Lycée Lakanal, Sceaux
MP – Mathématiques
A. Troesch

Pour le 20/11/2024, 21h00

DM n° 8 : structures algébriques

Ce DM est à rendre au format numérique, scanné en pdf en un seul fichier n'excédant pas 10 Mo. L'envoi se fera via Cahier-de-Prépa avant la date et heure ci-dessus.

Le problème 1 présente la classification (et donc la description complète) de tous les groupes abéliens finiment engendrés. Il est assez progressif, et quelques questions sont vraiment dures en fin de sujet (IV-4 et V-2 notamment). Mais réfléchissez-y quand-même !

Le problème 2 est facultatif (à ne pas rendre). Il porte sur un résultat qui est la base de l'étude générale de la structure des groupes. La démonstration utilise un certain nombre de techniques très classiques et importantes sur les groupes : actions de groupe, équation aux classes, conjugaison, lemme de Cauchy, quotients de groupes etc. Ce sont des notions et des thèmes qu'on peut retrouver dans les concours les plus prestigieux.

Dans les deux problèmes, on parle un peu d'ensembles quotients et de groupes quotients. Voici quelques rappels utiles :

- si $\mathcal{R}$ est une relation d'équivalence sur E, l'ensemble quotient est l'ensemble formé des classes d'équivalence. C'est donc une partition de E. Par exemple, l'ensemble des classes d'équivalence pour la relation de congruence modulo n est $\mathbb{Z}/n/ZZ$. L'ensemble quotient est noté $E/\mathcal{R}$
- Si E est muni d'une opération $+$, on dit qu'une relation d'équivalence $\mathcal{R}$ est une congruence si elle respecte $+$, c'est-à-dire :
$$x\mathcal{R}x' \text{ et } y\mathcal{R}y' \Longrightarrow (x+y)\mathcal{R}(x'+y').$$
Ainsi, la classe d'équivalence de $x+y$ ne dépend que de la classe d'équivalence de x et de celle de y, et pas des représentants choisis. C'est cette condition qui permet de « passer l'opération $+$ au quotient », de sorte à définir une opération compatible sur E.
C'est comme cela qu'on a défini les opérations sur $\mathbb{Z}/n\mathbb{Z}$ dans le cours.
- Si G est un groupe abélien, et H est un sous-groupe de G, une classe modulo H est un ensemble aH (en notation multiplicative) ou $a+H$ (en notation additive). Par analogie avec $n\mathbb{Z}$, cela permet de définir une notion de congruence. Si on se place en notation additive, on dit que y est congru à a modulo H si $y \in a+H$, donc si $y-a \in H$. Cela définit une relation d'équivalence.
Par exemple, si $G=\mathbb{Z}$ et $H=n\mathbb{Z}$, la congruence modulo $n\mathbb{Z}$ correspond à la congruence modulo n que vous connaissez.
- Dans le cas multiplicatif commutatif, de même, y et congru à a ssi $ya^{-1} \in H$, c'est-à-dire $y=aH$.
- Les classes d'équivalence pour cette relation (en notation additive) sont les classe modulo H, à savoir les aH. On retrouve la partition introduite en cours pour étudier le théorème de Lagrange. On montre facilement (dans le cas abélien) que la relation de congruence modulo H porte bien son nom, dans le sens où c'est une congruence pour la loi $+$. On peut donc passer la loi au quotient, en la définissant directement sur les classes modulo H. Concrètement, cela définit un produit sur les classes
$$(aH)\cdot(bH)=(ab)H.$$
Cette loi définit alors une structure de groupe sur l'ensemble des classes. C'est ce qu'on appelle le groupe quotient de G par H, et on le note G/H.
- Le cas de $\mathbb{Z}/n\mathbb{Z}$ est un cas particulier de cette construction, avec $G=\mathbb{Z}$ et $H=n\mathbb{Z}$.
- Dans le cas non commutatif, les choses sont un peu plus compliquées. Il faut distinguer les classes à gauche Ha et les classes à droite aH. On peut toujours définir des relations de congruence à gauche, et congruence à droite modulo H. Mais cette fois, ces relations portent mal leur nom, puisqu'en général, ce ne sont pas des congruences pour $+$. Une condition suffisante (mais en fait aussi nécessaire) pour que ce soit le cas est que pour tout a, $aH=Ha$. On dit dans ce cas que H est un sous-groupe normal (ou distingué) de G. Et c'est donc la condition pour pouvoir passer $+$ au quotient. On vérifie facilement alors que cela définit encore. une structure de groupe sur le quotient.

Problème 1 – Structure des groupes abéliens de type fini

On dit qu'un groupe abélien G (noté additivement) est de type fini s'il existe un système générateur (ou famille génératrice) fini(e) X de G, autrement dit, s'il existe un nombre fini d'éléments $(x_i)_{i\in[\![1,n]\!]}$ tels que

$$G = \langle x_1\rangle + \langle x_2\rangle + \cdots + \langle x_n\rangle = \{\alpha_1 x_1 + \cdots + \alpha_n x_n, \quad (\alpha_1,\ldots,\alpha_n) \in \mathbb{Z}^n\}.$$

Le but de ce problème est de montrer le théorème de structure des groupes abéliens de type fini, stipulant que tout groupe abélien de type fini est isomorphe à un groupe

$$\mathbb{Z}^k \times (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_\ell\mathbb{Z}),$$

où on a une chaîne de divisibilité $d_\ell \mid d_{\ell-1} \mid \cdots \mid d_1$, avec $d_1 \geqslant 2$.
Dans tout le problème, les groupes sont supposés abéliens, et notés additivement.

Partie I – Sommes directes

Soit G un groupe abélien (additif), et H_1 et H_2 deux sous-groupes de G. On définit la somme

$$H_1 + H_2 = \{h_1 + h_2 \mid h_1 \in H_1, h_2 \in H_2\}.$$

On dit que la somme est directe si pour tout $x \in H_1 + H_2$, l'écriture de x sous la forme $x = h_1 + h_2$ est unique (avec $h_1 \in H_1$ et $h_2 \in H_2$) On désigne dans ce cas par $H_1 \oplus H_2$ la somme directe.

1. Dans $\mathbb{Z}^2$, soit $H_1 = \mathbb{Z}\cdot(2,1) = \{n(2,1), n \in \mathbb{Z}\}$ et $H_2 = \mathbb{Z}\cdot(0,2)$. Décrire la somme $H_1 + H_2$. Est-elle directe ?
2. Dans $(\mathbb{Z},+)$, décrire la somme $a\mathbb{Z} + b\mathbb{Z}$, où $(a,b) \in (\mathbb{Z}^*)^2$. Est-elle directe ?
3. Soit H_1 et H_2 deux sous-groupes d'un groupe abélien G.
   (a) Montrer que $H_1 + H_2$ est un sous-groupe de G.
   (b) Montrer que si $H_1 + H_2$ est directe, alors les groupes $H_1 \oplus H_2$ et $H_1 \times H_2$ sont isomorphes.
4. Montrer que si H_1, H_2 et H_3 sont des sous-groupes d'un groupe abélien G, on a :

   $$(H_1 + H_2) + H_3 = H_1 + (H_2 + H_3),$$

   et que si les deux sommes du membre de gauche sont directes, il en est de même des deux sommes du membre de droite. Cela nous autorise à écrire plus simplement $H_1 + H_2 + H_3$, et dans le cas où les sommes sont directes, $H_1 \oplus H_2 \oplus H_3$, et plus généralement $H_1 + \cdots + H_n$ et $H_1 \oplus \cdots \oplus H_n$.

Partie II – Groupes abéliens libres de type fini

- *On définit de façon plus générale une somme d'une infinité de sous-groupes $(H_i)_{i\in I}$ par*

  $$\sum_{i\in I} H_i = \left\{ \sum_{i\in I} h_i \mid h_i \in H_i, \text{ presque tous nuls} \right\},$$

  ce qui signifie que dans chacun des sommes, seul un nombre fini *de termes h_i est non nul. On dit que la somme est directe (et on la note alors $\bigoplus_{i\in I} H_i$) si tout élément de la somme se décompose de façon unique de cette manière.*
- *Une partie X de G est génératrice si $< X >= G$. Une famille $(x_i)_{i\in I}$ d'éléments de G est génératrice si $\{x_i, i \in I\}$ est une partie génératrice.*
- *On dit qu'un groupe abélien G est libre s'il existe une famille génératrice $(x_i)_{i\in I} \in G^I$ tel que pour tout tout $i \in I$, $\langle x_i\rangle$ est isomorphe à $\mathbb{Z}$, et tel que*

  $$G = \bigoplus_{i\in I} \langle x_i\rangle .$$

  On dit dans ce cas que $(x_i)_{i\in I}$ est une base de G.
- *On dit qu'un groupe abélien G est de type fini s'il existe une famille génératrice finie $(x_1,\ldots,x_n)$ de G.*

On se donne un groupe abélien G, supposé libre et de type fini.

1. Soit $(x_1,\ldots,x_n)$ une famille génératrice finie. Soit $(y_i)_{i\in I}$ une base infinie de G. En considérant les décompositions des x_i en sommes de y_i, montrer qu'il existe une sous-famille finie $(y_i)_{i\in J}$ de $(y_i)_{i\in I}$ telle que pour tout $\ell \in [\![1,n]\!]$, $x_\ell \in \bigoplus_{j\in J} \langle y_j\rangle$.
   En déduire que toute base de G est finie.

2. Soit $(x_1, \ldots, x_n)$ une base de G. Soit $\varphi : G \mapsto G$ définie par $x \mapsto 2x$.
   (a) Montrer que φ est un morphisme de groupes.
   (b) Montrer que $\varphi(G)$ est un groupe libre dont une base est donnée par $(2x_1, \ldots, 2x_n)$.
   (c) Quel est le cardinal de l'ensemble des classes de G modulo $\varphi(G)$?
3. Déduire du résultat précédent que toute base de G est de cardinal n. Ce cardinal commun est appelé rang du groupe libre G.

Partie III – Groupes abéliens sans torsion

- *On dit qu'un groupe abélien G est sans torsion si tout $x \neq 0$, x est d'ordre infini.*
- *On dit qu'un groupe abélien G est un groupe de torsion si tout $x \in G$ est d'ordre fini.*
- *On dit qu'un groupe abélien est de type fini s'il admet une famille génératrice finie.*

1. $\mathbb{Q}$ est-il un groupe de torsion ? un groupe sans torsion ? Même question pour le groupe quotient $\mathbb{Q}/\mathbb{Z}$. Même question pour $\mathbb{C}^*$.
2. Montrer qu'un groupe abélien libre est sans torsion.
3. On veut montrer que réciproquement, un groupe sans torsion de type fini est libre. Soit G un groupe abélien de type fini, sans torsion.
   (a) On suppose que G n'admet pas de base. Justifier, pour toute famille génératrice X de cardinal fini, l'existence du minimum m_X de l'ensemble
   $$C_X = \left\{ \sum_{x \in X} |n_x| \;\middle|\; n_x \in \mathbb{Z} \text{ non tous nuls et } \sum_{x \in X} n_x x = 0. \right\},$$
   puis l'existence d'une famille génératrice X de cardinal minimal n telle que m_X soit minimale parmi les familles génératrices de cardinal n. On se donne une telle famille et des coefficients n_x associés réalisant le minimum m_X.
   (b) Montrer que l'existence d'un élément $x \in X$ tel que $|n_x| = 1$ contredirait la minimalité du cardinal de X.
   (c) On suppose donc que pour tout $x \in X$, $|n_x| \neq 1$. Justifier qu'il existe x et y dans X tels que $0 < |n_x| < |n_y|$ et $|n_x|$ ne divise pas $|n_y|$.
   (d) En effectuant la division euclidienne de $|n_y|$ par $|n_x|$, trouver une famille génératrice de G contredisant la minimalité de m_X.
4. En déduire que tout groupe libre de type fini sans torsion est isomorphe à un groupe $\mathbb{Z}^n$, et ceci pour une unique valeur de n.

Partie IV – Groupes de torsion

On suppose ici que G est un groupe abélien de torsion de type fini non réduit à $\{0\}$.

1. Montrer que G est un groupe fini.
2. Soit x un élément de G d'ordre maximal, cet ordre étant noté d_1. Montrer que pour tout y de G, l'ordre de y divise d_1.
3. Soit H le sous-groupe de G engendré par x. Justifier que la loi de groupe de G passe au quotient sur l'ensemble G/H des classes d'équivalence modulo H, et qu'elles définissent sur G/H une structure de groupe.

*4. Justifier que G est isomorphe à $H \times G/H$.

Indication : Contruire un morphisme de G sur H prolongeant l'identité de H. Pour cela considérer l'ensemble des couples (K, φ) où K est un sous-groupe intermédiaire entre H et G, et φ prolonge l'identité, et le munir d'un ordre (inclusion, et prolongement des fonctions). Considérer un élément maximal, et si $K \neq G$, essayer de prolonger en un $y \notin K$. Pour $ny \in K$, avec $n > 0$ minimal, cela implique de choisir $\varphi(y)$ tel que $n\varphi(y) = \varphi(ny)$, ce dernier étant connu. Donc il faut réussir à « diviser » $\varphi(ny)$ par n dans H. On peut le faire directement, ou bien en remarquant que H est isomorphe à un $\mathbb{U}_m$, et donc plonger le problème dans $\mathbb{U}$ où la division (multiplicativement, c'est la racine) se fait bien, puis revenir à $\mathbb{U}_m$, en se servant de la maximalité de l'ordre de x.

5. En déduire qu'il existe une chaîne d'entiers strictement supérieurs à 1, tels que $d_\ell \mid d_{\ell-1} \mid \cdots \mid d_1$, telle que G soit isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_\ell\mathbb{Z}$.

Partie V – Théorème de structure des groupes de type fini

On démontre ici le résultat annoncé dans l'introduction. On se donne G un groupe abélien de type fini, et on définit $T(G)$ le sous-ensemble de G formé des éléments d'ordre fini de G.

1. Montrer que $T(G)$ est un sous-groupe de G, et que le groupe quotient $G/T(G)$ est un groupe libre de type fini et sans torsion.
2. En déduire le théorème de structure donné dans l'introduction du problème.
3. Démontrer l'unicité des exposants n et d_i.

Le problème suivant n'est pas à rendre.

Problème 2 – Théorèmes de Sylow

Le but de ce problème est de démontrer des théorèmes d'existence de certains p-sous-groupes d'un groupe fini donné. Pour tout entier premier p, on appelle p-groupe un groupe dont le cardinal est p^k, pour un certain entier k. Soit G un groupe fini quelconque. On considère α tel que $n = p^\alpha m$, où $p^\alpha \wedge m = 1$. Autrement dit, α est la p-valuation de n. On appelle p-sous-groupe de Sylow de G un sous-groupe de cardinal p^α.

Le premier théorème de Sylow affirme l'existence d'un p-sous-groupe de Sylow. Le second affirme que tous les sous-groupes de Sylow sont conjugués, dans un sens qui sera défini dans la partie II. Le troisième théorème de Sylow précise le résultat en affirmant que le nombre de p-sous-groupes de Sylow divise n et est congru à 1 modulo p.

Nous démontrons dans ce problème le premier théorème de Sylow, de deux façons différentes, et une partie du troisième.

Nous rappelons le théorème de Lagrange, théoriquement hors-programme, selon lequel l'ordre d'un sous-groupe H de G divise l'ordre de G, dont on déduit en particulier que l'ordre de tout élément de G divise l'ordre de G.

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

Nous étudions dans cette partie le cas simple des p-sous-groupes de Sylow du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$. Nous supposons que $n = p^\alpha m$, où p est premier et $p^\alpha \wedge m = 1$, avec $\alpha > 0$.

1. Soit $S = \{\overline{mk}, k \in [\![0, p^\alpha - 1]\!]\} \subset \mathbb{Z}/n\mathbb{Z}$. Montrer que S est un p-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) Justifier l'existence d'un entier naturel β tel que l'ordre de x soit p^β.
   (b) En déduire que $x \in S$.
3. Montrer que S est l'unique p-sous-groupe de Sylow de $\mathbb{Z}/n\mathbb{Z}$.

Cela prouve les deux théorèmes de Sylow pour les groupes $\mathbb{Z}/n\mathbb{Z}$.

Partie II – Actions de groupe, stabilisateurs, orbites

Soit $(G, \times)$ un groupe, de neutre e, et X un ensemble. On appelle ***action du groupe*** *G* ***sur*** *X la donnée d'une application (correspondant à une loi de composition externe sur X d'ensemble d'opérateur G) :*

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g \cdot x \end{array}$$

vérifiant les deux axiomes suivants :

(i) $\forall (g, g') \in G, \quad \forall x \in X, \quad g \cdot (g' \cdot x) = (gg') \cdot x$

(ii) $\forall x \in X, \quad e \cdot x = x.$

On dit que G opère sur X via *l'action ci-dessus.*
Étant donné un groupe G opérant sur X, on définit pour tout $x \in X$ respectivement l'orbite et le stabilisateur de x par :

$$\omega(x) = \{g \cdot x, \quad g \in G\} \qquad et \qquad \mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\}.$$

1. Quelques exemples.
   (a) Étant donné un sous-groupe H de G, montrer que H opère « par translation à gauche » sur G, via l'action $(h, g) \in H \times G \mapsto h \cdot g = hg$. Décrire les orbites de G sous cette action.

(b) La « translation à droite » $(h, g) \mapsto gh$ définit-elle une action de groupe ? Si non, comment modifier sa définition pour en faire une action de groupe ?

(c) Étant donné un groupe G, montrer que G opère sur lui-même « par automorphisme intérieur » ou « par conjugaison » via l'action $(g, a) \mapsto g \cdot a = gag^{-1}$. Les orbites sous cette action sont appelées classes de conjugaison. Deux éléments a et b situées dans une orbite commune sont dits conjugués.

(d) Soit G un groupe, et X l'ensemble de ses sous-groupes.

i. Montrer que pour tout $H \in X$ et tout $g \in G$, $\{gxg^{-1},\ x \in H\}$, est un sous-groupe de G. On le note gHg^{-1}.

ii. Montrer que G opère sur X via l'action $(g, H) \mapsto gHg^{-1}$.

Deux sous-groupes H et H' sont dits conjugués s'ils sont dans la même orbite sous cette action, ce qui revient à dire qu'il existe $g \in G$ tel que $H' = gHg^{-1}$.

2. Soit G un groupe opérant sur un ensemble X, et soit $x \in X$. Montrer que le stabilisateur $\mathrm{Stab}(x)$ de x est un sous-groupe de G.

3. Soit G un groupe opérant sur un ensemble X, et soit $\mathcal{R}$ la relation sur X définie par : $x\mathcal{R}y$ si et seulement si $y \in \omega(x)$.

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

(b) En déduire que 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 $\varphi : G \to \omega(x)$ définie par $\varphi(g) = g \cdot x$. Montrer que $g'^{-1}g \in \mathrm{Stab}(x)$ si et seulement si $\varphi(g) = \varphi(g')$.

(b) En déduire que $|\omega(x)| = \dfrac{|G|}{|\mathrm{Stab}(x)|}$.

5. Une application :

Soit G un groupe opérant sur un ensemble X fini. On note X_G l'ensemble des points fixes de cette opération, c'est-à-dire des points x de X tels que $gx = x$ pour tout $g \in G$. On note $\Omega_1, \ldots, \Omega_n$ les orbites deux à deux distinctes de X sous l'action de G, et non réduites à un point.

(a) Montrer que

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

(b) En déduire que si G est d'ordre p^n, avec p premier et $n \in \mathbb{N}^*$, alors $|X_G| \equiv |X| \mod [p]$.

(c) Soit G un groupe d'ordre p^n, p premier et $n \in \mathbb{N}^*$. Montrer que le centre $Z(G) = \{x \in G \mid \forall y \in G, xy = yx\}$ de G n'est pas réduit au groupe trivial.

Partie III – Démonstration du premier théorème de Sylow par Wielandt

Dans cette partie, on se fixe un groupe G de cardinal $p^\alpha m$, avec $\alpha \in \mathbb{N}$, et $p^\alpha \wedge m = 1$. On considère X l'ensemble des parties de G de cardinal p^α, et Y l'ensemble des p-sous-groupes de Sylow de G. On fait opérer G sur X par translation à gauche : pour tout g de G et tout $E \in X$,

$$g \cdot E = \{gx \mid x \in E\}.$$

On adoptera de façon symétrique la notation $E \cdot g$, ou plus simplement Eg pour désigner l'ensemble obtenu de E par multiplication à droite de chacun de ses éléments par g.

1. Montrer que cela définit bien une action de G sur X.

2. En étudiant des propriétés de l'application $\varphi_x : \mathrm{Stab}(E) \to E$ définie par $g \mapsto g \cdot x$, montrer que $|\mathrm{Stab}(E)| \leqslant p^\alpha$.

3. (a) Montrer que si $|\mathrm{Stab}(E)| = p^\alpha$, alors $E = \mathrm{Stab}(E) \cdot x$, où x est un élément quelconque de E.

(b) Montrer que s'il existe $S \in Y$ et $x \in G$ tel que $E = Sx$, alors $|\mathrm{Stab}(E)| = p^\alpha$.

On pourrait démontrer de même (et on admet) que si $\mathrm{Stab}'(E)$ désigne le stabilisateur de E sous l'action à droite de G sur X définie par $g \cdot E = Eg^{-1}$, alors $\mathrm{Stab}'(E)$ est de cardinal p^α si et seulement s'il existe un sous-groupe de Sylow $S \in Y$ et $x \in G$ tels que $E = xS$, et que dans ce cas, $S = \mathrm{Stab}'(E)$.

(c) Montrer que si $(S, S') \in Y^2$, avec $S \neq S'$, alors S et S' ne sont pas dans une même orbite de X sous l'action de G.

4. À l'aide de la question précédente et de certains résultats de la partie 2, en déduire que

$$|X| \equiv m|Y| \ [p].$$

5. En appliquant dans un premier temps la question précédente à $G' = \mathbb{Z}/n\mathbb{Z}$, en déduire que

$$|Y| \equiv 1 \ [p].$$

Cela prouve le premier théorème de Sylow et la moitié du troisième.

Partie IV – Quatre lemmes

Dans cette partie, nous établissons quatre lemmes en vue de donner une autre démonstration du premier théorème de Sylow.
Tous les groupes considérés ici sont décrits en notation multiplicative. Étant donné un groupe G, on notera 1_G son élément neutre.

1. **Lemme de Cauchy**
   On se donne dans cette question un groupe G d'ordre n, et un nombre premier p tel que p divise n. Le but de cette partie est de prouver qu'il existe dans G au moins un élément d'ordre p. On montre plus précisément que le nombre de solutions de l'équation $x^p = 1_G$ est un multiple de p.

   On note E l'ensemble des p-uplets $(x_1, \ldots, x_p)$ d'éléments de G tels que $x_1 x_2 \ldots x_p = 1_G$, les indices de $(x_1, \ldots, x_p)$ étant considérés dans $\mathbb{Z}/p\mathbb{Z}$ (donc vus cycliquement, ce qui revient à définir un tel p-uplet comme une application de $\mathbb{Z}/p\mathbb{Z}$ dans G).
   On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur E par permutation des indices : étant donné k dans $\mathbb{Z}/p\mathbb{Z}$,

$$k \cdot (x_1, \ldots, x_p) = (x_{1+k}, \ldots, x_{p+k}).$$

   (a) Montrer que cela définit bien une action de groupe.
   (b) Quels sont les points fixes pour cette action ?
   (c) En déduire que le nombre de solutions de l'équation $x^p = 1_G$ est un multiple de p.
   (d) En déduire que le nombre d'éléments d'ordre p de G est congru à $p - 1$ modulo p.

   En particulier, pour tout groupe G et tout diviseur premier p de l'ordre de G, il existe un élément de G d'ordre p.

2. **Image réciproque d'un sous-groupe**
   Soit $f : G \longrightarrow H$ un morphisme de groupes, et K un sous-groupe de H. Montrer que $f^{-1}(K)$ est un sous-groupe de G.

3. **Groupes quotients**
   Soit G un groupe, et H un sous-groupe distingué de G, c'est-à-dire tel que pour tout $g \in G$, $gH = Hg$. On remarquera que ceci équivaut au fait que pour tout g de G, et tout h de H, $ghg^{-1} \in H$
   (a) Montrer que les relations de congruence à droite et à gauche sont identiques.
   (b) Montrer que cette relation est une congruence pour la loi du groupe. Ainsi, cette loi passe au quotient, et définit une loi de composition interne sur l'espace quotient noté G/H.
   (c) Montrer que cette loi de composition interne munit G/H d'une structure de groupe.

4. **Premier théorème d'isomorphisme**.
   Soit $f : G \longrightarrow H$ un morphisme surjectif de groupes multiplicatifs, et $\mathrm{Ker}(f)$ *le sous-ensemble de G des éléments $x \in G$ tels que $f(x) = 1_H$.*
   (a) Montrer que $\mathrm{Ker}(f)$ est un sous-groupe distingué de G.
   (b) Montrer que f est constante sur chacune des classes d'équivalences modulo $\mathrm{Ker}(f)$. Ainsi, f induit une application $\overline{f} : G/\mathrm{Ker}(f) \longrightarrow H$
   (c) Montrer que $\overline{f}$ est une bijection.
   (d) Donner une relation entre les cardinaux de G, H et $\mathrm{Ker}(f)$.

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

Soit G un groupe d'ordre $n = p^\alpha m$, avec $m \wedge p^\alpha = 1$ et $\alpha > 0$.

1. On suppose dans cette question que G est abélien.
   (a) Justifier l'existence d'un sous-groupe distingué H d'ordre p de G

(b) En raisonnant par récurrence, et en considérant $f^{-1}(S)$ où f est la projection canonique de G sur G/H, et S un p-sous-groupe de Sylow de G/H, prouver l'existence d'un p-sous-groupe de Sylow de tout groupe abélien.

2. On ne suppose plus G abélien. On fait agir G sur lui-même par conjugaison. On rappelle que le centre de G est l'ensemble $Z(G) = \{x \in G \mid \forall g \in G, \quad xg = gx\}$.

   (a) Montrer que $Z(G)$ est un sous-groupe abélien (et distingué) de G

   (b) Montrer, à l'aide de la partie II, que soit $|Z(G)|$ divisible par p, soit il existe une orbite non réduite à un point et de cardinal premier avec p.

   (c) Montrer le premier théorème de Sylow par récurrence, à l'aide, suivant la situation, soit du centre, soit du stabilisateur d'une orbite non réduite à un point.

Partie VI – Démonstration des deuxième et troisième théorèmes de Sylow

G est toujours un groupe d'ordre $p^a m$, $p \wedge m = 1$.
On montre le deuxième théorème de Sylow, en commençant par prouver un résultat un peu plus fort : étant donné un sous-groupe de Sylow S fixé, tout p-sous-groupe de G est contenu dans un conjugué de S.

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) À l'aide de résultats de la partie II, montrer que l'ensemble X_H des points fixes de X sous cette action vérifie :
   $$|X_H| \equiv m \mod [p].$$

   (b) En déduire qu'il existe un élément $x \in G$ tel que pour tout $h \in H$, $hxSx^{-1} = xSx^{-1}$.

   (c) En déduire que H est un sous-groupe de xSx^{-1}

   En particulier, le cardinal de xSx^{-1} étant égal à celui de S, tout p-sous-groupe est inclu dans un p-sous-groupe de Sylow

2. Montrer que les sous-groupes de Sylow sont deux à deux conjugués, donc que si S et S' sont deux sous-groupes de Sylow, il existe $x \in G$ tel que $S' = xSx^{-1}$.

   Ceci prouve le deuxième théorème de Sylow

3. On montre enfin le dernier point du troisième théorème de Sylow. Notons comme précédemment Y l'ensemble des p-sous-groupes de Sylow de G, et faisons agir G sur Y par conjugaison.

   (a) Décrire pour cette action l'orbite Ω_S dans Y d'un élément S de Y.

   (b) En déduire que pour tout $S \in Y$, on a $|Y| = \dfrac{|G|}{\mathrm{Stab}(S)}$ et conclure.