Leçon 104 : GROUPES ABÉLIENS ET NON ABÉLIENS FINIS

I/ GÉNÉRALITES SUR LES GROUPES FINIS

1) Définition et premières propriétés

Def 1. *G est un groupe fini s'il contient un nombre fini d'éléments. L'ordre de G est le cardinal de G.*

Def 2. *L'ordre de $a \in G$ est le plus petit $n \in \mathbb{N}$ tel que $a^n = e$*

Rqe 3. *L'ordre d'un élément a est le cardinal $| < a > | = |\{e, a, a^2, ..., a^{n-1}\}|$*

Ex 4. *Si $G = \mathbb{Z}/4\mathbb{Z}$, on a $O(3) = 4$*

Def 5. *Soit $H \leqslant G$.On considère la relation d'équivalence sur G suivante : $x\mathcal{R}y \iff x^{-1}y \in H$. Une classe d'équivalence est de la forme xH et est appelée classe à gauche suivant H.*

Def 6. *L'entier $Card(G/\mathcal{R})$ est appelé indice de H dans G, et noté $[G : H]$.*

TH 7 (Lagrange). *Si G est un groupe fini, l'ordre de tout sous-groupe H de G divise l'ordre de G.*

Cor 8. *Si $|G| = n$, l'ordre de tout élément de G divise n. En particulier, tout élément de G vérifie $a^n = e$.*

Def 9. *Soit G un groupe. On appelle centre de G, noté $Z(G)$ l'ensemble des éléments de G commutant avec tous les éléments de G.*

Def 10. *Un sous-groupe H est distingué dans G si : $\forall x \in G \quad xH = Hx$*

Rqe 11. *$Z(G)$ est distingué dans G*

2) Actions de groupe

Def 12. *On dit que G agit sur un ensemble X s'il existe une application $\varphi : G \to \mathfrak{S}_X$.*

Ex 13. *Action par multiplication à gauche, action par conjugaison*

Def 14. *Le stabilisateur d'un élément $x \in X$ est l'ensemble $G_x = \{g \in G : g.x = x\}$*

Rqe 15. $\forall x \in X \ G_x \leqslant G$

Def 16. *L'orbite d'un élément $x \in X$ est l'ensemble $\mathcal{O}_x = \{g.x : g \in G\}$*

TH 17. *Si $|G| < \infty \quad \forall x \in X \quad Card(G) = |\mathcal{O}_x||G_x|$*

TH 18 (Equation aux classes). *Si X et G sont finis, en notant x les représentants des classes d'éq, on a : $Card(X) = \sum_x Card(\mathcal{O}_x) = \sum_x \frac{Card(G)}{Card(G_x)}$*

TH 19. *G fini. Il existe une famille finie de sous-groupes stricts (H_i) (i.e $\neq G$ et e) de G telle que : $Card(G) = Card(Z(G)) + \sum_{i \in I} \frac{Card(G)}{Card(H_i)}$*

App 20. *Le centre d'un p-groupe est non trivial*

TH 21 (Cauchy). *Si $|G| = n$, $\forall p$ premier $p|n$, $\exists H \leqslant G$, $|H| = p$.*

TH 22 (Cayley). *Si $|G| = n$, G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.*

II/ GROUPES ABELIENS FINIS

Def 23. *Un groupe est dit abélien si tous ses éléments commutent.*

Ex 24. $(\mathbb{F}_q, +)$ *abélien d'ordre p^n*

1) Un exemple de groupe abélien fini : les groupes cycliques

Def 25. *Un groupe cyclique si $\exists g \in G \quad < g >= G$.*

Rqe 26. *Si G est cyclique alors $\exists n \in \mathbb{N} \quad G \simeq (\mathbb{Z}/n\mathbb{Z}, +)$*

Prop 27. *Le groupe multiplicatif d'un corps fini est cyclique*

Ex 28. $(\mathbb{F}_q^*, .)$

Prop 29. *Si G est cyclique alors G est abélien.*

Rqe 30. *Réciproque fausse : groupe de Klein*

TH 31. *Si $|G| = p$ premier alors G cyclique*

TH 32. *Un groupe G d'ordre n est cyclique ssi G contient au plus un sous groupe d'ordre d pour tout diviseur d de n*

Ex 33. *$\mathfrak{S}_3$ est non cyclique car a 3 ss groupes d'ordre 2*

Prop 34. $s \wedge n = 1 \iff \bar{s}$ *générateur de* $\mathbb{Z}/n\mathbb{Z} \iff \bar{s} \in (\mathbb{Z}/n\mathbb{Z})^*$

Prop 35. *$Aut(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$. En particulier, $Aut(\mathbb{Z}/n\mathbb{Z})$ est un groupe abélien.*

TH 36 (Restes Chinois). $\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \iff a \wedge b = 1$

Ex 37. $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ *d'où* $Aut(\mathbb{Z}/6\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})^* \simeq (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^* \simeq \{1\}\ \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}$.

2) Quelques propriétés sur les groupes abéliens finis

Prop 38. *G abélien* $\iff G = Z(G)$

Prop 39. *Les groupes d'ordre p premier, sont abéliens.*

Prop 40. *Les groupes d'ordre p^2 (p premier) sont abéliens.*

Rqe 41. *Faux pour p^3 : ex H_8*

Prop 42. *G abélien $\Rightarrow$ tout sous-groupe de G est distingué.*

Ex 43. *H_8 est non abélien.*

3) Théorème de structure

Def 44. *L'exposant de G est le plus petit n tel que $\forall g \in G \quad g^n = e$.*

Lemme 45.

$$i : \begin{array}{ccl} G & \to & \hat{\hat{G}} \\ g & \mapsto & \chi : \begin{array}{ccc} G & \to & \mathbb{C} \\ g & \mapsto & \chi(g) \end{array} \end{array}$$ *est un isomorphisme de groupes*

Lemme 46. *G et $\hat{\hat{G}}$ ont même exposant*

TH 47. *Si G abélien fini alors $\exists r \in \mathbb{N}$ et $N_1, N_2, ..., N_r \in \mathbb{Z}$ où N_1 est l'exposant de G et $N_{i+1}|N_i$ tel que $G \simeq \prod_i \mathbb{Z}/N_i\mathbb{Z}$. De plus, la décomposition est uniques.*

App 48. $\mathbb{Z}/24\mathbb{Z}$

III/ GROUPES NON ABELIENS FINIS

1) Groupes de Sylow

Def 49. *Si $|G| = p^\alpha m$ avec p premier $p|n$ et $p \nmid m$, on appelle p-sous groupe de Sylow de G un sous-groupe P de cardinal p^α.*

Rqe 50. *P est un p-groupe et $[G : P] \wedge p = 1$.*

Lemme 51. *Soit $H \leqslant G$ et S un p-sylow de G. Alors $\exists a \in G \quad aSa^{-1} \cap H$ est un p-Sylow de H.*

Prop 52. *$P = \{A = (a_{ij}) : a_{ij} = 0$ si $i > j$ et $a_{ii} = 1\}$ est un p-Sylow de $\mathbb{F}_p$.*

TH 53 (Sylow). *Soit G un groupe, de cardinal $|G| = p^\alpha m$ avec $p \nmid m$.*

(1) *G contient au moins un p-Sylow.*

(2) *Les p-Sylow sont conjugués (et donc leur nombre k divise n).*

(3) *On a $k \equiv 1[p]$ (donc $k|m$).*

Cor 54. *Soit S un p-Sylow de G :*
$S \rhd G \iff$ *S est l'unique p-Sylow de G* $\iff k = 1$

App 55. *Un groupe d'ordre 63 n'est pas simple (i.e, a des sous groupes distingués non triviaux)*

Ex 56. *Il existe un unique groupe d'ordre 15 à isomorphisme près.*

2) Groupes symétrique et alterné

Def 57. *$\forall n \in \mathbb{N}^*$ on note $\mathfrak{S}_n$ le groupe des permutations (appelé groupe symétrique) de $\{1, ..., n\}$ muni de la loi de composition.*

Rqe 58. $|\mathfrak{S}_n| = n!$

Def 59. *On appelle transposition, notée $\tau_{i,j} = (ij)$, la permutation permutant les éléments i et j.*

TH 60. *Tout élément de $\mathfrak{S}_n$ se décompose en produit de transpositions.*

Def 61. *Si $\sigma \in \mathfrak{S}_n$, et $a \in \{1, ..., n\}$, on définit l'orbite de a suivant σ l'ensemble $\mathcal{O}_\sigma(a) = \{\sigma^k(a), k \in \mathbb{Z}\}$.*

Def 62. *On dit que $\sigma \in \mathfrak{S}_n$ est un cycle si, parmi les $\mathcal{O}_\sigma(a)$, il n'existe qu'une seule orbite non réduite à un élément. Autrement dit, si $\exists p \geqslant 2$ et $a \in \{1, ..., n\}$ tels que $\mathcal{O}_\sigma(a) = \{a, \sigma(a), ..., \sigma^{p-1}(a)\}$ et $\forall x \notin \mathcal{O}_\sigma(a) \quad \sigma(x) = x$.*

Ex 63. – *Une transposition est un cycle de longueur 2*

– *Dans* $\mathfrak{S}_5$, $\sigma = (135) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$ *est un cycle de support* $\{1,3,5\}$

Rqe 64. *Des cycles à supports disjoints commutent.*

TH 65. *Toute permutation non triviale se décompose, de manière unique à l'ordre près, en produit de cycles à support deux à deux disjoints.*

Ex 66. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ *de* $\mathfrak{S}_4$ *n'est pas un cycle car* $\sigma = (12)(34)$

Prop 67. *Si* $\gamma = (a_1 ... a_p) \in \mathfrak{S}_n$ *est un cycle d'ordre* p *et si* $\sigma \in \mathfrak{S}_n$, *on a :* $\sigma\gamma\sigma^{-1} = (\sigma(a_1)...\sigma(a_p))$

Def 68. *La signature est le morphisme* $\varepsilon : \mathfrak{S}_n \to \{-1,1\}$ *défini par* $\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j)-\sigma(i)}{j-i}$

Def 69. *On définit le groupe alterné* $\mathfrak{A}_n$ *comme le noyau du morphisme* ε.

Rqe 70. $\mathfrak{A}_n \lhd S_n$ *avec* $|\mathfrak{A}_n| = n!/2$.

Prop 71. $\mathfrak{A}_n$ *est engendré par les 3-cycles.*

IV/ APPLICATIONS

1) Groupes d'ordre pq et p^2q

Def 72. *Un groupe est simple s'il ne possède pas de sous-groupes distingués non triviaux.*

Prop 73. *Si* $|G| = pq$ $p<q$ *premier et* $p \nmid q-1$, *alors* $G \simeq \mathbb{Z}/pq\mathbb{Z}$

Prop 74. *Si* $|G| = pq$ $p<q$ *premiers alors* G *n'est pas simple*

Prop 75. *Si* $|G| = p^2q$ $p<q$ *premiers alors* G *n'est pas simple*

Prop 76. *Si* $|G| = p^2q$ $p<q$ *premiers* $q \not\equiv 1[p]$ *et* $q \nmid p^2-1$ *alors* G *abélien*

App 77. *Si* $|G| = 15$ *alors* $G \simeq \mathbb{Z}/15\mathbb{Z}$.

2) Représentation des groupes finis

Def 78. *Soit* $V \simeq \mathbb{C}^n$. *Une représentation de* G *dans* $GL(V)$ *est un morphisme* $\rho : G \to GL(V)$.

Def 79. *Le caractère* χ *d'une représentation* ρ *est défini par* $\chi : G \to \mathbb{C}$, $s \mapsto tr(\rho(s))$.

Def 80. $\mathbb{C}[G] = \{f : G \to \mathbb{C}\}$.

Def/Prop 81. *On définit un produit scalaire* $<.,.>$ *sur* $\mathbb{C}[G]$ *par* $<\varphi,\psi> = \frac{1}{|G|}\sum_{s\in G} \varphi(s)\overline{\psi(s)}$

Def 82. *Un caractère irréductible est le caractère d'une représentation dont les seuls sous-espaces G-invariants sont* $\{0\}$ *et* G.

Prop 83. $<\chi,\chi> = 1 \iff \chi$ *irréductible*

Prop 84. *Les caractères irréductibles forment une base de* $H = \{f \in \mathbb{C}[G] : f \text{ est centrale}\}$.

Prop 85. *Le nombre de représentations irréductibles est égal au nombre de classes de conjugaison de* G.

Lemme 86. $Isom(T) \simeq \mathfrak{S}_4$

TH 87. *Table de caractères de* $\mathfrak{S}_4$.

3) Classification des groupes d'ordre 60

Def 88. *Le groupe dérivé de* G *est défini par* $D(G) = < xyx^{-1}y^{-1} : x,y \in G >$.

Prop 89. *Un groupe abélien est simple ssi il est d'ordre premier*

TH 90. $\mathfrak{A}_n$ *est simple pour* $n \geqslant 5$

Cor 91. $D(\mathfrak{A}_n) = \mathfrak{A}_n$ *pour* $n \geqslant 5$ *et* $D(\mathfrak{S}_n) = \mathfrak{A}_n$ *pour* $n \geqslant 2$.

Prop 92. *Tout groupe simple d'ordre 60 est isomorphe à* A_5

4) Automorphismes de $\mathfrak{S}_n$

Def 93. *Soit* $a \in G$. *On appelle automorphisme intérieur associé à a le morphisme de groupe* $i_a : G \to G$, $g \mapsto gag^{-1}$.

Prop 94. *Soit* $\varphi \in Aut(\mathfrak{S}_n)$. *Si* φ *transforme transposition en transposition, alors* φ *est intérieur.*

Lemme 95. *Soit* $\varphi \in \mathfrak{S}_n$. *On suppose* $n = k_1 + k_2 + ... + k_n$ *cycles disjoints,* k_1 *cycles d'ordre 1,* k_2 *cycles d'ordres 2, ...*k_n *cycles d'ordre n. Alors si* $c(\sigma)$ *est le centralisateur de* σ, *on a :* $|c(\sigma)| = \prod_{i=1}^{n} k_i! i^{k_i}$.

TH 96. $\forall n \neq 6$ $\quad Aut(\mathfrak{S}_n) = Int(\mathfrak{S}_n)$.

Prop 97. $Aut(\mathfrak{S}_6) \neq Int(\mathfrak{S}_6)$.

RECASAGES : 101,104,105,108

Automorphismes de $\mathfrak{S}_n$

$\boxed{\text{THÉORÈME : Si } n \neq 6,\ \mathcal{A}ut(\mathfrak{S}_n) = \mathcal{I}nt(\mathfrak{S}_n)}$

Proposition 1 : Soit $\varphi \in \mathfrak{S}_n$, si φ transforme les transpositions en transpositions alors φ est intérieur.
On sait que $\mathfrak{S}_n$ est engendré par les transpositions . On a même que $\mathfrak{S}_n$ est engendré par les transpositions de la forme $\tau_i = (1i)$ pour $i \geqslant 2$. *En effet, pour $i, j \in [\![1, n]\!]$, $(ij) = (1j)(1i)(1j)$.*
Comme $\varphi \in \mathcal{A}ut(\mathfrak{S}_n)$, $\varphi(\tau_i)$ est une transposition (*envoie générateur sur générateur*). De plus, si $i \neq j$, τ_i et τ_j ne commutent pas car ne sont pas à supports disjoints, donc $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ne commutent pas non plus.
Si on pose $\varphi(\tau_2) = (\alpha_1\alpha_2)$, on peut supposer quitte à renuméroter que $\varphi(\tau_3) = (\alpha_1\alpha_3)$. *En effet, si on suppose $\varphi(\tau_3) = (\alpha_2\alpha_r)$, on renumérote α_2 en α_1 et α_r en α_3.*
Ainsi, pour tout $i \geqslant 2$, on peut écrire $\varphi(\tau_i) = (\alpha_1\alpha_i), \{\alpha_1, ..., \alpha_n\} = \{1, ..., n\}$. En effet, s'il existait $i \in [\![2, n]\!]$ tel que $\varphi(\tau_i) \neq (\alpha_1\alpha_i)$, par exemple $\varphi(\tau_i) = (\alpha_2\alpha_3)$, on aurait $(\alpha_1\alpha_2)(\alpha_1\alpha_3)(\alpha_2\alpha_3) = (\alpha_1\alpha_3)$ et donc par φ^{-1}, cela donnerait $(12)(13)(1i) = (13)$ ce qui est faux car $(12)(13)(1i) = (i321)$. De plus, les α_i sont distincts sinon φ ne serait pas injective. *(En effet, supposons $\alpha_i = \alpha_j$ avec $i \neq j$. $\varphi(\tau_i) = (\alpha_1\alpha_i) = (\alpha_1\alpha_j) = \varphi(\tau_j)$, et donc en appliquant φ^{-1}, on obtient $\tau_i = \tau_j$ avec $i \neq j$.)*
Posons $\alpha = \begin{pmatrix} 1 & 2 & ... & n \\ \alpha_1 & \alpha_2 & ... & \alpha_n \end{pmatrix} \in \mathfrak{S}_n$. On a :
$\forall i \geqslant 2\ i_\alpha(\tau_i) = \alpha\tau_i\alpha^{-1} = (\alpha(1)\alpha(i)) = (\alpha_1\alpha_i) = \varphi(\tau_i)$, donc i_α (automorphisme intérieur) coïncide avec φ sur les τ_i qui engendrent $\mathfrak{S}_n$ donc coïncide avec φ partout : d'où $\varphi = i_\alpha$.

Lemme 2 : Soit $s \in \mathfrak{S}_n$, on suppose que $n = k_1 + 2k_2 + ... + nk_n$ avec $k_i \in \mathbb{N}$ et que s est le produit de $k_1 + ... + k_n$ cycles disjoints (k_1 1-cycles, k_2 2-cycles,..., k_n n-cycles). Alors si $c(s)$ est le centralisateur de s, on a : $|c(s)| = \prod_{i=1}^{n} k_i! i^{k_i}$
On rappelle que le centralisateur d'un élément $x \in \mathfrak{S}_n$ est l'ensemble $c(x) = \{\sigma \in \mathfrak{S}_n : \sigma.x = x.\sigma\} = \{\sigma \in \mathfrak{S}_n : \sigma.x\sigma^{-1} = x\}$.
s est un produit de cycles disjoints. Étudions le centralisateur d'un i-cycle, puis d'un produit de k_i i-cycles, puis de s.

- Un i-cycle peut s'écrire de i façons différentes. Ainsi, pour un i-cycle, il y a i éléments dans son centralisateur. (*En effet, si γ est un i-cycle $(a_1...a_n)$, on a $c(\gamma) = \{\sigma \in \mathfrak{S}_n : \sigma\gamma\sigma^{-1} = \gamma\} = \{\sigma \in \mathfrak{S}_n : \sigma\gamma\sigma^{-1} = (\sigma(a_1)...\sigma(a_i)) = (a_1...a_i)\}$*)
- Pour trouver le cardinal du centralisateur d'un produit de k_i i-cycles, il faut choisir tout d'abord un i-cycle : on a k_i choix de i-cycles (qui sont disjoints) et i éléments dans son centralisateur : d'où k_ii choix. On choisit un deuxième i-cycle : on a $k_i - 1$ choix avec toujours i éléments dans le centralisateur... On raisonne comme cela jusqu'à la fin et on

trouve que le centralisateur d'un produit de k_i i-cycles contient $k_i!i^{k_i}$ éléments.

- Ainsi $|c(s)| = \prod_{i=1}^{n} k_i!i^{k_i}$ (car les cycles sont à supports disjoints et pour obtenir un élément dans le centralisateur de $s = \prod \sigma_i$, il suffit de prendre n'importe quelle combinaison d'éléments dans les centralisateurs des σ_i.

Lemme 3 : Si $\varphi \in Aut(\mathfrak{S}_n)$ et τ une transposition alors $c(\varphi(\tau)) = \varphi(c(\tau))$

- Montrons que $\varphi(c(\tau)) \subset c(\varphi(\tau)$, i.e, $c(\tau) \subset \varphi^{-1}(c(\varphi(\tau)))$. Soit $\sigma \in \mathfrak{S}_n$. Alors $\sigma\tau = \tau\sigma$. De plus, il existe σ_0 et $\tau_0 \in \mathfrak{S}_n$ tels que $\sigma = \varphi^{-1}(\sigma_0)$ et $\tau = \varphi^{-1}(\tau_0)$. Ainsi on a $\sigma_0\tau_0 = \tau_0\sigma_0$ (car $\sigma\tau = \tau\sigma \iff \varphi^{-1}(\sigma\tau) = \varphi^{-1}(\tau\sigma) \iff \varphi^{-1}(\sigma)\varphi^{-1}(\tau) = \varphi^{-1}(\tau)\varphi^{-1}(\sigma) \iff \sigma_0\tau_0 = \tau_0\sigma_0$) i.e $\sigma_0 \in c(\tau_0)$. Donc $\sigma_0 = \varphi(\sigma) \in c(\tau_0) = c(\varphi(\tau))$ d'où $\sigma \in \varphi^{-1}(c(\varphi(\tau)))$.
- Montrons que $c(\varphi(\tau)) \subset \varphi(c(\tau))$. Soit $\sigma \in c(\varphi(\tau))$. Alors $\sigma\varphi(\tau) = \varphi(\tau)\sigma$. de plus, il existe $\sigma_0 \in \mathfrak{S}_n$ tel que $\sigma)\varphi(\sigma_0)$ d'où $\varphi(\sigma_0\tau) = \varphi(\tau\sigma_0)$, i.e, $\sigma_0\tau = \tau\sigma_0$ i.e $\sigma_0 \in c(\tau)$. Donc $c(\varphi(\tau)) \subset \varphi(c(\tau))$.

DÉMONSTRATION THÉORÈME :

Soit $\varphi \in \mathfrak{S}_n$. Si τ est une transposition, alors $\varphi(\tau)$ est un produit de k transpositions disjointes.
Montrons que k=1.
Par le lemme 3, on a $|c(\varphi(\tau))| = |\varphi(c(\tau))| = |c(\tau)|$. Or par le lemme 2, on a que $|c(\tau)| = 2(n-2)!$. *(En effet, τ étant une transposition est un 2-cycle et donc peut être vu comme un produit de $(n-2)$ 1-cycle et d'un 2-cycle (à supports disjoints). Ensuite, on applique la formule du lemme 2*). De même, comme $\varphi(\tau)$ est un produit de k transpositions à supports disjoints, on obtient $|c(\varphi(\tau))| = 2^k k!(n-2k)$. Ainsi , on établit l'égalité suivante :

$$\begin{aligned}
2(n-2)! = 2^k k!(n-2)! \iff \frac{(n-2)!}{2^{k-1}k!(n-2k)!} = 1 \underset{n-2k=n-2-(k-2)}{\overset{\textit{En remarquant que}}{\iff}} \frac{\binom{n-2}{2k-2}(2k-2)!}{k!2^{k-1}} = 1 \\
\iff \frac{\binom{n-2}{2k-2}(2k-2)(2k-4)...2 \times (2k-3)(2k-5)...3}{k!2^{k-1}} = 1 \\
\iff \frac{\binom{n-2}{2k-2}2^{k-1}(k-1)(k-2)... \times (2k-3)(2k-5)...3}{k!2^{k-1}} = 1 \\
\iff \frac{\binom{n-2}{2k-2}(2k-3)(2k-5)...3}{k} = 1
\end{aligned}$$

Si $2k-3 > k$ l'équation ne pourra jamais être vraie. Donc notre seule chance pour que l'équation soit vraie sous conditions est que $2k-3 \leqslant k$. Or $2k-3 > k \iff k > 3$. Donc on cherche quelles conditions amène l'équation suivant les valeurs de $k \leqslant 3$.

- si $k = 1$: $\binom{n-2}{0} = 1$ OK
- si $k = 2$: $\frac{\binom{n-2}{2}}{2} = 1 \iff n^2 - 5n + 2 = 0$ Or $\Delta = 17$ donc les solutions de cette équation du second degré ne sont pas entières : ABSURDE
- si $k = 3$: $\frac{(n-2)!}{4!(n-6)!} = 1 \iff (n-2)(n-3)(n-4)(n-4) = 24 \iff n = 6$. Donc OK si k=3 et n=6

CONCLUSION : Donc, si $n \neq 6$, φ envoie une transposition sur une transposition (car k=1) donc d'après la proposition, φ est intérieur.

Classification des groupes d'ordre pq

Combes, *Algèbre et Géométrie*, page 94

Théorème :
Soit G un groupe fini d'ordre pq où $p < q$ sont des nombres premiers.

1. Si q n'est pas congru à 1 modulo p, alors G est cyclique, isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.
2. Si q est congru à 1 modulo p, à isomorphisme près G a deux structures possibles : ou bien G est abélien, cyclique, isomorphe à $\mathbb{Z}/pq\mathbb{Z}$, ou bien G n'est pas commutatif et alors G est isomorphe à $(\mathbb{Z}/q\mathbb{Z}) \rtimes_\theta (\mathbb{Z}/p\mathbb{Z})$ où $\theta \in Hom(\mathbb{Z}/p\mathbb{Z}, Aut(\mathbb{Z}/q\mathbb{Z}))$ est tel que $\theta(\bar{1}) = \gamma$ est d'ordre p dans $Aut(\mathbb{Z}/q\mathbb{Z})$.

D'après les théorèmes de Sylow, il existe dans G un sous-groupe H d'ordre q et un sous-groupe K d'ordre p. Le nombre n_q de q-sous-groupes de Sylow est congru à 1 modulo q et divise p. Comme on a $p < q$, cela nécessite $n_q = 1$ donc H est distingué dans G.

D'après le théorème de Lagrange, $|H \cap K|$ divise $|H| = q$ et $|K| = p$. On a donc $|H \cap K| = 1$ et $H \cap K = \{e\}$. Puisque $H \lhd K$, le théorème montre que HK est un sous-groupe de G et que $HK/H \simeq K/(H \cap K) = K$. On en déduit que $|HK| = |H||K| = pq = |G|$ et donc que $HK = G$. G est donc un produit semi-direct de H et de K, isomorphe à $(\mathbb{Z}/q\mathbb{Z}) \rtimes_\theta (\mathbb{Z}/p\mathbb{Z})$, où θ ets un homomorphisme de $\mathbb{Z}/p\mathbb{Z}$ dans $Aut(\mathbb{Z}/q\mathbb{Z})$.

Les p-sous-groupes de Sylow, sont les conjugués de K dans G. Leur nombre n_p est congru à 1 modulo p et divise q. Donc $n_p = 1$ ou $n_p = q$. Si $n_p = q$, alors q est congru à 1 modulo p d'après le théorème de Sylow.

1. Supposons que q ne soit pas congru à 1 modulo p. D'après ce qui précède, $n_p = 1$ et donc K est distingué dans G. Le produit semi-direct précédent est alors un produit direct $H \times K$. Comme p et q sont premiers, H et K sont cycliques. Leurs ordres étant premiers entre eux, G est cyclique isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.
2. Supposons q congru à 1 modulo p. L'ordre de l'image de $\theta : \mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/q\mathbb{Z})$ divise l'ordre p de $\mathbb{Z}/p\mathbb{Z}$ et vaut p ou 1 (dans ce dernier cas, l'action est triviale.

   Si θ est l'action triviale, alors le produit semi-direct $(\mathbb{Z}/q\mathbb{Z}) \rtimes_\theta (\mathbb{Z}/p\mathbb{Z})$ est un produit direct. Comme en 1., G est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.

   Supposons maintenant que θ ne soit pas l'action triviale. On a que $Aut(\mathbb{Z}/q\mathbb{Z})$ est cylique, d'ordre $\varphi(q) = q - 1$ (ici divisible par p). Il existe dans $Aut(\mathbb{Z}/q\mathbb{Z})$ un unique sous-groupe Γ d'ordre p. On a donc $\Gamma = Im(\theta)$. Puisque $\mathbb{Z}/p\mathbb{Z}$ et $\Gamma = Im(\theta)$ ont le même ordre, θ est un isomorphisme de $\mathbb{Z}/p\mathbb{Z}$ sur Γ, déterminé par le choix de $\theta(\bar{1}) = \gamma$ parmi les $p-1$ générateurs de Γ. Vérifions que les $p-1$ choix possibles de $\theta(\bar{1})$ conduisent à des produits semi-directs isomorphes. Soit θ' un autre isomorphisme de $\mathbb{Z}/p\mathbb{Z}$ sur Γ. Alors $\alpha = \theta'^{-1} \circ \theta$ est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$. Il existe alors un isomorphisme f de G_θ sur $G_{\theta'}$.

Application : si $p = 2$ et si $q > 2$ est premier, un groupe G d'ordre $2q$ est soit isomorphe à $\mathbb{Z}/2q\mathbb{Z}$, soit isomorphe au groupe diédral D_p.

En effet, d'après la proposition, G n'a que deux structures possibles : l'une abélienne et $G \simeq \mathbb{Z}/2q\mathbb{Z}$, l'autre non abélienne. Comme D_q est d'ordre $2q$ et non abélien, il représente l'autre alternative.