**Chapitre 6. Théorie des groupes  
I. Généralités sur les groupes**  
Soit un ensemble  
Une **loi de­ composition interne (l.c.i)** sur est une application de dans   
Une lci est **associative**, / l’ensemble + l.c.i est appelé **demi-groupe** si la priorité des opérations n’a pas d’importance dans un produit, càd . Dans ce cas les parenthèses peuvent être omises : .  
Une lci est **commutative** si l’ordre des opérations n’a pas d’importance dans un produit, càd   
Deux termes **commutent** pour la l.c.i si   
On appelle **élément central** un élément qui commute avec tous les autres éléments  
On appelle **centre** l’ensemble des éléments centraux.  
Tout est central ssi il y a commutativité.  
Un élément de est **neutre** pour la l.c.i si composer un terme de par l’élement à gauche ou à droite, ne change pas le terme.  
 est qualifié de **monoïde** si sa l.c.i est associative et admet un neutre = demi-groupe + neutre.  
Si une lci admet un neutre, celui-ci est unique  
Tout terme commute avec le neutre s’il existe.  
Si une l.c.i admet neutre, **symétrique à gauche** de / **symétrique à droite** de signifie que le produit est égal au neutre. **Symétrique =** symétrique à gauche ET à droite. **Symétrisable =**  symétrique. Parler de symétrique suppose l’existence d’un neutre.  
Deux termes symétriques (à gauche ET droite) commutent.  
Sous associativité, tout élément a au plus un symétrique.  
Si une l.c.i admet un neutre, celui-ci est unique et est son propre symétrique  
Un élément est dit **simplifiable à gauche (resp droite)** (dans toute expression par la lci) si dans toute égalité de produits ou il est à gauche (resp. droite) dans les deux membres, on a toujours égalité si on l’enlève dans les deux membres à gauche (resp droite).  
Symétrisable à gauche (resp. droite) implique simplifiable à gauche (resp. droite)  
**Ensemble Produit.**Le **produit** **d’un élément**  **par un élément** est l’élément   
L’**ensemble** **produit** **d’une partie** **par une partie** est l’ensemble des produits . Attention a priori . Attention a priori , , sont des choses différentes. Il vaudrait mieux préciser à quel def on se réfère en écrivant .  
Sous associativité,le **produit d’une famille** **finie d’éléments** est l’élément   
Sous associativité, le **produit d’une famille finie de parties** est l’ensemble des produits des parties.   
L’associativité est présupposée car sinon le produit dépend aussi du placement des parenthèses ce qui rend la notion peu élégante. A priori dépend de l’ordre.  
Sous associativité + commutativité, le produit de parties est commutatif, le produit de familles finies est indépendant de l’ordre.  
Sous associativité + commutativité + neutre, le **produit d’une famille infinie de parties** est l’ensemble des produits finis provenant d’elle (de n’importe quelles parties dans n’importe quel ordre). La commutativité est présupposée car cette notion ne dépend pas de l’ordre, et sous cette condition généralise plus élégamment le produit fini de parties. L’existence du neutre est supposée pour permettre une autre interprétation comme ensemble des produits infinis de termes dont un nombre fini n’est pas neutre.  
fini  
Un **groupe** est un ensemble muni d’une lci sur tel que 1)2) et 3)  
1) la l.c.i est associative (associativité)  
2) la l.c.i admet un neutre (il y a un neutre)  
3) tout élément est symétrisable par la l.c.i (symétrisabilité) (parler de 3 suppose de toute manière 2)  
Dans tout groupe, il y a un unique neutre, et tout élément admet un unique symétrique appelé **inverse** et noté en notation multiplicative ou en notation additive. On peut ainsi définir l’application inverse sur tout le groupe.   
Un groupe est dit **commutatif/abélien** si sa loi est commutative  
Un élément d’un groupe commute toujours avec son symétrique, et avec l’élément neutre.  
L’**ensemble inverse** d’une partie d’un groupe, est l’ensemble des inverses d’éléments de la partie. On note l’ensemble inverse d’une partie .  
L’inverse d’un groupe est le groupe.   
**Regles de calcul.**Sous associativité (dans un demi-groupe à fortiori dans un groupe) on peut définir composer fois sans se soucier de l’ordre  **/   
 /**  et  **/**Sous associativité, Composer fois revient à faire le produit de composer fois puis fois ou l’inverse indistinctement. / Sous associativité, Composer fois revient à composer d’abord fois puis fois ou l’inverse indistinctement. /   
Sous associativité, Si deux termes commutent, alors on peut les élever chacun à une puissance différente quelconque, ca commute toujours.   
Sous symétrisabilité, tout élément est simplifiable (à gauche/droite) d’une expression.  
Dans un groupe, l’inverse du produit est le produit des inverses en inversant l’ordre des lettres.   
**I.2. Sous-Groupes.** Soit un groupe  
Définitions équivalentes :  
Un **sous-groupe** d’un groupe est une partie non-vide stable par produit et inverse.   
Un **sous-groupe** d’un groupe est une partie qui muni de la loi induite, forme encore un groupe.  
On note si sous-groupe de , si sous-groupe propre de   
Tous les sous-groupes sont des groupes et possèdent le même élément neutre, celui du groupe.   
 et sont des sous-groupes de . Tout groupe ayant au moins deux éléments possède donc au moins deux sous-groupes distincts.  
Le centre d’un groupe est un sous-groupe. Propre ssi groupe non abélien.  
L’intersection quelconque de sous-groupes d’un groupe est un sous-groupe du même groupe.   
L’union d’une famille de sous-groupes totalement ordonnée pour l’inclusion est un sous-groupe du même groupe.  
Exemples : , , , ,   
Les sous-groupes de sont les , entier. L’ensemble des complexes de module 1 est un sous-groupe propre de . Le groupe linéaire général est un sous-groupe du groupe symétrique. Le groupe des similitudes affines/linéaires d’un espace affine/vectoriel euclidien est un sous-groupe du groupe linéaire général de .   
Soit un groupe, les définitions suivantes sont équivalentes:  
Le **sous-groupe engendré** par une partie non vide est le plus petit sous-groupe (au sens inclusion) contenant la partie.  
Le **sous-groupe engendré** par une partie non vide est l’intersection de tous les sous-groupes contenant la partie.  
Le **sous-groupe engendré** par une partie non vide est l’ensemble de tous les produits finis d’éléments provenant de la partie ou de son inverse.  
On note le sous-groupe engendré par une partie Si la partie est égale à son inverse, en particulier si elle s’exprime comme union de sous-groupes. Le sous-groupe engendré par la partie est l’ensemble de tous les produits finis d’éléments de la partie.  
 Le produit d’un nombre fini de sous-groupes (dans n’importe quel ordre) est inclus dans le sous-groupe engendré par leur union.   
Il y a égalité ssi le produit est un sous-groupe  
Sous commutativité (dans un groupe abélien) il y a toujours égalité. Le produit de la famille est indépendant de l’ordre et est toujours un sous-groupe.  
 **Théorème.** Le produit de deux sous-groupes écrit dans un sens ou l’autre est identique ssi ce produit (dans un sens ou l’autre) est un sous-groupe ssi ce produit (dans un sens ou l’autre) est engendré par l’union de ses 2 sous-groupes.  
 ssi sous-groupe ssi sous-groupe (ssi ssi )  
Pour une famille finie de sous-groupes, Si le produit de chaque paire de la famille est un sous-groupe alors le produit de la famille est un sous-groupe et est indépendant de l’ordre.  
Le sous-groupe engendré par un unique élément est l’ensemble des puissances (resp. multiples) relatives de l’élément.   
On note de façon compacte   
Sous commutativité   
Sous commutativité   
Une **partie génératrice** d’un groupe, est une partie dont le sous-groupe engendré est le groupe lui-même. On dit que la partie **engendre/génère** le groupe. Toute partie engendre son sous-groupe engendré.Un groupe est dit **monogène** s’il est engendré par un singleton. Un **générateur** est un élément qui engendre le groupe.  
Un groupe est dit **de type fini** s’il est engendré par un ensemble fini d’éléments.  
Un groupe fini est de type fini, mais réciproque fausse ( est engendré par )  
Un groupe est dit **cyclique** s’il est monogène et fini.  
L’**ordre** d’un élément dans un groupe est le cardinal de son sous-groupe engendré. Peut être fini ou infini. Si est l’élément, on le note   
Dans tout groupe l’élément neutre est le seul élément d’ordre .  
Tout élément non nul de est d’ordre infini.  
**I.3. Morphismes de groupes.**Soient , groupes. Un **morphisme de groupes** est une application d’un groupe dans un autre telle que l’image de tout produit est le produit des images.   
L’ensemble des morphismes de dans est noté Un **endomorphisme de groupes** est un morphisme d’un groupe dans lui-même.  
Soit un morphisme de groupes L’image d’un neutre est un neutre.   
L’image de l’inverse est l’inverse de l’image.   
L’image d’une puissance (resp. multiple) est la puissance de l’image.   
L’image d’un sous-groupe est un sous-groupe.   
L’image réciproque d’un sous-groupe est un sous-groupe.   
L’**image d’un morphisme de groupes** estl’image de l’application   
Le **noyau d’un morphisme de groupes**  est l’image réciproque du neutre   
L’image est un sous-groupe du groupe d’arrivée.  
Le noyau est un sous-groupe du groupe de départ.  
Morphisme surjectif équivaut à son image = groupe d’arrivée.  
Morphisme injectif équivaut à son noyau = singleton neutre.  
La composée de morphisme de groupes est un morphisme de groupe.  
Un groupe est l’**image homomorphe** d’un autre, si c’est l’image de l’autre par un morphisme de groupes surjectif.  
L’**injection canonique** d’une partie d’un ensemble est l’application   
L’injection canonique d’un sous-groupe dans son groupe est un morphisme injectif de groupes.  
Exemples :L’application classe de est un morphisme surjectif de groupes.  
L’application est un morphisme de groupes.  
L’application déterminant du groupe des matrices inversibles d’un corps commutatif dans le groupe est un morphisme de groupe dont le noyau est appelé **groupe linéaire spécial** noté et est donc un sous-groupe de   
**I.4. Isomorphismes de groupes. Automorphismes**Un **isomorphisme de groupes**, est un morphisme de groupes bijectif càd isomorphisme ssi (definition categorique).  
L’ensemble des isomorphismes de groupes entre est note Ex : est un isomorphisme de groupes.  
L’application est un isomorphisme de groupes.  
L’application isomorphisme de groupes.  
Un **automorphisme de groupes** est un isomorphisme d’un groupe dans lui-même = iso+endomorphisme  
Si alors est un automorphisme de groupes.  
On note l’ensemble des automorphismes de groupes d’un groupe .  
Si un groupe, est un automorphisme. C’est un **automorphisme intérieur**L’inverse d’un automorphisme intérieur est l’automorphisme intérieur de l’inverse   
L’ensemble des automorphismes intérieurs est note et est un sous-groupe   
Le groupe est trivial ssi est abelien. **II. Sous-groupes distingués et groupes quotients  
II.1. Classes à gauche, classes à droite**Soit sous-groupe de G , la relation d’équivalence **à droite (resp. à gauche) selon/modulo H** est définie par (resp. )  
On note les classes d’équivalences à droite resp. à gauche , elles forment donc une partition de . On note resp. l’ensemble quotient.  
L’indice à droite (resp. à gauche) d’un sous-groupe de noté resp. est le cardinal de l’ensemble quotient resp.   
Les classes à droite (resp. à gauche) associées à un sous-groupe sont en bijection avec , et donc les une avec les autres, et donc ont toutes même cardinal, celui de .  
**Th. de Lagrange.** Si sous-groupe d’un groupe fini alors fini et (gauche/droite)  
Donc le cardinal du sous-groupe divise celui de , et donc l’indice ne dépend pas de la convention gauche/droite, il y a autant de classes à gauche que de classes à droite modulo H.  
 est la taille d’une classe, est le nombre de classes.  
Un groupe de cardinal premier admet pour seuls sous-groupes et . **II.2. Sous-groupe distingués et groupe quotient  
II.2.1. Suites exactes**Une **suite exacte** est un diagramme , ou les sont des groupes, les sont des morphismes, et de plus , l’image d’un morphisme est le noyau du suivant.  
Si est injectif, isomorphe a un sous-groupe de   
Si est surjectif, doit être le morphisme trivial egal au neutre partout d’image .  
**Une section** est un morphisme qui admet un morphisme inverse gauche : c’est un tel que . C’est un morphisme inverse droit.  
**Une rétraction** est un morphisme qui admet un morphisme inverse droit. C’est un morphisme inverse gauche. Une rétraction est donc toujours associée à une section.  
Une **suite exacte courte** est une suite exacte de la forme   
Dans ce cas est surjectif, et est injectif.  
Une **extension de groupes** est une suite exacte courte dans le cadre de la théorie des groupes.  
Pour on dit que  **est une extension de par** .  
Un **scindage à droite d’une suite exacte courte** est une section de (du 2eme morphisme, càd droite),  
c’est donc et   
Un **scindage à gauche d’une suite exacte courte** est une rétraction de (du 1er à gauche), c’est donc et   
**Une suite exacte courte est scindée à gauche (r. droite)** si elle admet un scindage à gauche (r. droite)  
**II.2.2. Sous-groupes distingués**Un sous-groupe H est **distingué/normal** dans G ce qu’on note ou encore «  **existe** » ssi les classes a gauches modulo H ne sont plus discernables des classes a droites modulo H ssi ssi ssi est invariant par tout automorphisme intérieur. Dans ce cas on écrira simplement .  
Si la loi du groupe est compatible avec la relation, on peut définir **loi quotient**   
Ainsi ssi muni de sa loi quotient est un groupe. Il y a donc une certaine analogie entre sous-groupe distingué et diviseur en théorie des nombres.  
La loi quotient est aussi l’unique loi sur qui fait de un morphisme de groupes. est la **projection canonique** sur H, c’est un morphisme surjectif de noyau , et   
On peut résumer le théorème précèdent par la suite exacte   
**Th. factorisation.** Un morphisme de groupes , **est factorisable** sur un sous-groupe de càd tel que ssi ssi .

Dans ce cas est unique, est un morphisme de groupes et on a ,

De plus est surjective ssi l’est et est injective ssi .  
**Th isomorphisme 1** Le noyau d’un morphisme groupes est un sous-groupe distingué de et induit un isomorphime de Remarque : ce théorème se généralise en dehors de la théorie des groupes, pour tout quotient.   
Les sous-groupes distingués d’un groupe sont exactement les noyaux de morphismes partant de .  
Pour , le groupe alterné est sous-groupe distingué du groupe symétrique comme ker de   
Le groupe special lineaire est un sous-groupe distingué de comme noyau du det.  
Dans un groupe abélien, tous les sous-groupes sont distingués.  
Tout sous-groupe d’indice 2 dans un groupe est distingué.   
Dans un groupe , les sous-groupes et sont toujours distingués.Un **groupe simple** est un groupe dont ses seuls sous-groupes distingués sont et .  
Un groupe de cardinal premier est simple c’est-à-dire est simple avec premier.  
Si , le groupe alterne est simple.  
Les groupes simples sont analogues aux nombres premiers. Si un groupe est simple on ne peut pas le décomposer par dévissage en produit de groupes plus petits. **II.3. Centre et groupe dérivé  
Le centre d’un groupe** est l’ensemble   
Le centre d’un groupe est un sous-groupe distingué de ce groupe. existe  
Tout sous-groupe de est distingué dans .  
Un groupe est abélien ssi il coïncide avec son centre.  
Si ,   
Le **groupe des quaternions** est un groupe ou la multiplication est definie par la regle des signes et les formules   
Le centre du groupe des quaternions est   
Le **groupe dérivé d’un groupe**  note est le sous-groupe de engendré par les éléments de la forme . Ces éléments sont appelés **commutateurs** du groupe .  
Le groupe dérivé d’un groupe est un sous-groupe distingué càd existe.  
Le groupe dérivé d’un groupe abélien est le groupe trivial .  
On peut « rendre abélien » un groupe en le quotientant par son groupe dérivé .  
 existe et est abélien. De plus si pour un autre sous-groupe existe et est abélien, alors . **II.4. Sous-groupes du quotient et théorème d’isomorphisme**Via la projection canonique,Si existe, fixer 1 sous-groupe de revient à fixer 1 sous-groupe K de G contenant   
Si existe, fixer un sous-groupe distingué de revient a fixer un sous-groupe distingué de contenant . Résultat plus général que le cadre de la théorie des groupes.  
Pour tout diviseur d’un entier , admet un sous-groupe de cardinal , ce sous groupe est unique et noté .  
Soit   
Si existe et alors existe, existe, et   
**Th isom. 2.** Si existe alors est un sous-groupe, existe, existe et   
Si existe alors (( existe et ) ssi existe)  
**Th isom. 3.** Si existe, existe, et c’est-à-dire + simplement si existe, alors   
Le centre d’un groupe est toujours distingué, càd existe toujours.  
Les sous-groupes de sont et sont tous distingués. **III. Génération de groupes  
III.1. Groupes monogènes cyclique**Un groupe est dit **monogène** s’il est engendré par un singleton. Un **générateur** est un élément qui engendre le groupe. Un groupe est dit **de type fini** s’il est engendré par un ensemble fini d’éléments.  
Un groupe est dit **cyclique** s’il est monogène et fini.  
Un groupe monogène est abélien.  
Un groupe est monogène de cardinal infini ssi il est isomorphe a   
Un groupe est cyclique ssi il est isomorphe a un   
**L’ordre d’un groupe** est le cardinal de son ensemble.  
**L’ordre d’un élément d’un groupe**, est l’ordre du groupe monogène engendre par cet élément. On le note ou bien .  
Si est d’ordre fini alors .  
Dans , est un générateur ssi  **III.2. Groupes libres**Un groupe libre permet de modéliser les expressions en théorie des groupes. On le formalise comme un langage formel, dans lequel les mots représentent des expressions entre éléments d’un groupe. Si on avait pas l’associativité, a priori pour une expression il faudrait un arbre de syntaxe.  
Une lettre de l’alphabet du langage représente l’expression d’un élément d’un groupe. Pour modéliser le fait qu’un élément d’un groupe a toujours un inverse on suppose que chaque lettre est associée à une autre lettre, et correspondent au même symbole, mais l’un représente l’inverse de l’autre. On peut supposer par ex, **l’alphabet de la forme**  et on note soit , soit .  
Un **mot du groupe libre** est donc une suite finie de **lettres** de . Un mot représente l’expression de composer les symboles éléments dans le même ordre par la l.c.i. du groupe. Ex représente le fait de prendre un premier élément , puis l’inverse d’un deuxième , et de calculer leur produit, le mot modélise l’expression , on confondra la notation d’une expression et de son mot.  
Comme dans les langages formels, on peut définir la concaténation, un mot est la concaténation de ses lettres, on peut définir un mot vide note .  
Un **mot réduit** du groupe libre sur X est un mot dont deux lettres consécutives ne sont jamais associées autrement dit, c’est une expression dans laquelle on a simplifie les , ou les consécutifs.  
On peut toujours réduire un mot, en supprimant tous ses ou consecutifs.   
Deux mots sont équivalents ssi ils ont même forme réduite. Autrement dit l’expression qu’ils représentent est la même du point de vue des lois d’un groupe.  
Le **groupe libre sur l’ensemble de symboles**  est note et est forme de l’ensemble des mots réduits, autrement dit on a quotienté par la relation précédente, la forme réduite étant un représentant canonique. On peut munir cet ensemble d’une loi qui correspond à faire la concaténation puis simplifier l’expression en obtenant le mot réduit correspondant.  **est le groupe libre.**L’élément neutre du groupe libre est le mot vide .  
Toute application a valeurs dans un groupe peut s’écrire avec un unique morphisme de groupes . De plus prolonge , cad . Autrement dit, si on affecte des lettres symboles a certains éléments de , alors on peut definir ce que veut dire toute expression contenant ces symboles, correspond a évaluer l’expression formée de ces symboles dans G.  
Autrement dit admet un unique **morphisme d’évaluation** prolongeant .  
Le groupe libre d’un singleton est   
Dès que le cardinal de est n’est plus abélien, et est beaucoup plus compliqué.  
Le groupe libre d’un ensemble dénombrable est un ensemble dénombra ble. (Par denom. de denom.)  
**III.3. Présentation d’un groupe**L’inclusion d’une partie d’un groupe peut être prolongée par l’unique morphisme d’évaluation , dont l’image n’est autre que le sous-groupe engendre par la partie .  
On a donc toujours . Si est bijective, alors .  
Dans le cas non injectif, càd , une **présentation d’un groupe** G est un couple ou est une partie generatrice de G et est une partie de telle que est le plus petit sous-groupe distingué de contenant R. (Prendre est trop grand, donc on restreint pour la def). On note une présentation avec mots reduits. TODO A clarifier.  
Tout groupe infini admet un sous-groupe propre non trivial.  
Tout groupe fini de cardinal non premier admet un sous-groupe propre non trivial. **IV. Action d’un groupe sur un ensemble  
IV.1. Définitions**Une **action à gauche (resp. à droite)** **d’un groupe G sur un ensemble X** correspond à  
une application telle que (resp. ) et (resp. .  
En posant (resp. ), une action peut se voir comme un morphisme de groupes quelconque ou est le groupe symétrique de X (ensemble des bijections dans X) muni de la composition orientée (resp. Inverse la composition pour conv. droite!). Un groupe **agit à gauche (droite)** **sur un ensemble X** si admet une action à gauche (droite) sur X.  
On considèrera des actions à gauche, mais les résultats sont analogues pour les actions à droites.  
Une action est **fidèle** ssi ssi son morphisme est injectif.  
Ainsi on peut « rendre » une action fidèle en factorisant son morphisme associé, sur son noyau, cela modifie le groupe mais pas l’ensemble sur lequel il agit.  
Un action est **triviale** si son morphisme l’est, càd d’image l’identité de , cad   
**Deux éléments de l’ensemble sont sur une même orbite** ssi .  
«Etre sur la même orbite » définit une relation d’équivalence sur , de classes les **orbites** , on peut écrire   
On note l’ensemble des orbites de X sous l’action de G.   
Une action est **transitive** ssi cad ssi il n’y a qu’une seule orbite sur X.  
Dans ce cas pour tout point , est surjective.  
L’action sur une orbite, est donc toujours transitive, et est surjective  
Le **stabilisateur de**  pour l’action est le sous-groupe de  :  est un **point fixe de l’action sur G** si cad cad   
On note l’ensemble des points fixes de l’action sur G.   
On note pour , , Dire dire  **IV.2. Exemples : groupe symétrique et action d’un groupe sur lui-même**Une action de groupe sur un ensemble est **-transitive** si pour deux ensembles de points distincts dans , .  
L’action naturelle de sur correspond au morphisme , elle est transitive, et même -transitive.  
Pour cette action, le stabilisateur d’un point de , est isomorphe a et le quotient est en bijection avec l’orbite du point qui n’est autre que , donc a éléments. Ainsi on retrouve . Les sous-groupes de d’indice sont toujours isomorphes a . Le groupe cyclique engendré par une permutation agit encore sur mais l’action n’est pas transitive en général.  
**Th. de Cayley.** Tout groupe est isomorphe à un sous-groupe d’un groupe de permutations.  
Tout groupe fini de cardinal est isomorphe a un sous-groupe de Tout groupe agit sur lui-même en prenant sa l.c.i. comme action : (resp. )  
Cette action est l’**action par translation à gauche** (resp. à droite).  
Tout sous-groupe agit également sur en restreignant la l.c.i. de , les orbites de cette action a gauche (resp. a droite) sont les classes a droite (resp. a gauche) modulo H.  
Un groupe agit sur tout quotient (à gauche/droite) par un sous-groupe :   
Cette **action quotient** est transitive mais en général pas fidèle.  
Tout groupe agit sur lui-même par conjugaison par automorphisme intérieur : .  
Une **classe de conjugaison** est une orbite pour cette **action de conjugaison**.  
2 éléments d’un groupe sont **conjugués** ssi ils sont dans la même classe de conjugaison ssi   
Le **centralisateur=commutant** de est le stabilisateur de pour l’action de conjugaison , c’est donc aussi l’ensemble des éléments qui commutent avec . **IV.3. Equation aux classes et formule de Burnside**On précise le lien entre orbite et stabilisateur. Soit groupe agissant sur un ensemble , et soit .  
Les orbites de sous l’action de forment une partition de et est une bijection.   
De plus, l’action est compatible sur avec l’action quotient de sur dans le sens suivant   
Si et sont finis, la taille d’une orbite divise la taille du groupe .  
   
Deux éléments d’une même orbite ont leur stabilisateur et conjugués, donc de même cardinal.  
**Formule des classes.** Pour et finis,   
**Equation aux classes**. Pour et finis,   
**Equation aux classes pour** **la conjugaison**. avec   
Pour un nombre premier, un **-groupe** est un groupe fini de cardinal avec .  
Le centre d’un -groupe divise et a au moins éléments   
Tout groupe d’ordre est abélien.  
Soit un -groupe agissant sur un ensemble fini, alors   
Si -groupe agissant sur un ensemble fini et ne divise pas , l’action admet au - 1 point fixe  
**Formule de Burnside.** Soit G un groupe fini agissant sur un ensemble fini.   
Alors d’une part   
D’autre part, le nombre d’orbites de est   
Soit l’action quotient à gauche d’un groupe fini sur un sous-groupe . Alors et c’est le plus grand tel que existe. **V. Produits de groupes  
V.1. Produits directs  
Produit externe :** Relativement à une structure algébrique, on peut toujours définir le produit cartésien de structures, et le munir d’opérations produits, la structure produit hérite des propriétés algébriques. C’est le **produit direct externe**, l’ensemble est le même que celui du produit cartésien.  
Le produit direct externe vérifie la propriété universelle : TODO  
Le sous-ensemble du produit constitué des familles a support fini (avec un nb fini de termes non neutre) est appelé **produit restreint externe.** Parfois, le terme de somme est utilisé même si on a un produit cartésien. Dans le cas où la famille est finie, il n’a pas de distinction entre restreint et pas restreint.  
Le produit restreint externe vérifie la propriété universelle : TODO  
Si l’opération est commutative, la prop. universelle se simplifie.  
**Produit interne : Pour les groupes.** Dans un groupe, le **produit interne** de sous-groupes est l’ensemble produit des sous-groupes, les éléments produits le constituant pour qu’ils aient un sens sont nécessairement a support fini.  
Le **produit restreint interne** de sous-groupes d’un groupe est un produit interne, telle que le produit externe correspondant à ce produit, doit être isomorphe au produit interne. Cela revient à exiger :  
1) 2 éléments provenant de 2 sous-groupes distincts de la famille commutent toujours  
2) l’unicité de l’écriture d’un élément sur le produit restreint interne.  
Les sous-groupes d’un produit restreint interne sont alors automatiquement distingués dans le groupe et engendrent le groupe.  
Dans le cas où la famille est finie et/ou si le groupe est abélien on utilise le terme de **produit direct interne** plutôt que restreint interne.  
**G est le** **produit direct interne d’une famille finie** de sous-groupes ssi 1)/1’) + 2)/2’) + 3)/3’)  
1) 2 éléments provenant de 2 sous-groupes distincts de la famille commutent toujours.  
Sous 2)+3), on peut remplacer 1 par 1’) Tous les sous-groupes sont distingués, càd tout existe.  
2) Le groupe est produit des sous-groupes (l’ordre n’importera pas)  
Sous 1) on peut remplacer par 2’) Le groupe est engendré par les sous-groupes   
3) Tout sous-groupe intersecté au produit de tous les autres sous-groupes donne le singleton neutre.  
En fait sous 1)2), on peut affaiblir 3 légèrement 3’)   
Récapitulatif pour 2 sous-groupes :  
**G est** **produit direct interne de 2 sous-groupes** et ssi  
Le produit externe est isomorphe a càd ssi  
1) / H et K sont distingués dans G.  
2) / / /   
3)   
Remarque 2) + 3)   
Dans ce cas on note .   
On peut enlever 2) si on exige juste que sont en produit direct. On peut enlever 1) si grp abéliens.  
2 sous-groupes abéliens sont en produits direct interne ssi ssi   
N sous-groupes abéliens sont en produit direct interne ssi ssi   
**V.2. Produit semi-direct**On sait que deux sous-groupes distingués dans G, sont en produit direct interne ssi 2)+3)  
Deux sous-groupes dont seul l’un est supposé distingué, sont en **produit semi-direct interne** ssi  
ssi ssi la restriction a de la surjection canonique est un isomorphisme de ssi la surjection canonique se scinde par un morphisme tel que .  
Pour , , alors   
Comme agit par conjugaison sur , isomorphe au produit muni de . Avec la conjugaison.Soit un morphisme de groupes avec , deux groupes, on note l’image d’un .  
Le **produit semi-direct externe (à droite) d’un groupe par un groupe selon un morphisme (càd action à gauche de sur )** est le produit cartésien muni de la loi , on note **.** L’ordre importe contrairement au produit direct.  
 contient les sous-groupes , et et s’exprime toujours comme produit semi-direct interne de ces 2 sous-groupes.  
 mais pas forcément   
 existe, mais n’existe pas forcément.  
Résumé:  
Si on peut écrire avec existe, alors est isomorphe au produit semi-direct externe suivant la conjugaison .  
Pour un produit semi direct externe , en identifiant et , est un sous-groupe distingué dans , est isomorphe a . Attention avec cette identification, on ne peut pas toujours conclure suivant la conjugaison, (sinon serait inutile).  
**Différence semi-direct/direct.** Un produit semi-direct externe est direct ssi l’action est triviale ssi  existe ssi est commutatif.  
Il se peut qu’un produit semi-direct associé à une action non triviale soit isomorphe au produit direct qui lui est associé.  
**Caractérisation d’un produit semi-direct comme suite exacte courte scindée à droite**.  
Pour un produit semi-direct , on a scindée à droite.  
Si est une suite exacte courte scindée à droite de section , alors avec . induit un isomorphisme entre et .  
**Exemples**  
Soient groupe et sous-groupe de agissant sur par automorphismes interieurs. Cela définit un produit semi-direct qu’on note isomorphe a par   
Pour deux groupes on a   
, si est impair on peut choisir le produit direct.  
Soit groupes et morphismes tels que avec alors  scindée à droite par donc   
 avec l’action Si est premier, le groupe diédral est le seul produit semi-direct non trivial de  scindée par .   
Ce produit est direct ssi automorphisme. (vrai pour et impair, ou pour fini de caractéristique et ). avec la réduction modulo 2 n’est pas scindée à droite, donc pas un produit semi-direct. n’est pas scindée à droite donc n’est pas produit semi-direct du groupe de Klein par   
Pour et , , on a   
Tout groupe d’ordre 255 est cyclique. (par th de Sylow)  
CNS pour  **VI. Groupes abéliens de type fini\*  
VI.1. Structure des groupes abéliens de type fini** (notation additive)La donnée d’un groupe abélien est équivalente à celle d’un Z-module  
Un groupe abélien est **Z-libre** s’il existe une famille d’elements de tel que soit un isomorphisme. La famille est une **base** **du groupe abélien** .  
Une base d’un groupe abélien est une famille génératrice du groupe abélien.  
Il y a des groupes abéliens non Z-libres càd sans base, par ex   
Tout sous-groupe d’un groupe abélien Z-libre de base finie, est aussi Z-libre avec une base de cardinal inferieur. Toutes les bases du sous-groupe sont en fait de même cardinal fini.  
En particulier, si un groupe abélien est Z-libre, toutes ses bases ont même cardinal fini ou .  
Le **rang d’un groupe Z-libre** est le cardinal fini ou de n’importe laquelle de ses bases.  
Un groupe -libre de rang est donc isomorphe a .  
Un **élément de Z-torsion d’un groupe** est un élément d’ordre fini dans ce groupe.  
On note le **groupe de torsion** de G, càd l’ensemble des éléments de Z-torsion d’un groupe .  
Un groupe est de torsion ssi il est égal à son groupe de torsion.   
Un groupe est **sans torsion** si son groupe de torsion est trivial. càd 0 seul elem. d’ordre fini.  
Le groupe de torsion d’un groupe est un sous-groupe du groupe.  
Un groupe de type fini et de torsion, est de cardinal fini.  
Un groupe abélien de type fini a donc un groupe de torsion de cardinal fini.  
Un groupe Z-libre est sans torsion.  
Un groupe abélien de type fini sans torsion est Z-libre de rang fini.  
N Z-modules en produit direct interne ssi ssi   
Un groupe abélien de type fini admet toujours un sous-groupe H, Z-libre de rang () tel que et est fini. Cela ramène l’étude de G à celle d’un groupe abélien fini.  
On note l’ensemble des éléments d’un groupe d’ordre une puissance de un nombre premier, et on note l’ensemble des nombres premiers tels que .  
Pour un groupe abélien fini , est fini et . Ramène l’étude de G à celle des   
Un groupe d’ordre avec premier, est soit cyclique isomorphe a soit isomorphe a , ces deux derniers n’étant pas isomorphes l’un de l’autre.  
**L’exposant d’un groupe**  (notation +) est le plus petit entier tq .  
Un groupe fini est toujours d’exposant fini, le ppcm des ordres de ses éléments.  
Un groupe cyclique est d’exposant fini l’ordre de n’importe lequel de ses générateurs.  
Un premier ssi   
Pour un groupe abélien fini , son ordre et son exposant et ont mêmes diviseurs premiers donc l’ordre divise une puissance de l’exposant .  
Autrement dit un premier ssi   
**Théorème de Cauchy 1.** Pour diviseur premier de alors   
Pour un groupe abélien fini , tous les sont des -groupes. Ramène l’étude aux p-groupes abéliens  
Un -groupe abélien est isomorphe à avec une suite finie unique.  
Finalement un groupe abélien de type fini se décompose avec unique, uniques premiers, et uniques entiers.  
Un groupe abélien fini est isomorphe à avec une suite finie unique.  
A comparer avec la structure des modules de type fini sur les anneaux principaux. **VI.2. Automorphismes des groupes cycliques**Soit un groupe cyclique d’ordre isomorphe à . On note G multiplicativement.  
La classe d’un élément engendre G ssi cet élément x est premier avec n. (Bézout).  
On note l’ensemble des générateurs de , c’est un groupe pour la loi produit de l’anneau quotient.  
L’**indicatrice d’Euler** d’un entier est le nombre de générateurs de cad   
 par l’isomorphisme .  
**Th restes Chinois.** Si alors , de plus   
Cela ramène l’étude a celle des avec premier et   
Dans le cas est un corps, , de plus est cyclique isomorphe a   
Pour premier et ,   
   
Soit un nombre premier et un entier  
Si et alors   
Si et alors   
Si et alors   
Le groupe des inversibles de n’est pas toujours cyclique. **VI.3. Sous-groupes discrets de**Un sous-groupe de R est soit dense, soit de la forme avec . S’il est dense il est non monogène.  
Comme avec , n’est pas monogène, c’est un sous-groupe dense de R.  
Un sous-groupe de est **discret** ssi son intersection avec n’importe quel compact de a un nombre fini de point, cad ssi sa topologie induite par celle de est discrète.  
Un sous-groupe de R est donc soit dense soit discret dans R. est un sous-groupe discret de .  
Un sous-groupe discret de est de la forme avec libre dans   
Cette famille est donc une Z-base de .  
Un **réseau de**  est un sous-groupe discret de de rang .  
Réseaux = Objets centraux en mathématiques. Apparaissent en théorie algébrique des nombres, et théorie des groupes algébriques commutatifs complexes.  
Le **domaine fondamental d’un réseau associe a une Z-base** de est l’ensemble   
Le domaine fondamental est Lebesgue-mesurable de mesure independant de la base , car avec donc .  
**Le volume d’un réseau de**  est donc la mesure de n’importe quel domaine fondamental de ce reseau.  
**Th. Minkowski.** Dans une partie mesurable de de mesure > au volume d’un réseau, on peut trouver deux points distincts de la partie telle que la différence (vecteur les joignant) appartient au réseau.  
Si une partie mesurable de est convexe et symétrique par rapport à 0 et sa mesure avec un reseau, alors l’intersection de la partie et du reseau contient un point non nul. Cela est encore vrai au cas limite si on rajoute l’hypothèse que la partie est compacte.  
Ex : Le **minimum essentiel d’un réseau** est la plus petite norme d’un element non nul du reseau.  
Le theoreme de Minkowski permet de majorer ce min essentiel. TODO (illisible)  
Il existe un 2nd théorème de Minkowski appelé théorème des minima successifs   
**VI.4. Caractères d’un groupe abélien fini (Serre Cours d’arithmétique)**  
**Un caractère d’un groupe abélien fini** , correspond à un morphisme du groupe vers le groupe multiplicatif des complexes.  
**Le dual d’un groupe abélien fini**, est l’ensemble des caractères de ce groupe.  
Pour faire l’analogie avec les formes linéaires, on pourrait noter   
L’image d’un élément d’un groupe abélien fini, par un caractère du groupe, est une racine -ième de l’unité avec   
Dans un groupe cyclique d’ordre engendré par , pour une racine -ième de l’unité fixée , alors il existe un unique caractère de ce groupe tel que .   
Ainsi, pour un groupe cyclique d’ordre , est un isomorphisme de groupes, et on sait dans ce cas que . Donc étant aussi , on a   
Tout caractère d’un sous-groupe d’un groupe abélien fini , peut être prolongé en caractère du groupe .  
L’opération de restriction est un morphisme de groupes surjectif, de noyau les caractères de triviaux sur , est donc isomorphe à   
On a donc une suite exacte   
Le dual d’un groupe abélien fini, est aussi un groupe abélien fini de même cardinal.   
**Relations d’orthogonalité.**  
Pour un caractère d’un groupe abélien fini ,   
Pour un élément d’un groupe abélien fini ,   
Pour un groupe abélien fini, on a donc   
Pour un élément d’un groupe abélien fini, est un caractère du dual .  
L’application est un isomorphisme de groupes.  
**Exemples de caractères** : Pour ,   
 et est un ev isomorphe à donc de dimension .  
**Lemme d’indépendance de Dedekind.** Une famille finie de caractères distincts sur un groupe fini, forment une famille libre du ev .  
Ainsi   
Pour un groupe fini, abélien.  
En général   
On peut montrer le théorème de classification des groupes abéliens finis.  
Un groupe abélien fini est isomorphe à son dual, (non canoniquement). On le sait dans le cas cyclique et .  
Sur un groupe abélien fini, sur , est un produit scalaire hermitien.  
Pour ,   
Pour ce produit scalaire, les caractères de forment une base orthonormale, (et donc une famille libre). **VII. Le groupe symétrique  
VII.1. Propriétés élémentaires du groupe symétrique  
Le groupe symétrique d’ordre n,** (ou ) est le groupe des bijections de muni de la composition. Il est abélien ssi   
Une **permutation** est un élément du groupe symétrique.  
Le **support d’une permutation** est l’ensemble des points non fixes par elle.  
Si avec sont des elements distincts de le **p-cycle** est la permutation définie par et partout ailleurs.  
 est le **support du -cycle**.  
Un -cycle est d’ordre dans le groupe symétrique.  
Une **transposition** est un 2-cycle , se note parfois .  
Deux cycles à supports disjoints commutent.  
Toute permutation du groupe symétrique s’écrit comme produit de cycles à supports disjoints de façon unique à permutation près des cycles.  
L’ordre d’une permutation est le ppcm des ordres des cycles de sa décomposition en cycles.  
Si est un -cycle et alors est encore un -cycle.  
Dans , tous les cycles d’ordre fixé sont conjugués.  
Le centralisateur dans d’un -cycle est son groupe engendré.  
La classe de conjugaison d’une permutation est définie de façon unique par la suite croissante des ordres des cycles de sa décomposition. La somme de ces ordres vaut . Une classe de conjugaison correspond donc à un élément de   
La suite croissante des ordres des cycles de la décomposition de peut être compris comme le type de . Une autre façon de le définir est :  
Pour il existe un unique appelé **type de**  tel que est le nombre de -cycles dans la décomposition de en produit de cycles à supports disjoints, et est le nombre de points fixes de .  
Une classe de conjugaison dans correspond donc à un type fixé. Càd 2 permutations sont conjuguées ssi elles ont même type.  
 le nombre de permutations de commutant avec est   
 le nombre de permutations de dont le type est , est   
La probabilité pour que deux permutations choisies uniformément et indépendamment dans commutent est .   
**Hardy et Ramanujan 1918.**   
Les ensembles suivants engendrent le groupe symétrique d’ordre :  
Les transpositions pour   
Les transpositions pour   
Les transpositions pour   
La transposition et le cycle   
Une **inversion d’une permutation**  est une paire telle que . **VII.2. Le groupe alterné  
La signature** est l’unique morphisme de groupes non trivial   
La signature d’une permutation est si le nombre d’inversions est paire, -1 sinon, càd .  
On a   
La signature d’une transposition est . Donc la signature est à valeurs dans le groupe .  
Le produit de transpositions a donc pour signature   
Un -cycle est d’ordre et de signature . (On peut le décomposer en transpositions).  
Le **groupe alterné d’ordre n** est le noyau de la signature dans le groupe symétrique.   
Une permutation **paire** est un élément de , une permutation **impaire** est élément de . Autrement dit la parité d’une permutation est la parité de son nombre d’inversions.  
Le groupe alterné d’ordre n est un sous-groupe d’indice 2 du groupe symétrique d’ordre n.  
 agit -transitivement sur . agit -transitivement sur .  
Pour les 3-cycles, engendrent le groupe . Si les 3-cycles sont de plus conjugués dans .  
Pour tout -cycle est un carré, est engendré par les carrés.  
Pour est le seul sous-groupe d’indice 2 du groupe .  
**Th. du a Galois\*.** Le groupe alterné d’ordre est un groupe simple. (pas , car )  
Si , les groupes dérivés de et sont donnés par et .  
Si , les seuls groupes distingués de sont et   
Tout sous-groupe d’indice de est isomorphe a  **VII.3. Automorphismes de**La connaissance des automorphismes de permet de déterminer les actions d’un groupe sur et par suite les produits semi-directs impliquant   
Un automorphisme intérieur est un automorphisme de , qui est trivial ssi commute avec tout element de .   
La suite est une suite exacte courte, et des que le centre est trivial , n’est pas abélien, donc  
Pour   
Pour , tout automorphisme du groupe symétrique est un automorphisme intérieur, donc  
Pour on a .  
Un automorphisme du groupe symétrique qui transforme les transpositions en transpositions, est un automorphisme intérieur.  
Si ,   
Si , le groupe n’est ni abélien, ni monogène, ni cyclique.  
 et n’est jamais direct pour .  
Dans , il y a -cycles () **VIII. Sous-groupes de Sylow**   
**VIII.0. p-groupes**Pour un nombre premier, un **-groupe** est un groupe fini de cardinal avec .  
Le centre d’un -groupe divise et a au moins elements   
**Théorème de Cauchy 1.** Dans un groupe fini, pour tout diviseur premier de son cardinal, on peut trouver un élément d’ordre ce diviseur. (par récurrence forte et équation aux classes).  
Pour premier, un groupe fini est un -groupe ssi tous ses elements sont d’ordre une puissance de .Tout sous-groupe et tout quotient d’un p-groupe est encore un p-groupe.  
Un groupe dont un sous-groupe est un p-groupe normal et le quotient par lui estun p-groupe, est un p-groupe. Un produit semi-direct de deux p-groupes est un p-groupe.  
Le produit restreint d’une famille de p-groupes est un p-groupe.  
Dans un p-groupe, l’indice d’un sous-groupe est soit infini, soit une puissance de .  
Tout p-groupe est nilpotent donc résoluble. **VIII.1. Sous-groupes de Sylow**La question principale est inverse de Lagrange : étant donné un diviseur de l’ordre d’un group fini, existe-t-il un sous-groupe de cardinal ? Pas vrai en général car et n’a pas de sous-groupe d’ordre 6.Soit un nombre premier, et un groupe fini.Un **-Sylow d’un groupe fini** , est un sous-groupe de cardinal , avec et .  
Une autre définition possible est un **-Sylow d’un groupe fini**  est un -sous-groupe maximal de G pour l’inclusion. Un -Sylow est un -sous-groupe d’indice premier avec .  
Exemple : Si corps a éléments, le groupe est fini de cardinal le nombre de bases de . Càd .  
L’ensemble des matrices triangulaires supérieures de avec des 1 sur la diagonale, est un -Sylow de car de cardinal . **VIII.2. Théorèmes de Sylow  
Th. Sylow 1.** Un groupe fini G dont est un diviseur premier de son cardinal, contient au moins un -Sylow et alors pour tout sous-groupe de , tel que est un -Sylow de .  
Soit un groupe fini , on note avec . Alors pour tout , admet un -sous-groupe de cardinal .  
Tout -sous-groupe d’un groupe fini , peut etre inclus dans un -Sylow du groupe.  
**Th de Cauchy 2.** Un groupe fini G dont est un diviseur premier de son cardinal, contient au moins un sous-groupe d’ordre . Ce sous-groupe est cyclique donc on retrouve le théorème de Cauchy 1.  
**Th. Sylow 2.** Pour fixé, les -Sylows d’un groupe fini sont 2 à 2 conjugués.   
**Th. Sylow 3.** Le nombre de -Sylow distincts de , divise et   
Un -Sylow d’un groupe fini est distingué ssi c’est l’unique -Sylow pour ce fixé. **VIII.3. Quelques applications et compléments**Tout groupe de cardinal 45 est isomorphe a l’un des produits directs ou   
Si groupe de cardinal avec premiers, alors  
Si ne divise pas ,   
Si divise , ou avec l’unique action non triviale de sur   
Un groupe simple de cardinal est isomorphe au groupe alterne d’ordre 5.  
Soit un groupe fini, et un diviseur premier fixe du cardinal de G, alors   
Tous les -Sylows de G sont distingués ssi le groupe G est produit direct de ses -Sylows.  
**Argument de Frattini.** Soit un groupe fini, un sous-groupe distingué, et un p-Sylow de . Alors avec le centralisateur de S cad   
En particulier, si est un sous-groupe de G contenant le centralisateur d’un -Sylow du groupe G, alors est egal a son centralisateur .

**Complément 1. Algorithme de Todd-Coxeter  
1.1. Un premier exemple  
1.2. Description de l’algorithme  
Complément 2. Géométrie diophantienne  
2.1. Approximation diophantienne  
2.2. L’équation de Pell**

**Exercices.**Dans un groupe quelconque ,   
Si l’union de deux sous-groupes est un groupe, alors l’un deux est inclus dans l’autre.  
L’intersection de deux sous-groupes de cardinaux finis et premiers entre eux, est le groupe trivial.  
Le produit interne de deux sous-groupes d’ordre deux premiers distincts, est un sous-groupe cyclique.  
Le produit externe de sous-groupes de cardinaux est cyclique ssi   
Un groupe dans lequel tout carré est nul, est abélien. De plus s’il est fini et non trivial, il est isomorphe a .  
Un sous-groupe d’indice du groupe symétrique avec premier , est un sous-groupe d’indice ou . Montre qu’il n’y a pas de sous-groupe de d’ordre ou , bien que , donc fournit un contre-exemple réciproque Lagrange.  
Dans un groupe abélien si alors   
Un groupe fini tel que l’équation a au plus solutions, est un groupe cyclique.  
Un sous-groupe d’un groupe fini, dont l’indice est le plus petit facteur premier de , est distingué.  
Un groupe fini d’ordre tel que , est cyclique.  
**Tchebycheff\*.**Si alors premier tel que .  
**Symbole de Legendre.** TODO  
Tout entier naturel est somme de quatre carrés d’entiers\*.