Pour le 05/03/2020

DM n° 14 : Groupes

Problème 1 – 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) :*

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

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.