Leçon 103 - Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.

Extrait du rapport de jury

Dans un premier temps, la notion de conjugaison dans un groupe doit être introduite, développée et illustrée dans des situations variées. On doit proposer des situations où la conjugaison aide à résoudre certains problèmes (par exemple, en transformant un élément en un autre plus simple à manipuler). On peut aussi illustrer et utiliser le principe du "transport par conjugaison" voulant que hgh^{-1} ait la même "nature géométrique" que g.
Ensuite, il est attendu de développer l'intérêt de la notion de sous-groupe distingué en particulier en regard de la structure de groupe obtenue par quotient d'un groupe, le lien entre sous-groupe distingué et noyau de morphisme de groupes, ainsi que la factorisation d'un morphisme de groupe au travers d'un tel quotient. Il est souhaitable de proposer quelques résultats bien choisis mettant en évidence l'utilisation de ces notions : citons par exemple le lien entre les sous-groupes de l'un et de l'autre et la caractérisation interne des produits directs. L'examen de la simplicité de certains groupes peut être proposé.
Comme indiqué dans le sujet, il est demandé de présenter des exemples pertinents utilisés pour obtenir des résultats significatifs. De tels exemples sont nombreux en théorie des groupes mais il est souhaitable d'en proposer dans d'autres domaines, comme en arithmétique, en géométrie et en algèbre linéaire.
Pour aller plus loin, les candidates et candidats peuvent poursuivre en illustrant ces notions en théorie des représentations des groupes finis (classes de conjugaison et nombres de représentations irréductibles, treillis des sous-groupes distingués lu dans la table de caractères, etc.).
La notion de produit semi-direct et les théorèmes de Sylow débordent du programme. Il est possible de les évoquer, mais en veillant à les illustrer par des exemples et des applications.

Présentation de la leçon

Je vais vous présenter la leçon 103 intitulée : "Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.". La notion de conjugaison est très importante en algèbre car elle conduit à la notion de sous-groupe distingué qui sont utilisés pour étudier les groupes via les dévissages en suite de quotients successifs et de faire sortir l'importance des groupes simples. C'est le fil directeur que nous donnerons à cette leçon.
Dans une première partie on s'intéresse à la conjugaison dans un groupe avec un premier point consacré à l'action de conjugaison où l'on rappelle la définition ainsi que le vocabulaire associé puis quelques exemples puis on deuxième point où l'on donne une application aux p-groupes via l'étude des points fixes sous une action et en corollaire la cas de la conjugaison qui conduit à la classification des groupes d'ordre p^2.
Dans une deuxième partie on s'intéresse aux sous-groupes distingués en commençant par quelques généralités. On donne ainsi la définition d'un sous-groupe distingué ainsi que quelques exemples et les premières propriétés avant d'en arriver à la notion de classe et d'indice d'un sous-groupe. Cette notion d'indice est très importante car elle permet de donner une condition suffisante pour être un sous-groupe distingué. On introduit dans un deuxième point la notion de groupe quotient qui est construite à partir de celle de sous-groupe distingué et on donne en théorème 28 un résultat de correspondance bijective entre les sous-groupes de G contenant H et les sous-groupes de G/H. On termine cette partie avec les théorèmes d'isomorphismes en commençant par le théorème de factorisation ainsi que le premier théorème d'isomorphisme qui sont les plus utilisés avant de donner les deux derniers théorèmes d'isomorphisme.
Dans une troisième partie on étudie quelques sous-groupes distingués remarquables en commençant par le cas du centre. On définit ainsi le centre d'un groupe puis l'on donne les centres de différents groupes. On passe ensuite au cas du groupe dérivé définit comme le sous-groupe engendré par les commutateurs. On donne ensuite quelques propriétés en rapport avec les sous-groupes distingués avant de donner quelques exemples de groupes dérivés de différents groupes. On termine cette partie avec un rapide dernier point sur le groupe des automorphismes intérieurs en faisant le lien le centre et le groupe des automorphismes.
Dans une quatrième partie on s'intéresse à la notion de dévissage de groupe dans le but de mieux connaître sa structure interne. On commence par parler de la simplicité d'un groupe et des théorèmes de Sylow : on donne la définition d'un groupe simple et on donne plusieurs exemples avant de montrer que $\mathfrak{A}_n$ et $\mathrm{SO}_3(\mathbb{R})$ sont des groupes simples. On introduit ensuite la théorie de Sylow via quelques définitions ainsi que les théorèmes de Sylow qui permettent de donner des résultats de classification ou de simplicité. Dans un deuxième point on parle du produit direct en en donnant la définition interne et externe ainsi que la caractérisation. On finit cette partie par le cas du produit semi-direct en donnant la définition externe et interne puis quelques exemples et caractérisations.
On termine cette leçon avec une dernière partie consacrée à d'autres notions où

l'on commence par le normalisateur en en donnant la définition ainsi que quelques propriétés de base. On passe ensuite aux groupes résolubles en introduisant tout d'abord la notion de suite de composition et de Jordan-Hölder. On donne ensuite des propriétés classiques sur un groupe résoluble avant de faire le lien avec la suite dérivée qui donne une caractérisation très utile de la résolubilité d'un groupe ainsi que des résultats intéressants comme on peut le voir dans toute la fin de ce point. Enfin, on finit par quelques applications de la notions de groupe résoluble avec des résultats très puissants comme le théorème de Burnside, de Gauss-Wantzel, d'Abel-Ruffini et de Shafarevich qui sont à la fois des résultats fondamentaux de l'algèbre et des sujets de recherche récents.

Plan général

I - Conjugaison dans un groupe
1 - Action de conjugaison
2 - Application aux p-groupes

II - Généralités sur les sous-groupes distingués
1 - Sous-groupe distingué
2 - Groupe quotient
3 - Les théorèmes d'isomorphisme

III - Sous-groupes distingués remarquables
1 - Le centre d'un groupe
2 - Le groupe dérivé
3 - Les automorphismes intérieurs

IV - Application au dévissage de groupes
1 - Simplicité d'un groupe et théorie de Sylow
2 - Produit direct
3 - Produit semi-direct

V - D'autres notions
1 - Normalisateur
2 - Groupes résolubles et lien avec la suite dérivée
3 - Applications de la notion de groupe résoluble

Cours détaillé

Dans toute cette leçon, on considère un groupe $(G,*)$ non trivial dont l'élément neutre est noté e_G, n un entier naturel non nul, un corps commutatif $\mathbb{K}$ et E un $\mathbb{K}$-espace vectoriel normé de dimension finie.

I Conjugaison dans un groupe

I.1 Action de conjugaison

Définition 1 : Action par conjugaison [Berhuy, p.171] :
On dit que G **agit sur lui-même par conjugaison** via l'action $\cdot : \left| \begin{array}{ccc} G\times G & \longrightarrow & G \\ (g,x) & \longmapsto & g\cdot x = gxg^{-1} \end{array} \right.$.

On note Int_g le morphisme φ associé à l'action "$\cdot$" (appelé **automorphisme intérieur**) et $\mathrm{Int}(G)$ l'ensemble des automorphismes intérieurs de G.

Remarque 2 : [Berhuy, p.171 + Perrin, p.15]
$*$ Cette action n'est pas fidèle en général (par exemple pour G abélien). Cette action n'est donc utilisé que lorsque le groupe G est non abélien car sinon tous les automorphismes intérieurs sont triviaux.
$*$ Les orbites pour cette action sont appelées **classes de conjugaison** et les stabilisateurs d'un élément sont appelés **centralisateurs**.

Exemple 3 : [Berhuy, p.211 + 217 + Rombaldi, p.146 + 148 + 150 + 199]
$*$ Le groupe $\mathrm{GL}_n(\mathbb{K})$ agit par conjugaison sur $\mathcal{M}_n(\mathbb{K})$ (on retrouve alors les notions de matrices semblables et les résultats de réduction qui en découlent).
$*$ Si $n\geq 5$, alors les 3-cycles sont tous conjugués dans $\mathfrak{A}_n$. De manière plus générale, deux permutations de $\mathfrak{S}_n$ sont conjuguées si, et seulement si, elles sont de même type.
$*$ Le conjugué dans $\mathrm{GL}(E)$ d'une transvection est une transvection.
De plus, pour $n\geq 3$, toutes les transvections différentes de Id_E sont conjuguées dans $\mathrm{SL}(E)$.
$*$ Le conjugué dans $\mathrm{GL}(E)$ d'une dilatation est une dilatation de même rapport.

I.2 Application aux p-groupes

Dans toute cette sous-partie, on considère p un nombre premier et on suppose que G agit sur un ensemble X non vide.

Définition 4 : p-groupe [Berhuy, p.180] :
On appelle **p-groupe** tout groupe fini d'ordre une puissance de p.

Proposition 5 : [Berhuy, p.181]
Si G est un p-groupe et que X est fini, alors $\mathrm{Card}(X) \equiv \mathrm{Card}\left(X^G\right) \ [p]$.
De plus, si p ne divise pas $\mathrm{Card}(X)$, alors $X^G \neq \emptyset$.

Corollaire 6 : [Berhuy, p.181]
Si G est un p-groupe non trivial, alors l'ensemble des éléments qui commutent avec tous les autres est non trivial.

Développement 1 : [A] [cf. BERHUY]

Proposition 7 : [Berhuy, p.194]
Soit p un nombre premier.
Si G est d'ordre p^2, alors $G \cong \mathbb{Z}/p^2\mathbb{Z}$ ou $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

II Généralités sur les sous-groupes distingués

Dans toute cette partie, on considère H un sous-groupe de G.

II.1 Sous-groupe distingué

Définition 8 : Sous-groupe distingué [Berhuy, p.135] :
On dit que H est un **sous-groupe distingué de** G lorsque pour tout $h \in H$ et tout $g \in G$, $ghg^{-1} \in H$.

Remarque 9 : [Berhuy, p.135 + Delcourt, p.20 + 21]
* Un sous-groupe distingué est donc stable par tout automorphisme intérieur de G et on peut alors définir une action par conjugaison de G sur H.
* Il existe des notions plus fortes comme les sous-groupes caractéristiques (stables par tout automorphisme de G) ou les sous-groupes pleinement invariants (stable par tout morphisme de G dans G).

Exemple 10 : [Berhuy, p.136]
* Si G est abélien, alors tout sous-groupe de G est distingué dans G.
* $\{e_G\}$ et G sont tous des sous-groupes distingués dans G.

Remarque 11 : [Berhuy, p.136]
Nous verrons plus loin que les sous-groupes distingués interviendront naturellement dans la construction de groupes quotients et qu'ils jouent un rôle capital en algèbre via les groupes simples et résolubles.

Proposition 12 : [Berhuy, p.139]
Soit f un morphisme de groupes.
$\mathrm{Ker}(f)$ est un sous-groupe distingué du groupe de départ.

Exemple 13 : [Berhuy, p.139 + 140]
* $\mathrm{SL}(E)$ est un sous-groupe distingué de $\mathrm{GL}(E)$ (car noyau du morphisme déterminant).
* $\mathfrak{A}_n$ est un sous-groupe distingué de $\mathfrak{S}_n$ (car noyau du morphisme signature).

Proposition 14 : [Perrin, p.34 + 35]
* L'intersection de deux sous-groupes distingués est distinguée.
* L'image réciproque d'un sous-groupe distingué par un morphisme de groupes est un sous-groupe distingué.
* L'image direct d'un sous-groupe distingué par un morphisme de groupes surjectif est un sous-groupe distingué.

Lemme 15 : [Berhuy, p.145]
Pour tout $a \in G$, on note $aH = \{ah,\ h \in H\}$ et $Ha = \{ha,\ h \in H\}$.
* La relation $\sim_g$ définie sur G par $(x \sim_g y) \iff (x^{-1}y \in H)$ est une relation d'équivalence et pour tout $x \in G$, $\overline{x} = xH$.
* La relation $\sim_d$ définie sur G par $(x \sim_d y) \iff (yx^{-1} \in H)$ est une relation d'équivalence et pour tout $x \in G$, $\overline{x} = Hx$.
* Pour tous $x, y \in G$, on a $(x \sim_g y) \iff \left(x^{-1} \sim_d y^{-1}\right)$.

Définition 16 : Classe à gauche modulo un sous-groupe [Berhuy, p.145] :
On appelle **classe à gauche modulo** H un ensemble de la forme xH avec $x \in G$.
On note alors G/H l'ensemble des classes à gauche.

Remarque 17 : [Berhuy, p.145 + 146]
* On définit de même les classes à droite modulo H et ces deux types de classes coïncident lorsque G est abélien.
* Les classes à gauche/à droite étant des classes d'équivalences pour une certaine relation d'équivalence sur G, elles partitionnent G et on a alors tous les résultats classiques sur les classes d'équivalence.

Définition 18 : Indice d'un sous-groupe [Berhuy, p.146] :
Le nombre de classe à gauche modulo H, lorsqu'il est fini, est appelé **indice de** H **dans** G et est noté $[G : H]$ (et c'est aussi le nombre de classe à droite modulo H).

Exemple 19 : [Berhuy, p.146]
Pour $G = \mathbb{Z}$ et $H = n\mathbb{Z}$, la relation d'équivalence associée à H n'est rien d'autre que la relation de congruence modulo n et donc $[\mathbb{Z} : n\mathbb{Z}] = n$.

Les notions de classes à gauche/à droite permettent de donner une caractérisation des sous-groupes distingués de G :

Lemme 20 : [Berhuy, p.147]
Les assertions suivantes sont équivalentes :
$*$ H est distingué dans G. $*$ Pour tout $x \in G$, $xH = Hx$.
$*$ Pour tout $x \in G$, $xHx^{-1} = H$.

Proposition 21 : [Berhuy, p.147]
Tout sous-groupe d'indice 2 de G est distingué dans G.

Proposition 22 : [Berhuy, p.215]
Si $n \geq 2$, alors le groupe alterné $\mathfrak{A}_n$ est l'unique sous-groupe d'indice 2 de $\mathfrak{S}_n$.

Théorème 23 : Théorème de Frobenius [Berhuy, p.179] :
Si G est fini et que tout diviseur premier de $\mathrm{Card}(H)$ est supérieur ou égal à $[G : H]$, alors H est distingué dans G.
En particulier, si p est le plus petit diviseur premier de G, alors tout sous-groupe d'indice p est distingué dans G.

II.2 Groupe quotient

Proposition 24 : [Berhuy, p.236]
Si H est un sous-groupe distingué de G, alors la loi interne définie sur G/H par $(\overline{x};\overline{y}) \longmapsto \overline{xy}$ est bien définie, de neutre $\overline{e_G}$ et induit sur G/H une structure de groupe.
De plus, l'application $\pi : G \longmapsto G/H$ définie par $x \longmapsto \overline{x}$ est un morphisme de groupes.

La réciproque étant également vraie, on suppose donc jusqu'à la fin de cette partie que H est distingué dans G.

Définition 25 : Groupe quotient [Berhuy, p.237] :
Le groupe G/H est appelé **groupe quotient de G par H**.

Remarque 26 : [Berhuy, p.237 + 238]
$*$ Si $[G : H]$ est fini, alors $\mathrm{Card}(G/H) = [G : H]$.
En particulier, si G est fini, alors on a $\mathrm{Card}(G/H) = \frac{\mathrm{Card}(G)}{\mathrm{Card}(H)}$.
$*$ Si G est abélien, tout sous-groupe de G est distingué et on peut toujours construire le groupe quotient.
$*$ La projection canonique $\pi : G \longmapsto G/H$ est surjective et de noyau H. Ainsi, tout sous-groupe distingué de G est le noyau d'un certain morphisme de groupes.

Exemple 27 : [Berhuy, p.238]
$*$ On a $G/G \cong \{\overline{e_G}\}$.
$*$ On a $G \cong G/\{e_G\}$ (l'isomorphisme étant donné par la projection canonique).
$*$ Le groupe $\mathbb{Z}/n\mathbb{Z}$ n'est rien d'autre que le groupe quotient de $\mathbb{Z}$ par $n\mathbb{Z}$.

Théorème 28 : [Berhuy, p.238]
La projection canonique $\pi : G \longrightarrow G/H$ induit une correspondance bijective entre l'ensemble des sous-groupes H' de G contenant H et l'ensemble des sous-groupes de G/H.
Plus précisément, si H' est un sous-groupe de G contenant le sous-groupe distingué H, alors on a $H'/H = \pi(H') = \left\{\overline{h'},\ h' \in H'\right\}$ est un sous-groupe de G/H.
Réciproquement, si S est un sous-groupe de G/H, alors $\pi^{-1}(S)$ est un sous-groupe de G contenant H, et ces deux constructions sont inverses l'une de l'autre.
Enfin, cette correspondance établit une bijection entre l'ensemble des sous-groupes distingués de G contenant H et l'ensemble des sous-groupes distingués de G/H.

II.3 Les théorèmes d'isomorphisme

Dans toute cette sous-partie, on considère un groupe $(G', \top)$ et un morphisme de groupes $f : (G, *) \longrightarrow (G', \top)$.

Théorème 29 : Théorème de factorisation [Berhuy, p.239] :
Si $H \subseteq \mathrm{Ker}(f)$, alors il existe un unique morphisme de groupes $\overline{f} : G/H \longrightarrow G'$ tel que $f = \overline{f} \circ \pi$. Ce morphisme est défini par : $\forall \overline{x} \in G/H,\ \overline{f}(\overline{x}) = f(x)$.
De plus, il y a une correspondance bijective entre $\mathrm{Hom}_{gr}(G/H, G')$ et l'ensemble $\{f \in \mathrm{Hom}_{gr}(G, G') \text{ tq } H \subseteq \mathrm{Ker}(f)\}$ via l'application $\varphi \longmapsto \varphi \circ \pi$ (et de réciproque $f \longmapsto \overline{f}$).

Lemme 30 : [Berhuy, p.240]
Le morphisme groupes $\overline{f} : G/\mathrm{Ker}(f) \longrightarrow G'$ est injectif.

Théorème 31 : Premier théorème d'isomorphisme [Berhuy, p.241] :
Le morphisme groupes $\overline{f} : G/\mathrm{Ker}(f) \longrightarrow G'$ induit un isomorphisme de groupes $G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$.

Exemple 32 : [Berhuy, p.241]
$*$ On a $\mathbb{C}^*/\mathbb{U} \cong \mathbb{R}_+^*$ via $z \longmapsto |z|$. $*$ On a $\mathbb{R}/2\pi\mathbb{Z} \cong \mathbb{U}$ via $\theta \longmapsto e^{i\theta}$.

Proposition 33 : [Perrin, p.106]
On a $\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{PSL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$.

Théorème 34 : [Perrin, p.106]
On a les isomorphismes suivants :
* $\mathrm{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$ et $\mathrm{PSL}_2(\mathbb{F}_3) \cong \mathfrak{A}_4$. * $\mathrm{PGL}_2(\mathbb{F}_4) = \mathrm{PSL}_2(\mathbb{F}_4) \cong \mathfrak{A}_5$.
* $\mathrm{PGL}_2(\mathbb{F}_5) \cong \mathfrak{S}_5$ et $\mathrm{PSL}_2(\mathbb{F}_5) \cong \mathfrak{A}_5$.

Théorème 35 : Deuxième théorème d'isomorphisme [Berhuy, p.242] :
Soit K un sous-groupe de G.
* Les ensembles KH et HK sont des sous-groupes de G et $< H, K >= HK = KH$.
* Le sous-groupe H est distingué dans HK et $H \cap K$ est distingué dans K, de sorte que l'on a un isomorphisme de groupes $HK/H \cong K/(H \cap K)$.

Corollaire 36 :
Sous les bonnes hypothèses des deux premiers théorèmes d'isomorphisme, on a $\mathrm{Card}(G) = \mathrm{Card}(\mathrm{Ker}(f))\,\mathrm{Card}(\mathrm{Im}(f))$ et $\mathrm{Card}(HK) = \mathrm{Card}(H)\frac{\mathrm{Card}(K)}{\mathrm{Card}(H\cap K)}$.

Théorème 37 : Troisième théorème d'isomorphisme [Berhuy, p.243] :
Soit K un sous-groupe distingué de G.
Si K est un sous-groupe de H, alors K est distingué dans H, H/K est distingué dans G/K et l'on a un isomorphisme de groupes $(G/K)/(H/K) \cong G/H$.

III Sous-groupes distingués remarquables

III.1 Le centre d'un groupe

Définition 38 : Centre d'un groupe [Berhuy, p.136] :
On appelle **centre de** G l'ensemble $Z(G) = \{z \in G \text{ tq } \forall g \in G,\ zg = gz\}$.

Remarque 39 : [Berhuy, p.136 + Perrin, p.12 + 15]
* $Z(G)$ est un sous-groupe abélien de G, il est donc distingué et on a $Z(G) = G$ si, et seulement si, G est abélien.
* $Z(G)$ est même un sous-groupe caractéristique (stable par tout automorphisme de G).
* $Z(G)$ est l'intersection de tous les centralisateurs $C_G(g)$ pour $g \in G$.

Exemple 40 : [Berhuy, p.136 + 137]
* $Z(\mathrm{GL}(E)) = \mathbb{K}^\times \mathrm{Id}_E$.
* $Z(\mathrm{SL}(E)) = Z(\mathrm{SL}(E)) \cap \mathrm{SL}(E) = \{\lambda \mathrm{Id}_E \text{ tq } \lambda \in \mathbb{K} \text{ et } \lambda^n = 1\}$.
* Si E est un espace euclidien, alors on a :

$$Z(\mathrm{O}(E)) = \{-\mathrm{Id}_E; \mathrm{Id}_E\} \text{ et } Z(\mathrm{SO}(E)) = \begin{cases} \mathrm{SO}(E) & \text{si } n = 1 \text{ ou } 2 \\ \{-\mathrm{Id}_E; \mathrm{Id}_E\} & \text{si } n \geq 4 \text{ est pair} \\ \{\mathrm{Id}_E\} & \text{si } n \geq 3 \text{ est impair} \end{cases}$$

* Si $n \geq 3$, alors $Z(\mathfrak{S}_n) = \mathrm{Id}_{[\![1;n]\!]}$.

Remarque 41 :
Grâce à la partie I.2, on sait que le centre d'un p-groupe non trivial n'est pas trivial et on peut alors classifier les groupes d'ordre p^2.

Proposition 42 : [Berhuy, p.285]
Si $G/Z(G)$ est un groupe monogène, alors G est abélien (et donc $G = Z(G)$).

Proposition 43 : [Delcourt, p.139]
* Si n est impair, alors centre de D_{2n} est réduit au sous-groupe trivial.
* Si n est pair, alors le centre de D_{2n} est égal à $\left\{\mathrm{Id}, \tau^{\frac{n}{2}}\right\}$ (avec τ une rotation de mesure d'angle $\frac{2\pi}{n}$).

Proposition 44 : [Delcourt, p.43 + 136]
Le groupe $\mathbb{H}_8$ (non commutatif !) possède 6 sous-groupes stricts et chacun est commutatif et distingué dans $\mathbb{H}_8$.
En particulier, $Z(\mathbb{H}_8) = \{-1; 1\}$.

Proposition 45 : [Perrin, p.105]
Le centre de $\mathrm{GL}_n(\mathbb{F}_q)$ est de cardinal égal à $q-1$ et celui de $\mathrm{SL}_n(\mathbb{F}_q)$ est de cardinal égal à $\mathrm{PGCD}(n, q-1)$.

III.2 Le groupe dérivé

Définition 46 : Groupe dérivé [Berhuy, p.321] :
On appelle **groupe dérivé de** G (noté $D(G)$) le sous-groupe engendré par les commutateurs (c'est-à-dire les éléments de la forme $[g, h] = ghg^{-1}h^{-1}$).

Lemme 47 : [Berhuy, p.286 + 321]
Soit H un sous-groupe distingué de G.
Si G/H est abélien, alors H contient $D(G)$. Réciproquement, si H est un sous-groupe contenant $D(G)$, alors H est distingué dans G et G/H est abélien

Proposition 48 : [Perrin, p.13]
$D(G)$ est l'intersection de tous les sous-groupes distingués H de G dont les quotients sont abéliens.
En particulier, $D(G)$ est un sous-groupe distingué de G (et même caractéristique !).

Proposition 49 : [Perrin, p.13]
$G/D(G)$ est abélien, c'est même le plus grand quotient abélien de G et ceci caractérise $D(G)$.

Définition 50 : Abélianisé d'un groupe [Delcourt, p.139] :
On appelle **abélianisé de** G (et noté G^{ab}), le groupe quotient $G/D(G)$.

Exemple 51 : [Perrin, p.13]
* Si G est abélien, alors $D(G) = \{e_G\}$ et $G^{ab} = G$.
* Si $n \geq 2$, alors $D(\mathfrak{S}_n) = \mathfrak{A}_n$ et $\mathfrak{S}_n^{ab} \cong \mathbb{Z}/2\mathbb{Z}$.
* Si $n \in \{1; 2; 3\}$, alors $D(\mathfrak{A}_n) = \left\{\mathrm{Id}_{[\![1;n]\!]}\right\}$.
* Si $n \geq 5$, alors $D(\mathfrak{A}_n) = \mathfrak{A}_n$ et $\mathfrak{A}_n^{ab} = \left\{\overline{\mathrm{Id}}\right\}$ * $D(\mathbb{H}_8) = \{1; -1\}$.

Proposition 52 : [Delcourt, p.136]
* Si n est impair, alors le groupe dérivé de D_{2n} est égal à $< \tau > \cong \mathbb{Z}/n\mathbb{Z}$.
* Si $n = 2m$ est pair, alors le groupe dérivé de D_{2n} est égal à $\langle \tau^2 \rangle \cong \mathbb{Z}/m\mathbb{Z}$.

Proposition 53 : [Berhuy, p.323]
Soit $G^{(2)}$ le sous-groupe de G engendré par les carrés des éléments de G.
* Si H est un sous-groupe distingué de G, alors $D(H)$ est distingué dans G.
En particulier, $D(G)$ est distingué dans G.
* On a $D(G) \subseteq G^{(2)}$.
De plus, si G est engendré par des éléments d'ordre 2, alors $D(G) = G^{(2)}$.

Théorème 54 : [Rombaldi, p.154]
Pour $n \geq 2$, on a :
* $D(\mathrm{SL}_n(\mathbb{K})) \subseteq D(\mathrm{GL}_n(\mathbb{K})) \subseteq \mathrm{SL}_n(\mathbb{K})$.
* Pour $n \geq 3$, $D(\mathrm{SL}_n(\mathbb{K})) = D(\mathrm{GL}_n(\mathbb{K})) = \mathrm{SL}_n(\mathbb{K})$.
* Pour $n = 2$, $\mathbb{K} \neq \mathbb{F}_2$ et $\mathbb{K} \neq \mathbb{F}_3$, $D(\mathrm{SL}_n(\mathbb{K})) = D(\mathrm{GL}_n(\mathbb{K})) = \mathrm{SL}_n(\mathbb{K})$.

Remarque 55 : [Rombaldi, p.155]
* Pour $\mathbb{K} = \mathbb{F}_2$, on a $\mathrm{GL}_n(\mathbb{K}) = \mathrm{SL}_n(\mathbb{K})$.
* Pour $n = 2$ et $\mathbb{K} = \mathbb{F}_2$, on a $D(\mathrm{SL}_n(\mathbb{K})) \cong \mathfrak{A}_3$.
* Pour $n = 2$ et $\mathbb{K} = \mathbb{F}_3$, on a $D(\mathrm{SL}_n(\mathbb{K})) \cong \mathbb{H}_8$.

Proposition 56 : [Berhuy, p.286]
Tout morphisme de groupes $f : G \longrightarrow G'$, avec G' un groupe abélien, se factorise en un morphisme de groupes $G/D(G) \longrightarrow G'$.

III.3 Les automorphismes intérieurs

Définition 57 : Automorphisme intérieur [Berhuy, p.131] :
On appelle **automorphisme intérieur de** G tout automorphisme de la forme Int_g, avec $g \in G$.

Proposition 58 : [Berhuy, p.131 + Delcourt, p.15]
L'ensemble $\mathrm{Int}(G)$ est un groupe pour la composition.
De plus, c'est un sous-groupe distingué de $\mathrm{Aut}(G)$.

Proposition 59 : [Berhuy, p.284]
On a l'isomorphisme de groupes $G/Z(G) \cong \mathrm{Int}(G)$.

Proposition 60 : [Perrin, p.30 + 33]
* Pour $n \neq 6$, on a $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$.
* Pour $n = 6$, on a $\mathrm{Aut}(\mathfrak{S}_n) \neq \mathrm{Int}(\mathfrak{S}_n)$ et $\mathrm{Int}(\mathfrak{S}_n)$ est un sous-groupe d'indice 2 dans $\mathrm{Aut}(\mathfrak{S}_n)$.

IV Application au dévissage de groupes

IV.1 Simplicité d'un groupe et théorie de Sylow

Dans toute cette sous-partie, on considère p un nombre premier.

Définition 61 : Groupe simple [Berhuy, p.140] :
On dit que G est un **groupe simple** lorsque $G \neq \{e_G\}$ et que G admet pour seuls sous-groupes distingués $\{e_G\}$ et G (c'est-à-dire les sous-groupes distingués triviaux).

Exemple 62 : [Berhuy, p.140]
* Le groupe $\mathrm{GL}(E)$ n'est pas simple puisque $\mathrm{SL}(E)$ est un sous-groupe distingué non trivial (sauf cas exceptionnels).
* Pour $n = 2$ le groupe $\mathfrak{S}_n$ est simple mais dès que $n \geq 3$ il ne l'est plus car contient $\mathfrak{A}_n$ comme sous-groupe distingué non trivial.
* Un groupe non abélien dont le centre est non trivial n'est pas simple (c'est par exemple le cas de $\mathrm{SL}(E)$ pour $n \geq 2$).
* Les groupes abéliens simples sont exactement (à l'isomorphisme près) les $\mathbb{Z}/p\mathbb{Z}$.

Remarque 63 : [Berhuy, p.140 + 252]
* La classification des groupes finis simples à l'isomorphisme près est connue. Son obtention à été un travail de longue haleine et la dernière version de la démonstration de cette classification nécessite environ 5 000 pages !
* On porte énormément d'intérêt aux groupes simples car se sont, en quelques sorte, les briques élémentaires dont "tout groupe fini est constitué" (équivalent des nombres premier en arithmétique + suite de Jordan-Hölder).

Développement 2 : [cf. ROMBALDI]

Théorème 64 : [Rombaldi, p.50] :
Pour $n = 3$ ou $n \geq 5$, le groupe $\mathfrak{A}_n$ est simple.

Remarque 65 : [Berhuy, p.219 + Perrin, p.28 + 37]
* En réalité, $\mathfrak{A}_5$ est le plus petit groupe simple non abélien (et tout groupe simple d'ordre 60 est isomorphe à $\mathfrak{A}_5$).
* Ce résultat est cohérent avec le théorème de Feit-Thompson (tout groupe simple fini et non abélien est d'ordre pair).
* Ce résultat a une importance historique majeure car il permet de montrer que pour $n \geq 5$, $\mathfrak{A}_n$ n'est pas résoluble et donc que les solutions des équations polynomiales de degré supérieur ou égal à 5 ne peuvent s'écrire à l'aide des quatre opérations élémentaires et de la racine carré.

Remarque 66 : [Perrin, p.30]
* Si $n = 4$, alors $\mathfrak{A}_n$ n'est pas simple car contient comme sous-groupe distingué $H = \left\{\mathrm{Id}_{[\![1;4]\!]}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\right\}$.
* De plus, $\mathfrak{A}_4$ est le plus petit groupe (à l'isomorphisme près) qui ne vérifie pas la réciproque du théorème de Lagrange.

Corollaire 67 : [Berhuy, p.220 + Delcourt p.139]
* Si $n \geq 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont exactement $\mathrm{Id}_{[\![1;n]\!]}, \mathfrak{A}_n$ et $\mathfrak{S}_n$ et on a $D(\mathfrak{A}_n) = \mathfrak{A}_n$.
* De plus, on a $D(\mathfrak{S}_n) = \mathfrak{A}_n$.

Remarque 68 : [Berhuy, p.220]
Si $n = 4$, alors il faut rajouter à la liste précédente le sous-groupe H de $\mathfrak{S}_4$.

Théorème 69 : [Francinou, p.67]
Le groupe $\mathrm{SO}_3(\mathbb{R})$ est simple.

Théorème 70 : [Perrin, p.102]
Le groupe $\mathrm{PSL}_n(\mathbb{K})$ est simple, sauf lorsque $n = 2$ et ($\mathbb{K} = \mathbb{F}_2$ ou $\mathbb{F}_3$).

Proposition 71 : [Perrin, p.17]
Soit H un sous-groupe de G distinct de G.
Si G est infini et que $[G : H] < +\infty$, alors G n'est pas simple.

Jusqu'à la fin de cette sous-partie, on suppose que G est de cardinal fini noté n.

Définition 72 : p-sous-groupe de G [Berhuy, p.311] :
On appelle **p-sous-groupe de G** tout sous-groupe de G de cardinal une puissance de p.

Jusqu'à la fin de cette partie, on écrit $\mathrm{Card}(G) = n = p^m q$ où $p \nmid q$ et $m \in \mathbb{N}^*$.

Définition 73 : p-sous-groupe de Sylow de G [Berhuy, p.311] :
On appelle **p-sous-groupe de Sylow de G** (ou plus simplement p-Sylow) tout sous-groupe de G d'ordre p^m.

Exemple 74 :
* $\mathbb{Z}/6\mathbb{Z}$ contient un 2-Sylow et un 3-Sylow (respectivement $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$).
* $\mathbb{Z}/56\mathbb{Z}$ contient un 2-Sylow et un 7-Sylow (respectivement $\mathbb{Z}/8\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$).

Théorème 75 : Théorème de Sylow [Berhuy, p.313] :
* Il existe des p-sous-groupes de Sylow de G et tout p-sous-groupe de G est contenu dans un p-Sylow.
* Le conjugué d'un p-Sylow est un p-Sylow et tous les p-Sylow de G sont conjugués entre eux. En particulier, si S est un p-Sylow de G, alors S est distingué dans G si, et seulement si, S est l'unique p-Sylow de G.
* Si n_p désigne le nombre de p-Sylow de G, alors $n_p \equiv 1\ [p]$ et $n_p | q$.

Exemple 76 : [Berhuy, p.315 + 328]
Tout groupe d'ordre 63 ou 255 n'est pas simple.

Corollaire 77 :
Tout groupe d'ordre pq avec $p < q$ qui sont deux nombres premiers n'est pas simple.

Corollaire 78 : [Berhuy, p.315]
Tout groupe d'ordre 33 cyclique.

Théorème 79 : Théorème de Cauchy [Berhuy, p.179] :
G possède au moins un élément d'ordre p.

Développement 3 : [B] [cf. BERHUY]

Proposition 80 : [Berhuy, p. 310]
Soit p un nombre premier supérieur ou égal à 3.
Si G est d'ordre $2p$, alors G est isomorphe à $\mathbb{Z}/2p\mathbb{Z}$ ou à D_{2p}.

IV.2 Produit direct

Définition 81 : Produit direct externe [Berhuy, p.293] :
On considère $G_1, ..., G_r$ des groupes.
Le groupe $G_1 \times ... \times G_r$ (muni de la loi de groupe naturelle) est appelé le **produit direct externe** des groupes $G_1, ..., G_r$.

Définition 82 : Produit direct interne [Berhuy, p.293] :
On considère r sous-groupes $H_1, ..., H_r$ de G, avec $r \geq 2$.
On dit que G est le **produit direct interne** de $H_1, ..., H_r$ (et on note alors $G = H_1 \odot ... \odot H_r$) lorsque les deux conditions suivantes sont réalisées :
* Dès que $i \neq j$, on a $h_i h_j = h_j h_i$ pour tout $(h_i, h_j) \in H_i \times H_j$.
* Tout élément g de G s'écrit de manière unique sous la forme $g = h_1 ... h_r$ avec h_i un élément de H_i.

Théorème 83 : [Berhuy, p.295]
Soient r sous-groupes $H_1, ..., H_r$ de G, avec $r \geq 2$.
On a $G = H_1 \odot ... \odot H_r$ si, et seulement si, les conditions suivantes sont satisfaites :
* Pour tout $i \in [\![1; r]\!]$, le sous-groupe H_i est distingué dans G.
* On a $G = \langle H_1, ..., H_r \rangle$.
* Pour tout $i \in [\![1; r-1]\!]$, on a $H_1 ... H_i \cap H_{i+1} = \{1_G\}$.

Dans le cas où G est fini, on peut remplacer la deuxième condition du théorème précédent par une condition plus simple à vérifier :

Corollaire 84 : [Berhuy, p.295]
Soient r sous-groupes $H_1, ..., H_r$ de G, avec $r \geq 2$.
On a $G = H_1 \odot ... \odot H_r$ si, et seulement si, les conditions suivantes sont satisfaites :
* Pour tout $i \in [\![1; r]\!]$, le sous-groupe H_i est distingué dans G.
* On a $\mathrm{Card}(G) = \mathrm{Card}(H_1) ... \mathrm{Card}(H_r)$.
* Pour tout $i \in [\![1; r-1]\!]$, on a $H_1 ... H_i \cap H_{i+1} = \{1_G\}$.

Corollaire 85 : [Berhuy, p.296]
Soient H et K deux sous-groupes de G.
On a $G = H \odot K$ si, et seulement si, les conditions suivantes sont satisfaites :
* Les sous-groupes H et K sont distingués dans G.
* On a $\mathrm{Card}(G) = \mathrm{Card}(H) \, \mathrm{Card}(K)$.
* $H \cap K = \{1_G\}$.

IV.3 Produit semi-direct

Dans toute cette sous-partie, on considère H et K deux groupes.

Proposition 86 : [Berhuy, p.298]
Soit $\rho : \left| \begin{array}{ccc} K & \longrightarrow & \mathrm{Aut}(H) \\ k & \longmapsto & \rho_k \end{array} \right.$ un morphisme de groupes.
La loi interne :
$$\cdot : \left| \begin{array}{ccc} (H \times K) \times (H \times K) & \longrightarrow & H \times K \\ ((h, k), (h', k')) & \longmapsto & (h\rho_k(h'), kk') \end{array} \right.$$
est une loi de groupe de neutre $(1_H, 1_K)$.

Définition 87 : Produit semi-direct externe [Berhuy, p.300] :
On considère $\rho : K \longrightarrow \mathrm{Aut}(H)$ un morphisme de groupes.
L'ensemble $H \times K$ muni de la loi de groupe précédente est appelé **produit semi-direct externe** de H et K par ρ (et on le note $H \rtimes_\rho K$).

Lemme 88 : [Berhuy, p.300]
Soit $\rho : \left| \begin{array}{ccc} K & \longrightarrow & \mathrm{Aut}(H) \\ k & \longmapsto & \rho_k \end{array} \right.$ un morphisme de groupes.
Les assertions suivantes sont équivalentes :
* On a $H \rtimes_\rho K = H \times K$.
* Le morphisme $\rho : K \longrightarrow \mathrm{Aut}(H)$ est trivial.
* Le sous-groupe $K' = \{(1_H, k), \ k \in K\}$ est distingué dans $H \rtimes_\rho K$.

On suppose désormais que H et K sont deux sous-groupes de G.

Définition 89 : Produit semi-direct interne [Berhuy, p.300] :
On dit que G est le **produit semi-direct interne** de H par K (et on note $G = H \rtimes K$) lorsque les conditions suivantes sont vérifiées :
* Le sous-groupe H est distingué dans G.
* Tout élément de G s'écrit de manière unique sous la forme $g = hk$ avec h un élément de H et k un élément de K.

Exemple 90 : [Berhuy, p.301]
* $\mathfrak{S}_E = \mathfrak{A}_E \rtimes \langle \tau \rangle$, avec τ une transposition fixée.
* $\mathrm{GL}(E) = \mathrm{SL}(E) \rtimes D$, avec D le sous-groupe de $\mathrm{GL}(E)$ formé des matrices de dilatation.
* On considère $\sigma \in D_{2n}$ une rotation de mesure d'angle $\frac{2\pi}{n}$ et $\tau \in D_{2n}$ une symétrie orthogonale dont l'axe passe par le centre du n-gone régulier et un des sommets.
Si l'on pose $H =< \sigma >$ et $K =< \tau >$, alors $D_{2n} = H \rtimes_\rho K$ où $\rho_1 = \mathrm{Id}_H$ et ρ_τ est le passage à l'inverse.

Proposition 91 : [Berhuy, p.301]
On a $G = H \rtimes K$ si, et seulement si, les conditions suivantes sont vérifiées :
* Le sous-groupe H est distingué dans G.
* On a $G = \langle H, K \rangle$ (ou, de manière équivalente, $G = HK$).
* On a $H \cap K = \{1_G\}$.

Exemple 92 : [Perrin, p.24]
Le groupe $\mathbb{Z}/8\mathbb{Z}$ n'est pas de la forme $H \rtimes K$.
En effet, comme $\mathbb{Z}/8\mathbb{Z}$ est abélien, le produit serait direct. Or, $\mathbb{Z}/8\mathbb{Z}$ n'est isomorphe ni à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, ni à $(\mathbb{Z}/2\mathbb{Z})^3$.

Corollaire 93 : [Berhuy, p.302]
On a $G = H \rtimes K$ si, et seulement si, les conditions suivantes sont vérifiées :
* Le sous-groupe H est distingué dans G. * On a $\text{Card}(G) = \text{Card}(H)\,\text{Card}(K)$.
* On a $H \cap K = \{1_G\}$.

Remarque 94 :
Grâce au théorème de structure et des produits (semi-)directs il est possible de classifier les groupes d'ordre 8 (soit : $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, D_8 et $\mathbb{H}_8$).

V D'autres notions

V.1 Normalisateur

Dans toute cette partie, on considère H un sous-groupe de G.

Définition 95 : Normalisateur [Berhuy, p.160] :
On appelle **normalisateur de** H **dans** G l'ensemble :

$$N_G(H) = \{g \in G \text{ tq } gHg^{-1} = H\}$$

Proposition 96 : Berhuy, p.160]
$N_G(H)$ est un sous-groupe de G dans lequel H est distingué et c'est le plus grand vérifiant cette propriété.

Exemple 97 : [Perrin, p.18]
Dans $\mathfrak{S}_3$, les trois sous-groupes à deux éléments sont conjugués et sont leurs propres normalisateurs.

Proposition 98 : [Delcourt, p.72]
Si G est un groupe fini, alors :
* Le nombre de conjugués de H est l'indice de son normalisateur.
* De même, le nombre de conjugués d'un élément de G est l'indice de son centralisateur.

Lemme 99 : Lemme de Frattini [Delcourt, p.75] :
Soient N un sous-groupe de G et S un p-Sylow de N.
Si G est fini, alors les conjugués de S dans G sont dans N et $G = NN_G(S)$.

Proposition 100 : [Delcourt, p.75]
Si G est un p-groupe et que H est un sous-groupe propre de G, alors soit H est normal dans G, soit il existe un conjugué de H, distinct de H, qui est inclus dans $N_G(H)$.

V.2 Groupes résolubles et lien avec la suite dérivée

Définition 101 : Suite de composition [Berhuy, p.246] :
On appelle **suite de composition de** G la suite finie de sous-groupes :

$$\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n := G$$

telle que pour tout $i \in [\![0;n-1]\!]$, G_i est un sous-groupe distingué de G_{i+1}.

Exemple 102 : [Berhuy, p.246 + 247]
* $\{\overline{0}\} \lhd \mathbb{Z}/2\mathbb{Z} \lhd \mathbb{Z}/6\mathbb{Z} \lhd \mathbb{Z}/12\mathbb{Z}$ est une suite de composition du groupe cyclique $\mathbb{Z}/12\mathbb{Z}$.
* Pour tout sous-groupe distingué H de G, la suite $\{e_G\} \lhd H \lhd G$ est une suite de composition de G.

Définition 103 : Suite de Jordan-Hölder [Berhuy, p.251] :
On appelle **suite de Jordan-Hölder de** G toute suite de composition de G dont les quotients sont des groupes simples.

Exemple 104 : [Berhuy, p.251]
* La suite $\{\overline{0}\} \lhd \mathbb{Z}/3\mathbb{Z} \lhd \mathbb{Z}/6\mathbb{Z}$ est une suite de Jordan-Hölder de $\mathbb{Z}/6\mathbb{Z}$.
* $\mathbb{Z}$ n'admet pas de suite de Jordan-Hölder.

Définition 105 : Groupe résoluble [Berhuy, p.259] :
On dit que G est un **groupe résoluble** lorsqu'il existe une suite fini de sous-groupes :

$$\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n := G$$

telle que pour tout $i \in [\![0;n-1]\!]$, G_i est un sous-groupe distingué de G_{i+1} et G_{i+1}/G_i est un groupe abélien.

Exemple 106 : [Berhuy, p.259]
* Tout groupe abélien est résoluble.
* Tout groupe cyclique est résoluble (car abélien)
* $\mathfrak{S}_3$ et $\mathfrak{S}_4$ sont résolubles. * Les groupes D_8 et $\mathbb{H}_8$ sont résolubles.
* $\mathfrak{A}_5$ et $\mathfrak{S}_4$ ne sont pas résolubles.

Remarque 107 : [Berhuy, p.259 + Delcourt, p.153]
Il existe d'autres notions plus fortes que celles de groupe résoluble (groupe super-résoluble, polycyclique, etc.).

Proposition 108 : [Berhuy, p.260]
Soit H un sous-groupe distingué de G.
H et G/H sont résolubles si, et seulement si, G est résoluble.

Corollaire 109 :
Si G est un groupe fini qui n'est pas simple et que tout groupe d'ordre strictement plus petit que $\text{Card}(G)$ est résoluble, alors G est résoluble.

Théorème 110 : Théorème de Feit-Thompson [ADMIS] [Berhuy, p.260] :
Tout groupe fini d'ordre impair est résoluble.
En particulier, tout groupe simple non commutatif est d'ordre pair.

Définition 111 : Suite dérivée d'un groupe [Berhuy, p.287] :
On appelle **suite dérivée de** G la suite $(D^n(G))_{n\in\mathbb{N}}$ définie par :

$$D^0(G) := G \text{ et } \forall n \in \mathbb{N},\ D^{n+1}(G) := D(D^n(G))$$

Théorème 112 : [Berhuy, p.287]
G est un résoluble si, et seulement si, sa suite dérivée est stationnaire à $\{e_G\}$.

Proposition 113 :
G est un groupe résoluble si, et seulement si, $D(G)$ est un groupe résoluble.

Théorème 114 :
Un groupe résoluble est simple si, et seulement si, il est cyclique et d'ordre un nombre premier.

Corollaire 115 :
Tout groupe simple fini est cyclique et d'ordre un nombre premier ou bien il est d'ordre pair.

Théorème 116 : [Escofier, p.170]
Si $n \geq 5$, alors $\mathfrak{A}_n$ n'est pas un groupe résoluble.
En particulier, $\mathfrak{S}_n$ n'est pas un groupe résoluble pour $n \geq 5$.

Théorème 117 :
Si G est résoluble et possède une suite de Jordan-Hölder, alors tous les quotients de cette suite sont cycliques et d'ordre un nombre premier.

Théorème 118 :
Si G est fini, alors :
G est résoluble si, et seulement si, G possède une suite de composition dont tous les quotients sont cycliques et d'ordre un nombre premier.

Proposition 119 : [Berhuy, p.261]
Soit p un nombre premier.
Tout p-groupe est résoluble.

V.3 Applications de la notion de groupe résoluble

Théorème 120 : Théorème de Burnside [Perrin, p.40] :
Soient p, q deux nombres premiers distincts et a, b deux entiers naturels.
Si G est un groupe fini d'ordre $p^a q^b$, alors G est résoluble.

Corollaire 121 :
Si $\text{Card}(G) < 60$, alors G est résoluble.

Théorème 122 : Théorème de Gauss-Wantzel [Berhuy, p.795] :
Soit n un entier naturel supérieur ou égal à 2.
Le n-gone régulier est constructible à la règle non graduée et au compas si, et seulement si, $n := 2^s \prod_{i=1}^r p_i$ (avec $s, r \in \mathbb{N}$ et $p_1, ..., p_r$ qui sont r nombres de Fermat distincts).

Exemple 123 : [Berhuy, p.805]
Il est possible de construire le pentagone régulier avec la règle non graduée et le compas.

Théorème 124 : Théorème d'Abel–Ruffini [Escofier, p.181] :
Si $n \geq 5$, alors l'équation polynomiale générale de degré n n'est pas résoluble par radicaux.

Théorème 125 : Théorème de Shafarevich [ADMIS] [Escofier, p.220] :
Tout groupe fini résoluble est le groupe de Galois d'une extension finie de $\mathbb{Q}$.

Remarques sur le plan

- On peut également parler de suite exacte (courte) et de théorie des représentations.
- Il faut penser à illustrer la leçon avec beaucoup d'exemple et pas juste des résultats théoriques.

Liste des développements possibles

- Classification des groupes d'ordre p^2 et $2p$.
- Simplicité de $\mathfrak{A}_n$ pour $n = 3$ et $n \geq 5$.
- Simplicité de $\mathrm{SO}_3(\mathbb{R})$.

Bibliographie

- Grégory Berhuy, *Algèbre : le grand combat*.
- Daniel Perrin, *Cours d'algèbre*.
- Jean-Étienne Rombaldi, *Mathématiques pour l'agrégation, Algèbre et Géométrie*.
- Jean Delcourt, *Théorie des groupes*.
- Serge Francinou, *Exercices de mathématiques, Oraux X-ENS, Algèbre 3*.
- Jean-Pierre Escofier, *Théorie de Galois*.