Lycée Louis-Le-Grand, Paris
MPSI 4 – Mathématiques
A. Troesch

Pour le 11/03/2019

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^α, on a l'existence de q tel que
$$k = p^\alpha q + r, \qquad \text{donc:} \qquad km = p^\alpha mq + rm \equiv rm\ [n].$$
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 $(k, \ell) \in [\![0, p^\alpha - 1]\!]$ tels que $k \neq \ell$, alors $|k - \ell| < p^\alpha$, donc $|m(k-\ell)| < n$, donc $mk \not\equiv m\ell[n]$. On en déduit que $\overline{mk} \neq \overline{m\ell}$.
• Ainsi, S est constitué d'exactement p^α éléments. $\boxed{S \text{ est donc un sous-groupe de Sylow de } \mathbb{Z}/n\mathbb{Z}}$.
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^α, on déduit du théorème de Lagrange que l'ordre de x divise p^α, donc, p étant premier, $\boxed{\text{l'ordre de } x \text{ est } p^\beta, \text{ pour un certain entier naturel } \beta \leqslant \alpha}$.
   (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 $\alpha - \beta \geqslant 0$, $\boxed{x = \overline{k} \in S}$.
3. On en déduit que $S' \subset S$, et comme par définition, S et S' ont même cardinal fini, $S' = S$.
Ainsi, $\boxed{\mathbb{Z}/n\mathbb{Z} \text{ admet un unique sous-groupe de Sylow, } S.}$

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^α 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 $\pi : /ZZ \to \mathbb{Z}/n\mathbb{Z}$ la projection canonique, qui est un morphisme de groupe, si G est un sous-groupe de $/ZZ/n\mathbb{Z}$, $\pi^{-1}(G)$ 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 π à $d\mathbb{Z}$, on obtient un morphisme surjectif $d\mathbb{Z} \to G$, 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 π 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 $\boxed{\{h \cdot g \mid h \in H\} = Hg}$, classe à droite modulo H.

(b) $\boxed{\text{La translation à droite ne définit pas une action}}$ si le groupe H n'est pas abélien, car en général, si on appelle φ 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 : $\boxed{\psi : (h, g) \mapsto gh^{-1}}$ 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) $inG \times X \mapsto x \cdot g$, 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 danbs 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, $\boxed{\text{la conjugaison définit bien une action de } G \text{ sur lui-même.}}$

(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 $\boxed{gHg^{-1} \in X}$.

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

2. Soit $x \in X$, et $\mathrm{Stab}(x)$ le stabilisateur de x. Montrons que $\mathrm{Stab}(x)$ est un sous-groupe de G.
- On a, par définition, $\mathrm{Stab}(x) \subset G$
- On a $e \cdot x = x$, par définition d'une action de groupe, donc $e \in H_x$.

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

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

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

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

3. (a) Montrons que $\mathcal{R}$ est une relation d'équivalence :
   - Soit $x \in X$, on a $e \times x = x$, donc $x \in \omega(x)$, donc $x\mathcal{R}x$, d'où la reflexivité 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 ${g'}^{-1}g \in \mathrm{Stab}(x)$. Alors

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

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

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

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

   (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,

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

   Or, par régularité de g, $g^{-1}g' \in \mathrm{Stab}(x)$ équivaut à $g' \in g\mathrm{Stab}(x)$. Ainsi, $\varphi^{-1}(\{y\}) = g\mathrm{Stab}(x)$, dont le cardinal est égal à $|\mathrm{Stab}(x)|$ (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 récirproque de tout point ayant même cardinal, on a $|G| = |\mathrm{Stab}(x)|\cdot|\omega(x)|$, soit : $\boxed{|\omega(x)| = \dfrac{|G|}{|\mathrm{Stab}(x)|}}$.

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

5. (a) Comme l'ensemble des orbites forme une partition de X, le cardinal de X est la somme des cardinaux des orbites. Or $\displaystyle\sum_{i=1}^{n} |\Omega_i|$ 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^α, les Ω_i ont un cardinal strictement supérieur à 1, et divisant p^α d'après 4(b). Ainsi, leur cardinal est p^β pour un certain $\beta \in [\![1, \alpha]\!]$. On en déduit que pour tout $i \in [\![1, n]\!]$, $|\Omega_i| \equiv 0\ [p]$.

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

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

(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, $|Z(G)| \equiv |G| \equiv 0\ [p]$.

Comme par ailleurs $Z(G)$ est non vide (car il contient le neutre), son cardinal est au moins p, donc $\boxed{Z(G) \text{ n'est pas réduit au groupe trivial}}$.

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 $\boxed{\text{action de } G \text{ sur } X}$ est alors la même que la démonstration de la question 1(d).

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

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

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

   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, $S \subset \mathrm{Stab}(E)$.

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

   (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 $\mathrm{Stab}'(X)$ 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 $\mathrm{Stab}'(E) = S$ (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, $\mathrm{Stab}(S') = S$, et pour la seconde, $\mathrm{Stab}(S') = S'$. On en déduit que $S = S'$.

   Ainsi, par contraposée, $\boxed{\text{deux sous groupes de Sylow distincts ne peuvent pas être dans la même orbite}}$.

   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 Ω l'ensemble des orbites, on obtient :

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

   Or :

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

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

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

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

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

- Tout ω de Ω' contient un sous-groupe de Sylow (question 3(a) avec $S = \mathrm{Stab}(E)$) et un seul (question 3(c)). Réciproquement, d'après 3(b), l'orbite ω d'un sous-groupe de Sylow S est dans Ω'. Ainsi, tout sous-groupe de Sylow appartient à un élément ω de Ω'.
  on en déduit qu'il y a autant de sous-groupes de Sylow que d'orbites ω dans Ω' ; 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^α 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^α, 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 $\ell \in [\![0, p-1]\!]$ et $(x_1, \cdots, x_p) \in E$. On a

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

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 $\overline{\ell} \cdot (x_1, \cdots, x_p)$ 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, $0 \cdot (y_1, \cdots, y_p) = (y_{1+0}, \cdots y_{n+0}) = (y_1, \cdots y_p)$.
- La deuxième condition est aussi vérifiée :

$$\alpha \cdot (\beta \cdot (y_1, \ldots, y_p)) = a \cdot (y_{1+\beta}, \cdots, y_{p+\beta}) = (y_{1+\beta+\alpha}, \ldots, y_{p+\beta+\alpha}) = (\alpha + \beta) \cdot (y_1, \ldots, y_n).$$

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 $\boxed{(x,\dots,x) \text{ tels que } x^p = 1}$.
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, $\boxed{|G_p| \equiv 0\ [p]}$.

(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 :

$$\boxed{n_p \equiv -1 \equiv p-1\ [p]}.$$

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 $k \in [\![1, p-1]\!]$) 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 $\boxed{f^{-1}(K) \text{ est un sous-groupe de } G}$.

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 $\boxed{\equiv_g \text{ et } \equiv_d \text{ sont identiques}}$. 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

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

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, $\boxed{\equiv \text{ est une congruence pour la loi du groupe } G}$

(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

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

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

On a bien vérifié tous les axiomes d'une structure de groupe : $\boxed{G/H \text{ est bien muni d'une structure de groupe}}$.
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)
- $\mathrm{Ker}(f) = f^{-1}(\{e\})$ est un sous-groupe de G d'après la question (3).
- Montrons que $\mathrm{Ker}(f)$ est distingué dans G. Il suffit pour cela de montrer que si $g \in G$ et $h \in \mathrm{Ker}(f)$, alors $ghg^{-1} \in \mathrm{Ker}(f)$. Soit donc $g \in G$ et $h \in \mathrm{Ker}(f)$. 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, $\boxed{\mathrm{Ker}(f) \text{ est un sous-groupe distingué de } G.}$

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

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

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

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

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

  On en déduit que $x \equiv y\ [H]$, 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 $\overline{f}$.

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

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

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

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

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, $\boxed{\text{il existe bien un sous-groupe distingué } H \text{ d'ordre } p}$.

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

Soit, pour tout α 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 $f : G \longrightarrow G/H$ l'application qui à x associe sa classe $\overline{x}$ 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 $\mathrm{Ker}(f) \subset S'$, on a $\mathrm{Ker}(\tilde{f}) = \mathrm{Ker}(f) = H$. Ainsi, en appliquant IV-4(d) à $\tilde{f}$, il vient :

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

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

Ainsi, $\boxed{\text{tout groupe abélien admet un } p\text{-sous-groupe de Sylow.}}$

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

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 $\boxed{Z(G) \text{ est distingué dans } G}$.

(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 Ω' 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 : $0 \equiv |Z(G)|\ [p]$, d'où une contradiction.

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

(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 $\mathcal{P}(1), \ldots, \mathcal{P}(n-1)$ 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 ω non réduite à un point, de cardinal premier avec p, donc divisant m. Soit $x \in \omega$ et $\mathrm{Stab}(x)$ le stabilisateur de x. Alors $\mathrm{Stab}(x)$ 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 $\mathrm{Stab}(x)$, qui admet un p-sous-groupe de Sylow, donc un sous-groupe S de cardinal p^α. Ce sous-groupe est aussi sous-groupe de G, de cardinal p^α. 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 $1 \leqslant \beta \leqslant \alpha$. 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^β. 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 $\overline{x}$ modulo T est alors un morphisme de groupe surjectif, de noyau $\mathrm{Ker}(f) = T$.
  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'isomophisme,
  $$|S| = |U| \times |T| = p^\alpha.$$
  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, $\mathcal{P}(n-1), \ldots, \mathcal{P}(n-1)$ entraînent $\mathcal{P}(n)$. D'après le principe de récurrence forte, $\mathcal{P}(n)$ est vraie pour tout n dans $\mathbb{N}$.

Ainsi, $\boxed{\text{tout groupe fini admet un } p\text{-sous-groupe de Sylow}}$.

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) :
   $$|X| = |X_H| + \sum_{o m \in \Omega'} |\omega|,$$
   où Ω' 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 $|\omega| \equiv 0\ [p]$. Ainsi,
   $$\boxed{|X_H| \equiv |X| = \frac{|G|}{|S|} = m \mod [p]}.$$
   (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 $\boxed{h(xSx^{-1}) = xSx^{-1}}$.
   (c) Il n'est pas dur de voir que xSx^{-1} est un sous-groupe de G, et que son cardinal est p^α. 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, $\boxed{H \text{ est un sous-groupe du sous-groupe de Sylow } xSx^{-1}}$.
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 $\boxed{S' = xSx^{-1}}$.
   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, Ω_S est très précisément $\boxed{\text{l'ensemble } Y \text{ des } p\text{-sous-groupes de Sylow}}$.
   (b) Ainsi, d'après II-3(b), $\boxed{|Y| = |\Omega_S| = \frac{|G|}{|\mathrm{Stab}(S)|}}$, 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 $\boxed{|Y| \text{ divise } n = |G|}$.
Le dernier point ($|Y| \equiv 1\ [p]$) a été démontré en partie III.