

MATHF-203 – Algèbre I

R. Petit

Année académique 2016 - 2017

Table des matières

1	Les groupes	1
1.1	Définitions	1
1.2	Groupes de transformation	2
1.3	Sous-groupes	2
1.4	Isomorphismes	3
1.5	Classes latérales et théorème de Lagrange	4
1.6	Sous-groupes normaux et homomorphismes	6
1.7	Groupes quotients	7
1.8	Théorèmes d'isomorphisme	9
1.8.1	Premier théorème d'isomorphisme	9
1.8.2	Deuxième théorème d'isomorphisme	9
1.8.3	Troisième théorème d'isomorphisme	9
2	Actions de groupes	10
3	Groupes abéliens	13
3.1	Groupes abéliens de type fini	16
4	Les théorèmes de Sylow	18
5	Classification des groupes finis	20
5.1	Produits direct et semi-direct de groupes	20

1 Les groupes

1.1 Définitions

Définition 1.1. Un *groupe* $(G, *)$ est un ensemble non-vidé G muni d'une loi de composition $*$: $G \times G \rightarrow G$ tels que :

- $*$ est associative ;
- G possède un élément neutre noté $e \in G$;
- chaque élément g de G possède un inverse noté g^{-1} .

Définition 1.2. Un ensemble non-vidé M muni d'une loi de composition $*$: $M \times M \rightarrow M$ associative telle que M admet un neutre par $*$ est appelé un *monoïde*.

Définition 1.3. Un monoïde $(M, *)$ est dit *abélien* (ou *commutatif*) lorsque $*$ est commutative.

Remarque. Un groupe est un monoïde admettant un inverse pour chaque élément. Dès lors, les résultats et définitions sur les monoïdes s'appliquent également aux groupes.

Proposition 1.4. Dans un groupe $(G, *)$, les équations :

$$x * a = b, \tag{1}$$

et :

$$a * y = b \tag{2}$$

admettent une unique solution, i.e. :

$$(x, y) = (b * a^{-1}, a^{-1} * b) \in G^2.$$

Démonstration. G est un groupe, du coup a et b admettent un inverse. L'existence de la solution est donc triviale.

Soit x , solution de (1). On a alors :

$$x = x * e = x * a * a^{-1} = b * a^{-1}.$$

Similairement pour y , solution de (2), on a :

$$y = e * y = a^{-1} * a * y = a^{-1} * b.$$

□

Proposition 1.5. Le neutre d'un groupe est unique, et l'inverse de tout élément l'est également.

De plus :

$$\forall a, b, c, d \in G : \begin{cases} c * a = d * a \Rightarrow c = d, \\ a * c = a * d \Rightarrow c = d. \end{cases}$$

Démonstration. EXERCICE.

□

Proposition 1.6. Si G est un ensemble non-vidé muni d'une loi de composition $*$ associative telle que (1) et (2) admettent une unique solution, alors $(G, *)$ est un groupe.

Démonstration. Pour chaque élément $a \in G$, prenons e_a^L tel que $e_a^L * a = a$ et e_a^R tel que $a * e_a^R = a$. Ces deux équations admettent une unique solution par hypothèse. On trouve alors :

$$e_a^L * a = a = a * e_a^R,$$

d'où l'on déduit :

$$a * e_a^L * a = a * a = a * e_a^R * a,$$

et donc $e_a^L = e_a^R$ en multipliant à gauche et à droite par a^{-1} . On en déduit l'unicité d'un neutre pour a et notons-le e_a . Montrons que ce neutre l'est pour tous les éléments de G . Prenons $(a, b) \in G^2$ et leur neutre respectif e_a et e_b . On peut écrire :

$$a * e_b * b = a * b = a * e_a * b,$$

d'où l'on déduit $e_a = e_b$ en multipliant à gauche par a^{-1} et à droite par b^{-1} . \square

Définition 1.7. Si $|G| < \infty$, on peut définir la *table de multiplication* de $(G, *)$ par un tableau de dimensions $|G| \times |G|$ reprenant tous les résultats de $g * h$ pour $g, h \in G$.

1.2 Groupes de transformation

Définition 1.8. Soit S un ensemble non-vidé. Soit G l'ensemble des bijections de S dans S . On définit la loi de composition :

$$\circ : G \times G \rightarrow G : (\psi, \varphi) \mapsto (\psi \circ \varphi),$$

tels que $\forall s \in S : (\psi \circ \varphi)(s) = \psi(\varphi(s))$.

Proposition 1.9. (G, \circ) est un groupe (de permutation sur S).

Démonstration. Le neutre est donné par $\text{Id} \in G$ où $\forall s \in S : \text{Id}(s) = s$. La loi \circ est trivialement associative, et l'inverse d'une fonction est bien définie sur les bijections. \square

Exemple 1.1. L'ensemble $\text{SO}(3, \mathbb{R})$ des rotations axiales passant par \mathcal{O} forme un groupe de transformations.

Remarque. Un groupe de transformation est composé de fonctions bijectives. L'ensemble G est donc un ensemble fonctionnel.

1.3 Sous-groupes

Définition 1.10. Soit $(G, *)$ un groupe, et soit $S \subset G$. Si $(S, *)$ est un groupe, alors on dit que $(S, *)$ est un *sous-groupe* de $(G, *)$.

Proposition 1.11. Soit $(G, *)$ un groupe. $S \subseteq G$ est un sous-groupe de G si et seulement si :

$$\forall a, b \in S : a * b^{-1} \in S.$$

Démonstration. \Rightarrow Trivial car S est un groupe.

\Leftarrow S est non-vidé, donc $e \in S$ car si $a \in S$, alors par hypothèse $e = a * a^{-1} \in S$. De même, soit $a \in S$. On sait que $a^{-1} = e * a^{-1} \in S$. Et S est stable par $*$ car si $a, b \in S$, on sait que $b^{-1} \in S$, et donc $a * (b^{-1})^{-1} \in S$. \square

Proposition 1.12. Si $\{S_\alpha \text{ t.q. } \alpha \in I\}$ est une famille de sous-groupes de $(G, *)$, alors $S := \bigcap_{\alpha \in I} S_\alpha$ est un sous-groupe de $(G, *)$ également.

Démonstration. On sait que $e \in S$ car $e \in S_\alpha$ pour tout $\alpha \in I$. Donc $S \neq \emptyset$. Prenons $a, b \in S$. On sait que $a, b \in S_\alpha$ pour tout $\alpha \in I$. Donc b^{-1} et $a * b^{-1}$ sont dans S_α pour tout $\alpha \in I$ également. Donc $a * b^{-1} \in S$. \square

Définition 1.13. Soit $(G, *)$ un groupe et soit $P \subseteq G$. On appelle le sous-groupe de G engendré par P le plus petit sous-groupe de G contenant P . On le note $\langle P \rangle$

Définition 1.14. Soit $(G, *)$ un groupe et soit $g \in G$. On appelle ordre de g le plus petit $n \in \mathbb{N}^*$ tel que $g^n = e$. On le note $\text{ord}(g)$.

L'ordre de $(G, *)$ est $|G|$.

Définition 1.15. Un groupe $(G, *)$ est dit *cyclique* lorsqu'il existe $g \in G$ tel que $G = \langle g \rangle := \langle \{g\} \rangle$.

1.4 Isomorphismes

Définition 1.16. Un *isomorphisme* entre deux groupes $(G, *)$ et (H, \star) est une bijection $\phi : G \rightarrow H$ telle que :

$$\forall g_1, g_2 \in G : \phi(g_1 * g_2) = \phi(g_1) \star \phi(g_2).$$

Remarque. La relation « être isomorphe » dans l'ensemble des groupes est une relation d'équivalence.

De plus, si G et H sont deux groupes finis, $\phi : G \rightarrow H$ est un isomorphisme si et seulement si ϕ est bijective, et la table de multiplication de H par $\phi(G)$ est l'image de la table de multiplication de G par G .

Proposition 1.17. Soit $\phi : (G, *) \rightarrow (H, \star)$ un isomorphisme de groupes. Alors :

- $\phi(e_G) = e_H$;
- $\forall g \in G : \phi(g)^1 = \phi(g^{-1})$.

Démonstration. On sait que $\phi(e_G) = \phi(e_G * e_G) = \phi(e_G) \star \phi(e_G)$. Dès lors, il est évident que $\phi(e_G)$ est le neutre de H .

Soit $g \in G$. On sait également que $e_H = \phi(e_G) = \phi(g * g^{-1}) = \phi(g) \star \phi(g^{-1})$. On a donc bien, en multipliant par $\phi(g)^{-1}$ à gauche que $\phi(g)^{-1} = \phi(g^{-1})$. \square

Théorème 1.18. Tout groupe est isomorphe à un groupe de transformation.

Démonstration. Soit $(G, *)$ un groupe, et soit $g \in G$. On définit $\phi : G \rightarrow \{\ell_g \text{ t.q. } g \in G\}$, où $\ell_g : G \rightarrow G : h \mapsto g * h$.

Pour $g \in G$, montrons que ℓ_g est bijective :

- il est évident que $\forall g, h, h' \in G : g * h = g * h' \iff h = h'$ par les règles de simplification ;
- $\forall h \in G : \ell_g(g^{-1} * h) = g * g^{-1} * h = h$.

On a donc que ℓ_g est bien bijective pour tout $g \in G$.

Montrons maintenant que $\phi : g \mapsto \ell_g$ est un isomorphisme de groupes :

- ϕ est surjective par définition.
- soient $g, h \in G$. $\ell_g = \ell_h$ si et seulement si pour tout $\gamma \in G$, on a $g * \gamma = h * \gamma$, et donc si et seulement si on a $g = h$. ϕ est donc injective.
- Soient $g, h, \gamma \in G$. $\phi(g * h)(\gamma) = g * h * \gamma = g * \ell_h(\gamma) = (\ell_g \circ \ell_h)(\gamma)$.

\square

Théorème 1.19. *Tout groupe cyclique est déterminé, à isomorphisme près, par l'ordre d'un élément g qui l'engendre.*

*Plus précisément, si $(G, *)$ est un groupe engendré par un élément g d'ordre $\text{ord}(g)$ fini, alors $G \cong (\mathbb{Z}_{\text{ord}(g)}, +)$; et si g est d'ordre infini, alors $(G, *) \cong (\mathbb{Z}, +)$.*

Démonstration. S'il existe $g \in G$ tel que $G = \langle g \rangle$ et $\text{ord}(g) \neq +\infty$, alors $G = \{e, g, \dots, g^{\text{ord}(g)-1}\}$.

Soit $\phi : \mathbb{Z}_{\text{ord}(g)} \rightarrow G : k \mapsto g^k$. ϕ est trivialement bijective, et on observe :

$$\phi(k+l) = g^{k+l} = g^k * g^l = \phi(k) * \phi(l).$$

Supposons maintenant qu'il existe $g \in G$ tel que $\text{ord}(g) = +\infty$ et $\langle g \rangle = G$. On pose :

$$\forall p \in \mathbb{N}^* : g^{-p} := g^{-1} * g^{1-p}.$$

Puisque $\text{ord}(g) = +\infty$, si $g^x = g^y$ pour $x, y \in \mathbb{Z}$, alors $x = y$. En reprenant le même ϕ étendu à \mathbb{Z} , on a bien, à nouveau, un isomorphisme de groupes. \square

Corollaire 1.20. *Tout groupe cyclique est commutatif.*

Démonstration. Étant isomorphe à \mathbb{Z}_n pour un certain $n \in \mathbb{N}$ ou à \mathbb{Z} , par passage à l'isomorphisme, la propriété d'additivité est conservée. \square

Proposition 1.21. *Si $(G, *)$ est un groupe cyclique, tout sous-groupe S de G est cyclique.*

Démonstration. Prenons $a \in G$ tel que $G = \langle a \rangle$. Posons $N := \{n \in \mathbb{Z} \text{ t.q. } a^n \in S\}$. Dans le cas fini, prenons \underline{n} , le plus petit entier positif de N . Supposons par l'absurde que $a^t \in S$ ne soit pas une puissance entière de $a^{\underline{n}}$. Par Euclide, on a :

$$\exists (q, r) \in \mathbb{Z} \times \mathbb{N} \text{ t.q. } t = q\underline{n} + r,$$

et donc :

$$a^t = a^{q\underline{n}} * a^r,$$

avec $0 \leq r < \underline{n}$. On sait que $a^t \in S$, et $a^{q\underline{n}} \in S$ (donc $a^{-q\underline{n}} \in S$). Dès lors, $a^r \in S$. Or \underline{n} est le plus petit entier positif tel que $a^{\underline{n}} \in S$. Il y a donc contradiction, et a^t est une puissance entière de $a^{\underline{n}}$. Dès lors, $S = \langle a^{\underline{n}} \rangle$. \square

1.5 Classes latérales et théorème de Lagrange

Dans cette sous-section, considérons que $(G, *)$ est un groupe, et que S est un sous-groupe de G .

Définition 1.22. Soient $(G, *)$ un groupe, et S un sous-groupe de G . On appelle *classe latérale gauche de S par $a \in G$* l'ensemble :

$$a * S := \{a * s \text{ t.q. } s \in S\}.$$

Similairement, une classe latérale droite est sous la forme :

$$S * a := \{s * a \text{ t.q. } s \in S\},$$

pour un certain $a \in G$.

Proposition 1.23. Deux classes latérales gauches $a * S$ et $b * S$ sont identiques ou sont d'intersection nulle.

Démonstration. Soient deux telles classes d'équivalences, telles que $a * S \cap b * S \neq \emptyset$. On sait alors qu'il existe $c \in a * S \cap b * S$. On en déduit $u, v \in S$ tels que $a * u = c = b * v$. On a alors, pour $s \in S$:

$$b * s = c * v^{-1} * s = a * u * v^{-1} * s.$$

Or u et v^{-1} sont dans S . Donc $b * S \subseteq a * S$.

Par un raisonnement similaire, on a $a * S \subseteq b * S$, et donc $a * S = b * S$. □

Proposition 1.24. Deux éléments $a, b \in G$ ont la même classe latérale gauche, i.e. $a * S = b * S$ si et seulement si $a^{-1} * b \in S$.

Démonstration. \Rightarrow $a * S = b * S = a * a^{-1} * b * S$. Donc $a^{-1} * b \in S$.

\Leftarrow On sait $S = e * S = s * S$ pour tout $s \in S$. Or $a^{-1} * b \in S$. Donc $S = a^{-1} * b * S$, ou encore $a * S = b * S$. □

Définition 1.25. On appelle *indice* d'un sous-groupe S de G le « nombre » de classes latérales gauches distinctes de S dans G .

Proposition 1.26. Il existe une bijection entre un sous-groupe S et chacune de ses classes latérales.

Démonstration. Soit $a \in G$. On considère $\phi : S \rightarrow a * S : s \mapsto a * s$.

ϕ est surjective par définition, et est trivialement injective. □

Corollaire 1.27. Il existe une bijection entre tout groupe $(G, *)$ et l'ensemble $S \times T$, pour S , un sous-groupe de G et T l'ensemble des classes latérales gauches distinctes de S dans G .

Théorème 1.28 (Théorème de Lagrange). Soient $(G, *)$ un groupe fini, et S un sous-groupe de G . L'ordre de G est un multiple de l'ordre de S .

Démonstration. Trivial par le corollaire précédent. □

Corollaire 1.29. Si p est un nombre premier, tout groupe $(G, *)$ à p éléments est isomorphe à $(\mathbb{Z}_p, +)$.

Démonstration. p est premier, donc $|G| \geq 2$. Soit g tel que $\text{ord}(g) > 1$ (c-à-d $g \neq e$). $S := \langle g \rangle$ est un sous-groupe de G , on en déduit par Lagrange que $|\langle g \rangle|$ divise $|G|$. Donc $|S| \in \{1, p\}$. Et comme $e, g \in S$ pour $g \neq e$, on a $|S| \geq 2$, et donc $|S| = p$. □

Corollaire 1.30. Si G est un groupe d'ordre fini n , pour tout $g \in G$, on a $\text{ord}(g)$ divise n .

Corollaire 1.31. Il n'existe, à isomorphisme près, que deux groupes d'ordre 4, à savoir \mathbb{Z}_4 et $V_4 := \mathbb{Z}_2 \times \mathbb{Z}_2$.

Corollaire 1.32. Tout groupe d'ordre fini $n \leq 5$ est commutatif.

1.6 Sous-groupes normaux et homomorphismes

Définition 1.33. Un sous-groupe N d'un groupe $(G, *)$ est dit *normal* lorsque ses classes latérales gauches sont des classes latérales droites, i.e. :

$$\forall a \in G : a * N = N * a.$$

Proposition 1.34. Soit N , un sous-groupe d'un groupe $(G, *)$. Les assertions suivantes sont équivalentes :

1. N est normal ;
2. $\forall a \in G : a * N = N * a$;
3. $\forall a \in G : a * N \subseteq N * a$;
4. $\forall a \in G : a * N * a^{-1} \subseteq N$.

Démonstration. On sait, par définition, que $1 \iff 2$, et $2 \Rightarrow 3$. En multipliant par a^{-1} à droite, on a $3 \iff 4$.

Montrons donc que $3 \Rightarrow 2$. En particulier, c'est vrai pour a^{-1} , et donc $a^{-1} * N \subseteq N * a^{-1}$, ou encore $N * a \subseteq a * N$. Avec 3, cela implique que $a * N = N * a$. \square

Définition 1.35. Un *homomorphisme* d'un groupe $(G, *)$ dans un groupe (H, \star) est une application $f : G \rightarrow H$ telle que :

$$\forall g_1, g_2 \in G : f(g_1 * g_2) = f(g_1) \star f(g_2).$$

Proposition 1.36. Si f est un homomorphisme de $(G, *)$ dans (H, \star) , alors l'image du neutre par f est le neutre de H , et l'inverse g^{-1} d'un élément $g \in G$ est envoyé sur $f(g)^{-1} \in H$.

Démonstration. Voir preuve de la Proposition 1.17. \square

Proposition 1.37. Si f est un homomorphisme de $(G, *)$ dans (H, \star) , alors :

1. $\text{Im } f := \{f(g) \text{ t.q. } g \in G\} =: f(G)$ est un sous-groupe de H ;
2. $\text{Ker } f := \{g \in G \text{ t.q. } f(g) = e_H\}$ est un sous-groupe *normal* de H .

Démonstration. Montrons d'abord que $\text{Im } f \leq H$. Prenons donc $g, g' \in G$. On a alors $f(g) \star f(g')^{-1} = f(g * g'^{-1}) \in \text{Im } f$ car f est un homomorphisme.

Montrons ensuite que $\text{Ker } f \leq G$. Prenons $g_1, g_2 \in \text{Ker } f$. On sait donc que :

$$f(g_1 * g_2^{-1}) = f(g_1) \star f(g_2)^{-1} = e_H \star e_H^{-1} = e_H.$$

On en déduit que $g_1 * g_2^{-1} \in \text{Ker } f$.

Montrons alors que pour tout $a \in G$, on a $a * \text{Ker}(f) * a^{-1} \subseteq \text{Ker } f$. Soit $g \in \text{Ker } f$. On calcule :

$$f(a * g * a^{-1}) = f(a) \star e_H \star f(a)^{-1} = f(a) \star f(a)^{-1} = e_H,$$

et donc $a * g * a^{-1} \in \text{Ker } f$, ou encore $a * \text{Ker}(f) * a^{-1} \subseteq \text{Ker } f$. $\text{Ker } f$ est donc bien un sous-groupe normal de G . \square

Remarque. Un isomorphisme est un homomorphisme tel que $\text{Ker } f = \{e_G\}$ et $\text{Im } f = H$ car f est respectivement injective et surjective.

Définition 1.38. Un homomorphisme d'un groupe $(G, *)$ dans lui-même est appelé un *automorphisme*.

Définition 1.39. Pour tout $g \in G$, on définit la *conjugaison par g* comme la fonction :

$$c(g) : G \rightarrow G : h \mapsto g * h * g^{-1}.$$

Proposition 1.40. Pour $g \in G$, la conjugaison par g est un automorphisme.

Démonstration. $c(g)$ est injective par les règles de simplification, et est surjective car pour tout $\gamma \in G$, on a :

$$c(g)^{-1}(\gamma) = g^{-1} * \gamma * g,$$

en effet :

$$c(g)(g^{-1} * \gamma * g) = g * (g^{-1} * \gamma * g) * g^{-1} = \gamma.$$

Donc $c(g)$ est bien surjective.

Et puisque $c(g)$ va de G dans G , c'est bien un automorphisme. □

Proposition 1.41. L'application $C : G \rightarrow \text{Aut}(G) \subset G^G : g \mapsto c(g)$ est un homomorphisme.

Démonstration. Soient $g, h, \gamma \in G$. On calcule :

$$\begin{aligned} C(g * h)(\gamma) &= c(g * h)(\gamma) = (g * h) * \gamma * (g * h)^{-1} = g * h * \gamma * h^{-1} * g^{-1} = c(g)(h * \gamma * h^{-1}) \\ &= c(g)(c(h)(\gamma)) = (c(g) \circ c(h))(\gamma). \end{aligned}$$

□

Proposition 1.42. Soit f un homomorphisme de groupe de $(G, *)$ dans (H, \star) . Deux éléments $x, y \in G$ ont la même image par f si et seulement si ils appartiennent à la même classe latérale de $\text{Ker } f$ dans G .

Démonstration. Soient x et y tels que $f(x) = f(y)$. On calcule :

$$f(x * y^{-1}) = f(x) \star f(y^{-1}) = f(y) \star f(y)^{-1} = e_H.$$

Donc $x * y^{-1} \in \text{Ker } f$, et donc $x * \text{Ker } f = y * \text{Ker } f$ par la Proposition 1.24. □

1.7 Groupes quotients

Soit $f : (G, *) \rightarrow (H, \star)$ un homomorphisme surjectif. Si $x' \in H$, alors il existe $x \in G$ tel que $f(x) = x'$. On a alors :

$$f^{-1}(\{x'\}) = x * \text{Ker } f.$$

Si $|\text{Ker } f| \geq 2$, prenons également $y' \in H$ et donc $y \in G$ tel que $f^{-1}(\{y'\}) = y * \text{Ker } f$.

On peut ensuite calculer :

$$x' \star y' = f(x) \star f(y) = f(x * y),$$

d'où l'on déduit :

$$f^{-1}(\{x' \star y'\}) = x * y * \text{Ker } f.$$

Définition 1.43. Soit N un sous-groupe normal du groupe $(G, *)$. On désigne par G/N l'ensemble des classes latérales de N dans G . Cela se lit G quotienté N .

Proposition 1.44. Soient $x * N$ et $y * N$ deux éléments de G/N . Si $x' \in x * N$ et $y' \in y * N$, alors :

$$x' * y' \in x * y * N.$$

Démonstration. On sait qu'il existe $m, n \in N$ tels que $x' = x * n$ et $y' = y * m$. Par normalité de N , on sait qu'il existe $m' \in N$ tel que $y' = n * y = y * n'$. Dès lors :

$$x' * y' = x * n * y * n' * m.$$

Or, $n' * m \in N$. Donc :

$$x' * y' \in x * y * N.$$

□

Définition 1.45. On définit le produit $\bar{*} : G/N \times G/N \rightarrow G/N : (x * N, y * N) \mapsto (x * N) \bar{*} (y * N) := x * y * N$.

Théorème 1.46. Soient $(G, *)$ un groupe et N un sous-groupe normal de G . Alors $(G/N, \bar{*})$ est un groupe.

Démonstration. $\bar{*}$ est interne par définition et par la proposition précédente, et est associative par associativité de $*$.

$(G/N, \bar{*})$ admet pour neutre $e * N = N$.

Soit $g * N \in G/N$. Il admet pour inverse $g^{-1} * N$ car $(g * N) \bar{*} (g^{-1} * N) = e * N = N$.

□

Définition 1.47. Le groupe $(G/N, \bar{*})$ est appelé le *groupe quotient de G par N* .

Définition 1.48. Soient $(G, *)$ un groupe, et $N \leq G$. La projection $\pi_N : G \rightarrow G/N : g \mapsto g * N$ est appelée la *projection canonique*.

Proposition 1.49. $\pi_N : (G, *) \rightarrow (G/N, \bar{*})$ est un homomorphisme.

Démonstration. Soient $g, h \in G$. $\pi_N(g * h) = g * h * N = (g * N) \bar{*} (h * N) = \pi_N(g) \bar{*} \pi_N(h)$.

□

Proposition 1.50. Si $(G, *)$ et (H, \star) sont deux groupes, $f : G \rightarrow H$ est un homomorphisme, et si N est un sous-groupe normal de G contenu dans $\text{Ker } f$, alors il existe un homomorphisme $\bar{f} : G/N \rightarrow H$ avec $\bar{f}(g * N) = f(g)$. De plus :

$$\text{Im } \bar{f} = \text{Im } f \quad \text{et} \quad \text{Ker } \bar{f} = \text{Ker}(f)/N.$$

Démonstration. \bar{f} est bien définie. Soient $g, g' \in G$. On calcule :

$$\bar{f}((g * N) \bar{*} (g' * N)) = \bar{f}(g * g' * N) = f(g * g').$$

Par propriétés de morphismes de f , on trouve donc :

$$\bar{f}((g * N) \bar{*} (g' * N)) = f(g) \star f(g') = \bar{f}(g * N) \star \bar{f}(g' * N).$$

$\text{Im } f = \text{Im } \bar{f}$ de manière triviale.

$g * N \in \text{Ker } \bar{f}$ si et seulement si $g \in \text{Ker } f$. On a alors bien $\text{Ker } \bar{f} = \{h * N \text{ t.q. } h \in \text{Ker } f\} = \text{Ker}(f)/N$.

□

1.8 Théorèmes d'isomorphisme

1.8.1 Premier théorème d'isomorphisme

Théorème 1.51. Si $f : (G, *) \rightarrow (H, \star)$ est un homomorphisme de groupes, il induit un isomorphisme :

$$G / \text{Ker}(f) \cong \text{Im } f.$$

Démonstration. $(\text{Im } f, \star)$ est un groupe car $\text{Im } f$ est un sous-groupe de H . $f : G \rightarrow \text{Im } f$ est un homomorphisme.

Considérons $N = \text{Ker } f$. $\bar{f} : G / \text{Ker}(f) \rightarrow \text{Im } f$ est surjectif car $\text{Im } f = \text{Im } \bar{f}$ et est injectif car $\text{Ker}(\bar{f}) = \text{Ker}(f) / \text{Ker}(f) = \{e * \text{Ker } f\} = \{e\}$. \bar{f} est donc un homomorphisme bijectif, ou encore, un isomorphisme. \square

1.8.2 Deuxième théorème d'isomorphisme

Théorème 1.52. Si K, N sont des sous-groupes de $(G, *)$, alors $K / (N \cap K) \cong (N * K) / N$, où on définit :

$$N * K := \{n * k \text{ t.q. } (n, k) \in N \times K\}.$$

Démonstration. Montrons que $N * K$ est un sous-groupe de G , i.e. $\forall x, y \in N * K : x * y^{-1} \in N * K$. Prenons donc $(x, y) \in (N * K)^2$. Il existe $n_x, n_y \in N$ et $k_x, k_y \in K$ tels que $(x, y) = (n_x * k_x, n_y * k_y)$. On a alors :

$$x * y^{-1} = n_x * k_x * k_y^{-1} * n_y^{-1}.$$

En posant $k := k_x * k_y^{-1} \in K$ (car K est un sous-groupe), on trouve :

$$x * y^{-1} = n_x * k * n_y.$$

Par normalité de N on sait qu'il existe $n \in N$ tel que $k * n_y = n * k$. On trouve alors :

$$x * y^{-1} = n_x * n * k = (n_x * n) * k \in N * K.$$

On observe maintenant que si N est normal dans G , alors il l'est dans $N * K$.

L'application $f : K \rightarrow (N * K) / N : k \mapsto k * N$ est un homomorphisme. Son noyau est $\text{Ker } f = \{k \in K \text{ t.q. } k * N = N\} = K \cap N$. $K \cap N$ est donc un sous-groupe normal de K . Par le théorème précédent, on a :

$$K / \text{Ker}(f) \cong \text{Im } f = (N * K) / N.$$

\square

1.8.3 Troisième théorème d'isomorphisme

Théorème 1.53. Si K et N sont deux sous-groupes normaux de $(G, *)$ tels que $K \subseteq N$, alors N / K est normal dans G / K et :

$$(G / K) / (N / K) \cong G / N.$$

Démonstration. Prenons $\pi_N : G \rightarrow G/N$ l'homomorphisme canonique. On a $K \subset \text{Ker } \pi = N$. Par le théorème précédent, il existe un homomorphisme $\bar{\pi} : G/K \rightarrow G/N : g * K \mapsto g * N$ surjectif de noyau $\text{Ker } \bar{\pi} = N/K$.

Puisque l'on en déduit G/K normal dans N/K , en appliquant le premier théorème d'isomorphisme à $\bar{\pi}$, on trouve :

$$(G/K) / (N/K) \cong G/N.$$

□

2 Actions de groupes

Définition 2.1. Une *action* (à gauche) d'un groupe $(G, *)$ sur un ensemble S est une application :

$$\phi : G \times S \rightarrow S : (g, x) \mapsto \phi(g, x)$$

telle que :

- $\forall x \in S : \phi(e_G, x) = x$;
- $\forall g_1, g_2 \in G : \forall x \in S : \phi(g_1 * g_2, x) = \phi(g_1, \phi(g_2, x))$.

S'il existe une action entre un groupe $(G, *)$ et un ensemble S , on dit que G agit sur S .

Remarque. Pour $g \in G, x \in S$ et ϕ une action de G sur S , on note souvent $gx = \phi(g, x)$.

Définition 2.2. Soit $(G, *)$ un groupe et $H \leq G$ un sous-groupe. Une action de H sur G est sous la forme $\phi(h, g) = h * g$. Une telle action est appelée *une translation à gauche* de H par G .

Exemple 2.1. La conjugaison $c(g)$ est une action.

Remarque. Soient $(G, *)$ un groupe et H, K deux sous-groupes de G avec K normal. H agit sur G/K par translation gauche :

$$(h, g * K) \mapsto (h * g) * K$$

Définition 2.3. Soit $(G, *)$ un groupe agissant sur un ensemble S . Cette action ϕ définit une relation d'équivalence sur S :

$$\forall x, x' \in S : x \sim x' \iff \exists g \in G \text{ t.q. } gx = x'.$$

Les classes d'équivalence induites par \sim (donc les éléments de S / \sim) sont appelées les *orbites* de S sous l'action de G .

On note :

$$\mathcal{O}_x := \{gx \text{ t.q. } g \in G\}$$

l'orbite de $x \in S$.

Proposition 2.4. Les orbites de S sous l'action de G forment une partition de S .

Définition 2.5. Si $|S / \sim| = 1$, on dit que l'action est transitive.

Définition 2.6. Soit $(G, *)$ un groupe agissant sur un ensemble S , et soit $x \in S$. On définit le *stabilisateur* de x dans G par :

$$G_x := \{g \in G \text{ t.q. } gx = x\}$$

Proposition 2.7. Le stabilisateur de $x \in S$ dans G est un sous-groupe de G .

Démonstration. Soient $a, b \in G_x$. On observe que :

$$\phi(b^{-1}, x) = \phi(b^{-1}, \phi(b, x)) = \phi(e_G, x) = x.$$

Dès lors, $b^{-1} \in G_x$. Montrons alors que $a * b^{-1} \in G_x$:

$$\phi(a * b^{-1}, x) = \phi(a, \phi(b^{-1}, x)) = \phi(a, x) = x.$$

□

Définition 2.8. Soit $(G, *)$ un groupe. G agit sur lui-même par conjugaison. Pour $x \in G$, on a :

$$G_x = \{g \in G \text{ t.q. } gxg^{-1} = x\} =: C_G(x),$$

que l'on appelle le *centralisateur* de x dans G .

Définition 2.9. Si G agit sur l'ensemble de ses sous-groupe par conjugaison, pour $K \leq G$, on définit :

$$G_K := \{g \in G \text{ t.q. } gKg^{-1} = K\} =: N_G(K),$$

que l'on appelle *normalisateur* de K dans G .

Remarque. On observe que $\langle x \rangle \leq C_G(x)$, et K est un sous-groupe normal de $N_G(K)$.

Remarque. Soient $(G, *)$ un groupe agissant sur un ensemble S , et G_x , le stabilisateur de x dans G . L'indice de G_x dans G (noté $[G : G_x]$) est égal à :

$$[G : G_x] = \frac{|G|}{|G_x|}.$$

Théorème 2.10. Soit $(G, *)$ un groupe agissant sur un ensemble S . Alors $\forall x \in S$, on a :

$$|\mathcal{O}_x| = [G : G_x].$$

Démonstration. L'application $\phi : G/G_x \rightarrow \mathcal{O}_x : gG_x \mapsto gx$ est une bijection car :

$$gG_x = \phi(g, G_x) = \{\phi(g, hx) \text{ t.q. } h \in G \text{ et } hx = x\} = \{\phi(g, x)\} = \{gx\}.$$

□

Corollaire 2.11. Si $(G, *)$ est un groupe fini, alors :

1. $\forall x \in G : |\{gxg^{-1} \text{ t.q. } g \in G\}| = [G : C_G(x)]$;
2. si \mathcal{O}_{x_i} pour $i = 1, \dots, m$ sont les classes de conjugaison, distinctes deux à deux, d'éléments de G (avec $x_i \in G$), alors :

$$|G| = \sum_{k=1}^m |\mathcal{O}_{x_k}| = \sum_{k=1}^m [G : C_G(x_k)] ;$$

3. la cardinalité de l'ensemble des sous-groupes de G qui sont conjugués à un sous-groupe K de G fixé, est égal à :

$$[G : N_G(K)],$$

qui divise $|G|$.

Définition 2.12. On définit le *centre* du groupe G par :

$$Z(G) := C(G) := \{x \in G \text{ t.q. } \forall g \in G : gxg^{-1} = x\}.$$

Remarque. On observe que $|\mathcal{O}_{x_i}| = 1 \iff x_i \in C(G)$. Cela amène à la *formule des classes* qui dit que :

$$|G| = |C(G)| + \sum_{j=1}^n |\mathcal{O}_{x_j}|,$$

où \mathcal{O}_{x_j} sont les classes de conjugaison contenant au moins 2 éléments.

Définition 2.13. Soit $\phi : G \rightarrow S$, une action d'un groupe G sur un ensemble S . Pour $g \in G$ fixé, on définit :

$$\phi : S \rightarrow S : x \mapsto \phi_g(x) = \phi(g, x) = gx.$$

Proposition 2.14. Pour $g \in G$ fixé, ϕ_g est une bijection de S dans S .

Démonstration. Soient $x, y \in S$. Si $\phi_g(x) = \phi_g(y)$, alors $x = \phi(g^{-1}, \phi_g(x)) = \phi(g^{-1}, \phi_g(y)) = y$.

De plus, soit $x \in S$. On sait que $\phi(g^{-1}, x) \in S$ par définition. Notons y cette valeur. On a alors :

$$\phi_g(y) = \phi_g(\phi(g^{-1}, x)) = x.$$

ϕ_g est donc injective et surjective. □

Définition 2.15. Notons $A(S) = \text{Sym}(S)$ le groupe des bijections de S dans S muni de la composition.

Théorème 2.16. Soit $\phi : G \times S \rightarrow S$. L'application $\tilde{\phi} : G \rightarrow A(S) : g \mapsto \phi_g$ est un homomorphisme de groupes.

Théorème 2.17. Si $(G, *)$ est un groupe, alors il existe un homomorphisme de groupes $\tilde{\phi} : G \rightarrow \text{Aut}(G)$ tel que $\text{Ker } \tilde{\phi} = C(G)$.

Lemme 2.18. Soit G , un groupe d'ordre fini p^n , pour p premier, et $n \in \mathbb{N}^*$. Soit S un ensemble fini sur lequel G agit. Si S_0 est un ensemble de points fixes de S sous l'action de G :

$$S_0 := \{x \in S \text{ t.q. } \forall g \in G : gx = x\},$$

alors :

$$|S| \equiv |S_0| \pmod{p}.$$

Démonstration. On écrit S comme une union disjointe d'orbites sous l'action de G . On remarque que l'orbite \mathcal{O}_x d'un point $x \in S$ ne contient qu'un seul point (donc x) si et seulement si $x \in S_0$. Donc :

$$S = S_0 \sqcup \mathcal{O}_{x_1} \sqcup \mathcal{O}_{x_2} \sqcup \dots \sqcup \mathcal{O}_{x_n},$$

pour $|\mathcal{O}_{x_i}| \geq 2$.

On sait que $|\mathcal{O}_{x_i}|$ divise $|G|$ pour tout i . Or, seules les puissances de p divisent $|G|$, donc p divise $|\mathcal{O}_{x_i}|$. Or :

$$S \setminus S_0 = \mathcal{O}_{x_1} \sqcup \dots \sqcup \mathcal{O}_{x_n}.$$

Du coup :

$$|S| - |S_0| = pK,$$

pour un certain $K \in \mathbb{N}^*$, et donc :

$$|S| \equiv |S_0| + pK \equiv |S_0| \pmod{p}.$$

□

Théorème 2.19 (Théorème de Cauchy). Soit $(G, *)$ un groupe fini, et p un nombre premier qui divise $|G|$. Alors G possède au moins un élément $g \in G$ tel que $\text{ord}(g) = p$.

Démonstration. On pose :

$$S := \{(g_1, \dots, g_p) \in G^p \text{ t.q. } g_1 \dots g_p = e_G\}.$$

Puisque $g_p = (g_1 \dots g_p)^{-1}$, on a $|S| = |G|^{p-1}$, et par hypothèse, p divise $|G|$. Soit $H \cong \mathbb{Z}_p$, le groupe cyclique d'ordre p agissant sur S par permutations cycliques du type :

$$\mathbb{Z}_p \times S \rightarrow S : (k, (g_1, \dots, g_p)) \mapsto k(g_1, \dots, g_p) := (g_{k+1}, \dots, g_p, g_1, \dots, g_k).$$

Posons alors :

$$S_0 := \{(g_1, \dots, g_p) \in S \text{ t.q. } g_1 = \dots = g_p\} = \{(g, \dots, g) \in S \text{ t.q. } g^p = e\}.$$

On sait $|S_0| \geq 1$ car $(e, \dots, e) \in S_0$. De plus, par le lemme précédent, p divise $|S_0|$, donc $|S_0| \geq 2$.

Il existe donc au moins une valeur $g \in G$ telle que $g \neq e_G$, et $g^p = e$. □

3 Groupes abéliens

Lemme 3.1. Si $(G, *)$ est un groupe cyclique, alors tout sous-groupe de G est cyclique.

Démonstration. Soit $g \in G$ tel que $G = \langle g \rangle$. Soit $H \leq G$, un sous-groupe de G . Posons :

$$A := \{\ell \in \mathbb{Z} \text{ t.q. } g^\ell \in H\}.$$

Prenons $\ell, m \in A$. On a alors $g^{\ell-m} = g^\ell * (g^m)^{-1}$, la composition de deux éléments de H . Donc $\ell - m \in A$, ce qui fait de A un sous-groupe de \mathbb{Z} . Si $A = \{0\}$, alors A est trivialement cyclique, et sinon soit n , le plus petit entier strictement positif de A . On a alors $A \cong n\mathbb{Z}$. □

Lemme 3.2. Soit $G = \langle g \rangle$, un groupe cyclique d'ordre $n \leq +\infty$, et soit $\ell \in \mathbb{N}^*$. Alors :

$$\left| \langle g^\ell \rangle \right| = \frac{n}{\text{GCD}(n, \ell)}$$

Démonstration. On cherche le plus petit entier positif k tel que $(g^\ell)^k = g^{k\ell} = e$. On a :

$$\begin{cases} \ell &= \text{GCD}(\ell, n)r \\ n &= \text{GCD}(\ell, n)s, \end{cases}$$

pour $s, r \in \mathbb{N}$, avec $\text{GCD}(r, s) = 1$. Si $g^{k\ell} = e$, c'est que n divise $k\ell$, et donc $\frac{n}{\text{GCD}(n, \ell)} = s$ divise k . De plus :

$$\left(g^\ell \right)^{\frac{n}{\text{GCD}(n, \ell)}} = g^{\frac{\ell n}{\text{GCD}(n, \ell)}} = g^{nr} = e^r = e.$$

On en déduit que $k = \text{ord}(g^\ell)$ divise $\frac{n}{\text{GCD}(n, \ell)}$. Donc $k = \frac{n}{\text{GCD}(n, \ell)}$. □

Exemple 3.1. On sait que $\mathbb{Z}_{30} = \langle 1 \rangle$. Alors $|\{5, 10, 15, 20, 25, 0\}| = |\langle 5 \rangle| = \frac{30}{5} = 6$.

Définition 3.3. Dans un groupe abélien, on prend pour convention d'écrire la loi de composition $+$, de noter l'inverse par de $g \in G$ par $-g \in G$, et de noter la composition n fois par $g^n = ng$.

Lemme 3.4. Soit $\varphi : H \rightarrow K$, un morphisme de groupes abéliens. Si $\text{Ker } \varphi$ et $\text{Im } \varphi$ sont engendrés par un ensemble fini, alors H l'est également.

Démonstration. Soient $\{k_1, \dots, k_r\}$ et $\{i_1, \dots, i_s\}$, ensembles générateurs respectivement de $\text{Ker } \varphi$ et $\text{Im } \varphi$. Pour $j = 1, \dots, s$, on prend $h_j \in H$ t.q. $\varphi(h_j) = i_j$. Montrons que $\{k_1, \dots, k_r\} \cup \{h_1, \dots, h_s\}$ est un ensemble générateur de H .

Soit $x \in H$. Il existe $(a_1, \dots, a_s) \in \mathbb{Z}^s$, tel qu'on peut écrire :

$$\varphi(x) = \sum_{k=1}^s a_k i_k.$$

Par définition des h_j et par propriétés de morphismes, on peut écrire :

$$\begin{aligned}\varphi(x) &= \sum_{k=1}^s a_k \varphi(h_k) = \varphi\left(\sum_{k=1}^s a_k h_k\right) \\ 0 &= \varphi(x) - \varphi\left(\sum_{k=1}^s a_k h_k\right) = \varphi\left(x - \sum_{k=1}^s a_k h_k\right) \\ \text{Ker } \varphi &\ni x - \sum_{k=1}^s a_k h_k,\end{aligned}$$

et donc il existe $(b_1, \dots, b_r) \in \mathbb{Z}^r$ tel qu'on peut écrire :

$$x - \sum_{k=1}^s a_k h_k = \sum_{t=1}^r b_t k_t,$$

ou encore :

$$x = \sum_{k=1}^s a_k h_k + \sum_{t=1}^r b_t k_t.$$

H est bien généré par $\{h_1, \dots, h_s, k_1, \dots, k_r\}$. □

Proposition 3.5. *Tout sous-groupe d'un groupe abélien finiment engendré est finiment engendré.*

Démonstration. Soit $\{g_1, \dots, g_n\}$, un ensemble générateur de G . Pour $1 \leq k \leq n$, on définit :

$$G_k := \langle g_1, \dots, g_k \rangle.$$

Soit H un sous-groupe de G , et posons $H_i := H \cap G_i$ pour $i = 1, \dots, n$.

Montrons ce résultat par récurrence sur G_k .

Pour $k = 1$, le groupe $G_k = G_1 = \langle g_1 \rangle$ est un groupe cyclique, et par propriété d'intersection (Proposition 1.12), on sait que H_1 est un sous-groupe, et cyclique qui plus est.

Supposons alors pour $j < n$ que tout sous-groupe de G_j est finiment engendré. Considérons alors la projection :

$$\phi_j : G_{j+1} \rightarrow G_{j+1}/G_n,$$

un morphisme de groupes. Intéressons-nous à la restriction de ϕ_j à H_{j+1} . Puisque $\text{Ker } \phi_j = G_n$, on trouve :

$$\text{Ker } \phi_j \Big|_{H_{j+1}} = H_{j+1} \cap G_n,$$

et $H_{j+1} \cap G_n$ est un sous-groupe de G_j . Or, par hypothèse, on suppose que tout sous-groupe de G_j est finiment engendré. Donc $\text{Ker } \phi_j \Big|_{H_{j+1}}$ est finiment engendré.

De plus, $\text{Im } \phi_j \leq G_{j+1}/G_n = \langle g_{j+1} + G_n \rangle$. Donc $\text{Im } \phi_j \Big|_{H_{j+1}} \leq \text{Im } \phi_j$ est finiment engendré.

Par le lemme précédent, on trouve que H_{j+1} est finiment engendré. La propriété est en particulier vraie pour $j = n$, et donc pour G . □

Théorème 3.6 (Théorème fondamental des groupes abéliens finis). Soit $(G, +)$ un groupe abélien fini. Alors il existe une unique suite $(n_1, \dots, n_{d(G)}) \in \mathbb{Z}^{d(G)}$ telle que :

$$\prod_{i=1}^{d(G)} n_i = |G|,$$

et :

$$G \cong \prod_{k=1}^{d(G)} \mathbb{Z}_{n_k},$$

avec $d(G)$ la cardinalité du plus petit générateur de G (au sens de l'inclusion), tel que $\forall 1 \leq k \leq d(G) : n_k$ divise n_{k+1} .

Démonstration. Montrons cela par récurrence. Si $d(G) = 1$, alors G est cyclique, et donc isomorphe à \mathbb{Z}_{n_1} .

Supposons alors $d(G) \geq 2$ tel que pour tout groupe abélien G' tel que $d(G') \leq d(G)$, le théorème est vrai. Soit m , le plus petit entier strictement positif tel qu'il existe $\{g_1, \dots, g_{d(G)}\}$, un ensemble générateur de G satisfaisant :

$$mg_1 + \sum_{k=2}^{d(G)} a_k g_k = 0. \quad (3)$$

Pour $i \in \{2, \dots, d(G)\}$, on pose :

$$a_i = mq_i + r_i,$$

pour $q_i \in \mathbb{N}$, et $r_i \in \mathbb{N}$ tel que $r_i \leq m$.

Posons ensuite :

$$h_1 := g_1 + \sum_{k=2}^{d(G)} q_k g_k.$$

L'équation (3) devient alors :

$$m \left(g_1 + q_2 g_2 + \dots + q_{d(G)} g_{d(G)} \right) + \sum_{k=2}^{d(G)} r_k g_k = mh_1 + \sum_{k=2}^{d(G)} r_k g_k = 0.$$

On trouve alors, par définition de m , $r_2 = \dots = r_{d(G)} = 0$, et donc $mh_1 = 0$, avec $m \neq 0$, donc m divise $\text{ord}(h_1)$. Or m est le plus petit entier avec cette propriété. Donc $m = \text{ord}(h_1)$.

On a un morphisme surjectif de groupes : $\Theta : \langle h_1 \rangle \times \langle g_2, \dots, g_{d(G)} \rangle \rightarrow G : (a, b) \mapsto a + b$. On observe que Θ est injective car $(a, b) \in \text{Ker } \Theta \iff a = b = e$ par (3). Donc Θ est un isomorphisme, et donc :

$$\exists G' \text{ t.q. } G \cong \mathbb{Z}_m \times G',$$

et par récurrence, on a $\exists (n_2, \dots, n_{d(G)})$ tel que :

$$G' \cong \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_{d(G)}}.$$

Il reste alors à montrer que m divise n_2 . On pose $n_2 = mq + r$, et on observe que $mh_1 + n_2 h_2 = 0$ si h_2 engendre \mathbb{Z}_{n_2} . On a donc :

$$m(h_1 + qh_2) + rh_2 = 0 \Rightarrow r = 0.$$

□

3.1 Groupes abéliens de type fini

Définition 3.7. Un groupe abélien est dit *de type fini* lorsqu'il est engendré par un ensemble fini.

Définition 3.8. La *torsion* T d'un groupe $(G, *)$ est définie par :

$$T := \{g \in G \text{ t.q. } \text{ord}(g) \preceq +\infty\}.$$

Remarque. On remarque que e est toujours dans la torsion du groupe dont il est le neutre.

Définition 3.9. Un groupe $(G, *)$ de torsion $T = \{e\}$ est dit *sans torsion*, et un groupe de torsion $T = G$ est dit *de torsion*.

Proposition 3.10. La torsion T d'un groupe abélien de type fini G est un sous-groupe de G .

Démonstration. Soient $x, y \in T$. On sait que $y^{-1} \in T$ car $\text{ord}(y) = \text{ord}(y^{-1})$. Puisque G est de type fini, on sait :

$$x = \sum_{i=1}^{d(G)} a_i g_i \quad \text{et} \quad y = \sum_{i=1}^{d(G)} b_i g_i,$$

pour $\{g_1, \dots, g_{d(G)}\} \subset G$ tel que $G = \langle g_1, \dots, g_{d(G)} \rangle$. Dès lors :

$$\text{ord}(x) \text{ord}(y)(x-y) = \text{ord}(x) \text{ord}(y) \sum_{i=1}^{d(G)} (a_i - b_i) g_i = \text{ord}(y) (\text{ord}(x)x) - \text{ord}(x) (\text{ord}(y)y) = \text{ord}(x)e - \text{ord}(y)e = e.$$

Dès lors, $x - y$ a un ordre fini qui divise $\text{ord}(x) \text{ord}(y)$ (à savoir $\text{LCM}(\text{ord}(x), \text{ord}(y))$). □

Théorème 3.11. Soit $(G, +)$ un groupe abélien sans torsion de type fini. Alors $G \cong \mathbb{Z}^{d(G)}$.

Démonstration. Soit $\hat{g} := \{g_1, \dots, g_{d(G)}\}$, une partie génératrice de G . On définit :

$$\Pi : \mathbb{Z}^{d(G)} \rightarrow G : (a_1, \dots, a_{d(G)}) \mapsto \sum_{i=1}^{d(G)} a_i g_i,$$

un morphisme de groupes surjectif.

Montrons que Π est injectif. Si $(a_1, \dots, a_{d(G)}) \in \text{Ker } \Pi$, alors :

$$\sum_{i=1}^{d(G)} a_i g_i = 0. \tag{4}$$

De plus, G est sans torsion, donc tout $g \in G$ tel que $g \neq e_G$ est d'ordre infini. En considérant $(a_1, \dots, a_{d(G)}) \neq (0, \dots, 0)$, on déduit qu'il existe au moins deux coefficients non-nuls. Prenons a_1 et a_2 (réorganisation des indices). Supposons $|a_1| > |a_2|$ sans perte de généralité.

Si $a_1 a_2 > 0$ (même signe), alors $|a_1 - a_2| < |a_1|$. L'équation (4) devient alors :

$$(a_1 - a_2)g_1 + a_2(g_1 + g_2) + \sum_{i=3}^{d(G)} a_i g_i = 0.$$

Si $a_1 a_2 < 0$ (signe opposé), alors $|a_1 + a_2| < |a_1| < |a_1 - a_2|$. L'équation (4) devient alors :

$$(a_1 + a_2)g_1 + a_2(g_2 - g_1) + \sum_{i=3}^{d(G)} = 0.$$

En réitérant un nombre fini de fois, on montre qu'il existe un élément différent de e_G d'ordre fini, ce qui est une contradiction.

Π est donc injective, donc bijective, et donc un isomorphisme. \square

Lemme 3.12. Soit $(G, +)$ un groupe abélien de type fini. G/T est un groupe sans torsion.

Démonstration. Soit $g \in G$ tel que $T \neq g + T \in G/T$. Dès lors, $g \notin T$, et donc, $\nexists n \in \mathbb{N} \text{ t.q. } ng + T = T$. \square

Lemme 3.13. Tout groupe abélien $(G, +)$ de type fini est isomorphe au produit direct d'un groupe abélien fini et d'un groupe abélien sans torsion de type fini.

Démonstration. T est un sous-groupe de G . Considérons G/T , qui est sans torsion (lemme précédent). Soit $\pi : G \rightarrow G/T$, la projection canonique. Par le Théorème 3.11, $G/T \cong \mathbb{Z}^\ell$, pour $\ell := d(G/T)$. Soit $\{g_1 + T, \dots, g_\ell + T\}$ un ensemble générateur de G/T .

Soit $f : G/T \rightarrow G : \sum_{i=1}^\ell a_i g_i \mapsto \sum_{i=1}^\ell a_i g_i$. f est un morphisme injectif, et donc :

$$\pi \circ f : G/T \rightarrow G/T = \text{Id}_{G/T}.$$

Soit $O : T \times G/T \rightarrow G : (t, x) \mapsto O(t, x) = t + f(x)$. O est surjectif. En effet :

$$\forall g \in G : \pi(g - (f \circ \pi)(g)) = \pi(g) - (\pi \circ f)(\pi(g)) = \pi(g) - \pi(g) = 0,$$

et donc $t(g) := g - (f \circ \pi)(g) \in \text{Ker } \pi = T$. Or :

$$g = g - (f \circ \pi)(g) + (f \circ \pi)(g) = t(g) + (f \circ \pi)(g) = O(g, \pi(g)).$$

De plus, O est injective car $O(t, x) = 0$ si et seulement si $t = -f(x)$, donc $f(x) \in T$ car $0 \in T$. f est un morphisme, donc si $f(x)$ est d'ordre fini, alors x est d'ordre fini car $f(nx) = nf(x)$. De plus, si x est d'ordre fini et f est injective, il faut $x = 0$ car x est dans la torsion de G/T . On a donc $O(t, x) = 0 \iff (t, x) = (0_T, 0_{G/T})$. \square

Théorème 3.14. Soit $(G, +)$ un groupe abélien de type fini. Alors il existe $\ell > 0$ et une suite unique d'entiers positifs (n_1, \dots, n_k) tel que n_j divise n_{j+1} pour $1 \leq j < k$ et $G \cong \mathbb{Z}^\ell \times \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$.

Démonstration. Montrons que $|T| < +\infty$. T est un groupe de torsion de type fini puisque G est de type fini. Il existe donc un générateur de $T : \{t_1, \dots, t_{d(T)}\}$ tel que pour $x \in T$:

$$x = \sum_{i=1}^{d(T)} a_i t_i.$$

Donc $|T| \leq \text{LCM}(a_1, \dots, a_{d(T)}) < +\infty$.

Par le lemme précédent et par le théorème fondamental des groupes abéliens finis, on a ce résultat ($T \cong \mathbb{Z}^{d(T)=\ell}$). \square

4 Les théorèmes de Sylow

Définition 4.1. Soit $(G, *)$ un groupe fini, et soit p un diviseur premier de $|G|$. Si H est un sous-groupe de G tel que $|H| = p^n$ pour un certain $n \in \mathbb{N}^*$, on dit que H est un p -sous-groupe de G . Si de plus, p ne divise pas $\frac{|G|}{|H|}$, on dit que H est un p (-sous-groupe de) Sylow de G .

Théorème 4.2 (Premier théorème de Sylow). Soit G un groupe fini et soit $p \in \mathbb{N}$ premier tel que p divise $|G|$. Alors G possède au moins un p -Sylow.

Démonstration. Montrons cela par récurrence sur $|G|$. Si $\exists \alpha \in \mathbb{N}^*$ tel que $|G| = p^\alpha$, alors G est son propre p -Sylow.

Supposons que le théorème soit faux pour un G d'ordre le plus petit possible. On a donc $\alpha \in \mathbb{N}$ et $m \in \mathbb{N}$ tels que $m > 1$, $\text{GCD}(p, m) = 1$ et $|G| = p^\alpha m$. On sait de plus (formule des classes) :

$$|G| = |Z(G)| + \sum_{k=1}^r [G : C_G(x_k)],$$

où $\mathcal{O}_{x_1}, \dots, \mathcal{O}_{x_r}$ sont les orbites (classes de conjugaison) de cardinalité ≥ 1 .

Cas 1 Supposons qu'il existe un j tel que p^α divise $|C_G(x_j)|$. Puisque $|C_G(x_j)| < |G|$, l'hypothèse nous donne un p -Sylow de $C_G(x_j)$, qui est également un p -Sylow de G , contradiction.

Cas 2 Supposons que pour tout $1 \leq j \leq r$: p^α ne divise pas $|C_G(x_j)|$. On sait :

$$\forall 1 \leq j \leq r : |G| = |C_G(x_j)| [G : C_G(x_j)].$$

Or p^α divise $|G|$, donc p^α divise $[G : C_G(x_j)]$ pour tout j . Par la formule des classes, on a alors p divise $|Z(G)|$.

De plus, $Z(G)$ est abélien. Par le théorème de Cauchy, il existe $x \in Z(G)$ tel que $\text{ord}(x) = p$. Étant donné que $\langle x \rangle$ forme un sous-groupe normal de G , on peut poser $G' := G / \langle x \rangle$. On a $|G'| = \frac{|G|}{p} = p^{\alpha-1} m < p^\alpha = |G|$. Donc par hypothèse de récurrence, il existe P' , un p -Sylow de G' d'ordre $p^{\alpha-1}$.

Or, tout sous-groupe de $G / \langle x \rangle$ est sous la forme $H / \langle x \rangle$, pour $H \leq G$. Il existe donc $P \leq G$ tel que $P / \langle x \rangle = P'$. Et donc :

$$|P'| = p^{\alpha-1} = \frac{|P|}{|\langle x \rangle|} = \frac{|P|}{p},$$

ou encore $|P| = p^\alpha$, et donc P est un p -Sylow de G , ce qui est une contradiction. □

Remarque. Si $|G| < +\infty$ et p est premier tel que p divise $|G|$, alors tout sous-groupe conjugué xPx^{-1} admet un p -Sylow.

Si un groupe G n'admet qu'un seul p -Sylow P , alors P est normal dans G .

Théorème 4.3 (Deuxième théorème de Sylow). Soit H , un p -sous-groupe d'un groupe fini G . Soit P , un p -Sylow de G . Alors il existe $x \in G$ tel que $H \subseteq xPx^{-1}$.

En particulier, tous les p -Sylow sont conjugués.

Démonstration. On regarde l'action de H par translation à gauche sur $S := G/P$:

$$\phi : H \times S \rightarrow S : (h, xP) \mapsto hxP.$$

Par le Lemme 2.18, pour :

$$S_0 = \{x \in S \text{ t.q. } \forall h \in H : \phi(h, xP) = xP\},$$

on a :

$$|G/P| = [G : P] = |S| = |S_0| \pmod{p}.$$

Or p ne divise pas $|S|$ car P est un p -Sylow. Donc $|S_0| \neq 0$. Donc il existe $xP \in S_0$. Or :

$$\begin{aligned} xP \in S_0 &\iff \forall h \in H : hxP = \phi(h, xP) = xP \\ &\iff \forall h \in H : x^{-1}hxP = P \\ &\iff \forall h \in H : x^{-1}hx \in P \\ &\iff x^{-1}Hx \subseteq P \\ &\iff H \subseteq xPx^{-1}. \end{aligned}$$

□

Corollaire 4.4. Si P est un p -Sylow de G , et P est un sous-groupe normal de G , alors P est l'unique p -Sylow de G .

Théorème 4.5 (Troisième théorème de Sylow). Soit G un groupe fini et soit p premier tel que p divise $|G|$. Le nombre de p -Sylow de G divise $|G|$ et est de la forme :

$$[G : N_G(P)] = kp + 1,$$

avec $k \in \mathbb{N}$.

Démonstration. Par le deuxième théorème de Sylow, ce nombre de p -Sylow est égal au nombre de conjugués d'un p -Sylow.

Pour P fixé, on a donc :

$$\left| \left\{ xPx^{-1} \text{ t.q. } x \in G \right\} \right| = |\mathcal{O}_P| = |P^G|.$$

On considère l'action de G sur les sous-groupes de G par conjugaison. Le stabilisateur de P dans cette action est $N_G(P)$. De plus :

$$|\mathcal{O}_P| = \left| \left\{ xPx^{-1} \text{ t.q. } x \in G \right\} \right| = [G : N_G(P)] \text{ divise } |G|.$$

On regarde l'action de P sur l'ensemble des p -Sylow par conjugaison :

$$\phi : P \times \mathcal{O}_P \rightarrow \mathcal{O}_P : (g, xPx^{-1}) \mapsto \phi(g, xPx^{-1}) = gxPx^{-1}.$$

Si S_0 désigne l'ensemble des p -Sylow fixes par cette action, on a :

$$\begin{aligned} Q \in S_0 &\iff \forall g \in P : gQg^{-1} = Q \\ &\iff P \leq N_G(Q). \end{aligned}$$

P et Q sont des p -Sylow de G , et des sous-groupes de $N_G(Q)$. Dès lors, P et Q sont conjugués dans $N_G(Q)$. Ainsi, on a $P = xQx^{-1}$, pour $x \in N_G(Q)$. Comme Q est normal dans $N_G(Q)$, on a $xQx^{-1} = Q$, et donc $P = Q$. Il y a donc un unique élément dans S_0 , et par la formule $|S| = |S_0| \pmod{p} = 1 \pmod{p}$, on trouve $|S| = 1 + kp$, pour $k \in \mathbb{N}$. □

5 Classification des groupes finis

Définition 5.1. Un groupe fini $(G, *)$ est dit *simple* s'il ne possède pas de sous-groupe normal non-trivial.

5.1 Produits direct et semi-direct de groupes

Définition 5.2. Le *produit direct* de deux groupes H et K est le groupe :

$$H \times K := \{(h, k) \text{ t.q. } h \in H, k \in K\},$$

muni de la loi de groupe définie par :

$$\forall (h, k), (h', k') \in H \times K : (h, k) \cdot (h', k') = (hh', kk').$$

Lemme 5.3. Soit $(G, *)$ un groupe. Soient $H, K \leq G$ tels que :

1. H, K sont normaux dans G ;
2. $G = HK := \{hk \text{ t.q. } (h, k) \in H \times K\}$;
3. $H \cap K = \{e\}$.

Alors $G \cong H \times K$.

Démonstration. $\psi : H \times K \rightarrow G : (h, k) \mapsto hk$ est un isomorphisme.

En effet :

$$\begin{aligned} hkh^{-1}k^{-1} &= h(kh^{-1}k^{-1}) \in H \text{ (car } H \text{ est normal dans } G) \\ &= (hkh^{-1})k^{-1} \in K \text{ (car } K \text{ est normal dans } G). \end{aligned}$$

Donc $hkh^{-1}k^{-1} = e$, ou encore $hk = kh$. Donc :

$$\psi((h, k)(h', k')) = \psi(hh', kk') = hh'kk' = hkh'k' = \psi(h, k)\psi(h', k').$$

Puisque ψ est un morphisme, il reste à montrer que ψ est bijective.

ψ est surjective par la seconde hypothèse, et injective car $\psi(h, k) = hk = e \iff h = k^{-1} \in H \cap K$, donc $h = k = e$. \square

Définition 5.4. Soient H et K deux groupes et soit $\varphi : K \rightarrow \text{Aut}(H)$, un morphisme de groupes défini par :

$$\begin{aligned} \forall h, h' \in H : \forall k, k' \in K : \varphi(k)(hh') &= \varphi(k)(h)\varphi(k)(h'), \\ \varphi(kk')(h) &= (\varphi(k) \circ \varphi(k'))(h). \end{aligned}$$

Le *produit semi-direct* de H et K (associé à φ), noté $H \rtimes_{\varphi} K$ est le groupe :

$$H \rtimes_{\varphi} K := \{(h, k) \in H \times K\},$$

avec la loi de groupe définie par :

$$(h, k) \cdot_{\varphi} (h', k') = (h\varphi(k)(h'), kk').$$

Remarque.

1. On a bien l'associativité de la loi de groupe :

$$\begin{aligned} ((h, k)(h', k'))(h'', k'') &= (h\varphi(k)(h'), kk')(h'', k'') = (h\varphi(k)(h')\varphi(kk')(h''), kk'k'') \\ &= (h\varphi(k)(h')\varphi(k)(\varphi(k')(h'')), kk'k'') = (h, k)(h'\varphi(k')(h''), k'k'') \\ &= (h, k)((h', k')(h'', k'')). \end{aligned}$$

De plus, le neutre est donné par :

$$e_{H \rtimes_{\varphi} K} = (e_H, e_K) \in H \rtimes_{\varphi} K,$$

et l'inverse de (h, k) est donné par :

$$(h, k)^{-1} = (\varphi(k^{-1})(h^{-1}), k^{-1}).$$

2. Le sous-groupe $\tilde{H} := \{(h, e_K) \text{ t.q. } h \in H\}$ est isomorphe à H et \tilde{H} est normal dans $H \rtimes_{\varphi} K$.

3. Le sous-groupe $\tilde{K} := \{(e_H, k) \text{ t.q. } k \in K\}$ est un sous-groupe de $H \rtimes_{\varphi} K$ isomorphe à K .

4. $G = H \rtimes_{\varphi} K$ est égal à $\tilde{H}\tilde{K}$, où $\tilde{H}\tilde{K} = \{(h, e_K)(e_H, k) \text{ t.q. } (h, k) \in H \times K\}$.

5. $\tilde{H} \cap \tilde{K} = \{(e_H, e_K)\}$.

Lemme 5.5. Soit $(G, *)$ un groupe, et soient $H, K \leq G$ tels que :

1. H est normal dans G ;
2. $G = HK$;
3. $H \cap K = \{e\}$.

Alors $G \cong H \rtimes_{\varphi} K$ où $\varphi : K \rightarrow \text{Aut}(H) : k \mapsto \varphi(k)$, avec :

$$\varphi(k) : H \rightarrow H : h \mapsto \varphi(k)(h) = khk^{-1}.$$

Démonstration. $\psi : H \rtimes_{\varphi} K \rightarrow G : (h, k) \mapsto hk$ est un isomorphisme.

En effet :

$$\psi((h, k)(h', k')) = \psi(h\varphi(k)(h'), kk') = \psi(hkh'h^{-1}, kk') = hkh'h^{-1}kk' = hkh'k' = \psi(h, k)\psi(h', k').$$

À nouveau, ψ est surjective car $G = HK$, et injective car $H \cap K = \{e\}$. □

Remarque. Si $\varphi : K \rightarrow \text{Aut}(H) : k \mapsto \text{Id}_H$ est le morphisme trivial, alors :

$$H \rtimes_{\varphi} K \cong H \times K.$$

Lemme 5.6. Soient H et K deux groupes. Soit $\varphi : K \rightarrow \text{Aut}(H)$, un morphisme de groupes.

— Si $\alpha \in \text{Aut}(K)$, alors $\varphi \circ \alpha =: \varphi' : K \rightarrow \text{Aut}(H)$ est un morphisme de groupes et :

$$H \rtimes_{\varphi'} K \cong H \rtimes_{\varphi} K.$$

— Si $\beta \in \text{Aut}(H)$, alors l'application $\tilde{\varphi} : K \rightarrow \text{Aut}(H) : k \mapsto \beta \circ \varphi(k) \circ \beta^{-1}$ est un morphisme de groupes et :

$$H \rtimes_{\tilde{\varphi}} K \cong H \rtimes_{\varphi} K.$$

Démonstration. Pour le premier point, prenons $\psi : H \rtimes_{\varphi'} K \rightarrow H \rtimes_{\varphi} K : (h, k) \mapsto (h, \alpha(k))$. On a :

$$\psi((h, k) \cdot_{\varphi \circ \alpha} (h', k')) = \psi(h\varphi(\alpha(k))(h'), kk') = (h\varphi(\alpha(k))(h'), \alpha(kk')) = \psi(h, k) \cdot_{\varphi} \psi(h', k').$$

Pour le second point, prenons $\psi' : H \rtimes_{\tilde{\varphi}} K \rightarrow H \rtimes_{\varphi} K : (h, k) \mapsto (\beta^{-1}(h), k)$. On a :

$$\begin{aligned} \psi'((h, k) \cdot_{\tilde{\varphi}} (h', k')) &= \psi'(h\tilde{\varphi}(k)(h'), kk') = \psi'\left(h\beta\left(\varphi(k)\left(\beta^{-1}(h')\right)\right), kk'\right) \\ &= \psi'\left(\beta^{-1}\left[h\beta\left(\varphi(k)\left(\beta^{-1}(h')\right)\right)\right], kk'\right) \\ &= (\beta^{-1}(h)\varphi(k)(\beta^{-1}(h')), kk') = (\beta^{-1}(h), k) \cdot_{\varphi} (\beta^{-1}(h'), k') \\ &= \psi(h, k) \cdot_{\varphi} \psi(h', k'). \end{aligned}$$

□

Lemme 5.7. Soit p premier. Le groupe $\text{Aut}(\mathbb{Z}_p)$ est isomorphe à $\mathbb{Z}_{p-1} \cong \mathbb{Z}_p^*$.

Démonstration. Soit $\sigma \in \text{Aut}(\mathbb{Z}_p)$. σ est entièrement déterminé par $\sigma(1) \neq 0$. Réciproquement, pour $q \in \mathbb{Z}_p^*$, on peut construire $\sigma_q \in \text{Aut}(\mathbb{Z}_p)$ tel que $\sigma_q(1) = q$.

Pour $n \in \{0, \dots, p-1\}$, on a $\sigma_q(n) = nq$, et donc $\sigma_q(n+m) = \sigma_q(n) + \sigma_q(m)$.

Pour $\psi : \text{Aut}(\mathbb{Z}_p) \rightarrow \mathbb{Z}_p^* : \sigma_q \mapsto \sigma_q(1)$ est un morphisme. On a $\text{Ker } \psi = \{\sigma_q \in \text{Aut}(\mathbb{Z}_p) \text{ t.q. } \sigma_q(1) = 1\}$, ou encore $\text{Ker } \psi = \{1\}$, et donc $\text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^*$. □

Lemme 5.8. Soient p, q deux nombres premiers, tels que $p < q$. Alors il existe un morphisme non-trivial de groupes :

$$\varphi : \mathbb{Z}_p \rightarrow \text{Aut}(\mathbb{Z}_q)$$

si et seulement si p divise $q-1$.

Démonstration. \Rightarrow Soit φ un morphisme non-trivial (c-à-d $\text{Ker } \varphi \neq \mathbb{Z}_p$). Puisque $\text{Ker } \varphi \leq \mathbb{Z}_p$, on a $\text{Ker } \varphi = \{0_{\mathbb{Z}_p}\}$. On a alors :

$$\varphi(\mathbb{Z}_p) = \mathbb{Z}_p \leq \text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{q-1},$$

et donc p divise $q-1$.

\Leftarrow Supposons que p divise $q-1$. Dès lors, on a :

$$\text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{q-1}$$

possède un sous-groupe d'ordre p . On prend un générateur de $\text{Aut}(\mathbb{Z}_p)$ donné par :

$$\varphi_{\beta} : \mathbb{Z}_p \rightarrow \text{Aut}(\mathbb{Z}_q) : k \mapsto \beta^{k \frac{q-1}{p}},$$

qui est un morphisme non-trivial. □

Proposition 5.9.

1. Soit φ_{β} , le morphisme précédent (pour p divise $q-1$). Alors $\mathbb{Z}_q \rtimes_{\varphi_{\beta}} \mathbb{Z}_p$ est un groupe non-abélien d'ordre $p \cdot q$.

2. Si φ et ψ sont deux morphismes non-triviaux de \mathbb{Z}_p dans $\text{Aut}(\mathbb{Z}_q)$, alors :

$$\mathbb{Z}_q \rtimes_{\varphi} \mathbb{Z}_p \cong \mathbb{Z}_q \rtimes_{\psi} \mathbb{Z}_p.$$

À isomorphisme près, il existe un unique produit semi-direct non-abélien de \mathbb{Z}_q avec \mathbb{Z}_p si p divise $q-1$.

Démonstration. Pour le premier point, $\mathbb{Z}_q \rtimes_{\varphi_{\beta}} \mathbb{Z}_p$ est non-commutatif :

$$\begin{aligned} (h, 0_{\mathbb{Z}_p})(0_{\mathbb{Z}_q}, k) &= (h, k) \\ (0_{\mathbb{Z}_q}, k)(h, 0_{\mathbb{Z}_p}) &= (\varphi_{\beta}(k)(h), k), \end{aligned}$$

et $\varphi_{\beta} \neq \text{Id}$ car φ_{β} est un morphisme non-trivial.

Pour le second point, on a φ et ψ deux morphismes non-triviaux. Alors $\text{Im } \varphi = \text{Im } \psi$ est l'unique sous-groupe de $\text{Aut}(\mathbb{Z}_q)$ engendré par $\beta^{\frac{q-1}{p}}$.

Si $\varphi(1) = \beta$ et $\psi(1) = \beta^k$, alors on a :

$$\psi = \varphi \circ \alpha,$$

où :

$$\alpha : \mathbb{Z}_p \rightarrow \mathbb{Z}_p : 1 \mapsto k.$$

On a donc l'isomorphisme entre les produits semi-directs. □

Théorème 5.10. Soient p et q deux nombres premiers avec $p < q$.

- Si p ne divise pas $q-1$, alors tout groupe d'ordre $p \cdot q$ est $\cong \mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$.
- Si p divise $q-1$, alors il existe, à isomorphisme près, exactement deux groupes distincts d'ordre pq :
 - le groupe cyclique $\mathbb{Z}_{pq} = \mathbb{Z}_p \times \mathbb{Z}_q$;
 - le groupe non-abélien $\mathbb{Z}_q \rtimes_{\varphi} \mathbb{Z}_p$.

Démonstration. Pour le premier point, soit G un groupe d'ordre pq . Il existe un unique p -Sylow H de G . On a :

$$|\{q\text{-Sylow}\}| = 1 + kq \text{ qui divise } |G| = pq.$$

Comme $1 + kq$ ne divise pas q , $1 + kq$ divise p , et donc $k = 0$. Le sous-groupe H est donc normal dans G ($H \cong \mathbb{Z}_q$).

Pour le second point, soit H le q -Sylow de G et K , un p -Sylow de G . Alors $G = HK$ et $H \cap K = \{e\}$ car $|H \cap K|$ divise à la fois $|H| = q$ et $|K| = p$ qui sont premiers entre eux.

H possède pq éléments distincts deux à deux. Supposons que $hk = h'k' \iff h'^{-1}h = k'k^{-1} \in H \cap K = \{e\}$, et donc $(h, k) = (h', k')$. □