

## DM n° 14 : Groupes

### Correction du problème 1 – Théorèmes de Sylow

#### Partie I – Étude des sous-groupes de Sylow de $\mathbb{Z}/n\mathbb{Z}$

1. • On a  $S = \{\overline{mk}, k \in \mathbb{Z}\}$ . En effet, l'inclusion directe est immédiate, et l'inclusion réciproque résulte du fait que si  $k \in \mathbb{Z}$ , et si  $r$  est le reste de la division euclidienne de  $k$  par  $p^\alpha$ , on a l'existence de  $q$  tel que

$$k = p^\alpha q + r, \quad \text{donc:} \quad km = p^\alpha mq + rm \equiv rm \pmod{n}.$$

Ainsi,  $\overline{km} \in S$ .

- Montrons que  $S$  est un sous-groupe de  $\mathbb{Z}/n\mathbb{Z}$ .

- \* De façon évidente,  $S \subset \mathbb{Z}/n\mathbb{Z}$ , et  $\overline{0} \in S$ .

- \* Soit  $(x, y) \in S^2$ . Il existe alors  $(k, \ell) \in \mathbb{Z}^2$  tels que  $x = \overline{mk}$  et  $y = \overline{m\ell}$ . On a alors  $x - y = \overline{m(k - \ell)} \in S$ . Ainsi, d'après la caractérisation des sous-groupes,  $S$  est un sous-groupe de  $\mathbb{Z}/n\mathbb{Z}$ .

- Soit  $(k, \ell) \in \llbracket 0, p^\alpha - 1 \rrbracket$  tels que  $k \neq \ell$ , alors  $|k - \ell| < p^\alpha$ , donc  $|m(k - \ell)| < n$ , donc  $mk \not\equiv m\ell \pmod{n}$ . On en déduit que  $\overline{mk} \neq \overline{m\ell}$ .

- Ainsi,  $S$  est constitué d'exactly  $p^\alpha$  éléments.  $S$  est donc un sous-groupe de Sylow de  $\mathbb{Z}/n\mathbb{Z}$ .

2. Soit  $S'$  un  $p$ -sous-groupe de Sylow de  $\mathbb{Z}/n\mathbb{Z}$ , et soit  $x \in S'$ .

- (a) L'élément  $x$  étant un élément du groupe  $S'$  d'ordre  $p^\alpha$ , on déduit du théorème de Lagrange que l'ordre de  $x$  divise  $p^\alpha$ , donc,  $p$  étant premier, l'ordre de  $x$  est  $p^\beta$ , pour un certain entier naturel  $\beta \leq \alpha$ .

- (b) On en déduit que  $\overline{p^\beta x} = 0$ , donc si  $k$  est un représentant dans  $\mathbb{Z}$  de  $x$ , il existe  $\ell \in \mathbb{Z}$  tel que  $p^\beta k = \ell n = \ell p^\alpha m$ , donc  $k = m\ell p^{\alpha-\beta}$ , et comme  $\alpha - \beta \geq 0$ ,  $x = \overline{k} \in S$ .

3. On en déduit que  $S' \subset S$ , et comme par définition,  $S$  et  $S'$  ont même cardinal fini,  $S' = S$ .

Ainsi,  $\mathbb{Z}/n\mathbb{Z}$  admet un unique sous-groupe de Sylow,  $S$ .

**Remarque :** Toute cette partie est en fait conséquence directe de la description générale des sous-groupes de  $\mathbb{Z}/n\mathbb{Z}$ , vue en exercice : ce sont les  $d\mathbb{Z}/n\mathbb{Z}$  où  $d$  divise  $n$ . Ces groupes sont de cardinal  $\frac{n}{d}$ . Le seul sous-groupe d'ordre  $p^\alpha$  est donc celui obtenu pour  $d = m$ . Il correspond bien à la description élémentaire donnée dans cette partie.

Pour rappel, la description des sous-groupes de  $\mathbb{Z}/n\mathbb{Z}$  s'obtient facilement à partir de la description des sous-groupes de  $\mathbb{Z}$ , qui sont les  $a\mathbb{Z}$ ,  $a \in \mathbb{N}$  (voir cours). En effet, en notant  $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  la projection canonique, qui est un morphisme de groupe, si  $G$  est un sous-groupe de  $\mathbb{Z}/n\mathbb{Z}$ ,  $\pi^{-1}(G)$  est un sous-groupe de  $\mathbb{Z}$ , donc de la forme  $d\mathbb{Z}$ . De plus, on doit avoir  $\pi(n) = 0 \in G$ , donc  $n \in d\mathbb{Z}$ , donc  $d$  est un diviseur de  $n$ . Enfin, en restreignant  $\pi$  à  $d\mathbb{Z}$ , on obtient un morphisme surjectif  $d\mathbb{Z} \rightarrow G$ , dont le noyau est  $n\mathbb{Z}$ . Avec le premier théorème d'isomorphisme démontré plus loin, on en déduit que  $G \simeq d\mathbb{Z}/n\mathbb{Z}$ , et on vérifie facilement que l'isomorphisme  $\tilde{\pi}$  obtenu en quotientant  $\pi$  correspond à l'inclusion de  $d\mathbb{Z}/n\mathbb{Z}$  dans  $\mathbb{Z}/n\mathbb{Z}$ .

Ce résultat peut aussi se montrer de façon élémentaire de la sorte : notant  $G = \{\overline{x_1}, \dots, \overline{x_k}\}$ , où les  $x_i$  sont des représentants des éléments 2 à 2 distincts de  $G$ , considérer  $d$  le pgcd des  $x_i$ , et montrer par double-inclusion que  $G = d\mathbb{Z}/n\mathbb{Z}$  (on pourra adapter la preuve du cours de la description des sous-groupes de  $\mathbb{Z}$ , en considérant la division euclidienne par  $d$ ).

#### Partie II – Actions de groupe, stabilisateurs, orbites

1. Quelques exemples.

- (a) • L'application donnant l'action de groupe est l'application de  $H \times G$  dans  $G$  donnée par  $h \cdot g = hg$  (où le point représente l'action de groupe, et le produit sans point représente la multiplication dans  $G$ ).  
 • On a bien, pour tout  $(h, h') \in H^2$ , et  $g \in G$ ,

$$h \cdot (h' \cdot g) = h \cdot (h'g) = h(h'g) = (hh')g = (hh') \cdot g,$$

l'avant-dernière égalité découlant de l'associativité dans  $G$ .

- On a également  $e_H \cdot g = e_H g = e_G g = g$ .

Ainsi,  $(h, g) \mapsto hg$  est une action du groupe  $H$  sur le groupe  $G$ .

L'orbite d'un élément  $g \in G$  est l'ensemble  $\{h \cdot g \mid h \in H\} = Hg$ , classe à droite modulo  $H$ .

- (b) La translation à droite ne définit pas une action si le groupe  $H$  n'est pas abélien, car en général, si on appelle  $\varphi$  l'application désignant cette loi de composition externe définie sur  $G$  :

$$\varphi(hh', g) = g(hh'),$$

alors que

$$\varphi(h, \varphi(h', g)) = g(h'h).$$

Pour avoir le premier axiome définissant une action de groupe, il faudrait avoir  $ghh' = gh'h$ , ce qui n'est pas vrai en toute généralité.

Pour régler le problème de l'inversion des deux termes, on peut faire précéder la multiplication à droite par  $h$  d'une opération qui justement inverse l'ordre des termes d'un produit, par exemple l'inversion :

$\psi : (h, g) \mapsto gh^{-1}$  définit une action de groupe puisque pour tout  $(h, h') \in H^2$  et tout  $g \in G$  :

- $\psi(e, g) = ge = g$
- $\psi(hh', g) = g(hh')^{-1} = gh'^{-1}h^{-1} = \psi(h, \psi(h', g))$ .

On peut aussi modifier la définition d'une action de groupe, en définissant une action de groupe à droite par  $(g, x) \mapsto xg$ , et en remplaçant le premier axiome par  $x \cdot (gg') = (x \cdot g) \cdot g'$ .

- (c) Vérifions que la conjugaison définit bien une action du groupe  $G$  sur lui-même. Ici encore on désigne avec un point l'action de groupe, et sans point le produit dans  $G$ . Pour tout  $(g, g', x) \in G^3$  :

- $e \cdot x = exe^{-1} = x$
- $(gg') \cdot x = (gg')x(gg')^{-1} = gg'xg'^{-1}g^{-1} = g \cdot (g'xg'^{-1}) = g \cdot (g' \cdot x)$ .

Ainsi, la conjugaison définit bien une action de  $G$  sur lui-même.

- (d) i. On note  $e$  le neutre de  $G$ . Soit  $H$  un sous-groupe de  $G$ ,  $g \in G$ , et  $H' = \{gxg^{-1}, x \in H\}$ . Montrons que  $H'$  est un sous-groupe de  $G$  :
- Puisque  $H$  est un sous-groupe de  $G$ ,  $e \in H$ , donc  $geg^{-1} \in H'$ , soit  $e \in H'$ .
  - Soit  $x'$  et  $y'$  dans  $H'$ . Il existe donc  $x$  et  $y$  dans  $H$  tels que  $x' = gxg^{-1}$  et  $y' = gyg^{-1}$ . On a alors :

$$x'y'^{-1} = gxg^{-1}(gyg^{-1})^{-1} = gxg^{-1}gy^{-1}g^{-1} = gxy^{-1}g^{-1}.$$

Or,  $H$  étant un sous-groupe de  $G$ ,  $xy^{-1} \in H$ , donc  $gxy^{-1}g^{-1} \in H'$ , soit  $x'y'^{-1} \in H'$ .

Ainsi, d'après la caractérisation des sous-groupes,  $H'$  est un sous-groupe de  $G$ , donc  $gHg^{-1} \in X$ .

- ii. • D'après la question précédente, l'application  $(g, H) \mapsto gHg^{-1}$  est bien définie de  $G \times X$  dans  $X$ .  
 • Soit  $H \in X$ , on a évidemment  $eHe^{-1} = H$   
 • Soit  $H \in X$ ,  $g, g' \in G$ . On a :

$$(gg') \cdot H = \{gg'x(gg')^{-1}, x \in H\} = \{g(g'xg'^{-1})g^{-1}, x \in H\} = \{gyg^{-1}, y \in g'Hg'^{-1}\} = g \cdot (g' \cdot H).$$

Ainsi,  $(g, H) \mapsto gHg^{-1}$  est une action du groupe  $G$  sur  $X$ .

2. Soit  $x \in X$ , et  $\text{Stab}(x)$  le stabilisateur de  $x$ . Montrons que  $\text{Stab}(x)$  est un sous-groupe de  $G$ .

- On a, par définition,  $\text{Stab}(x) \subset G$
- On a  $e \cdot x = x$ , par définition d'une action de groupe, donc  $e \in \text{Stab}(x)$ .

- Soit  $(g, h) \in \text{Stab}(x)^2$ . On a

$$(h^{-1}h) \cdot x = e \cdot x = x \quad \text{et} \quad (h^{-1}h) \cdot x = h^{-1} \cdot (h \cdot x) = h^{-1} \cdot x,$$

puisque  $h \in H_x$ . Ainsi,  $h^{-1} \cdot x = x$ , puis

$$(gh^{-1}) \cdot x = g \cdot (h^{-1} \cdot x) = g \cdot x = x,$$

puisque  $g \in \text{Stab}(x)$ . On en déduit que  $gh^{-1} \in \text{Stab}(x)$ .

D'après la caractérisation des sous-groupes,  $\boxed{\text{Stab}(x) \text{ est donc un sous-groupe de } G}$ .

3. (a) Montrons que  $\mathcal{R}$  est une relation d'équivalence :

- Soit  $x \in X$ , on a  $e \cdot x = x$ , donc  $x \in \omega(x)$ , donc  $x\mathcal{R}x$ , d'où la réflexivité de  $\mathcal{R}$ .
- Soit  $(x, y) \in X$  tel que  $x\mathcal{R}y$ . On a alors  $y \in \omega(x)$ , donc il existe  $g \in G$  tel que  $g \cdot x = y$ , donc

$$g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x,$$

donc  $x \in \omega(y)$ , d'où  $y\mathcal{R}x$ , d'où la symétrie de  $\mathcal{R}$ .

- Soit  $(x, y, z) \in X$  tel que  $x\mathcal{R}y$  et  $y\mathcal{R}z$ . On a alors  $y \in \omega(x)$  et  $z \in \omega(y)$ , d'où l'existence de  $g$  et  $h$  dans  $G$  tels que  $y = g \cdot x$  et  $z = h \cdot y$ , d'où  $z = h \cdot (g \cdot x) = (hg) \cdot x$ . Comme  $G$  est un groupe,  $hg \in G$ , donc  $z \in \omega(x)$ , d'où  $x\mathcal{R}z$ . D'où la transitivité de  $\mathcal{R}$ .

On déduit des trois points précédents que  $\boxed{\mathcal{R} \text{ est une relation d'équivalence}}$ .

- (b) Par définition même de  $\mathcal{R}$ , les classes d'équivalence pour la relation  $\mathcal{R}$  sont exactement les orbites de  $X$  sous l'action de  $G$ . Ainsi,  $\boxed{\text{l'ensemble des orbites forme une partition de } X}$ .

4. Soit  $G$  un groupe opérant sur un ensemble  $X$ . Soit  $x \in X$ .

- (a) Soit  $\varphi : g \mapsto g \cdot x$ , de  $G$  dans  $\omega(x)$ . Soit  $(g, g') \in G$  tels que  $g'^{-1}g \in \text{Stab}(x)$ . Alors

$$(g'^{-1}g) \cdot x = x \quad \text{donc} \quad g' \cdot x = g' \cdot ((g'^{-1}g) \cdot x) = (g'g'^{-1}) \cdot (g \cdot x) = e \cdot (g \cdot x) = g \cdot x.$$

Réciproquement, si  $g' \cdot x = g \cdot x$ , alors

$$(g'^{-1}g) \cdot x = g'^{-1} \cdot (g \cdot x) = g'^{-1} \cdot (g' \cdot x) = (g'^{-1}g') \cdot x = e \cdot x = x,$$

donc  $g'^{-1}g \in \text{Stab}(x)$ . Ainsi,  $\boxed{g'^{-1}g \in \text{Stab}(x) \text{ ssi } \varphi(g) = \varphi(g')}$ .

- (b) Soit  $x \in X$ . L'application  $\varphi : G \mapsto \omega(x)$  définie par  $g \mapsto g \cdot x$  est surjective, par définition d'une orbite. Soit  $y \in \omega(x)$ , et  $g$  tel que  $y = g \cdot x$ . D'après la question précédente,

$$\varphi^{-1}(\{y\}) = \{g' \in G \mid g^{-1}g' \in \text{Stab}(x)\}.$$

Or, par régularité de  $g$ ,  $g^{-1}g' \in \text{Stab}(x)$  équivaut à  $g' \in g\text{Stab}(x)$ . Ainsi,  $\varphi^{-1}(\{y\}) = g\text{Stab}(x)$ , dont le cardinal est égal à  $|\text{Stab}(x)|$  (d'après le cours, les classes de congruence modulo un sous-groupe ont toutes même cardinal). Ainsi, d'après le lemme des bergers, l'image réciproque de tout point ayant même cardinal,

on a  $|G| = |\text{Stab}(x)| \cdot |\omega(x)|$ , soit :  $\boxed{|\omega(x)| = \frac{|G|}{|\text{Stab}(x)|}}$ .

On peut aussi remarquer que l'application  $\varphi$  étant constante sur chaque classe  $g\text{Stab}(x)$ , elle passe au quotient, définissant une application (pas un morphisme) de  $(G/\text{Stab}(x))_g$  vers  $\omega(x)$ . L'équivalence de la question précédente permet de montrer l'injectivité, la surjectivité résultant celle de  $\varphi$ .

5. (a) Comme l'ensemble des orbites forme une partition de  $X$ , le cardinal de  $X$  est la somme des cardinaux des orbites. Or  $\sum_{i=1}^n |\Omega_i|$  est la somme des cardinaux des orbites non réduites à un point, et  $|X_G|$  est la somme des cardinaux des orbites réduites à un point (chaque orbite étant de cardinal 1, et ces orbites étant exactement les singletons dont l'unique élément est un point fixe de l'action). Ainsi, on a bien :

$$\boxed{|X| = |X_G| + \sum_{i=1}^n |\Omega_i|}.$$

- (b) Si  $G$  est d'ordre  $p^\alpha$ , les  $\Omega_i$  ont un cardinal strictement supérieur à 1, et divisant  $p^\alpha$  d'après 4(b). Ainsi, leur cardinal est  $p^\beta$  pour un certain  $\beta \in \llbracket 1, \alpha \rrbracket$ . On en déduit que pour tout  $i \in \llbracket 1, n \rrbracket$ ,  $|\Omega_i| \equiv 0 \pmod{p}$ .

Ainsi, en réduisant l'égalité de la question précédente modulo  $p$ , on obtient :

$$|X_G| \equiv |X| \pmod{p}.$$

- (c) Le centre  $Z(G)$  est égal à l'ensemble des points fixes de  $G$  sous l'action de  $G$  sur lui-même par conjugaison :  $g \cdot x = gxg^{-1}$ . Ainsi, d'après la question précédente,  $|Z(G)| \equiv |G| \equiv 0 \pmod{p}$ .

Comme par ailleurs  $Z(G)$  est non vide (car il contient le neutre), son cardinal est au moins  $p$ , donc

$$|Z(G)| \equiv 0 \pmod{p} \text{ n'est pas réduit au groupe trivial.}$$

### Partie III – Démonstration des théorèmes de Sylow par Wielandt

1. Soit  $E \in X$ , et  $g \in G$ . Alors,  $g$  étant régulier,  $x \mapsto g \cdot x$  est injective, et surjective de  $E$  dans  $g \cdot E$ , par définition de  $g \cdot E$ . Ainsi, il s'agit d'une bijection de  $E$  sur  $g \cdot E$ , donc  $|g \cdot E| = |E| = p^\alpha$ . On en déduit que  $g \cdot E \in X$ .

La preuve que la translation à gauche définit une action de  $G$  sur  $X$  est alors la même que la démonstration de la question 1(d).

2. Soit  $E \in X$ , et  $\text{Stab}(E)$  son stabilisateur par l'action définie dans la question précédente. Soit  $x \in E$ . Pour tout  $a \in \text{Stab}(E)$ ,  $a \cdot E = E$ , donc  $ax \in E$ . Considérons l'application  $\varphi_x : \text{Stab}(E) \rightarrow E$  définie par  $a \mapsto ax$ . Par régularité de  $x$  dans  $G$ ,  $\varphi_x$  est injective. Par conséquent,  $|\text{Stab}(E)| \leq |E| = p^\alpha$ .

3. (a) Si de plus,  $|\text{Stab}(E)| = p^\alpha$ , alors l'application  $\varphi_x$  est une injection entre deux ensembles finis de même cardinal, donc une bijection. On en déduit que

$$E = \text{Im}(\varphi_x) = \{ax \mid a \in \text{Stab}(E)\} = \text{Stab}(E) \cdot x.$$

Le choix de  $x \in E$  dans la question précédente était arbitraire.

- (b) Supposons qu'il existe  $S \in Y$  et  $x \in G$  tels que  $E = Sx$ . Par stabilité de  $S$ , tout élément  $g \in S$  est dans le stabilisateur de  $E$  :  $gE = gSx = Sx = E$ . Ainsi,  $S \subset \text{Stab}(E)$ .

Comme  $S$  est de cardinal  $p^\alpha$  et  $\text{Stab}(E)$  de cardinal au plus  $p^\alpha$ , cette inclusion est nécessairement une égalité :  $S = \text{Stab}(E)$ , puis  $|\text{Stab}(E)| = p^\alpha$ .

- (c) Soit  $S \neq S'$  dans  $Y$ . Considérons cette fois l'action sur  $E$ , définie par  $(X, g) \mapsto Xg^{-1}$ . On montre sans problème qu'il s'agit d'une action, comme en III-1. Pour éviter la confusion, notons  $\text{Stab}'(X)$  le stabilisateur de  $X$  sous cette action. En adaptant les arguments amenant III-3, on montre de même que si  $E = xS$  pour un élément  $x$  de  $G$  et un sous-groupe de Sylow  $S$ , alors  $\text{Stab}'(E) = S$  (en plus de la stabilité par produit de  $S$ , on utilise ici aussi la stabilité par inverse).

Supposons que deux sous-groupes de Sylow  $S$  et  $S'$  soient dans une même orbite sous l'action de  $G$ .

Il existe donc  $x$  dans  $G$  tel que  $S' = xS$ . On a aussi évidemment  $S' = eS'$ . La remarque précédente appliquée à ces deux égalités amènent, pour la première,  $\text{Stab}(S') = S$ , et pour la seconde,  $\text{Stab}(S') = S'$ . On en déduit que  $S = S'$ .

Ainsi, par contraposée, deux sous groupes de Sylow distincts ne peuvent pas être dans la même orbite.

On pouvait aussi s'en sortir de façon plus élémentaire, en remarquant que si  $S$  et  $S'$  sont dans la même orbite, il existe  $g$  tel que  $S' = g \cdot S$ , et comme le neutre  $e$  est dans  $S'$ , il existe  $g' \in S$  tel que  $gg' = e$ . Bien sûr,  $g' = g^{-1}$ , donc  $g^{-1} \in S$ , puis  $g \in S$ , puis  $S' = g \cdot S = S$ .

4. Puisque les orbites forment une partition de  $X$ , en notant  $\Omega$  l'ensemble des orbites, on obtient :

$$|X| = \sum_{\omega \in \Omega} |\omega|.$$

Or :

- Dans un premier temps, on peut remarquer que le cardinal de  $\text{Stab}(E)$  est le même pour tout élément  $E$  d'une même orbite  $\omega$ .

D'après III-2 et II-4(b), pour toute classe  $\omega$  telle que pour  $E \in \omega$ ,  $|\text{Stab}(E)| \neq p^\alpha$ , on a  $v_p(|\text{Stab}(E)|) < \alpha$ , donc d'après II-4(b),  $|\omega|$  est divisible par  $p$ . Ainsi, en notant  $\Omega'$  l'ensemble des classes telles que pour  $E \in \omega$ ,  $\text{Stab}(E)$  est de cardinal  $p^\alpha$ , on a :

$$|X| \equiv \sum_{\omega \in \Omega'} |\omega| [p].$$

- Toujours d'après II-4(b), pour tout élément  $\omega$  de  $\Omega'$ , le stabilisateur des éléments de  $\omega$  étant de cardinal  $p^\alpha$ , on a  $|\omega| = m$ . Ainsi,

$$|X| \equiv m|\Omega'| [p].$$

- Tout  $\omega$  de  $\Omega'$  contient un sous-groupe de Sylow (question 3(a) avec  $S = \text{Stab}(E)$ ) et un seul (question 3(c)). Réciproquement, d'après 3(b), l'orbite  $\omega$  d'un sous-groupe de Sylow  $S$  est dans  $\Omega'$ . Ainsi, tout sous-groupe de Sylow appartient à un élément  $\omega$  de  $\Omega'$ .

on en déduit qu'il y a autant de sous-groupes de Sylow que d'orbites  $\omega$  dans  $\Omega'$ ; ainsi  $|Y| = |\Omega'|$ , puis

$$\boxed{|X| \equiv m|Y| [p]}.$$

5. Le cardinal de  $X$  ne dépend pas de la structure de groupe de  $G$  mais seulement de son cardinal (il s'agit du nombre de sous-ensembles de  $G$  ayant  $p^\alpha$  élément). En particulier, ce cardinal est le même que celui de l'ensemble  $X'$  associé au groupe  $\mathbb{Z}/n\mathbb{Z}$ . En appliquant le résultat précédent au groupe  $\mathbb{Z}/n\mathbb{Z}$ , possédant un unique sous-groupe de Sylow d'après la partie 1, il vient donc :

$$|X| = |X'| \equiv m [p].$$

On revient donc au groupe  $G$  initial. On déduit de la question précédente que

$$m \equiv m|Y| [p],$$

et comme  $m$  est premier avec  $p^\alpha$ , donc aussi avec  $p$ ,  $m$  est inversible modulo  $p$ , donc

$$\boxed{|Y| \equiv 1 [p]}.$$

## Partie IV – Quatre lemmes

### 1. Lemme de Cauchy

- (a) Montrons que la loi donnée définit bien une action de  $\mathbb{Z}/p\mathbb{Z}$  sur  $E$

- Tout d'abord, soit  $\ell \in \llbracket 0, p-1 \rrbracket$  et  $(x_1, \dots, x_p) \in E$ . On a

$$\bar{\ell} \cdot (x_1, \dots, x_p) = (x_{\ell+1}, \dots, x_p, x_1, \dots, x_\ell).$$

Or,

$$(x_1 \cdots x_\ell)(x_{\ell+1} \cdots x_p) = e,$$

donc

$$x_1 \cdots x_\ell = (x_{\ell+1} \cdots x_p)^{-1},$$

donc

$$(x_{\ell+1} \cdots x_p) \cdot (x_1 \cdots x_\ell) = e.$$

On en déduit que  $\bar{\ell} \cdot (x_1, \dots, x_p)$  est encore un élément de  $E$ .

- Ici, contrairement à la définition et à tous les exemples traités ci-dessus, le groupe donnant l'action est noté additivement. Il faut faire attention à transcrire convenablement les propriétés requises pour l'action dans ce cadre. Tout d'abord,  $0 \cdot (y_1, \dots, y_p) = (y_{1+0}, \dots, y_{n+0}) = (y_1, \dots, y_p)$ .
- La deuxième condition est aussi vérifiée :

$$\alpha \cdot (\beta \cdot (y_1, \dots, y_p)) = \alpha \cdot (y_{1+\beta}, \dots, y_{p+\beta}) = (y_{1+\beta+\alpha}, \dots, y_{p+\beta+\alpha}) = (\alpha + \beta) \cdot (y_1, \dots, y_p).$$

Il s'agit donc bien d'une  $\boxed{\text{action de groupe}}$ .

- (b) Les points fixes sont les points dont toutes les coordonnées sont égales.

Ainsi, il s'agit des  $p$ -uplets  $(x, \dots, x)$  tels que  $x^p = 1$ .

Il y en a donc autant que de solutions de l'équation  $x^p = 1$ .

- (c) D'après II-5(b) (avec  $n = 1$ ), en notant  $G_p = \{x \mid x^p = 1\}$ , on a donc  $|E| \equiv |G_p| [p]$ . Or, un élément de  $E$  est déterminé par le choix quelconque des  $p - 1$  première coordonnées, imposant la dernière de façon unique :

$$y_p = (y_{p-1} \cdots y_1)^{-1}.$$

Par conséquent,  $|E| = n^{p-1} \equiv 0 [p]$ . Puisque  $p$  divise  $n$ ,  $|G_p| \equiv 0 [p]$ .

- (d) L'ensemble  $G_p$  est l'ensemble des éléments de  $G$  d'ordre divisant  $p$ , donc d'ordre 1 ou  $p$ . Il n'y a qu'un élément d'ordre 1 (le neutre), donc le nombre  $n_p$  d'éléments d'ordre  $p$  vérifie :

$$n_p \equiv -1 \equiv p - 1 [p].$$

**Remarque :** Le lemme de Cauchy étant très utile, il peut être intéressant de savoir faire rapidement sa preuve, mais en l'extrayant du contexte hors-programme des actions de groupe. On peut introduire la relation sur  $E$  définie par permutation circulaire des composantes du  $p$ -uplet. Si le  $p$ -uplet  $X = (x_1, \dots, x_p)$  n'est pas constitué de variables toutes égales, alors sa classe d'équivalence est de cardinal  $p$ . En effet, si ce n'est pas le cas, il existe une permutation circulaire non triviale (en décalant chaque coordonnée de  $k$ , avec  $k \in \llbracket 1, p - 1 \rrbracket$ ) laissant  $(x_1, \dots, x_p)$  invariant donc, avec les indices vus modulo  $p$ , pour tout  $n \in \mathbb{Z}$ ,  $x_{n+k} = x_n$ , et en itérant (dans un sens et dans l'autre),  $x_{n+\alpha k} = x_n$ , pour tout  $\alpha \in \mathbb{Z}$ . Comme  $k$  est premier avec  $p$ , il existe une relation de Bezout  $uk + vp = 1$ . On a alors, pour tout  $n \in \mathbb{Z}$ ,  $x_n = x_{n+uk} = x_{n+1-vp} = x_{n+1}$ , par  $p$ -périodicité de  $(x_n)$ , ce qui signifie bien que les  $x_i$  sont tous égaux. On termine alors de même que ci-dessus, en réduisant modulo  $p$  l'égalité entre le cardinal de  $E$  et la somme des cardinaux des classes d'équivalence, ne restant dans cette somme que les classes d'équivalence de cardinal 1, correspondant aux  $p$ -uplets  $(x, \dots, x)$ , avec  $x^p = 1$ . Le nombre de ces  $p$ -uplets est alors congru à 0 modulo  $p$ ; il s'agit aussi du nombre d'éléments  $x$  de  $G$  dont l'ordre divise  $p$ , donc est égal à 1 ou  $p$ . Comme  $e$  est le seul élément d'ordre 1, il reste bien  $p - 1$  modulo  $p$  éléments d'ordre  $p$ .

## 2. Image réciproque d'un sous-groupe

- Par définition,  $f^{-1}(K) \subset G$ .
- Puisque  $1_H \in K$  (car  $K$  est un sous-groupe), et puisque  $f(1_G) = 1_H$  (car  $f$  est un homomorphisme de groupes), on a bien  $1_G \in f^{-1}(K)$ .
- Soit  $(x, y) \in f^{-1}(K)$ . On a donc  $f(x) \in K$  et  $f(y) \in K$ . On a alors, par le fait que  $f$  est un homomorphisme de groupes, et par stabilité de  $K$  :

$$f(xy^{-1}) = f(x)f(y)^{-1} \in K.$$

Donc  $xy^{-1} \in f^{-1}(K)$ .

On déduit alors de la caractérisation des sous-groupes que  $f^{-1}(K)$  est un sous-groupe de  $G$ .

## 3. Groupes quotients

- (a) Les classes à gauche et à droite sont les mêmes. Or la partition des classes d'équivalences détermine de façon unique une relation d'équivalence. Ainsi, les relations  $\equiv_g$  et  $\equiv_d$  sont identiques. On notera simplement  $\equiv$  cette relation.
- (b) Soit  $(x, x', y, y') \in G^4$  tels que  $x \equiv x' [H]$  et  $y \equiv y' [H]$ . On a alors

$$x \in Hx' = x'H \quad \text{et} \quad y \in Hy',$$

Soit  $h$  et  $h'$  tels que  $x = x'h$  et  $y = h'y'$ . On a alors  $xy = x'hh'y'$

Or  $x'hh' \in x'H = Hx'$ , il existe donc  $h'' \in H'$  tel que  $x' = h''x'$ , puis  $xy = h''x'y'$ . Ainsi,  $xy \in Hx'y'$ , d'où  $xy \equiv x'y' [H]$ .

Ainsi,  $\equiv$  est une congruence pour la loi du groupe  $G$

- (c) • Soit  $C, D$  et  $E$  trois classes modulo  $H$ , et  $x, y, z$  des représentants dans  $G$  de ces classes. Alors, par définition, et par associativité dans  $G$  :

$$(C \times D) \times E = (\overline{xy})\overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x}(\overline{yz}) = C \times (D \times E).$$

D'où l'associativité de la loi définie sur  $G/H$ .

- On a  $H = \overline{1_G}$ . On a alors, pour toute classe  $C$ , de représentant  $x$  dans  $G$  :

$$H \times C = \overline{1_G} \times \overline{x} = \overline{1_G x} = \overline{x} = C.$$

Ainsi, il y a dans  $G/H$  un élément neutre, égal à  $H = \overline{1_G}$ .

- Soit  $C \in G/H$ , représentée par un élément  $x \in G$ . On a alors

$$x^{-1}x = 1_G = xx^{-1} \quad \text{donc:} \quad \overline{x^{-1}} \times \overline{x} = \overline{1_G} = \overline{x} \times \overline{x^{-1}}.$$

Ainsi,  $\overline{x^{-1}}$  est un symétrique de  $C$  dans  $G/H$

On a bien vérifié tous les axiomes d'une structure de groupe :  $G/H$  est bien muni d'une structure de groupe.

On peut remarquer que la loi de groupe est explicitement donnée par  $(aH) \cdot (bH) = (ab)H$ , ce qui est commode pour les manipulations. De plus, cette définition correspond aussi au produit terme à terme des éléments de  $aH$  et de  $bH$  (vérification facile).

#### 4. Premier théorème d'isomorphisme.

- (a) •  $\text{Ker}(f) = f^{-1}(\{e\})$  est un sous-groupe de  $G$  d'après la question (3).  
 • Montrons que  $\text{Ker}(f)$  est distingué dans  $G$ . Il suffit pour cela de montrer que si  $g \in G$  et  $h \in \text{Ker}(f)$ , alors  $ghg^{-1} \in \text{Ker}(f)$ . Soit donc  $g \in G$  et  $h \in \text{Ker}(f)$ . On a alors :

$$f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)1_H f(g)^{-1} = f(g)f(g)^{-1} = 1_H.$$

Ainsi,  $\text{Ker}(f)$  est un sous-groupe distingué de  $G$ .

- (b) Soit  $x \equiv y \pmod{\text{Ker}(f)}$ , on a donc  $xy^{-1} \in \text{Ker}(f)$ , d'où :

$$f(xy^{-1}) = 1_H \quad \text{soit:} \quad f(x)f(y)^{-1} = 1_H \quad \text{donc:} \quad f(x) = f(y).$$

Ainsi,  $f$  est constante sur chaque classe d'équivalence modulo  $\text{Ker}(f)$ . Elle induit donc une application  $\overline{f} : G/\text{Ker}(f) \rightarrow H$

- (c) • Soit  $C$  et  $D$  deux classes modulo  $\text{Ker}(f)$ , représentées par  $x$  et  $y$  respectivement. Supposons que  $\overline{f}(C) = \overline{f}(D)$ , soit  $f(x) = f(y)$ . On a alors

$$f(xy^{-1}) = f(x)f(y)^{-1} = 1_H, \quad \text{donc:} \quad xy^{-1} \in \text{Ker}(f).$$

On en déduit que  $x \equiv y \pmod{\text{Ker}(f)}$ , puis  $C = D$ . Donc  $\overline{f}$  est injective.

- Soit  $h \in H$ . Puisque par hypothèse,  $f$  est surjective, il existe  $x \in G$  tel que  $f(x) = h$ , donc  $\overline{f}(\overline{x}) = h$ , d'où la surjectivité de  $\overline{f}$ .

La fonction  $\overline{f}$  est injective et surjective, donc bijective.

- (d) On a donc  $|G/\text{Ker}(f)| = |H|$ . Or, on a vu dans le cours (cf démonstration du théorème de Lagrange) que

$$|G/\text{Ker}(f)| = \frac{|G|}{|\text{Ker}(f)|}.$$

On obtient donc la relation :  $|G| = |\text{Ker}(f)| \times |H|$ .

### Partie V – Une démonstration par récurrence du premier théorème de Sylow

1. On suppose dans cette question que  $G$  est abélien.

- (a) D'après le lemme de Cauchy, puisque  $p$  divise  $n$ , il existe un élément  $x$  d'ordre  $p$  dans  $G$ . Soit  $H = \{x^i, i \in \mathbb{Z}\}$  le sous-groupe monogène engendré par  $x$ .  $H$  est donc d'ordre  $p$ . Par ailleurs,  $G$  étant abélien, tout sous-groupe de  $G$  est évidemment distingué!

Ainsi, il existe bien un sous-groupe distingué  $H$  d'ordre  $p$ .

(b) Soit  $m \in \mathbb{N}$ , premier avec  $p$ .

Soit, pour tout  $\alpha$  dans  $\mathbb{N}$ , la propriété  $\mathcal{P}(\alpha)$ : Tout groupe abélien  $G$  d'ordre  $p^\alpha m$  admet un  $p$ -sous-groupe de Sylow.

Le cas  $\alpha = 0$  est trivial, un  $p$ -sous-groupe de Sylow étant dans ce cas d'ordre  $p^0 = 1$ . Le sous-groupe  $\{1_G\}$  convient.

Soit  $\alpha \in \mathbb{N}$ . On suppose que la propriété  $\mathcal{P}(\alpha)$  est vraie. Soit  $G$  un groupe abélien d'ordre  $p^{\alpha+1}m$ . D'après la question précédente (puisque  $\alpha + 1 > 0$ ),  $G$  admet un sous-groupe distingué  $H$  d'ordre  $p$ . Soit alors  $f : G \rightarrow G/H$  l'application qui à  $x$  associe sa classe  $\bar{x}$  modulo  $H$  (projection canonique). Puisque  $G/H$  est de cardinal  $p^\alpha m$  et est abélien, on peut lui appliquer l'hypothèse de récurrence : il existe un  $p$ -sous-groupe de Sylow  $S$  de  $G/H$ . On considère alors  $S' = f^{-1}(S)$ . D'après IV-2,  $S'$  est un sous-groupe de  $G/H$  et  $f$  se restreint en un morphisme de groupe surjectif  $\tilde{f}$  de  $S'$  sur  $S$ . Par ailleurs, puisque  $\text{Ker}(f) \subset S'$ , on a  $\text{Ker}(\tilde{f}) = \text{Ker}(f) = H$ . Ainsi, en appliquant IV-4(d) à  $\tilde{f}$ , il vient :

$$|S'| = |H| \times |S| \quad \text{donc:} \quad |S'| = p \times p^\alpha = p^{\alpha+1}.$$

On en déduit que  $S'$  est un  $p$ -sous-groupe de Sylow de  $G$ . On a bien prouvé  $\mathcal{P}(\alpha + 1)$ .

Par conséquent,  $\mathcal{P}(0)$  est vraie, et pour tout  $\alpha$  dans  $\mathbb{N}$ ,  $\mathcal{P}(\alpha)$  entraîne  $\mathcal{P}(\alpha + 1)$ . D'après le principe de récurrence,  $\mathcal{P}(\alpha)$  est vraie pour tout  $\alpha$  dans  $\mathbb{N}$ .

Ainsi, tout groupe abélien admet un  $p$ -sous-groupe de Sylow.

2. (a)
  - De façon évidente,  $Z(G) \subset G$  et  $1_G \in Z$ .
  - Soit  $(x, y) \in Z(G)^2$ . On a alors, pour tout  $g \in G$ ,

$$(xy)g = x(yg) = (yg)x = y(gx) = (gx)y = g(xy).$$

Ainsi,  $xy \in Z(G)$

- Soit  $x \in Z(G)$ . On a alors, pour tout  $g \in G$

$$g = (xx^{-1})g = x(x^{-1}g) = (x^{-1}g)x.$$

D'un autre côté :

$$g = g(x^{-1}x) = (gx^{-1})x.$$

Ainsi,  $(x^{-1}g)x = (gx^{-1})x$ , et  $x$  étant régulier,  $x^{-1}g = gx^{-1}$ . On en déduit que  $x^{-1} \in Z(G)$ .

Ainsi,  $Z(G)$  est un sous-groupe de  $G$ . De plus, tout élément de  $Z(G)$  commute avec tout élément de  $G$ , donc en particulier avec tout autre élément de  $Z(G)$ . Donc  $Z(G)$  est commutatif.

Puisque tout élément de  $Z(G)$  commute avec tout élément de  $G$ , pour tout  $z \in Z(G)$ , pour tout  $g \in G$ ,  $gzg^{-1} = gg^{-1}z = z \in Z(G)$ , donc  $Z(G)$  est distingué dans  $G$ .

- (b) Supposons que  $|Z(G)|$  soit non divisible par  $p$ . Les éléments de  $Z(G)$  sont les points fixes par l'action de  $G$  sur lui-même par conjugaison. Ainsi, d'après II-5(a), en notant  $\Omega'$  l'ensemble des orbites non réduites à un point pour cette action, on a :

$$|G| = |Z(G)| + \sum_{\omega \in \Omega'} |\omega|.$$

Si toutes les orbites  $\omega \in \Omega'$  sont de cardinal divisible par  $p$ , puisque  $p$  divise  $|G|$ , on obtient :  $0 \equiv |Z(G)| \pmod{p}$ , d'où une contradiction.

Ainsi, il existe au moins une classe  $\omega$  de cardinal différent de 1 et premier avec  $p$ .

- (c) Soit, pour tout  $n$  dans  $\mathbb{N}$ , la propriété  $\mathcal{P}(n)$ : Tout groupe d'ordre  $n$  admet un  $p$ -sous-groupe de Sylow.

La propriété est triviale pour  $n = 1$ .

Soit  $n > 1$ . On suppose que  $\mathcal{P}(1), \dots, \mathcal{P}(n-1)$  sont vrais. Soit  $G$  un groupe d'ordre  $n$ , et  $Z$  son centre. On écrit  $n = p^\alpha m$ , où  $p$  et  $m$  sont premiers entre eux. Si  $m = 1$ , le résultat est trivial ( $G$  est un  $p$ -sous-groupe de Sylow de lui-même). Supposons donc  $m > 1$ .



- Supposons  $|Z|$  premier avec  $p$ . Dans ce cas, il existe une orbite  $\omega$  non réduite à un point, de cardinal premier avec  $p$ , donc divisant  $m$ . Soit  $x \in \omega$  et  $\text{Stab}(x)$  le stabilisateur de  $x$ . Alors  $\text{Stab}(x)$  est un sous-groupe de  $G$ , et d'après II-4, son cardinal est  $p^\alpha k$ , où  $k = \frac{m}{|\omega|}$ . Comme  $|\omega| \neq 1$ ,  $p^\alpha k < n$ , et on peut donc appliquer l'hypothèse de récurrence à  $\text{Stab}(x)$ , qui admet un  $p$ -sous-groupe de Sylow, donc un sous-groupe  $S$  de cardinal  $p^\alpha$ . Ce sous-groupe est aussi sous-groupe de  $G$ , de cardinal  $p^\alpha$ . Il s'agit donc d'un  $p$ -sous-groupe de Sylow de  $G$ .
- Supposons  $|Z|$  non premier avec  $p$ . On note  $|Z| = p^\beta q$ , où  $p$  et  $q$  sont premiers entre eux ; on a alors  $1 \leq \beta \leq \alpha$ . Soit  $T$  un  $p$ -sous-groupe de Sylow  $T$  du groupe abélien  $Z$  (existe par la question 1,  $Z$  étant abélien, ce qui permet aussi de régler le cas éventuel où  $Z = G$ , cas dans lequel l'hypothèse de récurrence est inutilisable). Le groupe  $T$  est d'ordre  $p^\beta$ . par ailleurs,  $T$  est distingué dans  $G$  (même démonstration que pour  $Z$ ). On peut donc munir  $G/T$  d'une structure de groupe.

La projection  $f : G \longrightarrow G/T$ , qui à  $x$  associe sa classe  $\bar{x}$  modulo  $T$  est alors un morphisme de groupe surjectif, de noyau  $\text{Ker}(f) = T$ .

Par ailleurs  $|G/T| = p^{\alpha-\beta}m$ . Comme  $\beta > 0$ , on peut appliquer l'hypothèse de récurrence à  $G/T$  : soit  $U$  un  $p$ -sous-groupe de Sylow de  $G/T$ , donc de cardinal  $p^{\alpha-\beta}$ . On considère alors  $S = f^{-1}(U)$ . La restriction à  $S$  de  $f$  est surjective sur  $U$  et de noyau  $T$ , donc d'après le premier théorème d'isomorphisme,

$$|S| = |U| \times |T| = p^\alpha.$$

Ainsi,  $S$  est un sous-groupe de Sylow de  $G$ .

On a bien prouvé, dans tous les cas, que  $G$  admet un  $p$ -sous-groupe de Sylow.

Par conséquent,  $\mathcal{P}(n-1)$  est vraie, et pour tout  $n$  dans  $1, \mathcal{P}(n-1), \dots, \mathcal{P}(n-1)$  entraînent  $\mathcal{P}(n)$ . D'après le principe de récurrence forte,  $\mathcal{P}(n)$  est vraie pour tout  $n$  dans  $\mathbb{N}$ .

Ainsi, tout groupe fini admet un  $p$ -sous-groupe de Sylow.

## Partie VI – Démonstration des deuxième et troisième théorèmes de Sylow

1. Soit  $S$  un  $p$ -sous-groupe de Sylow de  $G$ . Soit  $H$  un  $p$ -sous-groupe de  $G$ . On fait opérer  $H$  sur l'ensemble  $X = (G/S)_g$  des classes à gauche  $xS$  par translation :  $h \cdot (xS) = (hx) \cdot S$ .

- (a) On a, d'après II-5(a) :

$$|X| = |X_H| + \sum_{\omega \in \Omega'} |\omega|,$$

où  $\Omega'$  est l'ensemble des orbites non réduites à un point. Or, d'après II-4(b), pour tout  $\omega \in \Omega'$ ,  $|\omega|$  divise  $|H|$ , donc est une puissance de  $p$ . Comme  $|\omega| \neq 1$ , on en déduit que  $|\omega| \equiv 0 \pmod{p}$ . Ainsi,

$$\boxed{|X_H| \equiv |X| = \frac{|G|}{|S|} = m \pmod{p}}.$$

- (b) Comme  $m$  n'est pas divisible par  $p$ , ceci implique qu'il existe au moins un point fixe, donc une classe  $xS$  telle que pour tout  $h \in H$ ,  $h(xS) = xS$ , puis  $h(xSx^{-1}) = xSx^{-1}$ .
- (c) Il n'est pas dur de voir que  $xSx^{-1}$  est un sous-groupe de  $G$ , et que son cardinal est  $p^\alpha$ . C'est donc un sous-groupe de Sylow. On a déjà justifié que dans ce cas, son stabilisateur pour l'action à gauche est lui-même (partie III). Or, le résultat précédent montre que tout  $h \in H$  est dans ce stabilisateur.

Ainsi,  $H$  est un sous-groupe du sous-groupe de Sylow  $xSx^{-1}$ .

2. Soit  $S$  et  $S'$  deux sous-groupes de Sylow. On applique le résultat précédent avec  $H = S'$ . On en déduit l'existence de  $x \in G$  tel que  $S' \subset xSx^{-1}$ , et pour des raisons de cardinalité, on en déduit que  $S' = xSx^{-1}$ .

Ainsi, les  $p$ -sous-groupes de Sylow sont deux à deux conjugués.

3. (a) Les  $p$ -Sylow étant deux à deux conjugués, et le conjugué d'un  $p$ -Sylow étant encore un  $p$ -Sylow,  $\Omega_S$  est très précisément l'ensemble  $Y$  des  $p$ -sous-groupes de Sylow.

- (b) Ainsi, d'après II-3(b),  $|Y| = |\Omega_S| = \frac{|G|}{|\text{Stab}(S)|}$ , le stabilisateur étant ici pris au sens de la conjugaison (ne pas s'embrouiller dans les différentes actions considérées).

Ceci permet de conclure de façon immédiate que  $|Y|$  divise  $n = |G|$ .

Le dernier point ( $|Y| \equiv 1 \pmod{p}$ ) a été démontré en partie III.