to\mathbb{Q},+$ un homomorphisme. Démontrer que $f\left(\frac{1}{m}\right)=\frac{f(1)}{m}$. En déduire tous les homomorphismes de $(\mathbb{Q},+)$ dans lui même.
Quels sont tous les homomorphismes **continus** de $(\mathbb{R},+)$ dans lui même.
Soit φ: $(\mathbb{R},+)\to\mathbb{C}^*,\times$ un homomorphisme continu. Démontrer qu'il existe un nombre complexe α tel que $\varphi(t)=\alpha^t$

Exercice 1.11. Le groupe affine de la droite.
Soit $\mathbb{K}$ un corps. On considère l'ensemble des transformations affines inversibles de $\mathbb{K}$, c'est-à-dire les transformations de la forme $z\to\lambda z+b$, ou $\lambda\in\mathbb{K}^*$, $a\in\mathbb{K}$. Montrer que Aff_1 est un groupe et que l'application de $\mathrm{Aff}_1\to\mathbb{K}^*$ qui a une transformation $z\to\lambda z+a$ associe sa partie linéaire $z\to\lambda z$est un homomorphisme ; quel est son noyau? Montrer que le groupe Aff_1 n'est jamais commutatif, sauf si $\mathbb{K}=\mathbb{Z}/2\mathbb{Z}$.
Montrer que le conjugué de la translation $z\to z+a$ par $z\to\lambda z+b$ est une translation

Exercice 1.12. Soit A un espace affine et E l'espace vectoriel sous-jacent. Montrer que l'application qui à une transformation affine bijective associe sa partie linéaire est un homomorphisme de groupe.

Montrer que le conjugué de la translation de vecteur u par la transformation affine g est la translation de vecteur $G(u)$ ou G est la partie linéaire de g.

Montrer que deux translations de vecteur non nul sont toujours conjuguées dans le groupe affine.

Si h est une homothétie de centre O et rapport λ, montrer que ghg^{-1} est une homothétie. Quelle est son centre et son rapport.

Montrer que deux homothéties sont conjuguées si et seulement si elles ont le même rapport.

Exercice 1.13. Si p est un nombre premier, et $n \in \mathbb{N}$, on pose $v_p(n)$ la plus grande puissance de p qui divise n. Si $x = \frac{a}{b} \in \mathbb{Q}_+$, on pose $v_p(x) = v_p(a) - v_p(b)$. Démontrer que $v_p = \mathbb{Q}_+^* \to \mathbb{Z}$ est un homomorphisme.

En déduire que $\left(\mathbb{Q}_+^*, \times\right)$ est isomorphe à $\oplus_{p \in \Pi} \mathbb{Z}$. Ce $\oplus$ veut dire les suite finies de nombres entiers nulles après un certain rang.

Exercice 1.14. On veut « simplifier » la liste des axiomes de groupes. On suppose que l'ensemble G est muni d'une loi de composition interne associative qui admet un élément neutre « à droite » e c'est à dire que pour tout x $x.e = x$, et tel que tout élément soit inversible à droite, c'est à dire que pour tout x il existe un élément x' tel que $x.x' = e$. Démontrer que $(G, .)$ est un groupe.

Exercice 1.15. Soit G un groupe fini. Montrer que, sauf si G a un ou deux éléments G admet un automorphisme. Se ramener au cas ou G est abélien, puis utiliser l'exercice 9.

Exercice 1.16. Soit G un groupe fini, et φ un automorphisme. On suppose que pour strictement plus que la moitié des éléments $\varphi(x) = x^{-1}$. Démontrer que $\varphi \circ \varphi = \mathrm{Id}_G$.

Exercice 1.17. Soit G un groupe d'ordre n, peut on trouver une suite d'éléments (pas forcément distincts) a_1, $a_2, ...a_n$ tels qu'aucun des produits $b_{k,l} = a_k a_{k+1} .... a_l$ soient égaux à e.

1.3.2 Sous groupes, groupe cycliques, quotients

Exercice 1.18. Montrer que l'ensemble des nombres complexes de la forme $n\sqrt{2} + m\left(\frac{3 + i\sqrt{41}}{739}\right)$, avec n,m dans $\mathbb{Z}$ forme un sous groupe de $(\mathbb{C}, +)$

Soit A, + un groupe abélien et α_1, ..., α_n des éléments de A . Montrer que l'ensemble des combinaisons linéaires à coefficients entiers des α_i forme un sous-groupe de A.

Exercice 1.19. Démontrer que les sous-ensembles suivant de l'ensembles des matrices carrée $M_2(\mathbb{C})$ sont des sous-groupes.

-Les matrices triangulaires supérieures avec des 1 sur la diagonale.

-Les matrices triangulaires supérieures avec des coefficients diagonaux non nuls

-Les matrices à coefficients dans $\mathbb{Z}$ et de déterminant 1 ou -1

-Les matrices de déterminant 1

-Les matrices réelles orthogonales.

-Les matrices de $M_2(\mathbb{C})$ de la forme $\begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix}$, avec $|a|^2 + |b|^2 \neq 0$

* Mêmes questions avec $M_n(\mathbb{C})$ au lieu de $M_2(\mathbb{C})$

Exercice 1.20. Si X est un ensemble et $f : X \to Y$ est une fonction, montrer que l'ensemble des bijections de X qui conservent f (c'est à dire $f \circ s = f$) est un groupe.

Si q est une forme quadratique non dégénérée sur un espace vectoriel de dimension finie, montrer que l'ensemble des transformations linéaires qui préserve q est un sous groupe du groupe linéaire (attention on ne suppose pas a priori que la transformation est inversible).

L'ensemble des isométries *inversibles* d'un espace métrique est un groupe.

* L'ensemble des isométries d'un espace métrique **compact** est un groupe.

* L'ensemble des isométries de l'espace de Hilbert n'est pas un groupe.

Exercice 1.21. L'ensemble des similitudes est un groupe.

L'ensemble des similitudes **directes** du plan euclidien est isomorphe au groupe affine de la droite complexe.

Le sous-groupe des similitudes directes est un sous-groupe normal du groupe des similitudes et le quotient est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ (considérer l'application $s \to$ le signe du déterminant de la partie linéaire de s.

Exercice 1.22. Dans le $\mathrm{GL}(2, \mathbb{C})$, quel est l'ordre (éventuellement infini) des matrices suivantes ?

$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -2+3i & -2+2i \\ 1-i & 3-2i \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$

Exercice 1.23. On considère un jeu de 52 cartes posé sur la table. Pour les mélanger on utilise juste des coupes : on coupe le paquet en deux parties (pas forcément égales) et on pose le tas du dessous au dessus. En répétant autant de fois qu'on veut l'opération, on obtient ainsi un groupe. Quel est il ?

Exercice 1.24. Si G est un groupe cyclique d'ordre n et k un entier qui divise n. En utilisant un isomorphisme avec le groupe des racines $n-$ièmes de l'unité, montrer que G contient exactement k éléments tels que $x^k = 1$.

Dans un groupe cyclique d'ordre 15, combien d'élément d'ordre exactement 1, 3 ou 5 ?

Dans un groupe d'ordre 77 combien y a t il d'éléments d'ordre exactement 77.

Exercice 1.25. Démontrer que le groupe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ n'est pas cyclique.

Exercice 1.26. Soit G un groupe cyclique d'ordre n impair. Démontrer que l'application $G \to G$ définie par $\varphi(x) = x^2$ est un isomorphisme. Montrer que ce n'est pas le cas si n est pair.

Exercice 1.27. Soit $g \in \mathrm{GL}_2(\mathbb{R})$ une matrice. On suppose que g est d'ordre fini. Montrer que $\det(g)$ vaut 1 ou -1. Si $\det(g) = -1$, alors en fait g est une symétrie (on pourra vérifier que g est diagonalisable).

Exercice 1.28. Si $g \in \mathrm{GL}_n(\mathbb{C})$ une matrice d'ordre fini, alors g diagonalisable et ses valeurs propres sont des racines de l'unité. Etudier la réciproque.

Classer les matrices d'ordre fini à conjugaison près dans $\mathrm{GL}(n,\mathbb{C}), \mathrm{SU}(n,\mathbb{C})$.

Exercice 1.29. Soit x un élément d'ordre n d'un certain groupe. Montrer que les éléments $e, x, x^2, ..., x^{n-1}$ sont tous distincts, et que $(x^k)^{-1} = x^{n-k}$.

Si x est d'ordre infini, alors tous les x^n sont distincts.

Exercice 1.30. Soit, G un groupe, u, v, x trois éléments de G, p, q deux entiers premiers entre eux. On suppose que u et v commutent et que $uv = vu = x$, puis que $u^p = x$, $v^q = x$. Démontrer que le groupe engendré par x est fini. Démontrer qu'il existe deux entiers p', q' tels que $u = x^{p'}, v = x^{q'}$.

Exercice 1.31. On considère le sous ensemble $\mathbb{H}$ de $M_2(\mathbb{C})$ formé des matrices $\begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix}$. Montrer que les sous ensembles suivants de $\mathbb{H}$ sont des groupes.

$\mathbb{H}^* = \mathbb{H} \backslash 0$

$S = \{q \in \mathbb{H} / \det q = 1\}$. En déduire que la sphère unité de l'espace euclidien de dimension 4 est munie d'une structure de groupe

Soit $\mathbb{H}_8 = \{\pm \mathrm{Id}, \pm I, \pm J, \pm K\}$, où $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, K = IJ = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$

Le groupe $\mathbb{H}_8$ est il-isomorphe au groupe $\mathbb{D}_{2\times 4}$?

Exercice 1.32. Soit E un espace vectoriel euclidien de dimension finie. On veut démontrer que tout élément du groupe orthogonal $O(E)$ est produit d'au plus $n-1$ réflexions. On rappelle qu'une réflexion par rapport à l'hyperplan h est la transformation qui vaut Id sur h et dont la restriction à la droite orthogonale $h^\perp$. Soit $B = (e_1, ...e_n)$ une base orthonormée de E et g un élément de $O(E)$.

On suppose que la dimension de Eg est $\geqslant 2$ et que $g(e_n) \neq e_n$. Construire une réflexion σ telle que $\sigma \circ g$ fixe e_n.

Conclure par récurrence sur la dimension.

Exercice 1.33. Soit E un espace vectoriel de dimension fini, $F \subset E$ un sous espace, et $G = \{g \in \mathrm{GL}(E) \,/\, g(F) = F\}$. Montrer que G est un sous groupe de $\mathrm{GL}(E)$.

Construire un homomorphisme surjectif $G \to \mathrm{GL}(F)$

Soit $H \subset G$ le sous groupe formé des éléments dont la restriction à E est l'identité. Montrer que H est normal dans G et montrer que G/H est le groupe des transformations linéaires de F.

Exercice 1.34. Soient G un groupe, $H < G$ un sous groupe et N un sous groupe normal de G, et $p : G \to G/N$ le quotient.

Démontrer que le sous-ensemble HN formé des produits d'un élément de H et d'un élément de N est un sous-groupe de G.

Démontrer que $HN = NH$

Démontrer que N est un sous-groupe normal de NH, et que $N \cap H$ est un sous groupe normal de H.

Démontrer que si $p : G \to G/N$ est la projection canonique, NH/N est isomorphe à $p(H)$ et à $H/N \cap H$.

Soit G le groupe des similitudes du plan euclidien, N le sous-groupe des translations. A quoi s'identifie HN, si H est le sous groupe des rotations autour de l'origine ?

Exercice 1.35. Soit G un groupe, $H \subset G$ un sous groupe. On dit que l'élément g normalise H si $gHg^{-1} = H$, et on appelle normalisateur de H, noté $N(H)$, l'ensemble des éléments qui normalisent H. Démontrer que $N(H)$ est un sous-groupe de G contenant H, et que le sous-groupe H y est normal.

Soit $X_1 \cup X_2$ une partition de l'ensemble X . Montrer que le sous groupe $S(X_1, X_2)$ de $S(X)$ qui conserve X_1 est isomorphe à $S(X_1) \times S(X_2)$.

Montrer que si g normalise ce sous groupe soit $g(S_1) = S_1$ et $g(S_2) = S_2$ soit $g(S_1) = S_2$ et $g(S_2) = S_1$

Quel est le normalisateur de $S(X_1, X_2)$? On pourra distinguer les cas ou X_1 et X_2 on même cardinal, ou pas.

Exercice 1.36. Si G est un groupe, le groupe *dérivé* de G est le sous-groupe engendré par les commutateurs, c'est -à-dire les éléments de la forme $aba^{-1}b^{-1}$. On le note $[G, G]$

Si φ est un automorphisme de G démontrer que $\varphi(aba^{-1}b^{-1}) = \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1}$.

En déduire que le groupe dérivé est normal.

On note G^{ab} le quotient $G/[G, G]$. Démontrer que G^{ab} est un groupe abélien que que si $\varphi : G \to A$ est un homomorphisme du groupe G vers le groupe abélien A , φ se factorise a travers G^{ab} c'est à dire qu'il existe un homomorphisme $\varphi' : G^{\mathrm{ab}} \to A$ tel que $\varphi = \varphi' \circ p$, ou $p : G \to G/[G, G]$ est la projection naturelle.

Démontrer que le groupe dérivé du groupe affine de la droite $\mathrm{Aff}(1, \mathbb{K})$ est le groupe des translations et que le quotient est $\mathbb{K}^*$.

Exercice 1.37. Si $N \lhd G$ est un sous groupe normal, on définit $[G, N]$ comme le sous groupe de N engendré par les éléments de la forme $gng^{-1}n^{-1}$. Démontrer que $[G, N]$ est un sous groupe normal de G. On suppose de plus que N est invariant. Démontrer que $[G, N]$ est aussi invariant.

Chapitre 2
Groupe opérant dans un ensemble

2.1 Groupes opérant dans un ensemble.

2.1.1 Introduction et exemple du groupe diédral.

Première définition : un groupe opère dans un ensemble X si on s'est donné un homomorphisme $G \to S(X)$.

La plupart du temps, un groupe est défini comme groupe opérant dans un ensemble.

Exemple 2.1. Le groupe symétrique $S(X)$ est défini comme groupe des permutations de X il opère sur X .

Exemple 2.2. Le groupe affine de E va nous servir d'exemple ; il opère non seulement dans le E mais aussi dans l'ensemble des droites, des triangles etc etc. Un transformation affine est exactement une bijection qui transforme les droites en droites. Il contient des tas de sous-groupes amusants : le groupe des homothéties, le groupe des translations, les transformations qui fixent un point (qui est le groupe linéaire) etc..

Soit Π_n un polygone régulier à n coté du plan euclidien (régulier veut dire que tous les cotés ont même longueur, et donc aussi tous les angles. On note O son centre qui est l'équibarycentre des sommets. On considère $\mathrm{Iso}(\Pi_n)$ le sous groupe du groupe des isométries du plan (ou même des transformations affines du plan) qui conserve P_n.

Proposition 2.3. *Si Π'_n est un autre polygone régulier d'un autre plan euclidien ayant le même nombre de cotés, et σ une similitude transformant Π_n en Π'_n, la conjugaison $\sigma x \sigma^{-1}$ induit un isomorphisme entre $\mathrm{Iso}(\Pi'_n)$ et $\mathrm{Iso}(\Pi_n)$. En particulier ces deux groupes sont isomorphes.*

Démonstration. Laissée au lecteur. □

Définition 2.4. *Le groupe des isométries de Π_n s'appelle le groupe diédral $\mathbb{D}_{2n}$.*

Théorème 2.5. *1. Le groupe des isométries conservant Π_n a exactement 2n éléments : les n rotations d'angle $k.\frac{2\pi}{n}$, et n symétries orthogonales, plus précisément.*

Si n est impair, par rapport aux axes Op, ou p est un sommet de Π_n.Si n est pair par rapport aux axes $\{p, -p\}$ u p est un sommet de Π_n, et aux axes $\{m, -m\}$. Ou m décrit le milieu des arêtes de Π

2. Le sous groupe des rotations est normal et son quotient est $\mathbb{Z}/2\mathbb{Z}$

3. Le groupe $\mathbb{D}_{2n}$ n'est pas commutatif. Si τ est une réflexion et ρ une rotation $\tau\rho\tau^{-1} = \rho^{-1}$.

Démonstration. Soit G ce groupe. Clairement G contient les 2n transformation décrites. Pour vérifier qu'il n'y en pas d'autre, considérons d'abord G^+ le sous groupe qui conserve l'orientation. Il opère sur l'ensemble des sommets de Π_n mais une rotation qui fixe O et 1 sommet est l'identité (on dit que l'opération est libre). Soit s un sommet et ρ la rotation qui transforme s en g.s. Alors $\rho^{-1}g$ fixe s donc c'est l'identité. Ainsi G^+ est constitué des n rotations d'angle $k.\frac{2\pi}{n}$, pour $k \in [\![0, n-1]\!]$.

Notons maintenant G^- le sous ensemble constitué des réflexions, de sorte que $G = G^+ \cup G^-$.

Choisissons σ n'importe quelle symétrie dans G. L'application $G \to G$ définie par $\varphi(g) = g.\sigma$ et bijective (elle est égale à son inverse) et interverti G^+ et G^- : il y a donc autant d'élément de G^- que d'éléments de G^+ et la liste que nous avons donnée est donc complète.

2. On donne deux démonstrations. D'abord G^+ est le noyau du déterminant. Aussi, tout sous-groupe d'indice 2 est normal .

3. Laissé en exercice : quand on se regarde dans un miroir, les aiguilles d'une montre tournent dans l'autre sens autrement dit $\tau\rho\tau^{-1} = \rho^{-1}$, si τ est une réflexion et ρ une rotation.

□

2.1.2 Terminologie : action de groupe, orbite d'un point.

Définition 2.6. *On dit que le groupe G opère/agit dans l'ensemble X si on s'est donné une application*

$$G \times X \to X$$
$$(g,x) \to g.x$$

Telle que :
pour tout triplet (g_1, g_2, x) de $G \times G \times X$, on ait $(g_1 g_2).x = g_1.(g_2.x)$
et pour tout x de X on ait $e.x = x$

Proposition 2.7. *Soit G un groupe opérant dans X*
L'application $x \to g.x$ est une bijection d'inverse $x \to g^{-1}.x$
L'application $G \to S(X)$ définie par $\varphi(g)(x) = g.x$ est un homomorphisme de groupe.

Démonstration. Comme $g^{-1}.g = g.g^{-1} = e$, on obtient le résultat. □

Réciproquement.

Proposition 2.8. *Soit G un groupe et $\varphi: G \to S(X)$ un homomorphisme. L'application d'évaluation $g.x = \varphi(g)(x)$ définit une opération de G dans X.* □

Définition 2.9. *Orbite d'un point. Si G opère dans X l'orbite du point x_0 est l'image de l'application $G \to X$ $g \to g.x_0$.*

Exemple 2.10. Le groupe des rotations autour d'un point O opère dans le plan. L'orbite d'un point est le cercle centré en O passant en ce point.

Le groupe orthogonal opère dans E_3 l'orbite d'un point est la sphère.

Proposition 2.11. *La relation $y \sim x$ si $y \in O_x$ est une relation d'équivalence. Les orbites sont les classes d'équivalence.*

Exemple 2.12. Les orbites de l'action du groupe des similitudes sur l'ensemble des triangles sont les triangles semblables.

Les orbites d'un point sous l'action d'un groupe sont des objets très jolis, parce qu'ils sont très symétriques.

Exemple 2.13. Si un groupe d'ordre 2 opère sur un ensemble dont le cardinal est impair, il y a un point fixe.

2.1.3 Équivariance.

L'équivariance est l'une des propriétés les plus importantes de la nature. Tellement importante que beaucoup de traité de théorie des groupes n'en parlent même pas tellement tout parait évident. Commençons par quelques exemples venant de la géométrie.

Exemple 2.14. Considérons le groupe affine qui opère dans le plan. il opère aussi dans les paires de points du plan (ou les triplet) et il conserve le milieu(le barycentre).

Proposition 2.15. *L'application « milieu » est affine, équivariante : si g est une application affine l'image par g du milieu de A et B est le milieu de $g(A)$ et $g(B)$.*

Démonstration. En fait une application affine est une application qui conserve les barycentres, donc en particulier les milieux. □

A titre d'application, démontrons un théorème facile de la géométrie élémentaire.

Proposition 2.16. *Soit (a,b,c) un triangle du plan, a',b',c' les milieux des cotés opposés. Alors les droites (a,a'), $(b,b')(c,c')$ sont concourantes.*

Démonstration. L'homothétie de centre a et de rapport 2 transforme c' en b et b' en c. Il transforme donc le milieu a'' de (b',c') en a' : l'intersection de $[a,a'] \cap [b',c'] = a''$

Soit $G = (b,b') \cap (c,c')$. On considère l'homothétie H de centre G et de rapport $-1/2$. Donc H transforme b en b', c en c'. Il transforme donc le milieu a' de b,c en le milieu a'' de b',c'. Mais a'' est le milieu de (a,a') □

Des tas de démonstrations sont faites -sans sans rendre compte- en utilisant l'équivariance.

Exemple : toujours le groupe des similitudes qui opère dans le plan. Si g est une similitude, g ne conserve pas les distances ni les aires, mais conserve le rapport des distances et le rapport des aires.

Plus précisément l'application $\rho : G \to \mathbb{R}^*, \times$ qui a une similitude associe la valeur absolue de son rapport de similitude est un homomorphisme de groupes. Notons d la distance entre deux point de l'espace, $A(x,y,z)$ l'aire du triangle de sommets (x,y,z), V le volume du tétraèdre (x,y,z,t)

Proposition 2.17. *Soient x,y,z,t quatre points de l'espace et g une similitude.*

Alors $d(g(x),g(y)) = \rho(g) d(x,y)$.
$A(g(x),g(y),g(z)) = \rho^2(g)\, A(x,y,z)$
$V(g(x),g(y),g(z),g(t)) = \rho^3 V(x,y,z,t)$

Avec ces exemples dans la tête, on peut formuler l'idée d'équivariance.

Définition 2.18. *Soit G, H deux groupe opérant respectivement sur deux ensembles X, Y, et $\varphi : G \to H$ un homomorphisme une application : $f : X \to Y$ est dite équivariante si $f(g.x) = \varphi(g) f(x)$*

Si H est le groupe trivial, une telle application est dite invariante.

Remarque 2.19. Etudier l'action d'un groupe dans un ensemble c'est étudier l'ensemble des propriétés invariantes par l'action de ce groupe.

Exemple 2.20. Le groupe affine agit sur l'espace affine. Il opère aussi sur l'ensemble des coniques. Il préserve leur type (parabole, hyperbole ou ellipse).

La groupe euclidien opère sur l'ensemble des coniques. Il conserve leur type et leurs paramètres (excentricité, longueur de grand axe, distance focale etc)

2.1.4 Terminologie : stabilisateur d'un point, classes de conjugaisons.

Si un groupe opère dans X et si x est un élément de X, on note $G_x = \{g / g.x = x\}$, l'ensemble des éléments de G qui fixent x..

Proposition 2.21. *L'ensemble G_x est un sous-groupe de G qu'on appelle le stabilisateur de x.*

Exemple 2.22. Le groupe $O(2)$ opère dans le plan. Le stabilisateur d'un point $u \neq 0$ est constitué de deux éléments l'identité, et la symétrie orthogonale par rapport à la droite $\mathbb{R}u$.

Deux points de la même orbite ont des stabilisateurs qui se ressemblent

Proposition 2.23. *$G_{g.x}$ est le sous-groupe gG_xg^{-1} de G_x.*
Autrement dit si h fixe le point x, ghg^{-1} fixe le point gx.

Exemple 2.24. Le groupe des rotations $\mathrm{SO}(3)$ opère sur la sphère $S^2 \subset \mathbb{R}^3$. Le stabilisateur d'un vecteur u est exactement le sous-groupe des rotations autour de l'axe u. Deux rotations sont conjuguées si et seulement si elle on même angle $[0, \pi]$, un conjuguant et un élément qui transforme l'axe de la première en celui de la seconde.

Rappel. Deux éléments g, g' d'un groupe G sont conjugués si il existe une élément h tel que $g' = hgh^{-1}$.

Si G est un groupe, nous avons vu que l'application $G \to \mathrm{Aut}(G)$ qui a un élément g associé la conjugaison par g est un homomorphisme de groupe. Comme $\mathrm{Aut}(G)$ est un sous-groupe de $S(G)$ on obtient ainsi une action de G sur lui même par conjugaison

Proposition 2.25. *Les orbites de l'action de G sur lui même par conjugaison sont les classes de conjugaison.*

Démonstration. L'action est donnée par $(g, h) \to ghg^{-1}$ donc h' est dans l'orbite de h si et seulement si h' et h sont conjugués. □

2.1.5 Classe à droite modulo un sous-groupe, théorème de Lagrange.

Soit G et $H < G$. On dit que deux éléments $g_1 g_2$ sont équivalents modulo H si $g_2 \in g_1.H$. C'est une relation d'équivalence (exercice).

Définition 2.26. *La classe à droite de g modulo H est la classe d'équivalence de g pour cette relation. c'est l'ensemble des g' tels qu'il existe un h dans H pour lequel $g' = gh$. On la note souvent $g.H$*

Proposition 2.27. *L'application $f_g : H \to G$ définie par $f_g(h) = gh$ induit une bijection de H avec la classe gH de g. Toutes les classes à droites modulo H sont donc en bijection avec H. S de plus le groupe H est fini, elles ont donc le même nombre d'éléments.*

Définition 2.28. *L'ensemble quotient G/H est l'ensemble des classes à droites modulo H.*

Si on choisi dans chaque classe un représentant $\theta: G/H \to G$, on obtient une bijection $G/H \times H \to G$ définie $\theta(x).h$. On a donc le célèbre théorème.

Théorème 2.29. *Lagrange* $|G| = |H| \times \mathrm{Card}(G/H)$

Démonstration. On écrit G comme réunion disjointe de ses classes modulo H. il y en a $\mathrm{Card}(G/H)$ et celle ci ont toute même cardinal $|H|$. □

Corollaire 2.30. *L'ordre de H divise l'ordre de G.*

Corollaire 2.31. *L'ordre d'un élément divise l'ordre du groupe*

Théorème 2.32. *Si p est premier tout groupe d'ordre p est cyclique, simple.*

Démonstration. Si $|G| = p$ est premier et si $g \in G - (e)$ l'ordre de g divise p, et est donc égal à p. Le groupe cyclique engendré par p est donc égal à G tout entier. □

2.1.6 Action transitive, espace homogène

Définition 2.33. *Une opération d'un groupe G sur un ensemble X est dite transitive si X est constitué d'une seule orbite. Dans ce cas on dit que X est un espace homogène sous l'action de G.*

Exemples.

Le groupe orthogonal est transitif sur la sphère.
Le groupe affine est transitif sur les triangles non dégénérés.
Le groupe des symétries du cube est transitif sur les sommets du cube.
Le groupe linéaire est transitif sur les couples de vecteurs indépendants, sur les triplets, sur les bases.

Proposition 2.34. *La multiplication à gauche induit une opération transitive de G dans G/H. Réciproquement si l'action de G sur X est transitive, si $x_0 \in X$ et $H = G_{x_0}$ est son stabilisateur, alors l'application d'orbite passe au quotient en une bijection $G/G_{x_0} \to X$.*

Démonstration. Par définition un élément de G/H est un sous ensemble de la forme gH : c'est l'image par g de la classe de l'élément neutre.

On considère l'application d'orbite $\varphi: G \to X$ définie par $\varphi(g) = gx_0$. Si g et g' sont dans la même classe modulo G_{x_0} il existe un h dans $H = G_{x_0}$ tel que $g' = gh$. Alors $g'x_0 = g(hx_0) = gx_0$. Donc φ passe au quotient en une application de G/G_{x_0} vers X. Cette application est surjective car φ l'est. Montrons qu'elle est injective : pour cela on remarque que si $\varphi(g) = \varphi(g')$ alors $\mathrm{gx}_0 = g'x_0$ donc $g^{-1}g' \in G_{x_0}$ et g, g' sont donc dans la même classe à droite modulo G_{x_0}. □

Donc en fait le mystérieux quotient G/H n'est autre qu'un espace homogène sous l'action de G dont le stabilisateur d'un point est H.

Exemple 2.35. La sphère S^2 est le quotient de SO(3) par SO(2) : le sous groupe de SO(3) qui fixe le vecteur $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ est le groupe des matrices de la forme $\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}$ ou A est une matrice orthogonale $(2,2)$ de déterminant 1.

Un cas particulier important est le cas ou le stabilisateur d'un point est un sous groupe normal.

Théorème 2.36. *Soit X un espace homogène de G. Les propriétés suivantes sont équivalentes.*

i. Le stabilisateur d'un point ne dépend pas du point.

ii. Le stabilisateur d'un point est un sous-groupe normal.

iii. Il existe sur X une structure de groupe telle que l'application d'orbite $G \to X$ définie par $\varphi(g) = g \times e$ soit un homomorphisme surjectif.

Démonstration. $i \Rightarrow ii$. Si H est le stabilisateur de gx_0 est gHg^{-1}. Donc si il ne dépend pas du point on a $gHg^{-1} = H$ pour tout g.

$ii \Rightarrow iii$. Soit N le stabilisateur de x_0 sait qu'il existe sur G/N une structure de groupe faisant de la projection un homomorphisme surjectif. L'application d'orbite passe au quotient en une bijection $G/N \to X$, équivariante, ce qui muni X d'une structure de groupe.

$iii \Rightarrow i$ En effet $\varphi(g)$ fixe l'élément neutre si et seulement si $g \in \ker(\varphi)$ et on sait que le noyau est normal. □

Remarque 2.37. Dans $ii \Rightarrow iii$, la structure de groupe qu'on construit dépend du choix du point base x_0. Par exemple l'action par rotation d'angle $k\frac{2\pi}{n}$ de $\mathbb{Z}$ sur les sommets d'un polygone régulier à n cotés est transitive, et le stabilisateur d'un sommet est normal (vu que $\mathbb{Z}$ est abélien). Mais un polygone n'a pas a priori de sommet préféré.

2.1.7 Exemples : les actions transitives de $\mathbb{Z}$.

Une action du groupe $(\mathbb{Z}, +)$ dans un ensemble X est juste la donnée d'une bijection σ de cet ensemble. On pose alors $n * x = \sigma^n x$.

Une action de $\mathbb{Z}$ est transitivite si et seulement si pour tout x, il existe un n tel que $\sigma^n x_0 = x$.

Exemple 2.38. Le shift est la transformation $\mathbb{Z} \to \mathbb{Z}$ $n \to n+1$ Cette bijection défini une action transitive de $\mathbb{Z}$.

Proposition 2.39. *Soit σ une bijection d'un ensemble X. On choisit un point x_0 dans X, et l'on note $\varphi : \mathbb{Z} \to X$ $\varphi(n) = \sigma^n x_0$ l'application d'orbite. On suppose que l'action ainsi définie est transitive.*

1. Si X est infini, l'application d'orbite $\mathbb{Z} \to X$ est bijective.

2. Si X est fini de cardinal n alors le stabilisateur de x_0 est $n\mathbb{Z}$ et φ passe au quotient en un bijection $\mathbb{Z}/n\mathbb{Z} \to X$.

C'est un cas particulier du théorème général $G/G_{x_0} \asymp \text{Orbite}(x_0)$

Remarque 2.40. Dans un cas comme dans l'autre la bijection dépend du choix de $x_0 = \varphi(0)$.

2.1.8 Exemple : les 3 actions d'un groupe sur lui-même.

Soit G un groupe. G agit sur lui-même de trois façons

-Action à gauche $g.x = gx$
-Action à droite $(g,x) = xg^{-1}$
-Conjugaison. $(g,x) \to gxg^{-1}$

C'est très utile de faire agir un groupe sur lui même par l'une de ces trois actions quand on ne sait pas quoi faire d'autre.

Proposition 2.41. *1. L'action de G sur lui-même par translation à gauche est libre et transitive.*

2. *Soit $H < G$ un sous-groupe. Les orbites de l'action à droite de H sur G sont exactement les classes à droites modulo H.*

3. *Le groupe H est normal si et seulement si les orbites de son action à droite sont les orbites de son action à gauche.*

Démonstration. 1. Si $gx = x$ alors $g = e$.
2. $g' \in gH \Leftrightarrow \exists h / g'h^{-1} = g \Leftrightarrow g$ est dans l'arbitre de g'.
3. Soit $g \in G$. Si sa classe a droite est égal à une classe à gauche il existe g' tel que $gH = Hg'^{-1}$. ALors il existe un $h \in H$ tel que $gh = e.g'^{-1}$ et $g' = h^{-1}g^{-1}$. Donc si la classe de g à gauche est égale à une classe à droite il existe un h te que $gH = Hgh$, soit $gHh^{-1} = \mathrm{Hg}$ ou $gHg^{-1} = H$, et g normalise H. Donc si toutes les classes à droite sont des classes à gauche le groupe H est normal. La réciproque est évidente. □

L'action d'un groupe sur lui-même par conjugaison est très utile. Nous étudierons tout particulièrement le cas du groupe symétrique et du groupe linéaire, mais donnons un peu de terminologie.

Définition 2.42. *Si $g \in G$, le centralisateur de g est l'ensemble des x tels que $gxg^{-1} = x$: c'est l'ensemble des points fixe de l'action de g sur G par conjugaison.*

Proposition 2.43. *Le centralisateur de g est le stabilisateur de g pour l'action de G sur lui même par conjugaison.* □

Définition 2.44. *Le centre d'un groupe est l'ensemble des g tels que pour tout x de G $gx = xg$.*

Proposition 2.45. *Le centre est un sous groupe normal de G qui est l'intersection de tous les centralisateur de G. Le groupe G est commutatif si et seulement si il est égal à son centre.* □

2.1.9 Equation aux classes. Actions de groupe finis sur des ensembles finis.

On écrit en même temps l'équation aux classes et sa démonstration.

Théorème 2.46. $|X| = \sum_{\text{orbites}} |O| = \sum_{\text{orbites}} |G/G_x| = |G| \sum_{\text{orbites}} |1/G_x|$

Démonstration. La première égalité est juste de dire que les orbites forment une partition de G car ce sont des classes d'équivalence. La seconde est la bijection entre l'orbite et l'espace homogène G/G_x, la troisième, le théorème de Lagrange. □

Corollaire 2.47. *(équations aux classes)* $|X| = \sum_{\text{orbites}} |G/G_x|$

Une célèbre application est le théorème du point fixe pour les actions des p groupes.

Définition 2.48. *Un p groupe est un groupe fini dont l'ordre est une puissance de p.*

Proposition 2.49. *Tout sous groupe d'un p groupe est un p groupe. Le cardinal d'un espace homogène d'un p groupe est une puissance de p.*

Démonstration. Lagrange nous dit que si $H < G$, alors $|G| = |H| \times \left|\frac{G}{H}\right|$ si $|G| = p^n$ alors les deux entiers du membre de droite sont aussi des puissances de p. □

Théorème 2.50. *(Du point fixe) Si un p-groupe fini opère dans un ensemble, on a* $|X^G| = |X|(p)$.
En particulier, l'action d'un p groupe sur un ensemble de cardinal non divisible par p a des points fixes.

Démonstration. On réduit modulo p l'équation aux classes : si x n'est pas fixe sont orbite a un cardinal divisible par p, d'ou le résultat. □

Exemple 2.51. si le groupe $\mathbb{Z}/2\mathbb{Z}$ opère sur un ensemble de cardinal impair, il a au moins un points fixe.

Corollaire 2.52. *Le centre d'un p-groupe fini est non trivial.*

Démonstration. Le groupe opère par lui-même par conjugaison. Donc comme il y a un point fixe e, il y en a au moins p. □

Théorème 2.53. *Tout groupe d'ordre* p^2 *est commutatif.*

Démonstration. Soit G un groupe d'ordre p^2. On va supposer que G n'est pas cyclique, donc il ne contient pas d'élément d'ordre p^2 et tout élément $\neq e$ est d'ordre p. On suppose aussi qu'il n'est pas commutatif. Soit Z le centre, et $g \notin Z$, alors g est d'ordre exactement p et engendre un groupe cyclique $1, g, ...g^{p-1} = C$. Tous les éléments de C commutent à Z et -sauf e- aucun n'est dans Z, car ils engendrent tous C. Donc l'application produit $C \times Z \to G$ est bijective. C'est un isomorphisme pour des raisons de cardinal, et en fait G est commutatif. □

On verra plus tard les théorèmes de Sylow qui vont plus loin sur ce sujet.

2.2 Le groupe symétrique.

Si X est un ensemble fini, on rappelle que $S(X)$est le groupe des permutations de X . Si $X = \{1, ..., n\}$ on le note S_n.

Avertissement 2.54. La permutation $\sigma \circ \tau$ consiste à faire d'abord τ ensuite σ.

Notation 2.55. *Etant donnée une permutation* σ*, on note* $\sigma = \begin{pmatrix} 1 & 2 & \cdot & \cdot & \cdot & n \\ \sigma(1) & \sigma(2) & \cdot & \cdot & \cdot & \sigma(n) \end{pmatrix}$

Du coup, on peut aussi noter $\sigma = \begin{pmatrix} 2 & 7 & \cdot & \cdot & \cdot & n-2 \\ \sigma(1) & \sigma(7) & \cdot & \cdot & \cdot & \sigma(n-2) \end{pmatrix}$ *à condition que sur la première ligne, on voit apparaitre chaque indice une fois et une seule.*

Dans cette notation, 1,...n, sont des *chiffres*, (des symboles) pas des *nombres*. Autrement dit, on pourrait les remplacer par des noms de fleurs, des lettres de l'alphabet et cela n'aurait pas d'importance. Le seul *nombre* dans cette histoire c'est l'entier n qui est le cardinal de l'ensemble considéré.

2.2.1 L'action de S_n sur $\{1, ..., n\}$.

Cette action est transitive. En effet si $i \in \{1, ..., n\}$ la bijection $1 \to i i \to 1$ et $j \to j$ si $j \neq 1, i$ montre que tous les points sont dans l'orbite de 1.

Notons que le stabilisateur de $\{n\}$ s'identifie à S_{n-1}. En appliquant le théorème de Lagrange, on obtient $|S_n| = n|S_{n-1}|$, et par récurrence

Proposition 2.56. $|S_n| = n!$

Au lieu de faire agir S_n sur l'ensemble $\{1, ..., n\}$, on peut le faire agir sur l'ensemble des $k-$uplets d'éléments distincts de cet ensemble. L'action est transitive, et en utilisant le théorème de Lagrange, nous voyons

Proposition 2.57. *Le nombre de k-uplets de* $\{1, ..., n\}$ *est* $\frac{n!}{(n-k)!}$

On peut aussi faire agir sur l'ensemble des sous ensembles à k éléments distincts de cet ensemble. L'action est transitive, et en utilisant Lagrange, nous voyons

Proposition 2.58. *Le nombre de sous-ensembles à k éléments de* $\{1, ..., n\}$ *est* $\frac{n!}{k!(n-k)!}$

2.2.2 Cycles.

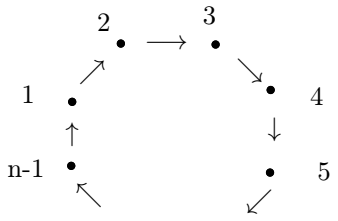
Si σ est une permutation, nous allons nous intéresser au sous-groupe qu'elle engendre : c'est donc un groupe cyclique.

Pour étudier cette permutation, on décompose l'ensemble $\{1, ..., n\}$ en sous ensembles disjoints, les orbites sous l'action de σ.

Définition 2.59. *Un cycle de longueur k est une permutation qui a une orbite ayant k élément, et qui fixe tous les autres points.*

Autrement dit si σ est un cycle de longueur k, il existe un n-uplet $i_1...i_k$ de $\{1, ..., n\}$ tel que $\sigma(i_j) = i_{j+1}$ si $j \neq k$ et $\sigma(i_k) = i_1$.

Exemple : $\begin{pmatrix} 1 & 2 & . & . & n-1 & n \\ 2 & 3 & . & . & n & 1 \end{pmatrix}$ que l'on dessine.



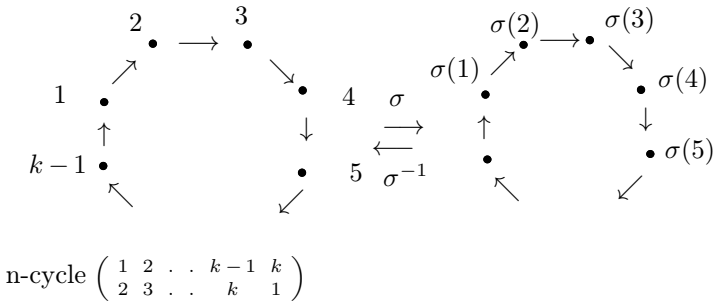
n-cycle $\begin{pmatrix} 1 & 2 & . & . & n-1 & n \\ 2 & 3 & . & . & n & 1 \end{pmatrix}$

Notation 2.60. *Pour désigner le cycle* $\sigma(i_j)=i_{j+1}$ *si* $j\neq k$ *et* $\sigma(i_k)=i_1$*, on note sur une seule ligne* $(i_1,i_2,...,i_k)$*. il est entendu que les autres indices ne bougent pas. Ainsi,* $\begin{pmatrix}1&2&..&n-1&n\\2&3&..&n&1\end{pmatrix}$ *se note plutôt* $(1,2,....,n)$*. Attention il y a k façons de décrire un cycle d'ordre k.*

Définition 2.61. *Une transposition est un cycle de longueur 2. On la note* $(i,j)=(j,i)$

Proposition 2.62. *Le conjugué du cycle* $(1,....,k)$ *par* σ *est le cycle* $(\sigma(1),\sigma(2),...,\sigma(k))$*. C'est un cycle de même longueur. Réciproquement deux cycles de même longueur sont conjugués.*

Démonstration. Il vaut mieux un joli dessin qu'un mauvais calcul.



On voit que si on prend un point a droite, qu'on lui applique σ^{-1}, puis le cycle de gauche puis σ^{-1} on a le second cycle : $\sigma C\sigma^{-1}=C'$

Proposition 2.63. *L'ordre d'un cycle de longueur k est k.*

Démonstration. Grâce à ce qui précède, il suffit de le démontrer pour $(1,....,k)$. Notons que $\sigma(i)=i+1\,(k)$ donc $\sigma^m(i)=i+m(k)$ et $\sigma^m=\mathrm{Id}\Leftrightarrow m=0(k)$ On peut aussi appliquer ce qui a été vu sur les espaces homogène de $\mathbb{Z}$ □

Lemme 2.64. *Tout cycle est produit de transposition.*

Démonstration. En effet on calcule facilement : $(1,2,...k)=(1,2)(2,3)(3,4)....(k-1,k)$
Donc par conjugaison $(\sigma(1),\sigma(2),...,\sigma(k))$=$((\sigma(1),\sigma(2))(s(2),\sigma(3)).....(\sigma(k-1),\sigma(k))$
□

Exemple 2.65. L'action $+1$ de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ est un cycle. La rotation d'angle $2\pi/n$ agissant sur un $n-$gone régulier est un cycle de longueur n.

2.2.3 Décomposition en produit de cycle.

Définition 2.66. *Le support d'une permutation* σ *est l'ensemble des i tels que* $\sigma(i)\neq i$*.*

Lemme 2.67. *Pour que deux permutations commutent il suffit que leurs supports soient disjoints.*

Démonstration. Si le support de σ et σ' sont disjoints, on peut écrire comme réunion disjointe de deux sous ensembles $X = Y \sqcup Y'$ tel que la restriction de σ à Y' soit l'identité ainsi que celle de σ' à Y. Les restrictions à Y et Y' de ces deux permutations commutent, donc elles commutent. □

Soit σ une permutation.

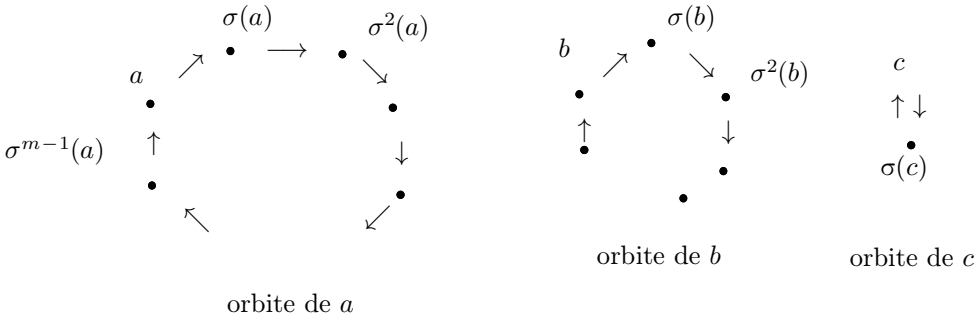
On décompose $X = \{1, ...n\}$ en orbites sous l'action du groupe cyclique engendré par σ, $X = X_1 \cup X_2 \cup ... \cup X_l$. L'ensemble X_i est donc fini avec n_i éléments, et la restriction de σ à ce sous ensemble engendre une action transitive.

La restriction de σ à X_i est donc un cycle d'ordre n_i, que nous noterons c_i. Nous avons donc démontré.

Proposition 2.68. *Avec ces notations, $\sigma = c_1.....c_l$ est un produit de cycles de supports disjoints* □.

Notre démonstration est effective. On va décomposer l'ensemble X sous l'action du groupe (cyclique) engendré par σ.

Pour construire cette décomposition, nous pouvons partir d'un point au hasard disons a, regarder son orbite sous l'action du groupe engendré par σ: $\sigma(a)$, $\sigma^2(a)$, $....\sigma^{m-1}(a)$. La restriction à cette orbite est manifestement un cycle d'ordre m. Puis on prend un second point b en dehors de l'orbite de a et on recommence, jusqu'à avoir un point dans chacune des orbites. Dans la pratique on fait un dessin de la permutation :



orbite de a orbite de b orbite de c

Corollaire 2.69. $c^k = c_1^k....c_l^k$

Corollaire 2.70. *L'ordre de σ est le ppcm des ordres des c_i.*

Corollaire 2.71. *Le groupe symétrique est engendré par les transpositions. En fait toute permutation est produit d'au plus n-1 transpositions.*

Démonstration. Tout cycle de longueur k est un produit de $k-1$ transpositions. □

On aurait pu donner une autre démonstration de ce résultat important, par récurrence sur le cardinal de X.

Démonstration. Si le cardinal de X est 1 il n'y a rien à démontrer. Sinon, on suppose que $X=\{1,....n\}$. Soit $\sigma\in S(X)$. Si $\sigma(n)=n$ l'hypothèse de récurrence montre que σ est le produit d'au plus $(n-2)$ transpositions de $\{1,...n-1\}$. Sinon, composons σ par $\tau=\begin{pmatrix}\sigma(n)\\ n\end{pmatrix}$. Alors $\tau\sigma(n)=n$. Donc $\tau\sigma$ est le produit d'au plus $n-3$ transpositions, ce qui montre que $\sigma=\tau(\tau\sigma)$ est produit d'au plus $n-1$ transpositions. □

2.2.4 La signature.

La signature d'une permutation est un des miracles de la nature (celui qui fait qu'il y a une gauche et une droite).

Théorème 2.72. *Il existe un homomorphisme surjectif $\varepsilon: S_n\to\{\pm1\}$. Celui-ci est unique.*
Il est caractérisé par $\varepsilon(\tau)=-1$ pour toute transposition. Si σ est un cycle d'ordre k, $\varepsilon(\sigma)=(-1)^{k-1}$

Démonstration.
Nous allons d'abord démontrer l'unicité. Notons que deux transpositions sont toujours conjuguées, donc ont la même image dans $\{\pm1\}$. Comme les transpositions engendrent S_n, si pour l'une $\varepsilon(\tau)=1$ alors $\varepsilon\equiv1$.

Pour montrer l'existence, on considère la fonction $f:\mathbb{R}^n-\Delta\to\mathbb{R}$ où $f(x)=\Pi_{i<j}(x_i-x_j)$
Si σ est une permutation, on pose $l_\sigma:\mathbb{R}^n\to\mathbb{R}^n$ $l_\sigma(x_1,....,x_n)=(x_{\sigma^{-1}(1)},....x_{\sigma^{-1}(n)})$

Lemme 2.73. $l_\sigma\times l_{\sigma'}=l_{\sigma\circ s'}$.

Proposition 2.74. *l'application $\varepsilon(\sigma)=\frac{f\circ l_\sigma}{f}$ est un homomorphisme de groupes $S_n\to\{\pm1\}$*

Notons que $f\circ l_\sigma=\pm f$ et que $f\circ l_{(n-1,n)}=-f$. Il en résulte que $\varepsilon(\tau)=-1$, et ε est l'homomorphisme souhaité. □

Exemple 2.75. Si c est un k cycle, $\varepsilon(c)=(-1)^{k-1}$.

Proposition 2.76. *On sait que toute permutation s'écrit (d'une unique façon) comme produit de cycles (disjoints). La signature est alors le nombre de cycles pair.* □

2.2.5 Le groupe alterné.

Définition 2.77. *Le groupe alterné, noté A_n est le sous groupe normal du groupe symétrique qui est le noyau de la signature.*

Proposition 2.78. *On a $|A_n|=\frac{n!}{2}$*

Démonstration. Comme la signature d'une transposition est -1, l'homomorphisme ε est surjectif et la formule de Lagrange donne le résultat. □

Proposition 2.79. *Si $n\geqslant4$, le groupe alterné est engendré par les 3-cycles*

Démonstration.
a) $(12)(23)=(123)$

b) $(12)(34) = (123)(234)$

Proposition 2.80. *Si $n \geqslant 5$ les 3-cycles sont conjugués dans A_n.*

Démonstration. Soient σ, σ' deux $3-$cycles. On sait qu'il sont conjugués dans S_n, ainsi on peut trouver α tel que $\alpha\sigma\alpha^{-1} = \sigma'$. Si α est dans A_n, on a terminé, sinon comme $n \geqslant 5$ il existe une transposition τ qui commute à σ. Alors $(\alpha\tau)$ conjugue σ et σ'. □

Une autre façon d'exprimer ce résultat est de dire.

Théorème 2.81. *Si $n \geqslant 5$ le groupe A_5 est 3-fois transitif sur $\{1, ..., n\}$ c'est à dire que pour tout couple triplet (a, b, c) , (a', b', c') de $\{1, ..., n\}$ il existe une permutation alternée σ telle que $\sigma(a, b, c)\sigma^{-1} = (a', b', c')$.*

Démonstration. En effet $\sigma(a, b, c)\sigma^{-1} = (\sigma(a), \sigma(b), \sigma(c))$ □

On fini ce chapitre par un résultat plus difficile.

Théorème 2.82. *Si $n \geqslant 5$ le groupe A_n est simple, c'est à dire qu'il n'a pas de sous groupe normal propre.*

Démonstration. Soit $N \lhd A_n$ un sous groupe normal non réduit à 1. On sait que les 3-cycles engendrent A_n et que ceux ci sont conjugués dans A_n. Pour vérifier que $N = A_n$ il suffit donc de vérifier que N contient un 3 cycle : en effet, si il en contient un, il les contient tous car N est normal.

Première étape. On va vérifier que le résultat est vrai pour $n = 5$, en étudiant l'action de A_5 sur lui même par conjugaison.

On regarde d'abord les classes de conjugaison dans S_5 des éléments de A_5 (qui a 60 éléments) : il a les 3 cycles qui sont au nombre de $2\binom{5}{2} = 20$, les 5 cycles qui sont au nombre de $4! = 24$, les produits de deux transpositions de supports disjoints qui sont au nombre de $5 \times 3 = 15$, et l'identité.

Lemme 2.83. *Les produits de deux transpositions sont conjuguées dans A_5.*

Démonstration. Si $(a, b)(c, d)e$ et $(a', b')(c', d')e'$ sont deux produits de deux transposition, notons que comme A_5 est 3-transitif on peut trouver σ dans A_5 telle que $\sigma(a) = a'; \sigma(b) = b', \sigma(e) = e'$. Alors $\sigma(\{c, d\}) = \{c', d'\}$ et donc σ conjugue la première et la seconde permutation.

□

Lemme 2.84. *Il y a une seule classe de conjugaison de 5-cycles dans A_5.*

Démonstration. Soit $\pi = (a, b, c, d, e, f)$ un 5 cycle. Si $\sigma \in A_5$ satisfait $\sigma(a) = 1, \sigma(b) = 2, \sigma(c) = 3$, alors $\sigma(\{e, f\}) = \{4, 5\}$ donc $\sigma\pi\sigma^{-1} = (1, 2, 3, 4, 5) = \alpha$ ou bien $(1, 2, 3, 5, 4) = \beta$. Soit $\tau = (2, 3, 5, 4, 1)$ alors $\tau\alpha\tau^{-1} = (2, 3, 5, 4, 1) = \beta$, donc il n'y a qu'une classe de conjugaison □

Soit donc N un sous groupe normal. Si il contient un 3-cycle, il les contient tous et donc c'est A_5 vu que les 3-cycles engendrent A_5. Supposons donc qu'il ne contiennent pas de 3-cycles.

Comme les produits de deux transpositions ou les 5-cycles sont conjugués, il les contient alors tous. Comme N est un sous groupe, sont ordre divise 60. Mais ni $15 + 1$ ni $24 + 1$ ne divisent 60. Donc il contient nécessairement des éléments de deux types différents et même il les contient tous. Si on y ajoute l'identité il y en a 24+15+1=40, qui ne divise toujours pas 60. Donc il contient un 3 cycle et c'est tout A_5.

Deuxième étape. Un fois qu'on sait que A_5 est simple, on considère un sous groupe normal N et un élément $\sigma \in N$ qui n'est pas l'identité. Quitte a conjuguer (ou à renuméroter), on peut supposer que $\sigma(1)=2$. On peut supposer que $\sigma(2)\neq 3$ (disons que c'est soit 1, soit 4) et on considère $\tau=(1,3,2)$, $\tau^{-1}=(1,2,3)$. On calcule $\rho=\tau\sigma\tau^{-1}\sigma^{-1}=(132)(\sigma(1)\sigma(2)\sigma(3))$. Notons que 2 n'est pas un point fixe de ρ. En effet $\rho(2)=\rho(\sigma(1))=\tau\sigma\tau^{-1}(1)=\tau\sigma(2)\neq 2$ car $\tau^{-1}(2)=3\neq\sigma(2)$.

Par ailleurs l'ensemble $(1,2,3,\sigma(1),\sigma(2),\sigma(3))$ a au plus 5 éléments vu que $\sigma(1)=2$. Ainsi ρ est une permutation paire d'un sous ensemble de 5 éléments non triviale. Comme le groupe A_5 est simple, il existe un cycle de longueur 3 dans le sous groupe normal qu'elle engendre. Comme tous les 3-cycles sont conjugués dans A_n le sous groupe normal contenant σ contient toutes les 3-cycles, et comme ceux ci engendre A_n, le groupe A_n est simple. □

2.3 Exercices du chapitre 2

2.3.1 Groupe opérant

Exercice 2.1. Le groupe affine, le groupe des similitudes, le groupe des isométries du plan.

Ces trois groupes opèrent dans le plan affine (euclidien). Donc dans l'ensemble des droites, des triangles (non dégénérés) et des coniques. Décrire dans chaque cas, les orbites, l'ensemble des orbites.

Trouver des exemples de fonctions invariantes ou équivariantes (angles , aires, distances, orthocentre, centre de gravité, centre du cercle inscrit etc) de l'action de ces groupes dans l'ensemble des triangles.

Exercice 2.2. Soit X un ensemble sur lequel un groupe fini G opère et $f: X\to\mathbb{R}$ une fonction. Montrer que la fonction $g(x)=\frac{1}{|G|}\sum f(gx)$ est invariante par G.

Exercice 2.3. Espace métrique. Soit X,d un espace métrique et F un sous groupe fini du groupe des homéomorphismes de X. Trouver une distance équivalente topologiquement à d pour laquelle F agit par isométries.

Exercice 2.4. On fait opérer $\mathrm{GL}(2,\mathbb{Z}/2\mathbb{Z})$ sur $(\mathbb{Z}/2\mathbb{Z})^2$ quelles sont les orbites ? En déduire un isomorphisme $\mathrm{GL}(2,\mathbb{Z}/2\mathbb{Z})$ avec le groupe S_3 des permutations d'un ensemble à trois éléments.

Exercice 2.5. Combien y a t il de partitions d'un ensemble à 4 éléments en deux sous-ensembles à 2 éléments.
En déduire un homomorphisme $S_4\to S_3$; quel est son noyau ?

Exercice 2.6. Le groupe $\mathrm{GL}_n(\mathbb{K})$, si $\mathbb{K}$ est un corps fini.
Soit $\mathbb{K}$ un corps. On fait agir $\mathrm{GL}_n(\mathbb{K})$ (les matrices (n,n)) sur l'espace $\mathbb{K}^n$ des vecteurs colonnes. Montrer que cette action a deux orbites.
Quel est le stabilisateur du vecteur $\begin{pmatrix}1\\0\\ \\0\end{pmatrix}$. Montrer que celui ci se surjecte sur $\mathrm{GL}_{n-1}(\mathbb{K})$, et que le noyau de la surjection est isomorphe à $\mathbb{K}^{n-1}$.
En déduire que si $\mathbb{K}$ est un corps fini a q éléments, $|\mathrm{GL}_n(\mathbb{K})|=(q^n-1)q^{n-1}|\mathrm{GL}_{n-1}(\mathbb{K})|$
Quel est le cardinal de $|\mathrm{GL}_n(\mathbb{K})|$?
On suppose que $\mathbb{K}=\mathbb{F}_p$ le corps à p éléments. Soit $B\subset\mathrm{GL}_n(\mathbb{K})$ le sous groupe des matrices triangulaires avec des 1 sur la diagonale. Quel est le cardinal de B?
Montrer que le cardinal de $\mathrm{GL}_n(\mathbb{F}_p)/B$ est congru à $(-1)^n$ modulo p
Soit $G<|\mathrm{GL}_n(\mathbb{F}_p)|$ un $p-$groupe. En faisant agir G sur $\mathrm{GL}_n(\mathbb{F}_p)/B$, démontrer que G est conjugué à un sous-groupe de B.
Quels sont tous les sous-groupes de $\mathrm{GL}_n(\mathbb{F}_p)$ de cardinal $p^{\frac{n(n-1)}{2}}$

Exercice 2.7. Le groupe des symétries du cube.
On considère un cube, par exemple le cube formé de l'enveloppe convexe des points de $\mathbb{R}^3$ $(\pm 1,\pm 1.\pm 1)$.
On veut étudier le sous-groupe G de $O(3)$ qui conserve ce cube.
Etant donné deux sommets voisins, A*,B montrer qu'il existe un élément de G transformant A en B.
En déduire que G est transitif sur les sommets et que le cardinal de G est divisible par 8.

Etant donné deux arêtes voisines, U,V montrer qu'il existe un élément de G transformant U en V.En déduire que g est transitif sur les arêtes. Et même sur les arêtes orientées. En déduire que le cardinal de G est multiple de 24.

Montrer que le stabilisateur d'une arête orientée est la réflexion par rapport au plan Oσ, et en déduire que G a 48 éléments.

Montrer que le centre de G est $Z(G) = \{\pm \mathrm{id}\}$, et que G s'identifie au produit $G^+ \times \{\pm \mathrm{Id}\}$

Montrer que $G^+ = G \cap \mathrm{SO}(3)$ a 24 éléments.

On considère les 4 grandes diagonales du cube. Montrer que G^+ opère transitivement sur cet ensemble, et en déduire un isomorphisme $G^+ \to S_4$

On considère les 3 plans verticaux parallèles aux faces et passant à l'origine. Montrer que G opère transitivement sur Π et en déduire un homomorphisme surjectif $G^+ \to S_3$ dont le noyau a 4 éléments. Quels-sont ils ?

Exercice 2.8. Formes quadratiques et théorème de Sylvester.

Soit E un espace vectoriel de dimension finie sur $\mathbb{R}$. On rappelle que l'application $q\colon E \to \mathbb{R}$ est une forme quadratique si il existe une forme bilinéaire symétrique $b\colon E \times E \to \mathbb{R}$ telle que $q(x) = b(x, x)$. On note $Q(E)$ l'ensemble des formes quadratiques sur E.

Montrer que l'application de $\mathrm{Gl}(E) \times Q(E) \to Q(E)$ définie par $g^*(q) = q \circ g^{-1}$ définit une action de groupe.

Rappeler le théorème de Sylvester sur la classification des formes quadratiques.

Quelles sont les orbites de l'action de $\mathrm{GL}(E)$ sur Q.

Exercice 2.9. Sous groupe finis du groupe affine.

Le corps de base est $\mathbb{R}$.

Soit A un espace affine E l'espace vectoriel sous jacent, $G(A)$ le groupe affine, $\mathrm{Gl}(E)$ le groupe linéaire.

On fait opérer $G(A)$ sur A. Démontrer que l'action est transitive. Quel est le stabilisateur d'un point O ?

Soit F un sous groupe fini du groupe affine $G(A)$. Démontrer que si $P \in A$ le barycentre $O = \frac{1}{|F|}\Sigma f(P)$ est fixe par F.

En déduire que F est conjugué à un sous groupe du groupe linéaire.

On fait opérer le groupe linéaire $\mathrm{GL}(E)$ sur l'ensemble des formes quadratiques définies positives. Montrer que le stabilisateur de q_0 est le groupe orthogonal $O(q_0)$.

Si q est une forme quadratique définie positive, démontrer que $\Sigma_{f \in F} q \circ f$ est une forme quadratique définie positive et invariante.

En déduire que si F est un sous groupe fini de $\mathrm{GL}_n(\mathbb{R})$, alors F est conjugué à un sous-groupe du groupe orthogonal.

Montrer que le sous-groupe de F qui conserve l'orientation est normal et d'indice 1 ou 2.

Montrer qu'un sous groupe fini de Aff(2) est soit un groupe cyclique soit un groupe diédral, et qu'il est conjugué dans le groupe affine au groupes des rotations d'angles multiple de $2\pi/n$ ou au groupe engendré par les symétries orthogonales autour de deux droites faisant un angle $2\pi/n$.

Exercice 2.10. Un groupe fini d'ordre 156 agit sur un ensemble X . Le stabilisateur d'un point est d'ordre 12 ; quel est le cardinal de son orbite.

Un groupe d'ordre 143 opère dans un ensemble de cardinal 108 ; montrer qu'il y a un point fixe.

Un groupe d'ordre 35 opère sans points fixes dans un ensemble de 19 éléments. Combien y a t il d'orbites ?

Exercice 2.11. On fait opérer un groupe sur lui même par conjugaison.

Montrer que si g est un élément d'ordre n l'ordre de son stabilisateur est un multiple de n. On l'appelle le centralisateur de G

On suppose que G a exactement deux classes de conjugaisons. Montrer que G est isomorphe à $\mathbb{Z}/2\mathbb{Z}$

Exercice 2.12. Théorème de Cauchy. Soit G un groupe fini et p un nombre premier ui divise l'ordre de G.

On considère $X \subset G^p$ le sous ensemble formé des p uplets $g_1, \ldots g_p$ tels que $g_1 \ldots . g_p = e$.

Quel est le cardinal de X.

En faisant opérer $Z/p\mathbb{Z}$ sur X par permutation cyclique, montrer que le nombre d'éléments d'ordre p est divisble par p et qu'en particulier G admet un élément d'ordre p.

Exercice 2.13. Soit G un groupe d'ordre $2p$, où p est un nombre premier. On suppose que G n'est pas commutatif

Montrer que G admet un élément d'ordre p. (on pourra utiliser le fait qu'un groupe dont tous les éléments sont d'ordre 2 est commutatif, isomorphe à $\mathbb{Z}/2\mathbb{Z}^n$).

a. Si g un élément d'ordre p. Montrer que le sous-groupe C engendré par g est d'indice 2, et que c'est un groupe cyclique, et qu'il est normal. On rappellera comment démontrer que tout sous-groupe d'indice 2 est normal.

Soit $\sigma \in G - C$. On considère l'automorphisme $S\colon C \to C$ défini par $S(g) = \sigma g \sigma^{-1}$

b. Montrer que $S \neq e$ (utiliser le fait que G n'est pas commutatif)

c. Soit $g \neq e$ un générateur de C, et k un entier tel que $S(g) = g^k$. Montrer que $k^2 = 1(p)$ et en déduire que $S(g) = g^{-1}$.

d. Montrer que G est isomorphe au groupe diédral d'ordre $2p$.

e. Quels sont tous (à isomorphisme près) les groupes d'ordre $2p$.

2.3.2 Groupe symétrique.

Exercice 2.14. Dessiner les permutations puis les décomposer en cycles disjoints

1. $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 8 & 2 & 7 & 9 & 6 & 10 & 3 & 1 & 4 \end{pmatrix}$;
2. $b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 1 & 7 & 10 & 2 & 6 & 9 & 8 \end{pmatrix}$;
3. $c = (1,2,3,4,5)(1,5,9)(2,4,9)$;
4. $d = (1,8,6,7)(8,6,7,5)(6,7,5,1)$;
5. $f = (1,2)(2,3)(3,4)(4,5)(5,6)(6,7)(7,1)$;
6. $h = (1,8)(1,7)(1,6)(1,5)(1,4)(1,3)(1,2)$.

Pour chacune de ces permutations, on déterminera l'ordre, la signature et on calculera σ^{15} et σ^{2018}.

Exercice 2.15. Combinatoire

1. On fait opérer le groupe symétrique S_n des bijections de l'ensemble $E_n = [\![1, ...n]\!]$ sur E_n

Quel est le stabilisateur de $\{n\}$. En déduire $\text{Card}(S_n) = n!$

2. On fait opérer S_n sur $\mathcal{P}(E_n)$ (ensemble des parties de n). On note $\mathcal{P}_k(E_n)$ l'ensemble des parties à k éléments. Montrer que les orbites de l'action sont exactement les $\mathcal{P}_k(E)$.

En déduire $\text{card}(\mathcal{P}_k) = \frac{n!}{k!(n-k)!} = \begin{pmatrix} n \\ k \end{pmatrix}$ puis

$2^n = \Sigma_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix}$

3. Une partition de E_n est une décomposition $E = \cup_{i=1}^{k} E_i$ en sous ensembles disjoints.

Si $p_1 + ... + p_k = n$ et $1 \leqslant p_1 \leqslant p_2 ... \leqslant p_k$ on considère la partition $E_1 = \{1, ..., p_1\}\, E_2 = \{p_1 + 1, ...p_1 + p_2\}, ...E_k = \{p_1 + ...p_{k-1} + 1, n\}$.

Quelles sont les orbites de l'action de S_n sur l'ensemble des partitions. En déduire que le nombre de partitions de l'ensemble E_n en k sous-parties ayant $p_1, ..., p_k$ éléments est $\frac{n!}{p_1! ... p_k!}$

4. Soit A un ensemble à k éléments et B un ensemble à $n \geqslant k$ éléments. On fait agir le groupe $S(A) \times S(B)$ sur l'ensemble des applications de A dans B.

Démontrer que l'ensemble des injections de A dans B se réduit à une seule orbite, et calculer son cardinal.

Exercice 2.16. Soit S_7 le groupe des permutations de l'ensemble {1, 2, 3, 4, 5, 6, 7}. On considère les permutations suivantes:

$$\sigma_1 = (1,2,3,4,5,6,7), \quad \sigma_2 = (1,3,2,6,4,5).$$

1. On pose $H_1 = \langle \sigma_1 \rangle$ et $H_2 = \langle \sigma_2 \rangle$. Calculer $|H_1|$ et $|H_2|$.
2. Déterminer $H_1 \cap H_2$.
3. Calculer $\sigma_2^{-1}, \sigma_2^{-1}\sigma_1\sigma_2$ et σ_1^5.
4. Soit $G = \langle \sigma_1, \sigma_2 \rangle$. Montrer que H_1 est un sous-groupe distingué de G.
5. Montrer que tout élément $g \in G$ s'écrit de manière unique sous la forme $g = h_2\, h_1$ avec $h_1 \in H_1$ et $h_2 \in H_2$.
6. Calculer $|G|$.

Exercice 2.17. L'opération qui consiste à couper un jeu de n cartes (par exemple 52) à la $k - i$ème est un cycle de longueur n si et seulement si le pgcd de k et n est égal à 1.

Exercice 2.18. Montrer que le groupe S_n est engendré par

1. les transpositions $(1, i)$, pour $2 \leq i \leq n$ (indication: pour i et j tels que $2 \leq i < j \leq n$, calculer $(1,i)(1,j)(1,i)$);
2. la transposition $(1,2)$ et le cycle $(2,3,...,n)$;
3. les transpositions $(i, i+1)$ pour $1 \leq i < n$;
4. la transposition $(1,2)$ et le cycle $(1,2,...,n)$.

Exercice 2.19. Dans S_4

1. Trouver les permutations σ telles que $\sigma^2 = (1,2)(3,4)$.

2. Soit $n \geq 2$. Existe-t-il un σ dans S_n tel que $\sigma^2 = (1,2)$?
3. Même question pour $n \geq 6$ et $\sigma^2 = (1,2)(3,4,5,6)$.

Exercice 2.20. Dans le groupe S_8, établir la liste des classes de conjugaison et de leurs ordre.

Montrer qu'il n'existe pas dans S_8 de sous-groupe cyclique d'ordre 9, de sous-groupe cyclique d'ordre 14.

Montrer qu'à conjugaison près S_8 ne contient qu'un seul sous-groupe d'ordre 7

Montrer que S_8 contient un sous-groupe d'ordre 14, isomorphe au groupe diédral D_{14}, et que celui ci est unique à conjugaison près.

Exercice 2.21. Les cycles $c = (123)$ et $c' = (132)$ ne sont pas conjugués dans A_4. Indication raisonner par l'absurde et noter que si σ conjugue c et c' alors $\sigma(4) = 4$.

Exercice 2.22. Quelle est la signature d'une permutation d'ordre 12, resp. 14, resp. 15, dans S_{10}

Exercice 2.23. Soit $(A, +)$ un groupe abélien et $\varphi : S_n \to A$ un homomorphisme. Montrer que les propositions suivantes sont équivalentes.

i. Il existe une transposition τ telle que $\varphi(\tau) \neq 0$
ii. Pour toute transposition τ $\varphi(\tau) \neq 0$
iii. L'image de φ est un groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et φ est (conjugué à) la signature.

Exercice 2.24. Démontrer que groupe alterné A_n est le sous groupe de S_n engendré par les commutateurs c'est à dire les élément de la forme $aba^{-1}b^{-1}$. Indication écrire le cycle $(1,2,3)$ comme produit de deux transpositions de S_3, puis comme commutateur.

Chapitre 3
Groupe abéliens de type fini.

3.1 Groupe abéliens de type fini.

Dans ce chapitre nous allons étudier les groupes abéliens (commutatifs).

Parfois, nous allons noter l'opération de groupe par un $+$ au lieu du traditionnel . ; ainsi nous le ferons systématiquement pour le groupe $\mathbb{Z}^n$, les groupes $\mathbb{Z}/n\mathbb{Z}$, les sous-groupes des groupes additifs d'un espace vectoriel etc. Mais dans certains cas, on garde la notation multiplicative, par exemple pour le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité, ou pour le groupe $\mathbb{K}^*$ des éléments inversibles d'un corps $\mathbb{K}$.

Définition 3.1. *Un groupe abélien est dit de type fini si il est engendré par un nombre fini d'éléments.*

Le but de ce paragraphe est d'étudier les groupes abéliens **de type fini**, les groupes de types infinis étant trop compliqués pour l'instant.

Exemple 3.2. Si $M \subset \mathbb{Q}$ est un sous-ensemble on note $\mathbb{Z}[M] < \mathbb{Q}$ le plus petit sous anneau de $\mathbb{Q}$ contenant 1 et M. Les groupes $\mathbb{Z}[1/p]$ pour p premier sont tous deux a deux non isomorphes. Plus généralement si M est un sous ensemble (fini ou infini) de l'ensemble des nombres premiers $\mathbb{Z}[1/M]$ est un groupe qui détérmine M: on voit ainsi que $(\mathbb{Q}, +)$ contient une famille non dénombrable de groupes abéliens deux à deux non isomorphes.

3.1.1 Sous-groupes et quotients des groupes cycliques.

Un groupe cyclique est, rappelons-le, un groupe engendré par un élément. Des fois cet élément est connu, des fois pas. Même pour le groupe $(\mathbb{Z}, +)$, il y a deux choix possible. Si le groupe en question n'a pas de générateur préféré, et si il a n éléments, autant le noter C_n. Il peut très bien être égal au groupe des racines $n-i$èmes de l'unité $\mathbb{U}_n$, ou à $\mathbb{Z}/n\mathbb{Z}$, ou un un groupe qui apparait dans un autre contexte, mais le nombre d'éléments détermine son type d'isomorphisme.

Rappelons que si $H < G$ est un sous-groupe, l'indice de H est le cardinal de l'ensemble G/H des classes à droites modulo H

Théorème 3.3. *Soit C_n un groupe cyclique d'ordre n.*

1. *Si d divise n, C_n contient un unique sous groupe d'ordre d : l'ensemble des g tels que $g^d = 1$. C'est un groupe cyclique d'ordre d.*
2. *Tout sous groupe de C_n est cyclique.*

Démonstration. Notons que 2 résulte de 1 qu'on démontre par deux méthodes très différentes.

Argument 1. Pour cela, on pense à C_n comme au groupe $\mathbb{U}_n$ des racines $n-i$èmes de l'unité. Le sous ensemble $\mathbb{U}_d$ des racines $d-i$èmes est un sous-groupe d'ordre d. Pour démontrer qu'il est le seul, rappelons que le théorème de Lagrange dit que tout sous groupe d'ordre d est contenu dedans.

Argument 2. Oon pense à C_n comme à $\mathbb{Z}/n\mathbb{Z}$. On utilise le fait que tout sous groupe de $\mathbb{Z}$ est de la forme $k\mathbb{Z}$. Si $H < C_n$ est un sous groupe son image réciproque est donc de la forme $k\mathbb{Z}$, où $n|k$, car $k\mathbb{Z} > n\mathbb{Z}$. Le groupe H est donc cyclique, comme quotient de $n\mathbb{Z}$, et c'est en fait $k\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z}$ pour $d = \frac{n}{k}$. □

Théorème 3.4. *Soit C_n un groupe cyclique.*

1. *Tout quotient de C_n est un groupe cyclique d'ordre divisant n.*
2. *Si d/n, le groupe C_n admet un unique quotient de cardinal d et isomorphe à C_d. On peut le réaliser comme l'image de $\varphi: C_n \to C_n$ définie par $\varphi(x) = x^{n/d}$.*

Démonstration. Le 1. est plus ou moins évident car un groupe cyclique est un groupe fini engendré par un seul élément. Pour réaliser concrètement ce quotient, on peut considérer l'homomorphisme, $\varphi: G \to G$ défini par $\varphi(x) = x^{n/d}$. Comme son noyau est d'ordre n/d son image est un groupe cyclique d'ordre d ; cela démontre 2.

□

Avertissement 3.5. Attention, l'homomorphisme φ de la démonstration n'induit pas du tout l'identité sur l'image. Par exemple si on pense à C_4 comme étant le groupe $\mathbb{U}_4$ des racines 4-ièmes de l'unité $\varphi(1) = \varphi(-1) = 1, \varphi(i) = \varphi(-i) = -1$.

3.1.2 Le lemme chinois.

Le résultat suivant est connu sous le nom de « Lemme Chinois ».

Théorème 3.6. *Soient a, b deux nombres premiers entre eux. Alors tout groupe cyclique d'ordre ab est isomorphe à un produit de groupe cyclique d'ordre a et d'un groupe cyclique d'ordre b.*

Démonstration. On en donne deux.

1. On sait que l'image de l'homomorphisme $\varphi : C_{ab} \to C_{ab}$ (resp. Ψ) défini par $\varphi(x) = x^b$ (resp. $\psi(x) = x^a$) est un groupe cyclique d'ordre a (resp. b). On en déduit donc que l'image de l'homomorphsime $\Phi = (\varphi, \psi)$ est un sous-groupe de $C_a \times C_b$. Montrons que Φ est injectif. En effet d'après le théorème de Bézout il existe deux nombres u, v tels que $au + bv = 1$ donc si $x^a = x^b = e$, $x = x^{au+bv} = (x^a)^u (x^b)^v = e$. Ainsi Φ est injective, donc bijective pour des raisons de cardinal.

2. On sait que l'ensemble $C_a = \{x/x^a = 1\}$ (resp, $C_b = \{x/x^b = 1)$ est un sous-groupe cyclique d'ordre a (resp. b) de C_{ab}. Grâce au théorème de Bézout, on voit que l'intersection de ces deux sous-groupes est réduite à 1. Donc l'application produit réalise un isomorphisme $C_a \times C_b \to C$. □

Deux autres démonstrations. La première démonstration utilise le fait qu'un groupe cyclique d'order n est isomorphe à $\mathbb{U}_n$

On considère l'homomorphisme
$\varphi: \mathbb{U}_a \times \mathbb{U}_b \to \mathbb{U}_{ab}$
$\varphi(x, y) = x.y$

On va mq φ est un isomorphisme. En fait il suffit de mq φ est injectif, par des rasions de cardinal.

si $x.y = 1$ alors $x = y^{-1}$ est une racine a-ième de l'unité et une racine b iè de l'unité comme $ap + bq = 1$, $x = x^1 = (x^a)^p \times (x^b)^q = 1$

La deuxième démonstration utilise le fait qu'un groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$

ψ: $\mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$
$x \to (\bar{x}, \bar{x})$
si $\psi(x) = 0$ alors x est divisible par a,b donc (Gauss) il est divisbnle par ab. il est nul dans $\mathbb{Z}/ab\mathbb{Z}$.

On en déduit, par récurrence sur l'entier k, le théorème suivant :

Théorème 3.7. *Soient $a_1, ..., a_k$ des nombres premiers entre eux deux à deux. Alors tout groupe cyclique d'ordre $a_1....a_k$ est isomorphe à un produit $\Pi_{i=1}^k C_{a_i}$ de groupes cycliques d'ordre a_i.* □

Exemple 3.8. Si la décomposition en facteurs premiers de n est $n = \Pi_{i=1}^k p_i^{a_i}$, on a $\mathbb{Z}/n\mathbb{Z} \simeq \Pi_{i=1}^k \mathbb{Z}/p_i^{a_i}\mathbb{Z}$.

On pourrait se demander si on peut décomposer un groupe cyclique d'ordre p^n (par exemple $\mathbb{Z}/p^n\mathbb{Z}$) en produit ou pas.

Proposition 3.9. *C_{p^n} n'est pas un produit de deux groupes.*

Démonstration. On raisonne par l'absurde et on suppose que C_{p^n} est un produit. Comme tout sous-groupe d'un groupe cyclique est cyclique, C_{p^n} serait de la forme $C_{p^{n_1}} \times C_{p^{n_2}}$ avec $n_1 + n_2 = n$. Mais dans $C_{p^{n_1}} \times C_{p^{n_2}}$ tout élément est d'ordre $p^{\max(n_1,n_2)}$, et ce groupe ne contient pas d'élément d'ordre exactement p^n : il n'est donc pas isomorphe à C_{p^n}. □

3.1.3 Groupe abéliens libres types finis et sous-groupes de $\mathbb{Z}^n$, première approche.

Dans ce paragraphe nous allons étudier le groupe $\mathbb{Z}^n$, ses sous-groupes, ses automorphismes, et les homomorphismes de $\mathbb{Z}^n$ vers $\mathbb{Z}^m$.

Définition 3.10. *On dit qu'un groupe abélien est de type fini si il est engendré par un nombre fini d'éléments.*

Si le groupe abélien A est engendré par des éléments $a_1, ...a_k$ l'homomorphisme φ_A: $\mathbb{Z}^k \to A$ définit par $\varphi_A \begin{pmatrix} n_1 \\ n_2 \\ \\ n_k \end{pmatrix} = \Sigma_{i=1}^k n_i a_i$ est surjectif.

Définition 3.11. *Un groupe abélien libre de rang n est un groupe isomorphe à $\mathbb{Z}^n$.*

Proposition 3.12. *Un groupe abélien est libre si on peut choisir un système de générateurs A tel que φ_A soit un isomorphisme.*□

Commençons par une observation importante.

Théorème 3.13. *Si $\mathbb{Z}^n$ est isomorphe à $\mathbb{Z}^p$ alors $n = p$.*

Démonstration. Notons en effet $\Lambda = \mathbb{Z}^l$. L'ensemble 2Λ des éléments de la forme $2x$, pour $x \in \Lambda$, est un sous-groupe, et $\Lambda/2\Lambda = \mathbb{Z}/2\mathbb{Z}^l$ a exactement l élément. On a donc $l = \log_2(\Lambda/2\Lambda)$ et l est bien déterminé par Λ. □

Proposition 3.14. *Soient A, B deux groupes abéliens libres de rangs n et p.*

La somme $A \oplus B$ est un groupe abélien libre de rang $n+p$

L'ensemble $\mathrm{Hom}(A,B)$ *est un groupe abélien libre de rang $n.p$ isomorphe au groupe additifs des matrices (p,n) à coefficients entiers*

En particulier le dual $\mathrm{Hom}(A,\mathbb{Z}) = A'$ *est aussi un groupe abélien libre.*

Démonstration. $\mathbb{Z}^n \oplus \mathbb{Z}^p = \mathbb{Z}^{n+p}$, $\mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z}^p) = \mathbb{Z}^p \oplus \cdots \oplus \mathbb{Z}^p$ (n facteurs), $\mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z}) = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (n fcateurs). □

Remarque 3.15. Un groupe abélien libre est un peu comme un espace vectoriel, sauf qu'à la place d'un corps comme ensemble de scalaires, on met les nombres entiers. On parle de $\mathbb{Z}-$module libre. Dans le cas de $\mathbb{Z}^n$ les éléments sont des matrices $(n,1)$ à coefficients entiers, on parle volontiers de vecteurs.

Définition 3.16. *Soit Λ un groupe abélien libre. On dira qu'une famille finie de vecteurs $A \subset \Lambda$ est libre (sur $\mathbb{Z}$) si l'équation $\Sigma_{a \in A} n_a a = 0$ implique que tous les n_a sont nuls.*

Exemple 3.17. Le sous-groupe engendré par une famille d'éléments d'un groupe abélien libre est l'ensemble des combinaisons linéaires **à coefficients entiers** de ces éléments.

Définition 3.18. *Une $\mathbb{Z}$-base du groupe abélien libre Λ est une famille de vecteurs libres sur $\mathbb{Z}$ qui engendre Λ.*

Proposition 3.19. *Soit $A = \{a_1, ...a_k\} \subset \Lambda$ un ensemble fini et $\varphi_A = \mathbb{Z}^k \to \Lambda$ l'homomorphisme $\varphi_A(x_1, ..., x_k) = \Sigma_{i=1}^k x_i a_i$. Alors A est libre si et seulement si φ_A est injectif, et A est génératrice si et seulemnt si φ_A est surjective.*

Démonstration. Laissée en exercice. □

Lemme 3.20. *Tout sous-groupe d'un groupe abélien libre de rang n est libre de type fini, et de rang inférieur ou égal à n*

Démonstration. La démonstration se fait par récurrence sur l'entier n. On peut supposer que $\Lambda = \mathbb{Z}^n$.

Initialisation. Le cas $n = 1$ a déjà été vu. On sait qu'un sous groupe de $\mathbb{Z}$ est soit 0 soit $a\mathbb{Z}$, donc libre de rang 0 ou 1.

Induction. On pose $e_1 = \begin{pmatrix} 1 \\ 0 \\ . \\ 0 \end{pmatrix}$, et considère la suite d'homomorphismes :

$$\mathbb{Z}e_1 = \ker(\pi) \ \to \ \mathbb{Z}^n \ \overset{\pi}{\to} \ \mathbb{Z}^{n-1} \ \to \ 0$$

Par définition, l'image du vecteur $\begin{pmatrix} x_1 \\ x_2 \\ . \\ x_n \end{pmatrix} \in \mathbb{Z}^n$ par π est $\begin{pmatrix} x_2 \\ x_3 \\ . \\ x_n \end{pmatrix} \in \mathbb{Z}^{n-1}$.

Soit Λ un sous-groupe de $\mathbb{Z}^n$. Grâce à la l'hypothèse de récurrence, on sait que son image dans $\mathbb{Z}^{n-1}$ est un groupe libre de type fini engendré par $f'_1, ...f'_d$, avec $d \leqslant n-1$ Regardons le noyau de la restriction de la projection π à Λ. Si il est réduit à 0, l'homomorphisme π induit un isomorphisme, et on a terminé. Sinon, c'est un sous groupe de $\mathbb{Z}e_1$, donc engendré par un élément $f_1 = ae_1$. Relevons les f'_i en des éléments f_i de Λ. On vérifie que $f_1, ...f_d$ est une base de Λ. □

Théorème 3.21. *Soit $\Gamma \subset \Lambda$ un sous-groupe d'un groupe abélien libre de rang n. Il existe une base $e_1, ...e_n$ de Λ et des entiers $d_1, ...d_r$ tels que $d_i | d_{i+1}$ et $\Gamma = \mathbb{Z}d_1e_1 \oplus ...\mathbb{Z}d_re_r$.*

Démonstration. On va démontrer ce résultat par récurrence sur l'entier n.

Initialisation. On sait qu'un sous-groupe Γ de $\mathbb{Z}$ est de la forme $d\mathbb{Z}$. L'unicité de d se voit en disant que c'est le cardinal de $\mathbb{Z}/\Gamma$

Induction. Si $\Gamma = 0$ il n'y a rien à démontrer. Sinon, on considère l'image par Γ de toutes les formes linéaires sur $\Lambda = \mathbb{Z}^n$, c'est à dire $\Lambda'(\Gamma) \subset \mathbb{Z}$. C'est un sous groupe de $\mathbb{Z}$, donc de la forme $d_1\mathbb{Z}$.

Il y a un élément de Γ, disons e_1' et une forme linéaire φ de Λ' telle que $\varphi(e_1') = d_1$. Mais, si on fixe une base, toutes les coordonnées de e_1' sont divisibles par d_1, donc il existe un vecteur e_1 dans Λ tel que $d.e_1 = e_1'$

Lemme 3.22. $\Lambda = \mathbb{Z}e_1 \oplus \ker\varphi$ *et* $\Gamma = d_1.\mathbb{Z}e_1 \oplus \ker\varphi \cap \Gamma$

Démonstration. Cela résulte de $x = \varphi(x)e_1 + (x - \varphi(x)e_1)$
On remarque que cette écriture décompose n'importe quel élément de Λ comme somme d'un ceteur proportionnel à e_1 et d'un vecteur de $\ker(\varphi)$, dou la première égalité.
Pour la seconde, on remarque que si $x \in \Gamma$ $\varphi(x) \in d_1\mathbb{Z}$, donc $\varphi(x)e_1 \in \Gamma \cap d_1.\mathbb{Z}e_1 = \mathbb{Z}e_1'$. ET par différnce $(x - \varphi(x)e_1) \in \Gamma$ et bien entenud est toujours dans $\ker(\varphi)$ □

Pour terminer l'argument de récurrence, nous remarquons $\ker\varphi$ est libre. En effet tout sous groupe de $\mathbb{Z}^n$ est libre. Il est de rang $n-1$ car on sait $\text{rang}(\ker(\varphi)) + 1 = \text{rang}(\Lambda)$. On peut donc appliquer l'hypothèse de récurrence à $\ker\varphi \cap \Gamma < \ker\varphi$, ce qui termine la démonstration.
□

On peut alors obtenir un théorème dit théorème de structure des groupes abéliens de type finis

Théorème 3.23. *Soit Γ un groupe abélien de type fini. Il existe des entiers $d_1, ...d_k$ et un entier r tels que : $d_i > 1$ et pour tout i $d_i | d_{i+1}$, et A est isomorphe à $\mathbb{Z}^r \oplus_{i=1}^k \mathbb{Z}/d_i\mathbb{Z}$*

Les entiers r (le rang) et d_i (les diviseurs élémentaires) déterminent A a isomorphisme près. Il s'appelent le rang et les diviseurs élémentaires du groupe Γ.

Démonstration.

La partie « existence » du théorème de structure résulte du théorème précédent : on écrit Γ comme quotient d'un groupe abélien libre Λ, et on choisi une base adaptée au noyau $\ker\varphi$. Quitte à changer de base, on peut supposer que $\Lambda = \mathbb{Z}^n$ et $\ker\varphi = d_1\mathbb{Z}e_1 + ... + d_k\mathbb{Z}e_k$. On pose $r = n - k$, et on a le résultat.

La partie difficile est l'unicité. Mais l'existence étant établie on remarque que

Lemme 3.24. *Soit Γ un groupe abélien de type fini. La réunion de tout ses sous-groupes finis est un groupe fini et Γ/F est libre.* □

Démonstration. Dans l'écriture $\Gamma \simeq \mathbb{Z}^r \oplus_{i=1}^k \mathbb{Z}/d_i\mathbb{Z}$, on remarque que $F = \oplus_{i=1}^k \mathbb{Z}/d_i\mathbb{Z}$ est la réunion de tous les sous-groupes finis. Le quotient de Γ par F est le groupe $\mathbb{Z}^r$ qui est libre de rang r. □

Pour conclure, nous devons donc démontrer

Lemme 3.25. *Si $A = \oplus_{i=1}^k \mathbb{Z}/d_i\mathbb{Z}$ est isomorphe à $\oplus_{j=1}^l \mathbb{Z}/l_i\mathbb{Z}$ avec $d_i > 1, l_j > 1$ et si pour tout i $d_i | d_{i+1}$ et pour tout j, $l_j | l_{j+1}$ alors $k = l$ et $d_i = l_i$.*

Soit p le plus petit diviseur premier de d_1. C'est aussi le plus petit diviseur premier de l_1, car c'est le plus petit ordre d'un élément de A.

Soit $f = A \to A$ l'homomorphisme $f(x) = px$. L'image de f est $\oplus_{i=1}^{k}\mathbb{Z}\,/\,(d_i\,/\,p)\mathbb{Z}$ ou $\oplus_{i=1}^{l}\mathbb{Z}/l_i/p\mathbb{Z}$. Par récurrence, sur l'ordre du groupe, on doit donc avoir que le nombre de $l_i > p$ est égal au nombre de $d_i > p$ t de plus $\frac{l_i}{p} = \frac{d_i}{p}$ pour les l_i. Pour ds'assurer que le nombre d l_i égaux à p est égal au nombre de d_i, il suffit alors de regarder l'ordre de A. □

3.1.4 Les deux classifications des groupes abéliens finis.

Comme cas particulier du théorème sur les groupes abéliens de type fini, nous obtenons.

Théorème 3.26. *Soit A un groupe abélien fini. Il existe un entier k et des entiers $d_1, ...d_k$ tels que : pour tout i, $d_i > 1$, $d_i | d_{i+1}$, et A est isomorphe à $\oplus_{i=1}^{k}\mathbb{Z}/d_i\mathbb{Z}$. Ces entiers sont uniques.*

Définition 3.27. *Les nombres d_i sont les diviseurs élémentaires de A.*

Remarque 3.28. Un groupe abélien fini est bien défini, à isomorphsime près par ses diviseurs élémentaires.

Pour aller plus loin, nous avons la définition de composante primaire d'un groupe abélien fini.

Définition 3.29. *Soit p un nombre premier. Si A est un groupe abélien fini, on note $A_p = \{x\,/\,\exists n \quad \text{tq}\, p^n x = 0\}$. Le groupe A_p s'appelle la composante p primaire de G.*

Remarque 3.30. Si p ne divise pas l'ordre de A la composante p-primaire est réduite à 0.

Théorème 3.31. *Si A est un groupe abélien fini, alors A est la somme directe de ses composantes $p-$primaires.*

Démonstration. Soit $\{p_1, ...p-k\}$ l'ensemble des diviseurs premiers de A. On considère l'application $\varphi : \oplus A_{p_i} \to A$ qui a $(x_1, ...x_k)$ associe $x_1 + \cdots + x_k$. Il s'agit de voir que c'est un isomorphisme.

Si $x \in A$, il engendre un groupe cyclique. En appliquant le lemme chinois a ce groupe, on voit que x est bien dans l'image de φ. Pour évaluer le noyau considérons $(x_1, ...x_k)$ tel que $x_1 + \cdots + x_k = 0$. Soient $p_i^{n_i}$ les ordres des x_i. Multiplions tout par $p_2^{n_2}....p_k^{n_k} = q$. Alors $qx_1 = 0$, mais q est premier à l'ordre de x_1 donc $x_1 = 0$. De même pour les autres x_i et φ est bijective. □

Remarque 3.32. le théorème 3.31 est une version sophistiquée du Lemme Chinois $\mathbb{Z}\,/\,p_1^{n_1}....p_k^{n_k}\mathbb{Z} = \oplus_{i=1}^{k}\mathbb{Z}\,/\,p_i^{n_i}\mathbb{Z}$. On écrit $A = \oplus_p A_p$. Exemple $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z})^2$

Remarque 3.33. On utilise pas « fini », mais simplement le fait que tout élément est d'ordre fini. Un groupe dont tout élément est d'ordre fini est dit « groupe de torsion ». Un groupe abélien de torsion est la somme dircete de ses composantes p primaires, ou p désigne l'ensmebles des nombres premiers.

Théorème 3.34. *Soit A un groupe abélien fini, p_1, $....p_k$ les diviseurs premiers de $|A|$. Alors A s'écrit d'une unique façon comme somme directe de groupes cycliques d'ordre $p_1^{\alpha_1^1}$, $...p_1^{\alpha_{n_1}^1}$, ...;, $p_k^{\alpha_1^k}, ...p_k^{\alpha_{n_k}^k}$*

Démonstration. On décompose A en somme directe de ses composantes primaires puis on applique le théorème de classification à chaque composante. □

Remarque 3.35. Nous disposons donc de deux classifications des groupes abéliens finis qui ne sont pas les mêmes.

3.2 Algèbre linéaire dans $\mathbb{Z}^n$

3.2.1 Le groupe $\mathrm{GL}(n,\mathbb{Z})$ et les matrices élémentaires.

Le groupe $\mathrm{GL}(n,\mathbb{Z})$ est le groupes des matrices (n,n) à coefficients entiers, inversible, et dont l'inverse est aussi à coefficients entiers.

Proposition 3.36. *Une matrice de $M(n,\mathbb{Z})$ est dans $\mathrm{GL}(n,\mathbb{Z})$ si et seulement si son déterminant est ± 1.*

Démonstration. Le déterminant d'une matrice à coefficients entiers est à coefficients entiers. Si $AB = \mathrm{Id}$ $\det(A)\det(B) = 1$. Dons si de plus B est à coefficients entiers, $\det(A)$ est un élément inversible de $\mathbb{Z}$ soit ± 1. Réciproquement la formule de Cramer $A^{-1} = \frac{1}{\det(A)}\mathrm{Cof}^t(A)$ montre que si $\det(A) = \pm 1$ et si A est à coefficients entiers, son inverse l'est aussi. Ici $\mathrm{Cof}(A)$ est la matrice des cofacteurs : $\mathrm{Cof}(A)_{i,j} = \det(A_{i,j})$, où $A_{i,j}$ est obtenue à partir de A en enlevant sa $i-i$ème ligne et sa $j-i$ème colonne, et $\mathrm{Cof}^t(A)$ est sa transposée. □

Le groupe $\mathrm{GL}(n,\mathbb{Z})$ opère sur l'ensemble des bases de $\mathbb{Z}^n$ est cette opération est libre et transitive : une famille de vecteurs est une base de $\mathbb{Z}^n$ si, et seulement si, la matrice formée par ses coordonnées est inversible. Autrement dit étant une base B, il existe un unique élément g de $\mathrm{GL}(n\mathbb{Z})$ tel que $B = gB_0$, où B_0 c'est la base canonique de $\mathbb{Z}^n$. EN fait g est la matrice dont les vecteurs coonnes sont les éléments de B. On en déduit donc :

Proposition 3.37. *Le groupe $\mathrm{GL}(n,\mathbb{Z})$ est le groupe des automorphismes du groupe $\mathbb{Z}^n$.*□

Les matrices élémentaires jouent un rôle important en algèbre linéaire.

Définition 3.38. *Les matrices élémentaires de $M(n,\mathbb{Z})$ sont les matrices $E_{i,j}$ (avec $i \neq j$) dont tous les coefficients sont nuls sauf à la i-ième colonne et j-ième ligne ou on a mis un 1.*

Notons que $E_{ij}e_i = e_j$ et $E_{ij}e_k = 0$ sinon.

Si $i \neq j$, on définit aussi la matrice S_{ij} par $S_{ij}(e_k) = e_k$ si $k \neq i, j$, $S_{ij}(e_j) = e_i$ et $S_{ij}(e_i) = e_j$.

Nous savons depuis longtemps que les matrices ainsi définies permettent de décrire les opérations élémentaires sur les lignes et les colonnes. Décrivons d'abord les opérations sur les colonnes $(C_i)_{1 \leqslant i \leqslant n}$.

On note $M(m,n,\mathbb{Z})$ les matrices à m lignes, n colonnes et à coefficients entiers.

Lemme 3.39. *Soit $M \in M(m,n,\mathbb{Z})$. Multiplier M à droite par S_{ij} , revient à échanger les deux colonnes i, j. Remplacer la colonne C_i par $C_i + aC_j$ c'est multiplier M à droite par la matrice $Id + aE_{ij}$.*□

De même on peut décrire les opérations sur les lignes $(L_j)_{1 \leqslant j \leqslant m}$.

Lemme 3.40. *Soit $M \in M(m,n,\mathbb{Z})$. Multiplier M à gauche par S_{ij}^m , revient à échanger les deux lignes i, j. Remplacer L_i par $L_i + aL_j$ c'est multiplier à gauche par la matrice $\mathrm{Id} + aE_{ij}^m$.*□

Corollaire 3.41. *L'inverse de $\mathrm{Id} + aE_{\mathrm{ij}}$ est $Id - aE_{\mathrm{ij}}$* □

Ces deux lemmes vont nous permettre d'étudier l'action à gauche (resp. droite) de $\mathrm{GL}(m,\mathbb{Z})$ (resp. $\mathrm{GL}(n,\mathbb{Z})$) sur $M(m,n,\mathbb{Z})$.

3.2.2 La méthode du pivot de Gauss, et les équations à coefficients entiers

On va étudier l'action à gauche de $\mathrm{GL}(m,\mathbb{Z})$ sur $M(m,n,\mathbb{Z})$

Théorème 3.42. *Soit $M \in M(n,\, m,\, \mathbb{Z})$. Il existe une matrice inversible Q dans $\mathrm{GL}(m,\, \mathbb{Z})$, produit de matrices élémentaires, et des entiers $a_1,\, ...a_d$ tels que la matrice MQ soit étagée* $\begin{pmatrix} a_{11} & 0 & & & & & \\ a_{21} & a_{22} & 0 & & & & \\ a_{31} & a_{32} & a_{33} & 0 & & 0 & \\ & & & . & 0 & & \\ & & & & a_{mm} & 0\ 0 & 0 \end{pmatrix}$ si $m \geqslant n$ *ou* $\begin{pmatrix} a_{11} & 0 & & & \\ a_{21} & a_{22} & 0 & & \\ a_{31} & a_{32} & a_{33} & 0 & \\ . & & & . & 0 \\ & & & & a_{mm} \\ a_{m+1,1} & & & & a_{m+1m} \\ & & & & \\ a_{n,1} & & & & a_{n,m} \end{pmatrix}$ *si $n>m$.*

Démonstration. La démonstration se fait par récurrence sur l'entier m, en notant que si $m=1$ la matrice est déjà étagée.

Si tous les coefficients de la première ligne sont nuls sauf le premier, on raisonne par mouvement élémentaire sur la matrice $(n-1,\, m-1)$ obtenue en enlevant la première ligne et la première colonne.

Si la première ligne a un seul coefficient non nul, on se ramène au cas précédent en échangeant la colonne correspondante avec le première. Si la première ligne est nulle on ne la change pas.

Sinon, considérons le plus petit coefficient non nul de cette première ligne en valeur absolue. Disons qu'il est sur la colonne i. Pour chaque colonne j, on considère la division euclidienne de $a_{1,j}=d_j a_{1,i}+r_{1,j}$. On enlève d_j fois C_i à C_j et on est ramené à une matrice dont la première ligne a pour coefficient $a_{1,j}$ et les $r_{1,j}$ strictement plus petit ou nuls. On recommence jusqu'à n'avoir qu'un seul coefficient non nul. □

Ce théorème, et surtout sa démonstration constructive, suffisent largement à « résoudre » les équations de la forme $AX = B$ ou $A \in M(m,\, n,\, \mathbb{Z})$ est une matrice à coefficients entiers $B \in \mathbb{Z}^m$, $X \in \mathbb{Z}^n$ X est l'inconnue et les matrices A, B sont connues. Ces équations sont tellement importantes qu'on leur a donné un petit nom.

Définition 3.43. *Une équation de la forme $AX = B$ ou $A \in M(m,\, n,\, \mathbb{Z})$ est une matrice à coefficients entiers$B \in \mathbb{Z}^m$, $X \in \mathbb{Z}^n$, ou X est l'inconnue est une équation diophantienne linéaire.*

Cependant, si on veut aller plus loin et établir la structure de l'ensemble des solutions on peut établir un résultat plus fort.

Théorème 3.44. *Soit $M \in M(n,m,\mathbb{Z})$. Il existe des matrices inversibles P, Q dans $\mathrm{GL}(m,\mathbb{Z})$ et $\mathrm{GL}(n,\mathbb{Z})$, produit des matrices élémentaires et des entiers positifs $a_1,\, ...a_d$ tels $a_1|a_2|...a_d$ et tels que la matrice PMQ n'ait que des coefficients diagonaux* $\begin{pmatrix} a_1 & & & & & & \\ & a_2 & & & & & \\ & & a_3 & & 0 & & \\ & & & & & & \\ & 0 & & a_d & 0 & & \\ & & & & 0 & & 0 \\ & & & & & 0 & \end{pmatrix}$.

Démonstration. La démonstration de ce résultat se fait exactement comme la méthode du pivot usuel, à quelques variantes près. Elle est algorithmique. La première étape est de faire apparaitre le pgcd des coefficients en haut à gauche avec des 0 à sa droite et en dessous.

1. Si l'un des coefficients de la matrice est le pgcd des coefficients, on l'amène en haut à gauche grâce à (au plus) deux mouvements l'un sur les lignes l'autres sur les colonnes.

$$\begin{pmatrix} a_{11} & 0 & & & 0 \\ 0 & \times & \times & & \\ 0 & & & & \\ & & & & \\ & & & & \\ 0 & X & & & \times \end{pmatrix}$$

Pour chaque indice de colonne C_k on remplace alors C_k par $C_k - q_k C_1$ ou $q_k a_{11} = a_{1k}$ pour faire apparaitre des 0 sur la première ligne puis L_k par $L_k - p_k L_1$ où $p_k a_{11} = a_{k1}$ pour faire apparaitre des 0 sur la première colonne.

RQ on a utilisé $m+n$ opérations au plus.

2. Sinon on regarde le plus petit coefficient en valeur absolue disons $a_{i,j}$. Pour chaque k (indice de colonne) coefficients situés sur sa ligne disons $a_{i,k}$, on remplace la colonne correspondante C_k par $C_k - d_k C_i$ et soit on a remplacé tous les coefficients par des 0 soit on a diminué strictement le plus petit coefficient. Si on a pas diminué strictement le plus petit coefficient, on fait la même chose pour les lignes. Après un nombre fini d'étape, le plus petit coefficient se trouve en haut à gauche avec des 0 sur sa ligne et sa colonne. Si ce n'est pas le PGCD des coefficients, il y a un autre coefficient quelque part qu'il ne divise pas. Par deux mouvements sur les lignes et les colonnes, on l'amène à la position $(2,2)$. Notre matrice est équivalente à

$$\begin{pmatrix} a_{11} & 0 & & & 0 \\ 0 & a_{22} & * & & * \\ 0 & * & & & \\ & * & . & & * \\ & & & & \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix} \to \begin{pmatrix} a_{11} & \mathrm{pa}_{11} \\ 0 & a_{22} \end{pmatrix} \to \begin{pmatrix} a_{11} & pa_{11} \\ -a_{11} & r \end{pmatrix}$$

on écrit $a_{22} = pa_{11} + r$ avec $0 \neq r < |a_{11}|$. On ajoute pC_1 à C_2 puis on retire L_1 à L_2 pour faire apparaitre r à la place de a_{22}. On a alors un plus petot coefficient strictemnt plus petit.

3. Une fois que le coefficient en haut à gauche est le pgcd des coefficients, avec des 0 sur sa ligne et sa colonne, on est ramené à étudier la matrice $(n-1, m-1)$ obtenue en enlevant la première ligne et la première colonne. □

Corollaire 3.45. *Le groupe* $\mathrm{GL}(n,\mathbb{Z})$ *est engendré par les matrices élémentaires* $Id + E_{ij}$ *et* $S_{i.j}$

On considère une matrice $M \in \mathrm{GL}(n,\mathbb{Z})$, je sais que je vais trouver des matrices produit de matrice sélémentaires P, Q inversibles et à coefficient entiers telles que

$$PMQ = \begin{pmatrix} a_1 & & & & \\ & a_2 & & & \\ & & a_3 & & \\ & & & & \\ & & & & a_n \end{pmatrix} \quad a_i \in \mathbb{N} \text{ ou } \mathbb{Z}$$

comme $\det(M) = \pm 1$, on a a_i=+-1, car si le produit d'entiers est 1 cveux ci valent 1 ou -1
$PMQ = \mathrm{Id}$ et $M = P^{-1}Q^{-1}$ qui bien un produit de matrices léémentaires.

Démonstration. La matrice diagonale à coefficients entiers positifs $\begin{pmatrix} a_1 & & & & \\ & a_2 & & & \\ & & a_3 & & \\ & & & & \\ & & & & a_d \end{pmatrix}$ est dans $\mathrm{GL}(n,\mathbb{Z})$ si et seulement si $a_1 = \cdots = a_d = 1$. Par la méthode du pivot, on trouve deux matrices P et Q élémentaires telles que $PMQ = Id$ soit $M = P^{-1}Q^{-1}$. □

3.3 Exercices du chapitre 3

On note $(C_n, .)$un groupe cyclique d'ordre n, $(\mathbb{Z}/n\mathbb{Z}, +)$ le groupe des entiers modulo n et $(\mathbb{U}_n, .)$ le groupe des racines n-ièmes de l'unité. Dans cette liste, p est un nombre premier, et tous les groupes sont abéliens, parfois notés additivement, parfois multiplicativement.

3.3.1 Groupe abéliens.

Exercice 3.1. Le produit d'une racine d'ordre exactement a de l'unité et d'une racine d'ordre exactement b est encore une racine de l'unité. Quel peut être son ordre ? c'est plus facile si on suppose que a et b sont premiers entre eux.

Si a et b son premier entre eux, alors les polynômes $x^a - 1$ et $x^b - 1$ ont une seule racine commune.

Exercice 3.2. Soit $\varphi: C_{p^n} \to C_{p^n}$ défini par $\varphi(x) = x^p$ quel est le noyau, quelle est l'image ?

Exercice 3.3. Construire un isomorphisme entre $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/15\mathbb{Z}$.

Construire un isomorphisme entre $\mathbb{U}_3 \times \mathbb{U}_5$ et $\mathbb{U}_{15}$.

Exercice 3.4. Quels sont les diviseurs élémentaires de $G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})^2 \oplus \mathbb{Z}/9\mathbb{Z}$

$G = \oplus_p A_p \quad$ où $A_p = \{g \in G \text{ dont } l'\text{ordre est une puissance de } \quad p\}$

Exercice 3.5. Si p est un nombre premier, démontrer que $C_{p^n} \times C_{p^m}$ n'est pas un groupe cyclique.

Exercice 3.6. Soit p un nombre premier. Combien le groupe $C_{p^2} \times C_{p^4} \times C_{p^8}$ a-t-il d'éléments d'ordre p?

Exercice 3.7. (Vu en cours avec une autre méthode) Soit $n_1 \leqslant n_2 \leqslant n_3$, $m_1 \leqslant m_2 \leqslant m_3$ 6 nombres entiers et p un nombre premier. On suppose que $C_{p^{n_1}} \times C_{p^{n_2}} \times C_{p^{n_3}}$ est isomorphe à $C_{p^{m_1}} \times C_{p^{m_2}} \times C_{p^{m_3}}$ Démontrer que $m_i = n_i$. On pourra considérer l'homomorphisme $\Phi(x) = x^p$ (quel est le noyau , quelle est l'image)

Généraliser à un produit arbitraire de groupe cycliques.

Exercice 3.8. En utilisant la classification, déterminer quels sont les classes d'isomorphisme de groupes abéliens d'ordre 20, 40 , 35

Exercice 3.9. Dans $(\mathbb{Q}, +)$ tout sous groupe de type fini est isomorphe à $\mathbb{Z}$.

Exercice 3.10. A faire sans la classification, mais juste la décomposition en composantes primaires.

Quelles sont les composantes $p-$primaires possibles des groupes d'ordre 21,30, 462

Démontrer que les groupes abéliens d'ordre 30030 sont tous cycliques

Exercice 3.11. Si A est un groupe abélien fini, ses composantes p primaires sont invariantes par tout automorphisme de A. Pour un groupe abélien A d'ordre 35 déterminer :

les sous-groupes, les sous groupes invariants par tout automorphisme de A.

Exercice 3.12. Soit p un nombre premier et G un groupe abélien isomorphe à $C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_k}}$ avec $n_1 \geqslant n_2 ... \geqslant n_k$. Démontrer que si $H < G$ et si $H = C_{p^{l_1}} \times C_{p^{l_2}} \times \cdots \times C_{p^{l_k}}$ avec $l_1 \geqslant n_2 ... \geqslant l_p$ alors $l_1 \leqslant n_1, ...l_k \leqslant n_k$.

Exercice 3.13. Soit p un nombre premier. Combien $C_{p^4} \times C_{p^3} \times C_{p^2}$ a t il d'éléments d'ordre exactement p.

Exercice 3.14. Quel est le groupe des automorphismes d'un groupe abélien d'ordre 21.

Exercice 3.15. Soit $n \in \mathbb{N}$. On note $\mathbb{Z}[1/n]$ le sous groupe de $\mathbb{Q}$ engendré par 1

3.3.2 Algèbre linéaire dans $\mathbb{Z}^n$

Exercice 3.16. Quel est le noyau de f et le quotient de $\mathbb{Z}^n$ par $\ker(f)$:

De $\mathbb{Z}^2$, où $f\begin{pmatrix} x \\ y \end{pmatrix} = 2x - y$

De $\mathbb{Z}^3$, où $f\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3x + 6y + 6z \\ 6x + 13y + 5z \end{pmatrix}$

De $\mathbb{Z}^3$ par où $f\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3x + 9y + 9z \\ 9x - 3 + 9z \end{pmatrix}$

Exercice 3.17. Résoudre les équations suivantes à coefficients entiers.

1. $3x + 6y + 6z = 4, 6x + 13y + 5z = 7$
2. $2x + 7y - 3y = 11, 4x + 5y + 3z = 2$

Exercice 3.18. Soit G un groupe fini abélien. On suppose que pour tout entier n l'équation $z^n = e$ a au plus n solutions. En utilisant la classification démontrer que G est cyclique.

Si $\mathbb{K}$ est un corps, démontrer que tout sous-groupe fini de $\mathbb{K}^*, \times$ est cyclique.

Exercice 3.19. Soit (G,+) un groupe abélien de type fini. Existe-t-il un élément $a \neq 0$ tel que pour tout entier n, l'équation $nx = a$ admette une solution.

Chapitre 4

* Groupes nilpotents et théorèmes de Sylow.

On va parler de groupes finis.

4.1 Théorèmes de Sylow.

On fixe un nombre premier p.

Définition 4.1. *Un $p-$ groupe fini est un groupe fini dont l'ordre est une puissance de p.*

Exemple 4.2. La composante p primaire d'un groupe abélien fini est un p groupe fini. Il est de la forme $\mathbb{Z}/p^{n_1}\mathbb{Z}\times ...\times \mathbb{Z}/p^{n_k}\mathbb{Z}$

Exemple 4.3. Le groupe $T_n(p)$ des matrices triangulaires supérieures avec des 1 sur la diagonale et à coefficients dans le corps $\mathbb{F}_p$ est un groupe d'ordre $p^{\frac{d(d-1)}{2}}$.

$\begin{pmatrix} 1 & & & & \\ & 1 & \times & \times & \\ 0 & & 1 & \times & \\ & 0 & & 1 & \\ & & & & 1 \end{pmatrix}$ à coefficients dans le corps $\mathbb{F}_p$ en bijection avce $(\mathbb{F}_p)^{\frac{d(d-1)}{2}}$

Définition 4.4. *Soit G un groupe fini, et p^d la plus grande puissance de p divisant $|G|$. Un sous p-Sylow de G est un sous-groupe de G d'ordre p^d.*

Théorème 4.5. *Soit p un diviseur premier de l'ordre du groupe fini G. Alors G contient un $p-$*Sylow*. Et deux p Sylow sont conjugués dans G.*

Remarque 4.6. On a démontré qu'un groupe abélien fini est la somme directe de ses composantes p primaire $G=\oplus A_p$, en particulier $|G|=\Pi|A_p|$ et donc le composantes p primaires de G sont ses ses Sylow.

On va démontrer un

Lemme 4.7. *Soit Γ un groupe fini, et $\Lambda<\Gamma$ un $p-$*Sylow*. Soit $G<\Gamma$ un sous-groupe. Alors G contient un $p-$*Sylow*, et celui-ci est conjugué dans Γ à un sous groupe de Λ.*

$|\Gamma|=p^n \quad r$ avec $r\in\mathbb{N}, r\wedge p=1$ et $|\Lambda|=p^n$., en particulier, $|\Gamma/\Lambda|=r$

Démonstration. On fait opérer G dans l'ensemble Γ/Λ, et on écrit l'équation aux classes.

$|\Gamma/\Lambda|=\sum_{\text{orbite}} G/G_\gamma$

Ecrivons $|G|=p^dq$. Nous allons montrer que l'un des G_γ est un $p-$Sylow de G.

Pour tout élément γ le sous-groupe G_γ est conjugué à un sous groupe de Λ, c'est donc un $p-$groupe et $|G_\gamma| = p^k$. Il en résulte que si aucun des p -groupes G_γ n'est un Sylow ($p^k < p^d$), le cardinal de chaque orbite G/G_γ est divisible par p, et donc aussi celui de l'espace homogène $|\Gamma/\Lambda|$, ce qui est une contradiction. Donc l'un des stabilisateurs est un Sylow, ce qui veut dire que non seulement G admet un Sylow, mais qu'en plus il est conjugué, dans Γ à un sous groupe de Λ. □

Remarque 4.8. La partie « deux p Sylow de G sont toujours conjugués » est ainsi démontrée sous réserve d'existence. Si $S < G$ est un $p-$Sylow et S' un autre, on sait qu'il existe un g tel que $gS'g^{-1} < S$.

On sait que tout sous groupe est isomorphe à un sous groupe du groupe symétrique S_n, pour $n = |G|$. En effet $G \to S(G)$ qui à g associe la multiplication à gauche est un homomorphisme.

Or S_n est un sous groupe de $\mathrm{GL}_n(\mathbb{F}_p)$. Matrices de permutaions des vecturs d'un $\mathbb{F}_p$ espace vectoriel de dimension p. Pour conclure, il suffit de démontrer

Proposition 4.9. *Le groupe $T_n(p)$ constitué des matrices triangulaires supérieures avec des 1 sur la diagonale, dont le cardinal est $|T_n(p)| = p^{\frac{n(n-1)}{2}}$ est un p- Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$. Plus précisément :*

1. $|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1) \times p^{n-1} \times \mathrm{GL}(n-1, \mathbb{F}_p)$
2. $|\mathrm{GL}(n, \mathbb{F}_p)| = p^{\frac{n(n-1)}{2}} \times \Pi_{i=1}^{n}(p^i - 1) \times (p-1)^n = p^{\frac{n(n-1)}{2}} q$ *avec* $q = 1(p)$.

Démonstration. Pour démontrer le premier point, on fait opérer $\mathrm{GL}(n, \mathbb{F}_p)$ sur $\mathbb{F}_p^n$. Le stabilisateur de $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ est $\begin{pmatrix} 1 & a \\ 0 & A \end{pmatrix}$ ou $\times$ est n'importe quel nombre non nul, a n'importe quel élément de F_p^{n-1} et A un élément de $\mathrm{GL}(n-1, \mathbb{F}_p)$. Le cradinal du stabilisateur de ce vecteur est donc $p^{n-1} \times \mathrm{GL}(n-1, \mathbb{F}_p)$.

Je connais le groupoe, le stabilisateur d'un point, il me reste à dércire l'orbite qui est simplemnt $\mathbb{F}_p^n - 0$: tout vecteur non nul est le prmier vecteur d'une base. Son cardinal est $p^n - 1$

$|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1) \times p^{n-1} \times \mathrm{GL}(n-1, \mathbb{F}_p)$ résulte de la formule de Lagrange $|G| = |O| \times |G_x|$, ou x est ici le vecteur $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

Le second point en résulte par récurrence sur l'entier n □

Les p-Sylow sont des sous groupes importants, et souvent ont doit étudier leur normalisateur.

Définition 4.10. *Si $H < G$ est un sous groupe, $N(H) = \{g \in G / gHg^{-1} = H\}$ est le plus grand sous groupe de G dans lequel H est normal.*

Proposition 4.11. *Soit $S < G$ un $p-$Sylow. Alors S est un sous groupe invariant de $N(S)$.*

Démonstration. En effet tous les $p-$ Sylow de $N(S)$ sont conjugués dans $N(S)$ à S , donc par définition égaux à S. Comme un automorphisme envoie un $p-$ Sylow dans un autre, tout automorphisme de $N(S)$ préserve S. □

4.2 Groupes nilpotents

Pour illustrer l'interêt des théorèmes de Sylow, nous allons donner une application à l'étude des groupes nilpotents.

Rappelons que le centre d'un groupe est $Z(G)=\{x\in G/\forall g\in G, xg=gx\}$. C'est un sous groupe normal de G.

On peut définir l'idée de groupe nilpotent par récurrence.

Définition 4.12. *On dit qu'un groupe est nilpotent de classe k si son centre est non réduit à 0 et si $G/Z(G)$ est nilpotent de classe $k-1$.*

Exemple 4.13. Un groupe abélien est un groupe nilpotent de classe 1.

Exemple 4.14. Tout sous groupe et tout quotient d'un groupe nilpotent est nilpotent

Exemple 4.15. Le groupe $T_n(p)$ est nilpotent de classe $n-1$.(Exercice)

Proposition 4.16. *Tout p groupe fini est nilpotent.*

Démonstration. On a vu (équation aux classes) qu'un p groupe fini a un centre non trivial. Le quotient par son centre est encore un p groupe fini, et on a ainsi le résultat par récurrence sur l'ordre du groupe. □

Souvent, les démonstrations concernant les groupes nilpotents se font par récurrence.

Proposition 4.17. *Soit G un groupe nilpotent et $H<G$ un sous groupe propre. Alors alors H est un sous groupe propre de son normalisateur $N(H)=(g\in G/gHg^{-1}=H)$.*

Démonstration. Si $Z(G)\not\subset H$ $N(H)>Z(G)$ et on a fini. Sinon, $Z(G)<H$. On regarde l'image $\bar{H}$ de H dans $G/Z(G)$. Comme $H\neq G$ et $H>Z(G)$, $\bar{H}\neq G/Z(G)$. Par récurrence $N(\bar{H})\neq\bar{H}$. Soit $g\in G$ dont l'image normalise $\bar{H}$. Montrons qu'il normalise $H=\pi^{-1}(\bar{H})$. En effet $ghg^{-1}h^{-1}$ se projette sur un élément de $\bar{H}$ donc est dans H. □

Théorème 4.18. *Tout groupe nilpotent est le produit direct de ses groupes de Sylow.*

Remarque 4.19. Dans le cas des groupes abéliens, c'est déjà vu : tout groupe abélien est le produit de ses composantes primaires.

Démonstration.

Lemme 4.20. *Les $p-$Sylow de G sont normaux.*

Démonstration. Soit S un $p-$Sylow. Soit g un élément qui normalise $N(S)$. La conjugaison par cet élément est un automorphisme de $N(S)$, mais S est invariant dans $N(S)$ donc g normalise S. Ainsi $N(N(S))=N(S)$ et donc $N(S)=G$, puisque G est nilpotent. □

Comme les sous-groupes Sylow sont normaux, on parle du Sylow de G et non pas d'un $p-$ Sylow.

Lemme 4.21. *Si G est nilpotent, les sous-groupes de Sylow de G commutent.*

Démonstration. Soit S un p-Sylow et S' un p' Sylow, avec $p\neq p'$. Leur intersection est réduite à $\{e\}$ car l'ordre de ce sous-groupe divise p et p'. Si $g\in S$, $g'\in S'$ $gg'g^{-1}g'^{-1}=g\,(g'g^{-1}g'^{-1})=(gg'g^{-1})g'^{-1}$, et $gg'g^{-1}g'^{-1}\in S\cap S'$ donc $gg'=g'g$. □

Si $|G|=p_1^{n_1}....p_k^{n_k}$ et si pour tout k S_k est le $p-$Sylow de G, l'application produit $S_1\times\cdots\times S_k\to G$ est un homomorphisme. Pour sur convaincre qu'il est bijectif considérons son noyau N les p_i Sylow de N sont conjugués dans S_i, mais $N\cap S_i=\{e\}$. Donc $N=\{e\}$, l'application produit est injective et donc bijective pour des raisons de cardinal. □

Corollaire 4.22. *Un groupe fini est nilpotent si et seulement si il est le produit de ses sous-groupes de Sylow.*

4.3 Exercices sur le chapitre 4.

4.3.1 Théorèmes de Sylow

Exercice 4.1. Si p est un nombre premier, il existe un unique (à isomorphisme près) groupe d'ordre p^2 qui n'est pas cyclique.

Exercice 4.2. Soit G un groupe fini et P un p-Sylow. Soit $H < G$ un p-groupe démontrer que H est conjugué dans P (faire opérer H dans G/P et écrire l'équation aux classes).

Si de plus H est un p-Sylow montrer que H est conjugué dans P, et que le nombre de conjugués de P divise l'ordre de G/P.

Exercice 4.3. Soit G un groupe fini, $P < G$ un $p-$Sylow, et $N = \{g \in G / gNg^{-1} < N\}$ le normalisateur de P. Démontrer que tout élément de N d'ordre une puissance de p est dans P.

Exercice 4.4. Si p est un nombre premier quels sont les $p-$Sylow de S_p.

Quels sont les sous-groupes de Sylow de S_4.

Quels sont les $p-$Sylow de S_{p^2} (on pourra commencer a décrire les sous groupes isomorphes à $(C_p)^2$.

Exercice 4.5. Soit G un groupe fini et p un nombre premier. En faisant opérer P sur G/P démontrer que le nombre de p Sylow est congru à 1 modulo p.

4.3.2 Nilpotence.

Exercice 4.6. On suppose que G est un groupe fini et que pour tout nombre premier p divisant $|G|$, il contient un unique $p-$Sylow. Démontrer que le centre de G est non trivial, et que G est nilpotent.

Exercice 4.7. Si G est un $p-$groupe fini et si $m||G|$, alors G contient un sous groupe normal d'ordre m et un quotient d'ordre m

Exercice 4.8. La suite centrale ascendante d'un groupe G est la suite des sous-groupes définies par récurrence par

$Z_0 = \{e\}, Z_1 = Z(G) = \{g / \forall h, ghg^{-1}h^{-1} = 1\}, ...Z_k(G) = \{g / \forall h, ghg^{-1}h^{-1} \in Z_{k-1}(G)\}$.

Démontrer que la suite centrale ascendante est une suite de sous-groupes invariants de G et que l'image de Z_{n+1} dans G/Z_n est le centre de ce groupe.

Démontrer que G est nilpotent de classes n si et seulement si $G = Z_n(G)$

Exercice 4.9. Le sous groupe de S_6 engendré par $(1,2,3,4), (1,2,3), (2,5), (5,6)$ est il nilpotent ?

Exercice 4.10. Soit G un groupe nilpotent dont l'ordre est le produit de k nombres premiers (égaux ou distincts) montrer que la classe de nilpotence de G est inférieure à k.

Exercice 4.11. Si G est un groupe, et $H \lhd G$ un sous-groupe normal, on définit $[G, H] < H$ le sous groupe engendré par les éléments de la forme $ghg^{-1}h^{-1}$ de H.

1. Démontrer que $[G, H] < H$ est un sous-groupe normal de G

La suite centrale descendante d'un groupe G est la suite des sous-groupes définies par récurrence par $H_0 = G, H_1 = [G, G], ...H_k = [G, H_{k-1}]$

2. Démontrer que la suite centrale ascendante est une suite de sous-groupes invariants de G

3. Démontrer que le k-ième terme de la suite centrale ascendante, Z_k contient $[G, Z_{k+1}]$.

4. Démontrer que si G est nilpotent de classe n, c'est à dire si $Z_n = G$, la suite centrale descendante s'arrête en n étapes, c'est à dire que $H_n = \{e\}$

5. Démontrer la réciproque de 4.

6. Démontrer que G est nilpotent de classes n si et seulement si $G = Z_n(G)$

7. Démontrer que tout sous groupe et tout quotient d'un groupe nilpotent est nilpotent