I) Définitions et premières propriétés des groupes finis [PER]

1) Définition et exemples de groupes finis

↑9-11

Définition 1 (Groupe fini): Soit $(G,*)$ un groupe, si G est de cardinal fini alors on dit que $(G,*)$ est un groupe fini. On appelle ordre de G, noté $|G|$, le cardinal de G.

Exemples de groupes finis 2: i) $(S_n, \circ)$ avec S_n l'ensemble des bijections de $[\![1,n]\!]$ dans $[\![1,n]\!]$. On a $|S_n| = n!$

ii) $(\mathbb{Z}/n\mathbb{Z}, +)$ avec $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'entier modulo n. On a $|\mathbb{Z}/n\mathbb{Z}| = n$

iii) $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ avec $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$. On a $|(\mathbb{Z}/n\mathbb{Z})^*| = \#\{k \in [\![1,n-1]\!] \mid k \wedge n = 1\} = \varphi(n)$

iv) $(GL(n,\mathbb{F}_q), \times)$ avec $GL(n,\mathbb{F}_q)$ l'ensemble des matrices inversibles à coefficients dans $\mathbb{F}_q$.

v) $(D_n, \circ)$ avec D_n l'ensemble des isométries du plan laissant invariant le polygône régulier à n côtés. On a $|D_n| = 2n$.

vi) $(Q_8, *)$ avec $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ et $i*i = j*j = k*k = i*j*k = -1$, $i*j = -j*i = k$, $j*k = -k*j = i$ et $k*i = -i*k = j$. On a $|Q_8| = 8$.

2) Propriétés des groupes finis

Définition 3 (ordre d'un élément): Soit G un groupe fini et $x \in G$. on appelle ordre de x le plus petit $n \in \mathbb{N}^*$ tel que $\underbrace{x * \cdots * x}_{n \text{ fois}}$, soit l'élément neutre de G.

Exemple 4: i) Si $n \in \mathbb{N}$ et $k \in [\![1,n]\!]$ alors $(12\cdots k)$ est d'ordre k dans S_n.

ii) Si $n \in \mathbb{N}$ et $k \in [\![1,n-1]\!]$ alors $\bar{k}$ est d'ordre $\frac{n}{n \wedge k}$ dans $\mathbb{Z}/n\mathbb{Z}$.

iii) La rotation d'angle $\frac{2\pi}{n}$, notée r, est d'ordre n dans D_n.

Définition 5 (classes à gauche): Soit G un groupe fini et H un sous-groupe de G. On appelle classe à gauche de $a \in G$ relativement à H le sous-ensemble de G : $aH = \{g = ah, h \in H\}$. Ces classes forment une partition de G. Leur ensemble est noté G/H et on appelle indice de H, noté $(G:H)$, le cardinal de G/H.

Exemple 6: $Q_8 = \{\pm 1\} \sqcup i\{\pm 1\} \sqcup j\{\pm 1\} \sqcup k\{\pm 1\} \Rightarrow (Q_8 : \{\pm 1\}) = 4$

Théorème 7 (Lagrange): Soit G un groupe fini et H un sous-groupe de G. Alors $|G| = |H|(G:H)$. En particulier, l'ordre de tout élément de G divise l'ordre de G.

Application 8: i) Tout groupe fini d'ordre p est cyclique.

ii) Soient $a, n \in \mathbb{N}$ avec $a \wedge n = 1$. Alors $a^{\varphi(n)} = 1 \ [n]$. Si n est premier alors $\varphi(n) = n-1$ et on retrouve le petit théorème de Fermat.

Définition 9 (Famille génératrice): Soit G un groupe et A une partie de G. On appelle sous-groupe engendré par A, noté $\langle A \rangle$, le plus petit sous-groupe de G (au sens de l'inclusion) contenant A.

Exemple 10: i) Si $k \wedge n = 1$ alors $\mathbb{Z}/n\mathbb{Z} = \langle \bar{k} \rangle$

ii) Si $T_n = \{\text{transpositions de } S_n\}$ alors $S_n = \langle T_n \rangle$

iii) $S_n = \langle (12), (12\cdots n) \rangle$ si $n \geq 3$.

iv) $Q_8 = \langle i, j \rangle$

Définition 11 (Sous-groupe distingué): Soit G un groupe et H un sous-groupe de G. On dit que H est distingué dans G, noté $H \lhd G$, si $\forall a \in G$ et $\forall h \in H$, $aha^{-1} \in H$. ($\Leftrightarrow \forall a \in G$, $aH = Ha$)

Propriété 12: Si G est un groupe et H un sous-groupe de G tel que $(G:H) = 2$ alors $H \lhd G$.

Exemples 13: i) $\langle r \rangle \lhd D_n$

ii) Tout sous-groupe d'un groupe abélien est distingué.

Propriété 14: Si $\varphi : G \to G'$ est un morphisme de groupe, alors $\ker \varphi \lhd G$. Réciproquement, si $H \lhd G$ alors G/H est muni d'une structure de groupe et $\exists \pi : G \to G/H$ morphisme surjectif de noyau H.

Définition 15 (A_n): Soit $n \in \mathbb{N}$, il existe un unique morphisme de S_n dans $\{\pm 1\}$ non trivial appelé la signature. On pose $A_n = \ker \varphi$.

Théorème 16 (d'isomorphisme): Si $\varphi : G \to G'$ est un morphisme de groupe alors $\operatorname{Im} \varphi \simeq G/\ker \varphi$.

Application 17: i) $A_n \lhd S_n$ et $|A_n| = \frac{n!}{2}$

ii) Tout groupe fini cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

iii) Si $p \geq 3$ est premier alors $(\mathbb{Z}/p\mathbb{Z})^*$ possède exactement $\frac{p-1}{2}$ carrés.

Définition 18 (Groupe simple): Un groupe G est dit simple si ses seuls sous-groupes distingués sont $\{1\}$ et G.

Exemples 19: i) $\mathbb{Z}/p\mathbb{Z}$ est simple ($\Leftrightarrow$) p premier

ii) Q_8 et les D_n pour $n \geq 2$ ne sont pas simples.

iii) A_n est simple $\forall n \geq 5$

iv) S_n n'est jamais simple $\forall n \geq 3$

II] Sous-groupes particuliers [PER] ↑ 17-18

Définition 20 (Centre) : On appelle centre de G le sous-groupe des éléments de G qui commutent avec tout les autres :
$Z(G) = \{a \in G \mid \forall g \in G,\ ag = ga\}$

Exemples 21 : i) G commutatif $\Leftrightarrow Z(G) = G$ ii) $Z(S_n) = \{Id\}\ \forall n \geq 3$

Propriété 22 : i) $Z(G) \lhd G$
ii) Si $G/Z(G)$ est cyclique alors G est abélien.

Application 23 : Soit G un groupe fini non commutatif et n_G le nombre de paires d'éléments de G qui commutent. Alors $n_G \leq \frac{5}{8}$.

Définition 24 (Groupe dérivé) : Soit G un groupe et $x, y \in G$. On appelle commutateur de x et y l'élément $[x;y] = xyx^{-1}y^{-1} \in G$. On appelle groupe dérivé de G, noté $D(G)$, le sous-groupe de G engendré par les commutateurs.

Exemples 25 : i) G est commutatif $\Leftrightarrow D(G) = 1$ ii) $D(Q_8) = \{\pm 1\}$
iii) $D(S_n) = A_n$ pour $n \geq 2$ iv) $D(A_n) = A_n$ pour $n \geq 5$
v) $D(GL(n, \mathbb{F}_q)) = D(SL(n, \mathbb{F}_q)) = SL(n, \mathbb{F}_q)$ sauf si $n=2, q=2$ ou $n=2, q=3$.

Propriété 26 : i) $D(G) \lhd G$
ii) $G/D(G)$ est le plus grand quotient abélien et cela caractérise $D(G)$.

Définition 27 (Action de groupe) : Soit G un groupe et X un ensemble, on dit que G opère sur X si on s'est donné une application $\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g \cdot x \end{array}$ vérifiant : $\forall g, g' \in G, \forall x \in X,\ g \cdot (g' \cdot x) = (gg') \cdot x$ et $\forall x \in X,\ 1 \cdot x = x$.

Exemple 28 : i) S_n agit sur $[\![1, n]\!]$ par $\sigma \cdot i = \sigma(i)$.
ii) G agit sur lui-même par $g \cdot a = ga$ et par $g \cdot a = gag^{-1}$.

Théorème 29 (Cayley) : Si G est fini de cardinal n, G est isomorphe à un sous-groupe de S_n.

Définition 30 (orbite / stabilisateur) : Si G opère sur X et si $x \in X$ on appelle stabilisateur de x : $G_x = \{g \in G \mid g \cdot x = x\}$ sous-groupe de G et on appelle orbite de x : $G \cdot x = \{g \cdot x,\ g \in G\}$ sous-ensemble de X.

Exemple 31 : Pour l'action de S_n sur $[\![1, n]\!]$ précédente on a $S_{n,1} \simeq S_{n-1}$

Propriété 32 : Soit G un groupe agissant sur un ensemble X et $x \in X$. L'application $\begin{array}{ccc} f : G/G_x & \longrightarrow & G \cdot x \\ gG_x & \longmapsto & g \cdot x \end{array}$ est une bijection.

Corollaire 33 : Si G est un groupe fini alors $\#(G \cdot x) = |G| / |G_x|$.

Application 34 : Un groupe fini ayant exactement deux classes de conjugaison est d'ordre 2.

Définition 35 (p-groupe) : Soit p un nombre premier. Un p-groupe est un groupe dont tout les éléments sont d'ordre une puissance de p.

Propriété 36 : Soit G un p-groupe opérant sur un ensemble X et soit $X^G = \{x \in X \mid \forall g \in G\ g \cdot x = x\}$ l'ensemble des points fixes de l'opération de G sur X. Alors $|X| \equiv |X^G| [p]$.

Théorème 37 (Cauchy) : Soit G un groupe fini et $p \mid |G|$. Alors il existe un élément de G d'ordre p.

Application 38 : Tout p-groupe fini est d'ordre une puissance de p.

Propriété 39 : Soit p un nombre premier et G un p-groupe. Alors $Z(G) \neq \{e\}$

Application 40 : i) Tout groupe d'ordre p^2 (p premier) est abélien.
ii) Tout groupe d'ordre p^α (p premier et $\alpha \geq 2$) est non simple.

[ULM] chapit

III) Théorème de Sylow [PER] ↑ 18-20

Définition 41 (p-sylow) : Soit G un groupe fini de cardinal $n = p^\alpha m$ avec $\alpha \geq 1$, p premier et $p \nmid m$. Un p-Sylow de G est un sous-groupe de G de cardinal p^α.

Exemples 42 : i) $\langle \bar{m} \rangle$ est un p-sylow de $\mathbb{Z}/p^\alpha m\mathbb{Z}$ ($p \nmid m$ p premier / $\forall \alpha$
ii) $P = \{A = (a_{ij}) \mid a_{ij} = 0$ si $i > j$ et $a_{ii} = \bar{1}\}$ l'ensemble des matrices triangulaires supérieures strictes sur $\mathbb{F}_p$ est un p-sylow de $GL(n, \mathbb{F}_p)$.

Définition 43 (normalisateur) : Soit G un groupe et H un sous-groupe de G. On appelle normalisateur de H dans G le groupe $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$. C'est le stabilisateur de H par l'opération $g \cdot H = gHg^{-1}$ de G sur ses sous-groupes.

Théorème 44 (Sylow) : Soit G un groupe fini tel que $|G| = p^\alpha m$ avec $p \nmid m$ p premier et $\alpha \geq 1$. Alors :
i) Si H est un sous-groupe de G qui est un p-groupe alors il existe un p-sylow S tel que $H \subset S$.
ii) les p-Sylow sont tous conjugués (et donc leur nombre k divise $|G|$)
iii) on a $k \equiv 1 [p]$ (et donc $k \mid m$)

Corollaire 45 : Si S est un p-Sylow de G alors :
$S \lhd G \Leftrightarrow S$ est l'unique p-Sylow de $G \Leftrightarrow k = 1$

Application 46 : i) Tout groupe d'ordre $p^\alpha q$ avec $p > q$ premiers n'est pas simple.
ii) Tout groupe d'ordre pqr avec p, q, r des premiers distincts n'est pas simple.
iii) Tout groupe non cyclique d'ordre < 60 n'est pas simple.
iv) Tout groupe d'ordre 77 est cyclique

Théorème 47 : Tout groupe simple d'ordre 60 est isomorphe à A_5.] DVP 1

[PER] ↑ 37

[ULM] ↑

] [ULM] ↑

IV) Représentations linéaires et caractères d'un groupe fini [GUM] chapitre 17

Définition 49: Soit V un $\mathbb{C}$ espace vectoriel de dimension finie. On appelle représentation linéaire sur $\mathbb{C}$ du groupe G tout morphisme $\rho: G \to GL(V)$. On dit que V est un G-module et on appelle degré de la représentation la dimension de V. Le représentation est dite fidèle si $\ker(\rho) = \{1\}$.

Exemple 49: $\rho: \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$, $\bar{x} \mapsto e^{\frac{2i\pi x}{n}}$ est une représentation de degré 1.

Définition 50 (Représentation irréductible): Un G-module V est dit:
i) irréductible si V et $\{0\}$ sont distincts et les seuls sous-G-modules de V.
ii) Complètement réductible si pour tout sous G-module W de V, $\exists L$ sous-G-module de V tel que $V = W \oplus L$.

Théorème 51 (Maschke): Si G est un groupe fini alors tout G-module est complètement réductible.

Théorème 52: Soient V un $\mathbb{C}$-espace vectoriel de dimension finie et $S \subseteq GL(V)$ un ensemble de matrices qui commutent entre-elles. Alors il existe une base dans laquelle les matrices de S sont simultanément triangulaires supérieures.

Corollaire 53: Un sous-groupe abélien fini A de $GL_n(\mathbb{C})$ peut être mis simultanément sous forme diagonale. En particulier:
- Toute représentation irréductible de A est de degré 1.
- Tout élément g d'un groupe fini est diagonalisable (car $\langle g \rangle \subset G$)

Définition 54 (Caractère): Soient G un groupe fini, $\rho: G \to GL(V)$ une représentation linéaire de G avec $\dim(V) = n$. Le caractère du G-module V est la fonction $\chi: G \to \mathbb{C}$, $g \mapsto \mathrm{Tr}(\rho(g))$. Le degré du caractère $\deg(\chi) = \chi(e)$ est la dimension de V.

Proposition 55: Soient G un groupe fini et V, W deux G-modules. Les caractères vérifient:
i) $\chi_{V \oplus W} = \chi_V + \chi_W$ ii) $\chi_{V \otimes W} = \chi_V \cdot \chi_W$ iii) $\chi_{V^*}(g) = \chi_V(g^{-1})$ $\forall g \in G$
iv) $\chi_{\mathrm{Hom}(V,W)} = \chi_{V^*} \cdot \chi_W$

Théorème 56: Soit G un groupe fini, le nombre de caractères irréductibles de G est égal au nombre m de classes de conjugaisons de G. L'ordre du groupe est donné par $|G| = \sum_{i=1}^{m} \chi_i(e)^2$.

Corollaire 57: Soit G un groupe fini, tout caractère χ de G possède une unique décomposition de la forme $\chi = \sum_{i=1}^{m} a_i \chi_i$ où $a_i \in \mathbb{N}$ et les χ_i sont les caractères irréductibles (distincts) de G.

Définition 58: Soient G un groupe et χ un caractère de G. On appelle noyau du caractère χ et on note $\ker(\chi)$ l'ensemble $\{g \mid g \in G, \chi(g) = \chi(e)\}$ des éléments de G qui ont même image que le neutre par χ.

Théorème 59 (caractérisation des groupes simples): Un groupe fini G est simple si et seulement si tout caractère irréductible non trivial ($\neq 1_G$) de G a un noyau trivial ($\ker(\chi) = \{e\}$). — DVP2

V) Théorèmes de structure de groupes

Théorème 60 (Structure des groupes abéliens finis): Soit G un groupe abélien fini d'ordre $n \geq 2$. Alors il existe des entiers $q_1 \geq 2$, q_2 multiple de $q_1, \dots, q_k$ multiple de q_{k-1}, uniques, tels que $G \simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_k\mathbb{Z}$.

Définition 61 (Suite des invariants): La suite $q_1, \dots, q_k$ ci-dessus caractérise G à isomorphisme près et s'appelle la suite des invariants de G.

Application 62: i) Si G est d'ordre p^2 (p premier) alors $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $G \simeq (\mathbb{Z}/p\mathbb{Z})^2$.
ii) Si G est abélien fini alors $\exists x \in G$ d'ordre le PPCM des ordres des éléments de G.
iii) Si G est abélien fini alors $\forall d \mid |G|$ il existe un sous-groupe d'ordre d. — [COM] ↑ 66-6

Propriété 63: Si G est d'ordre $2p$ avec p premier alors $G \simeq \mathbb{Z}/2p\mathbb{Z}$ ou $G \simeq D_p$. — [COM] ↑ 95-96

Propriété 64: Soit G un groupe d'ordre 8 alors:
- Si G abélien alors $G \simeq \mathbb{Z}/8\mathbb{Z}$, $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ou $G \simeq (\mathbb{Z}/2\mathbb{Z})^3$.
- Si G non abélien alors $G \simeq D_4$ ou $G \simeq Q_8$.

Application 65: Caractérisation des groupes de petit ordre

Ordre de G	G (à isomorphisme près)
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$(\mathbb{Z}/2\mathbb{Z})^2$ ou $\mathbb{Z}/4\mathbb{Z}$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}$ ou $D_3 \simeq S_3$
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, D_4 ou Q_8
9	$\mathbb{Z}/9\mathbb{Z}$ ou $(\mathbb{Z}/3\mathbb{Z})^2$
10	$\mathbb{Z}/10\mathbb{Z}$ ou D_5
11	$\mathbb{Z}/11\mathbb{Z}$

Références: [PER] Daniel Perrin – Cours d'algèbre

[ULM] Felix Ulmer – Théorie des groupes

[COM] François Combes – Algèbre et géométrie

[FRA] Serge Francinou & Co. – Oraux X-ENS Algèbre 1

$\mathfrak{A}_5$ est le seul groupe simple d'ordre 60

Rubén Muñoz--Bertrand

7 décembre 2014

Référence : Felix Ulmer - *Théorie des groupes*, p.90-91.

Leçons : 101, 103, 104, 105.

Énoncé : Soit G un groupe simple d'ordre 60. Alors $G \cong \mathfrak{A}_5$.

Preuve : Soit H un sous-groupe de H d'indice $m > 1$, alors G agit transitivement sur les classes à gauche de H par translation. On obtient donc un morphisme $\varphi : G \to \mathfrak{S}_m$, dont le noyau, ne pouvant être G tout entier, est $\{e_G\}$ par simplicité du groupe. Le morphisme est donc injectif, ce qui nous donne $|\mathfrak{S}_m| \geqslant 60$, donc $m > 4$.

Supposons dans un premier lieu que $m = 5$, on a donc $G \overset{\varphi}{\hookrightarrow} \mathfrak{S}_5$, d'où $\mathcal{D}(G) \overset{\varphi}{\hookrightarrow} \mathfrak{S}_5 = \mathcal{A}_5$. Or comme G est simple, il n'est pas abélien, et donc $\mathcal{D} = G$. G s'injecte donc dans $\mathfrak{A}_5$ de même cardinal : les deux groupes sont donc isomorphes.

Il suffit de montrer que tout groupe simple d'ordre 60 possède un sous-groupe d'indice 5. Pour ce faire, nous allons raisonner par l'absurde et supposer qu'il n'y a pas de tel groupe dans G.

Soit $p \in \{2, 3, 5\}$ et P un p-Sylow de G ; on sait que le nombre de p-Sylows de G est égal à $n_p = (G : N_G(P)) > 5$. En appliquant le théorème de Sylow, comme $n_5|12$ et $n_5 \equiv 1[5]$ on a $n_5 = 6$. De même, puisque $n_3|20$ et $n_5 \equiv 1[3]$, $n_3 = 10$. Enfin, comme $n_2|15$ et $n_2 \equiv 1[2]$ on a $n_2 = 15$.

Considérons deux 2-Sylows distincts de G (ils sont de cardinal 4, donc abéliens) S_2 et S_2'. Supposons qu'il existe $g \neq e_G$ dans leur intersection. Alors le centralisateur $Z_G(g)$ contient alors les deux 2-Sylows et est donc de cardinal au moins 5, or comme ce sont des sous groupes de $Z_G(g)$, d'après le théorème de Lagrange $|Z_G(g)||4$, donc $Z_G(g) \geqslant 12$ et $(G : Z_G(g)) \leqslant 4$. Or $Z_G(g) \neq G$ car $Z(G) = \{e_G\}$ puisque le groupe est simple et non abélien. On aurait donc un sous-groupe propre de G d'indice inférieur à 5, ce qui est impossible.

Tous les 2-Sylows ont donc une intersection réduite à l'élément neutre. On peut faire exactement le même raisonnement pour les 3-Sylows et les 5-Sylows.

On compte alors $n_2(4-1) = 45$ éléments de G dont l'ordre est divisible par 2, $n_3(3-1) = 20$ éléments dont l'ordre et divisible par 3 et $n_5(5-1) = 24$ éléments dont l'ordre est divisible par 5. En fait, nous avons trouvé 89 éléments dans un groupe qui en contient 60, ce qui est absurde, donc G contient toujours un sous-groupe d'indice 5, donc $G \cong \mathfrak{A}_5$.

□

Une caractérisation des groupes finis simples

Rubén Muñoz--Bertrand

7 décembre 2014

Référence : Felix Ulmer - *Théorie des groupes*, p.158-159.

Leçons : 104, 107.

Énoncé : Un groupe fini G est simple si et seulement si tous ses caractères irréductibles non triviaux ont un noyau trivial.

Preuve : Soit G un groupe fini et ρ une représentation de G de caractère χ. On rappelle que $Ker(\chi) = \{g \in G \mid \chi(g) = \chi(e_G)\}$. Nous allons démontrer que $Ker(\chi) = Ker(\rho)$.

Il est clair que $Ker(\chi) \supset Ker(\rho)$. Prouvons l'autre inclusion. Soit $g \in G$. La matrice $\rho(g)$ est diagonalisable car d'ordre fini, et ses valeurs propres $(\lambda_i)_{i\in[|1,\dim(V)|]}$ sont des racines de l'unité distinctes, et donc d'ordre 1.

Comme $\chi(g) = \sum_{i=1}^{\dim(V)} \lambda_i$, on obtient avec l'inégalité triangulaire :

$$|\chi(g)| = \left|\sum_{i=1}^{\dim(V)} \lambda_i\right| \leqslant \sum_{i=1}^{\dim(V)} |\lambda_i| = dim(V) = \chi(e_G)$$

Avec égalité si et seulement si tous les λ_i sont égaux. Nous avons alors $\chi(g) = \chi(e_G)$ si et seulement si tous les λ_i valent 1, c'est à dire $\rho(g) = Id$ ou encore $g \in Ker(\rho)$.

Le noyau de chaque caractère de G est par conséquent un sous-groupe distingué de G. C'est valable en particulier pour les caractères irréductibles non triviaux qui auront donc pour noyau soit G soit $\{e_G\}$. Le premier cas étant impossible puisque sinon le caractère serait trivial, on a démontré l'implication.

Réciproquement soit H un sous-groupe distingué de G d'indice n. Considérons l'action de G sur G/H par translation à gauche. On obtient alors un morphisme $\varphi : G \mapsto \mathfrak{S}_n$ qui induit une représentation linéaire $\rho : G \mapsto V := GL(\mathbb{C}, n)$ que l'on obtient en associant à chaque permutation la matrice de permutation de vecteurs correspondante.

Soit χ le caractère associé à ρ. On a $Ker(\chi) = Ker(\rho) = H$. On a démontré que tout sous-groupe distingué est noyau d'un caractère de G.

D'après le théorème de Maschke, on peut décomposer (V, ρ) en somme directe de représentations irréductibles $V = \bigoplus_i a_i V_i$, donc $\chi = \sum_i a_i \chi_i$, où les χ_i sont les caractères irréductibles associées aux (V_i, ρ_i).

Nous avons vu tout à l'heure que $Ker(\chi) = Ker(\rho)$; la décomposition en caractères irréductibles de (V, ρ) nous donne $Ker(\rho) = \cap_i Ker(\rho_i)$, i.e. $H = \cap_i Ker(\chi_i)$. Par conséquent, si tous les caractères irréductibles non triviaux ont pour noyau $\{e_G\}$, alors soit $H = G$, soit $H = \{e_G\}$, c'est à dire que G est simple.

□