4. SOUS-GROUPES DISTINGUÉS, GROUPES SYMÉTRIQUES ET ACTIONS DE GROUPES
(Corrigé partiel)

Exerice 2. 1. Soit G un groupe et soient H, K deux sous-groupes distingués de G tels que $\mathrm{H}\cap\mathrm{K}=\{e\}$.

Quels que soient les éléments $h\in\mathrm{H}$ et $k\in\mathrm{K}$, $h^{-1}k^{-1}h\in\mathrm{K}$ puisque K est distingué et donc $h^{-1}k^{-1}hk\in\mathrm{K}$; on a de même $k^{-1}h^{-1}k\in\mathrm{H}$ et donc $h^{-1}k^{-1}hk\in\mathrm{H}$. Comme $\mathrm{H}\cap\mathrm{K}=\{e\}$, $h^{-1}k^{-1}hk=e$ et donc $hk=kh$.

Considérons l'application $f:\mathrm{H}\times\mathrm{K}\to\mathrm{G},\ (h,k)\mapsto hk$. Il s'agit d'un homomorphisme de groupes puisque

$$f((h,k)(h',k'))=f(hh',kk')=(hh')(kk')=hh'kk'=hkh'k'=f(h,k)f(h',k')$$

en vertu de ce qui précède. Si $(h,k)\in\mathrm{H}\times\mathrm{K}$ est contenu dans le noyau de f, $hk=e$; on a alors $h=k^{-1}\in\mathrm{H}\cap\mathrm{K}$ et donc $h=k=e$, ce qui prouve que f est injectif. L'image de f étant le sous-groupe HK de G constitué des éléments de la forme hk, $h\in\mathrm{H}$ et $k\in\mathrm{K}$, nous avons démontré que ce sous-groupe de G est isomorphe au groupe produit $\mathrm{H}\times\mathrm{K}$.

1bis. Considérons plus généralement un groupe G et des sous-groupes distingués $\mathrm{H}_1,\dots,\mathrm{H}_n$ de G. Quels que soient les éléments i et j de $\{1,\dots,n\}$, $\mathrm{H}_i\mathrm{H}_j=\mathrm{H}_j\mathrm{H}_i$ est un sous-groupe distingué de G : en effet, pour tous $h_i\in\mathrm{H}_i$, $h_j\in\mathrm{H}_j$ et $g\in\mathrm{G}$,

$$h_ih_j=h_ih_jh_i^{-1}h_i=(h_ih_jh_i^{-1})h_i\in\mathrm{H}_j\mathrm{H}_i\quad\text{et}\quad g(h_ih_j)g^{-1}=gh_ig^{-1}gh_jg^{-1}\in\mathrm{H}_i\mathrm{H}_j.$$

En raisonnant par récurrence sur n, on en déduit que, pour tout $i\in\{1,\dots,n\}$,

$$\widehat{\mathrm{H}}_i=\mathrm{H}_1\dots\mathrm{H}_{i-1}\mathrm{H}_{i+1}\dots\mathrm{H}_n$$

est un sous-groupe distingué de G.

Supposons maintenant que l'on ait $\mathrm{H}_i\cap\widehat{\mathrm{H}}_i=\{e\}$ pour tout $i\in\{1,\dots,n\}$. Nous allons vérifier que, sous cette hypothèse, le sous-groupe $\mathrm{H}_1\mathrm{H}_2\dots\mathrm{H}_n$ de G est isomorphe au groupe produit $\mathrm{H}_1\times\mathrm{H}_2\times\dots\times\mathrm{H}_n$.

Observons tout d'abord que l'on a $h_ih_j=h_jh_i$ pour tous $h_i\in\mathrm{H}_i$ et $h_j\in\mathrm{H}_j$ si $i\neq j$ puisque

$$h_j^{-1}h_i^{-1}h_jh_i\in\mathrm{H}_i\cap\mathrm{H}_j\subset\mathrm{H}_i\cap\widehat{\mathrm{H}}_i=\{e\}.$$

Il en découle que l'application

$$f:\mathrm{H}_1\times\dots\times\mathrm{H}_n\to\mathrm{G},\ \ (h_1,\dots,h_n)\mapsto h_1\dots h_n$$

est un homomorphisme de groupes. Si $(h_1,\dots,h_n)$ appartient au noyau de f, alors $h_1\dots h_n=e$ et donc, pour tout i, h_i est le produit des h_j^{-1} avec $1\leq j\leq n$ et $j\neq i$; on a ainsi $h_i\in\mathrm{H}_i\cap\widehat{\mathrm{H}}_i=\{e\}$ pour tout i et donc $h_1=\dots=h_n=e$.

L'homomorphisme f est par conséquent injectif, et il réalise ainsi un isomorphisme du groupe produit $\mathrm{H}_1\times\dots\times\mathrm{H}_n$ sur le sous-groupe $\mathrm{H}_1\dots\mathrm{H}_n$ de G.

2. Soit maintenant G un groupe abélien fini d'ordre n. Quel que soit le nombre premier p, on désigne par $\mathrm{G}(p)$ l'ensemble des éléments g de G dont l'ordre est une puissance de p ; il s'agit d'un sous-groupe de G car

$$\mathrm{ord}(gh)|\mathrm{ord}(g)\mathrm{ord}(h)$$

en vertu de la commutativité de G, et $\mathrm{ord}(gh)$ est donc une puissance de p si tel est le cas de $\mathrm{ord}(g)$ et $\mathrm{ord}(h)$. Notons que $\mathrm{G}(p)=\{e\}$ si p ne divise pas l'ordre n de G puisque $\mathrm{ord}(g)|n$ pour tout $g\in\mathrm{G}$.

– Quel que soit le nombre premier p divisant n, $\mathrm{G}(p)\cap(\mathrm{G}(q_1)\dots\mathrm{G}(q_r))=\{e\}$ si $q_1,\dots,q_r$ sont les facteurs premiers de n distincts de p : en effet, l'ordre d d'un élément g de $\mathrm{G}(q_1)\dots\mathrm{G}(q_r)$ est un produit de puissances de $q_1,\dots,q_r$ et ce ne peut être simultanément une puissance de p que si $d=1$, c'est-à-dire $g=e$. Comme tout sous-groupe d'un groupe abélien est distingué, nous sommes en mesure d'appliquer le résultat de la question précédente et nous en déduisons que l'homomorphisme

$$i_{\mathrm{G}}:\prod_{p|n}\mathrm{G}(p)\to\mathrm{G},\ \ (g_p)_{p|n}\mapsto\prod_{p|n}g_p$$

est un isomorphisme sur un sous-groupe de G. En fait, l'homomorphisme i_{G} est surjectif : écrivons en effet n sous la forme $n=\prod_{p|n}p^{v_p(n)}$ et posons $m_p=n/p^{v_p(n)}$ pour tout diviseur premier p de n. Les nombres entier m_p sont premiers entre eux dans leur ensemble et l'on dispose par conséquent une relation de Bézout

$$1=\sum_{p|n}u_pm_p.$$

Soit alors $g \in \mathrm{G}$ et posons $g_p = g^{u_p m_p}$. Comme

$$g_p{}^{p^{v_p(n)}} = g_p{}^{nu_p} = (g^n)^{u_p} = e$$

pour tout diviseur premier p de n, l'ordre de g_p est une puissance de p et donc $g_p \in \mathrm{G}(p)$. Puisque

$$g = g^{\Sigma_{p|n} u_p m_p} = \prod_{p|n} g^{u_p m_p} = i_{\mathrm{G}}((g^{u_p m_p})_{p|n}),$$

cela montre que i_{G} est surjectif. Nous avons ainsi démontré que le groupe G est isomorphe au produit direct de ses sous-groupes $\mathrm{G}(p)$, $p|n$.

– Considérons finalement deux groupes abéliens finis G et H d'ordre n. Quels que soient l'homomorphisme de groupes $f : \mathrm{G} \to \mathrm{H}$ et l'élément g de G, l'ordre de $f(g)$ dans H divise l'ordre de g dans G et donc $f(\mathrm{G}(p)) \subset \mathrm{H}(p)$ pour tout nombre premier p. Notant f_p la restriction de f au sous-groupe $\mathrm{G}(p)$, cela montre que f_p est un homomorphisme du groupe $\mathrm{G}(p)$ dans le groupe $\mathrm{H}(p)$. Réciproquement, si l'on dispose pour tout nombre premier p d'un homomorphisme de groupes $\varphi_p : \mathrm{G}(p) \to \mathrm{H}(p)$, on définit un homomorphisme de groupes $\varphi : \prod_{p|n} \mathrm{G}(p) \to \prod_{p|n} \mathrm{H}(p)$ en posant $\varphi((g_p)_{p\in|n}) = (\varphi_p(g_p))_{p|n}$ et on en déduit un homomorphisme de groupes $f : \mathrm{G} \to \mathrm{H}$ en posant $f = i_{\mathrm{H}} \circ \varphi \circ i_{\mathrm{G}}^{-1}$. Cette discussion prouve que l'application $f \mapsto (f_p)_{p|n}$ réalise une bijection entre l'ensemble des homomorphismes du groupe G dans le groupe H et l'ensemble des familles $(\varphi_p)_{p|n}$ d'homomorphismes des groupes $\mathrm{G}(p)$ dans les groupes $\mathrm{H}(p)$. Les isomorphismes de G sur H correspondent aux familles $(\varphi_p)_{p\in\mathscr{P}}$ constituées d'isomorphismes de $\mathrm{G}(p)$ sur $\mathrm{H}(p)$, de sorte que les groupes abéliens G et H sont isomorphes si et seulement si, pour tout nombre premier p divisant leur ordre, les groupes $\mathrm{G}(p)$ et $\mathrm{H}(p)$ sont isomorphes.

Remarque – Le résultat que l'on vient d'établir à la question 2 constitue la première étape en vue de la classification des groupes abéliens finis : pour comprendre un groupe abélien fini, il suffit de comprendre toutes ses composantes p-primaires, qui sont des groupes plus élémentaires. La seconde étape fait l'objet de l'exercice 2 de la fiche 5.

Exercice 3. Soit G un groupe fini, soit p le plus petit facteur premier de $|\mathrm{G}|$ et soit H un sous-groupe de G d'indice p. Nous allons démontrer que H est nécessairement un sous-groupe distingué de G.

1. Considérons l'action suivante de G sur l'ensemble G/H des classes à gauche modulo H :

$$\mathrm{G} \times (\mathrm{G}/\mathrm{H}) \to \mathrm{G}/\mathrm{H}, \quad (g, a\mathrm{H}) \mapsto (ga)\mathrm{H}.$$

(*Attention, il y a une erreur dans l'énoncé !*)

Soit K un sous-groupe de G et soit aH un élément de G/H. Le stabilisateur de aH dans K est le sous-groupe constitué des éléments k tels que $ka\mathrm{H} = a\mathrm{H}$, c'est-à-dire tels que $ka \in a\mathrm{H}$; c'est donc le sous-groupe $\mathrm{K}_a = \mathrm{K} \cap a\mathrm{H}a^{-1}$. L'orbite O_a de aH sous K est l'ensemble des classes kaH, $k \in \mathrm{K}$; c'est un sous-ensemble de G/H dont le cardinal est l'indice de K_a dans K :

$$|\mathrm{O}_a| = (\mathrm{K} : \mathrm{K}_a).$$

Puisque l'ordre de K divise l'ordre de G en vertu du théorème de Lagrange, nous en déduisons que le cardinal de O_a est un diviseur de l'ordre de G, compris entre 1 et $|\mathrm{G}/\mathrm{H}| = (\mathrm{G} : \mathrm{H}) = p$. Vu l'hypothèse initiale, cela conduit à l'alternative suivante :

– soit $|\mathrm{O}_a| = p = |\mathrm{G}/\mathrm{H}|$, auquel cas $\mathrm{O}_a = \mathrm{G}/\mathrm{H}$;
– soit $|\mathrm{O}_a| = 1$, auquel cas $\mathrm{K}_a = \mathrm{K}$.

De deux choses l'une : s'il existe un élément $a \in \mathrm{G}/\mathrm{H}$ tel que O_a soit de cardinal p, alors $\mathrm{O}_a = \mathrm{G}/\mathrm{H}$ et l'action du groupe K sur G/H est transitive ; sinon, $|\mathrm{O}_a| = 1$ pour toute classe $a\mathrm{H} \in \mathrm{G}/\mathrm{H}$ et le groupe K agit sur G/H en fixant chaque élément (action triviale).

2. Le sous-groupe H de G ne peut certainement pas opérer transitivement sur G/H : en effet, H fixe la classe $e\mathrm{H} = \mathrm{H}$ de l'élément neutre dans G/H et il y a donc au moins deux orbites distinctes sous H dans G/H. Vu la première question, nous en concluons que le groupe H opère sur G/H en fixant chaque élément : pour tous $h \in \mathrm{H}$ et $a \in \mathrm{G}$,

$$ha\mathrm{H} = a\mathrm{H}, \quad \text{c'est-à-dire} \quad a^{-1}ha \in \mathrm{H},$$

et H est donc un sous-groupe distingué de G.

Exercice 5. Soient $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$.

1. $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$, $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$, $\sigma^2\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix}$, $\sigma\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$.

2 & 4. La décomposition de σ en produit de cycles de supports disjoints est $\sigma = (1,2)(3,4,5)$; on a donc $\mathrm{ord}(\sigma) = \mathrm{ppcm}(2,3) = 6$.

La décomposition de τ est produit de cycles de supports disjoints est $\tau = (1,5)(2,3,4)$; on a donc $\mathrm{ord}(\tau) = \mathrm{ppcm}(2,3) = 6$.

La permutation $\sigma\tau$ est le cycle $(1,3,5,2,4)$; on a donc $\mathrm{ord}(\sigma\tau) = 5$.

3. Partons de $\tau = (1,5)(2,3,4)$. En conjuguant le cycle $(1,5)$ par la transposition échangeant 1 et 2, on obtient $(1,5) = (1,2)(2,5)(1,2)$ (voir la première question de l'exercice suivant), puis

$$(1,5) = (1,2)(2,3)(3,5)(2,3)(1,2) = (1,2)(2,3)(3,4)(4,5)(3,4)(2,3)(1,2).$$

On a d'autre part $(2,3)(2,3,4) = (3,4)$, donc $(2,3,4) = (2,3)(3,4)$, et finalement

$$\tau = (1,2)(2,3)(3,4)(4,5)(3,4)(2,3)(1,2)(2,3)(3,4).$$

Enfin, $(2,3) = (1,2)(1,3)(1,2)$ et $(3,4) = (1,3)(1,4)(1,3)$, donc

$$\tau = (1,5)(2,3)(3,4) = (1,5)(1,2)(1,3)(1,2)(1,3)(1,4)(1,3).$$

5. En vertu de la décomposition canonique des permutations σ et τ,

$$\sigma^{2008} = (1,2)^{2008}(3,4,5)^{2008} = (3,4,5) \quad \text{et} \quad \tau^{2008} = (1,5)^{2008}(2,3,4)^{2008} = (2,3,4)$$

car $2008 \equiv 0 \pmod 2$ et $2008 \equiv 1 \pmod 3$.

Exercice 6. 1. Soit $c = (a_1, \ldots, a_m)$ un cycle de longueur m dans $\mathfrak{S}_n$; rappelons que, par définition, c est la permutation de $\{1,\ldots,n\}$ égale à l'identité sur le complémentaire de $\{a_1,\ldots,a_m\}$ et telle que $c(a_1) = a_2, \ldots, c(a_{m-1}) = a_m, c(a_m) = a_1 0$.

Considérons une permutation σ dans $\mathfrak{S}_n$. Pour tout $i \in \{1,\ldots,m\}$,

$$\sigma c \sigma^{-1}(\sigma(a_i)) = \sigma(c(a_i)) = \begin{cases} \sigma(a_{i+1}) & \text{si } i \leq m-1 \\ \sigma(a_1) & \text{si } i = m \end{cases}.$$

D'autre part, pour tout élément k de $\{1,\ldots,n\}$ n'appartenant par à $\{\sigma(a_1),\ldots,\sigma(a_m)\}$, $\sigma^{-1}(k)$ n'appartient pas à $\{a_1,\ldots,a_m\}$, donc $c(\sigma^{-1}(k)) = \sigma^{-1}(k)$ et finalement $\sigma c \sigma^{-1}(k) = k$. Nous venons de vérifier que la permutation $\sigma c \sigma^{-1}$ est le cycle $(\sigma(a_1),\ldots,\sigma(a_m))$.

Nous allons maintenant vérifier que deux éléments de $\mathfrak{S}_n$ sont conjugués si et seulement si les longueurs des cycles intervenant dans leurs décompositions canoniques en produits de cycles de supports disjoints sont les mêmes (voir l'exercice suivant pour deux exemples explicites).

C'est une condition nécessaire. Soit $\tau \in \mathfrak{S}_n$ une permutation et soit $\tau = \prod_{i\in \mathrm{I}} c_i$ la décomposition de τ en un produit de cycles de supports disjoints. Quelle que soit la permutation $\sigma \in \mathfrak{S}_n$, $\sigma\tau\sigma^{-1} = \prod_{i\in\mathrm{I}} \sigma c_i \sigma^{-1}$ est une décomposition de τ en produit de cycles de supports disjoints en vertu de ce qui précède. Comme la décomposition d'une permutation en produit de cycles de supports disjoints est unique à l'ordre des facteurs près et comme les cycles c_i et $\sigma c_i \sigma^{-1}$ ont la même longueur, nous en déduisons que la condition est nécessaire.

C'est une condition suffisante. Considérons réciproquement deux permutations $\sigma_1, \sigma_2 \in \mathfrak{S}_n$ dont les décomposition en produit de cycles de supports disjoints s'écrivent sous la forme

$$\sigma_1 = \prod_{i\in\mathrm{I}} c_i^{(1)} \quad \text{et} \quad \prod_{i\in\mathrm{I}} c_i^{(2)}$$

avec longueur $\left(c_i^{(1)}\right) = \text{longueur}\left(c_i^{(2)}\right)$ pour tout $i \in \mathrm{I}$. Désignant respectivement par $\mathrm{E}_i^{(1)}$ et $\mathrm{E}_i^{(2)}$ les supports des cycles $c_i^{(1)}$ et $c_i^{(2)}$, on peut choisir pour tout $i \in \mathrm{I}$ une bijection τ_i de $\mathrm{E}_i^{(1)}$ sur $\mathrm{E}_i^{(2)}$ telle que

$$\tau_i c_i^{(1)} \tau_i^{-1} = c_i^{(2)};$$

en effet, si l'on écrit $c_i^{(1)} = (a_1^{(1)},\ldots,a_m^{(1)})$ et $c_i^{(2)} = (a_1^{(2)},\ldots,a_m^{(2)})$, il suffit de poser $\tau_i(a_k^{(1)}) = a_k^{(2)}$. Comme $\mathrm{E}_i^{(1)} \cap \mathrm{E}_j^{(1)} = \mathrm{E}_i^{(2)} \cap \mathrm{E}_j^{(2)} = \varnothing$ si $i \neq j$, il existe alors une unique bijection

$$\tau : \mathrm{E}^{(1)} = \bigcup_{i\in\mathrm{I}} \mathrm{E}_i^{(1)} \to \mathrm{E}^{(2)} = \bigcup_{i\in\mathrm{I}} \mathrm{E}_i^{(2)}$$

coïncidant avec τ_i sur $\mathrm{E}_i^{(1)}$ pour tout $i \in \mathrm{I}$. Enfin, les sous-ensembles $\mathrm{E}^{(1)}$ et $\mathrm{E}^{(2)}$ de $\{1,\dots,n\}$ ayant le même cardinal, on peut prolonger τ en une permutation de $\{1,\dots,n\}$ en choisissant n'importe quelle bijection de $\{1,\dots,n\} - \mathrm{E}^{(1)}$ sur $\{1,\dots,n\} - \mathrm{E}^{(2)}$. Par construction de τ, $\tau c_i^{(1)} \tau^{-1} = c_i^{(2)}$ pour tout $i \in \mathrm{I}$ et donc

$$\tau\sigma_1\tau^{-1} = \prod_{i\in\mathrm{I}} \tau c_i^{(1)} \tau^{-1} = \prod_{i\in\mathrm{I}} c_i^{(2)} = \sigma_2.$$

Nous avons ainsi vérifié que la condition est suffisante.

2. En vertu de la question précédente, il y a sept classes de conjugaison dans $\mathfrak{S}_5$:
– $\{1\}$,
– l'ensemble des transpositions,
– l'ensemble des cycles de longueur 3,
– l'ensemble des cycles de longueur 4,
– l'ensemble des cycles de longueur 5,
– l'ensemble des produits de deux transpositions de supports disjoints,
– l'ensemble des produits d'une transposition et d'un cycle de longueur 3 de supports disjoints.

Exercice 7. 1. Les décompositions canoniques de σ et σ' sont

$$\sigma = (1,5)(2,3,4)(6,7) \quad \text{et} \quad \sigma' = (1,2,5)(3,7)(4,6).$$

Puisque les longueurs des cycles figurant dans chacune de ces décompositions sont les mêmes – en l'occurence, deux cycles de longueur 2 et un cycle de longueur 3 – les permutations σ et σ' sont conjuguées. Définissons $\tau \in \mathfrak{S}_7$ par

$$\tau(1) = 3,\ \tau(5) = 7,\ \tau(6) = 4,\ \tau(7) = 6,\ \tau(2) = 1,\ \tau(3) = 2,\ \tau(4) = 5\,;$$

on a

$$\begin{aligned} \tau\sigma\tau^{-1} &= \tau(1,5)\tau^{-1}\tau(2,3,4)\tau^{-1}\tau(6,7)\tau^{-1} \\ &= (\tau(1),\tau(5))(\tau(2),\tau(3),\tau(4))(\tau(6),\tau(7)) \\ &= (3,7)(4,6)(1,2,5) = \sigma'. \end{aligned}$$

2. On a $\sigma = (1,2,6,7)(3,5,4)$ et $\sigma' = (1,3,4)(2,6)(5,7)$; comme les cycles apparaissant dans les décompositions canoniques des permutations σ et σ' n'ont pas les mêmes longueurs, ces permutations ne sont pas conjuguées.

Exercice 16. Soit G un groupe fini d'ordre n et soit p un nombre premier divisant n.

L'ensemble $\mathrm{X} = \{(x_1,\dots,x_p) \in \mathrm{G}^p \mid x_1\dots x_p = e\}$, où e est l'élément neutre de G, est de cardinal n^{p-1}. En effet, l'application

$$\mathrm{G}^{p-1} \to \mathrm{G}^p,\ \ (x_1,\dots,x_{p-1}) \mapsto \left(x_1,\dots,x_{p-1},(x_1\dots x_{p-1})^{-1}\right)$$

réalise une bijection entre G^{p-1} et X.

La permutation σ est d'ordre p ; en effet, $\sigma \neq \mathrm{id}$ et $\sigma^p = \mathrm{id}$, donc $\mathrm{ord}(\sigma) = p$.

La permutation σ fixe le point $(x_1,\dots,x_{p-1},x_p)$ de X si et seulement si

$$\sigma(x_1,\dots,x_{p-1},x_p) = (x_2,\dots,x_p,x_1) = (x_1,\dots,x_{p-1},x_p),$$

donc si et seulement si $x_1 = x_2 = \dots = x_{p-1} = x_p$. Par conséquent, l'application $\mathrm{G} \to \mathrm{G}^p,\ \ g \mapsto (g,g,\dots,g)$ induit une bijection entre le sous-ensemble $\{g \in \mathrm{G} \mid g^p = e\}$ de G et l'ensemble X^σ des points fixes de σ dans X. Observons que X^σ est non vide puisqu'il contient l'élément $(e,e,\dots,e)$.

L'action du groupe $\mathbb{Z}$ sur X définie par $n.x = \sigma^n(x)$ induit une action du groupe cyclique $\mathbb{Z}/p\mathbb{Z}$ puisque σ est d'ordre p. Si un point x de X n'est pas fixé par σ, son stabilisateur est un sous-groupe strict de $\mathbb{Z}/p\mathbb{Z}$ (c'est-à-dire distinct du groupe $\mathbb{Z}/p\mathbb{Z}$) et donc est réduit à l'élément neutre ; l'orbite de x est alors de cardinal p. Vu l'équation aux classes

$$|\mathrm{X}| = |\mathrm{X}^\sigma| + \sum_{\substack{\text{orbites O non réduites} \\ \text{à un élément}}} |\mathrm{O}|$$

et le fait que p divise $|\mathrm{X}| = |\mathrm{G}|^{p-1}$, nous en déduisons que p divise $|\mathrm{X}^\sigma|$. Enfin, comme $|\mathrm{X}^\sigma| \geq 1$, la permutation σ a au moins p points fixes distincts dans X et il existe par conséquent un élément g de G tel que $g \neq e$ et $g^p = e$. Nous avons ainsi démontré que le groupe G contient au moins un élément d'ordre p (thèorème de Cauchy).