TD n°9 : Structure des groupes finis
1-2/12/2022

Exercice 1. Des exemples de Sylows

Pour chacun des groupes suivants et chaque premier p intervenant dans son cardinal, donner un p-Sylow, l'identifier à un p-groupe classique, puis donner le nombre de p-Sylow.

1. Le groupe $\mathbb{Z}/28\mathbb{Z}$.
2. Le groupe $\mathfrak{S}_5$.
3. Le groupe $\mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})$.

Correction de l'exercice 1 :

1. Le cardinal s'écrit $28 = 4 * 7$. Le théorème des restes chinois donne un isomorphisme

$$\mathbb{Z}/28\mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

   Ceci illustre qu'un 2-Sylow (donc tous) isomorphe à $\mathbb{Z}/4\mathbb{Z}$, et ledit Sylow est distingué donc unique par abélianité que $\mathbb{Z}/28\mathbb{Z}$: c'est $7\mathbb{Z}/28\mathbb{Z}$. Un 7-Sylow (donc tous) est isomorphe à $\mathbb{Z}/7\mathbb{Z}$, et ledit Sylow est distingué donc unique par abélianité que $\mathbb{Z}/28\mathbb{Z}$: c'est $4\mathbb{Z}/28\mathbb{Z}$.

2. Le cardinal de $\mathfrak{S}_5$ s'écrit $120 = 8 * 3 * 5$.

   Un 5-Sylow est de cardinal 5 ; c'est le sous-groupe engendré par un 5-cycle. Il y en a $^{4*3*2}/_{4} = 6$ et ils sont isomorphes à $\mathbb{Z}/5\mathbb{Z}$.

   Un 3-Sylow est de cardinal 3 ; c'est le sous-groupe engendré par un 3-cycle. Il y en a $^{5*4*3}/_{3*2} = 10$ et ils sont isomorphes à $\mathbb{Z}/3\mathbb{Z}$.

   Un 2-Sylow est de cardinal 8 et contient chaque type cyclique qui donne des permutations d'ordre 2-primaire puisque les 2-Sylow sont conjugués et contiennent tous les 2-sous-groupes. Un 2-Sylow contient ainsi un 4-cycle et une transposition qui normalise le sous-groupe engendré. Supposons que mon 2-Sylow contienne $(1\,2\,3\,4)$. Le normalisateur du sous-groupe engendré commute au carré $(1\,3)(2\,4)$. Les seules tranpositions qui peuvent normaliser sont ainsi $(1\,3)$ et $(2\,4)$ et donnent le même 2-Sylow. Le seul sous-groupe isomorphe à $\mathbb{Z}/4\mathbb{Z}$ dans notre 2-Sylow est celui engendré par le 4-cycle. Ainsi, un 2-Sylow est la partie 2-primaire du normalisateur du sous-groupe engendré par un 4-cycle. Il y en a donc $^{5*4*3*2}/_{4*2} = 15$ et ils sont isomorphes à D_8.

3. À venir l'année prochaine, ou avant si vous me demandez.

Exercice 4. Une condition arithmétique sur les groupes simples

Soit G un groupe simple fini.

1. Démontrer que pour tout sous-groupe strict H, nous avons $|G| | [G : H]!$.
2. Démontrer que pour tout premier p, le cardinal de G divise $\mathrm{n}_p(G)!$ où $\mathrm{n}_p(G)$ est le nombre de p-Sylow.

Correction de l'exercice 4 :

1. L'action par multiplication à gauche donne un morphisme non trivial
$$G \to \mathfrak{S}_{G/H},$$
qui doit être injectif par simplicité de G. La relation de divisibilité en découle.
2. Le normalisateur d'un p-Sylow P est un sous-groupe d'indice $\mathrm{n}_p(G)$.

Exercice 5. Une réciproque à Lagrange

Démontrer que pour tout p-groupe G et tout diviseur p^i de son cardinal, il existe un sous-groupe distingué de G d'ordre p^i.

Correction de l'exercice 5 :

Voir dans le poly, proposition 1.9.

Exercice 6. Groupes d'ordre p^3

Soit p un nombre premier impair. Le but de cet exercice est de décrire à isomorphisme près les groupes finis de cardinal p^3. Nous donnerons trois méthodes selon l'ordre maximal d'un élément.

La première question traite du cas où il existe un élément d'ordre p^3 dans notre groupe G.

1. Démontrer que le groupe G est isomorphe à
$$\mathbb{Z}/p^3\mathbb{Z}.$$

Les questions suivantes traitent du cas où l'ordre maximal d'un élément de G est p^2.

2. Démontrer que si G est abélien, il est isomorphe à
$$\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$
3. Nous supposons désormais que G n'est pas abélien. Soit x un élément d'ordre p^2. Démontrer que $G/\mathrm{Z}(G)$ est isomorphe à $\left(\mathbb{Z}/p\mathbb{Z}\right)^2$ puis que x n'est pas central.
4. Nous supposons par l'absurde que tous les éléments qui ne sont pas dans $\langle x\rangle$ sont d'ordre p^2. Démontrer qu'il existe $y \notin \langle x\rangle$ tel que $x^p = y^p$.
5. Démontrer que $[x : y^{-1}]$ est central, puis que
$$(yx^{-1})^p = [x : y^{-1}]^{\frac{p(p-1)}{2}}.$$
6. En utilisant que p est impair, démontrer qu'il existe un élément d'ordre p qui n'appartient pas à $\langle x\rangle$ et en déduire que G est isomorphe au groupe
$$\mathbb{Z}/p^2\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z},$$
où $\varphi(a) = [z \mapsto (1+p)^a z]$.

Les questions suivantes traitent du cas où l'ordre maximal d'un élément de G est p, autrement dit où G est p-élémentaire.

7. Démontrer qu'il existe un sous-groupe distingué de G isomorphe à $\left(\mathbb{Z}/p\mathbb{Z}\right)^2$.
8. En considérant que les p-Sylow de $\mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$ sont conjugués, conclure que G est isomorphe à l'un des deux groupes
$$\left(\mathbb{Z}/p\mathbb{Z}\right)^3 \text{ et } \mathrm{U}_3(\mathbb{Z}/p\mathbb{Z}).$$

Correction de l'exercice 6 :

1. Le sous-groupe engendré par un élément d'ordre p^3 est isomorphe au groupe prédit et égal à G par cardinalité.
2. Simple utilisation du théorème de structure des groupes abéliens de type fini.
3. Le quotient par le centre ne peut être monogène et que le centre est non trivial. Ceci entraîne immédiatement la description du quotient par le centre. Puisque le centre est de cardinal p, nous savons que x n'est pas central.
4. La question précédente entraîne que $\mathrm{Z}(G) = \langle x^p \rangle$. Prenons $y \notin \langle x \rangle$. Cet élément est d'ordre p^2 par hypothèse et la description du quotient par le centre entraîne que y^p est un générateur du centre. Quitte à changer y par y^r pour r premier à p, nous pouvons supposer que $y^p = x^p$.
5. Le quotient par le centre étant abélien, nous avons $\mathrm{D}(G) \subseteq \mathrm{Z}(G)$. Ceci entraîne que le commutateur $[x : y^{-1}]$ est central. En écrivant

$$\begin{aligned}(yx^{-1})^p &= yx^{-1}yx^{-1}\dots yx^{-1} \\ &= y^2x^{-1}[x:y^{-1}]x^{-1}\dots yx^{-1} \\ &= y^2x^{-2}yx^{-1}\dots yx^{-1}[x:y^{-1}] \\ &\dots \\ &= y^px^{-p}[x:y^{-1}]^{\frac{p(p-1)}{2}}\end{aligned}$$

   où le passage à la troisième ligne utilise que le commutateur est central et où l'on fait ensuite remonter les y récursivement. En utilisant que $y^p = x^p$, cela conclut.
6. Puisque p est impair, il divise encore $p(p-1)/2$. Le commutateur est central, donc d'ordre divisant p ; ainsi la question précédente donne $(yx^{-1})^p$. Comme $y \notin \langle x \rangle$, l'élément yx^{-1} n'est pas trivial et fournit un élément d'ordre p n'appartenant pas à $\langle x \rangle$. Par le lemme d'Ore, le sous-groupe $\langle x \rangle$ est distingué et nous avons trouvé un complément, incarné par cet élément z d'ordre p. Le groupe G est produit semi-direct interne de $\langle z \rangle$ par $\langle x \rangle$. Il revient à calculer l'automorphisme de $\langle x \rangle$ d'ordre p donné par la conjugaison par z. Le groupes de ces automorphisme est isomorphe à $(\mathbb{Z}/p^2\mathbb{Z})^\times \cong \mathbb{Z}/p(p-1)\mathbb{Z}$. Les éléments d'ordre p sont engendrés par la multiplication par $(1+p)$ (voir TD ? ?). Quitte à choisir correctement le générateur de $\langle z \rangle$, la conjugaison par z est donc donnée par la puissance $(1+p)$-ième ce qui identifie G au produit semi-direct externe annoncé.
7. Le cours démontre que G possède un sous-groupe distingué d'ordre p^2. Puisque tous les éléments sont d'ordre p, il est effectivement isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$.
8. Les p-Sylow de $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ sont de cardinal p, conjugués à au groupe engendré par $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. Puisque tous les éléments sont d'ordre p, le sous-groupe distingué de la question précédente a un complément, qui agit par conjugaison comme l'un des p-Sylow de $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Quitte à bien choisir la manière d'identifier le sous-groupe de la question précédente à $(\mathbb{Z}/p\mathbb{Z})^2$, le complément agit par $\psi(1) = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. Il y a donc une seule classe d'isomorphisme de groupe d'exposant p non commutatif d'ordre p^3 et $\mathrm{U}_3(\mathbb{Z}/p\mathbb{Z})$ en est un.

Exercice 8. Groupe simple d'ordre 168

Cet exercice vise à démontrer qu'une groupe simple d'ordre 168 est isomorphe à $\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$. Nous fixons G un tel groupe.

1. Démontrer que les 7-Sylow de G sont au nombre de 8. Nous notons $\mathrm{Syl}(7)$ cet ensemble.
2. Soit $\iota : G \to \mathfrak{S}_{\mathrm{Syl}(7)}$ le morphisme induit par l'action par conjugaison. Démontrer que ι est injectif. Nous α un élément d'ordre 7 de G, démontrer que quitte à bien choisir la bijection de $\mathrm{Syl}(7)$ avec $\mathbb{P}^1(\mathbb{Z}/7\mathbb{Z})$, l'élément $\iota(\alpha)$ agit comme $x \mapsto x+1$.

En particulier, le sous-groupe engendré par α est un 7-Sylow fixe par conjugaison de α : c'est le sous-groupe identifié à ∞ que nous fixerons pour la suite.

3. Démontrer qu'un élément de $\mathfrak{S}_{\mathbb{P}^1(\mathbb{Z}/7\mathbb{Z})}$ qui normalise $\langle x \mapsto x+1\rangle$ s'écrit $x \mapsto ax+b$. Démontrer que quitte à renuméroter d'une manière qui laisse fixe $x \mapsto x+1$, un élément d'ordre 3 qui normalise $\langle x \mapsto x+1\rangle$ s'écrit $x \mapsto 2^k x$ pour un certain k.
4. Donner le cardinal du normalisateur d'un 7-Sylow. Démontrer qu'il existe un élément β d'ordre 3 dans le normalisateur de ∞ tel que $\iota(\beta) = [x \mapsto 2x]$.
5. Démontrer que l'action de G sur Syl(7) est 2-transitive. En déduire que $\mathrm{n}_G(3) \geq 28$ puis que cette inégalité est une égalité.
6. Démontrer que $|\mathrm{N}_G(\langle\beta\rangle)| = 6$. En comptant de manière très fine les éléments d'ordre 1, 7, 3, 6 ou une puissance de 2, démontrer que ce normalisateur ne peut être cyclique.
7. Soit γ un élément d'ordre 2 dans $\mathrm{N}_G(\langle\beta\rangle)$. Démontrer que l'action de γ est sans point fixe puis qu'elle permute ∞ et 0.
8. Démontrer que $\gamma\beta\gamma^{-1} = \beta^{-1}$ puis que γ envoie le triplet $(1,2,4)$ sur $(3,5,6)$, $(5,6,3)$ ou $(6,3,5)$. Dans tous les cas, démontrer que l'action de γ est celle d'une homographie.

Nous avons trouvé trois éléments α, β et γ qui agissent par homographies.

9. En considérant son indice dans G, démontrer que le sous-groupe $\langle\alpha, \beta, \gamma\rangle$ est égal à G tout entier.
10. En vérifiant que les homographies introduites sont bien dans $\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$, conclure.

Correction de l'exercice 7 :

1. Le cardinal s'écrit $168 = 8*3*7$. Le nombre de 7-Sylow est donc un diviseur de 24 congru à 1 modulo 7, et différent de 1 puisque G est simple et ne peut par conséquent pas contenu un unique 7-Sylow. Ainsi, les 7-Sylow de G sont au nombre de 8.
2. Par Sylow, l'action de G sur Syl(7) est transitive, ce qui implique que ι n'est pas trivial. Puisque G est simple, il en découle que ι est injectif.

   Par injectivité, l'image de ι est une permutation de 8 éléments, d'ordre 7. C'est donc un 7-cycle. En identifiant le point fixe à ∞ et numérotant le reste tel que le 7-cycle soit $(0\,1\,\ldots\,6)$, l'élément $\iota(\alpha)$ agit effectivement comme l'homographie $x \mapsto x+1$.
3. Soit τ un tel élément. La normalisation implique que pour un certain $i \not\equiv 0 \mod 7$ nous avons

   $$\tau \circ (x \mapsto x+1) = (x \mapsto x+i) \circ \tau$$

   ce qui se réécrit

   $$\forall x,\ \ \tau(x+1) = \tau(x) + i.$$

   Cette équation fonctionnelle donne $\tau(x) = ix + \tau(0)$. Prenons σ d'ordre 3 dans le normalisateur de $\langle x \mapsto x+1\rangle$. Puisqu'il agit sur $\mathbb{P}^1(\mathbb{Z}/7\mathbb{Z}) \setminus \{\infty\}$, il possède un point fixe et quitte à renuméroter cycliquement, nous pouvons supposer que σ fixe 0. En écrivant $\sigma(x) = ax+b$, le fait de fixer 0 implique que $b = 0$, puis son ordre impose que $a = 2^k$ pour un certain k (les seuls éléments d'ordre 3 de $(\mathbb{Z}/7\mathbb{Z})^\times$) sont 2 et 4.
4. Par la formule orbite stabilisateur pour l'action transitive de G sur les p-Sylow, nous savons que $|\mathrm{N}_G(P)| = {}^{|G|}/_{\mathrm{n}_G(p)}$ pour n'importe quel p-Sylow P. Ici, le normalisateur d'un 7-Sylow est de cardinal 21. Un élément d'ordre 3 dans ce normalisateur est envoyé par ι sur un élément d'ordre [1] exactement 3 qui normalise $\iota(\alpha)$. La question précédente montre que quitte à renuméroter correctement, l'action de α s'écrit $x \mapsto x+1$ et celle de β s'écrit $x \mapsto 2x$ ou $x \mapsto 4x$. En remplaçant éventuellement β par son inverse, nous pouvons supposer que β agit par $x \mapsto 2x$.

1. Ne pas oublier que ι est injective !

5. L'action de G sur Syl(7) est transitive par Sylow. De plus, le stabilisateur de ∞ contient α qui agit transitivement sur les autres 7-Sylows. Il en découle que l'action est 2-transitive.
   Considérons que l'action de β stabilise uniquement ∞ et 0. Pour toute paire $\{i, j\}$, considérons un élément $\delta \in G$ tel que $\delta \cdot \{\infty, 0\} = \{i, j\}$. L'élément $\delta\beta\delta^{-1}$ engendre un 3-Sylow et laisse fixe exactement i et j. Nous avons ainsi construit autant de 3-Sylows que de paires de 7-Sylows, i.e. nous en avons construit 28. Les conditions arithmétiques du théorème de Sylow concluent alors à l'égalité.
6. Par le même argument qu'à la question 4), il en découle que le normalisateur d'un 3-Sylow est de cardinal 3. Supposons que ce normalisateur soit cyclique par l'absurde et comptons les éléments. Il existe 1 élément d'ordre 1 : le neutre. Les 7-Sylow fournissent chacun 6 éléments d'ordre 7. Les 3-Sylow fournissent 2 éléments d'ordre 3. Si les normalisateurs de deux 3-Sylow s'intersectent en un élément d'ordre 6, alors ces normalisateurs s'intersectent aussi en un élément d'ordre 3. Or, puisqu'ils sont cycliques, les éléments d'ordre 3 sont exactement le 3-Sylow qui leur donnen naissance et ces 3-Sylows seraient sont donc identiques. Ainsi, chaque normalisateur de 3-Sylow fournit deux nouveaux éléments d'ordre 6. Au total nous avons listé
   $$1 + 8 * 6 + 28 * 2 + 28 * 2 = 161$$
   éléments. Puisqu'un 2-Sylow possède exactement 7 éléments d'ordre une puissance non triviale de 2, il en découle qu'il existe une unique 2-Sylow, ce qui contredit la simplicité de G. Le normalisateur de $\langle\beta\rangle$ n'est pas cyclique.
7. Soit γ d'ordre 2. Les normalisateurs de 7-Sylows sont de cardinal impair ce qui entraîne que γ n'appartient à aucun d'eux, i.e. que γ agit sans point fixe. Comme γ normalise $\langle\beta\rangle$, il stabilise les points fixes de β. L'action de γ stabilise $\{\infty, 0\}$ sans les fixer : elle permute ces deux éléments.
8. Le normalisateur de $\langle\beta\rangle$ n'étant pas cyclique, les éléments β et γ ne commutent pas ce qui fournit la première identité. Nous pouvons écrire
   $$\iota(\beta) = \infty\, 0\, (1\, 2\, 4)\, (3\, 6\, 5)$$
   et l'identité $\gamma\beta\gamma^{-1} = \beta^{-1}$ passé à ι implique que γ envoie le triplet $(1, 2, 4)$ sur $(3, 5, 6)$, $(5, 6, 3)$ ou $(6, 3, 5)$.
   Dans le premier cas, la permutation $\iota(\gamma)$ s'écrit
   $$\iota(\gamma) = (\infty\, 0)\, (1\, 3)\, (2\, 5)\, (4\, 6)$$
   qui correspond à l'homographie $x \mapsto {}^3\!/_x$. Les autres cas sont similaires.

Remarque : prouver que $\mathrm{N}_G(\langle\beta\rangle)$ n'est pas abélien est primordial sans quoi l'action de $\iota(\gamma)$ ne saurait être une homographie.

9. Puisqu'il contient des éléments d'ordre 7, 3 et 2, ce sous-groupe est d'indice divisant 4. La deuxième question de l'exercice 4 conclut alors que ce sous-groupe ne peut être strict.
10. La translation $x \mapsto x + 1$ ne pose aucun problème. Pour les autres, il suffit de montrer que la matrice associée à la représentation de notre homographie a un déterminant qui est un carré dans ${}^{\mathbb{Z}}\!/_{7\mathbb{Z}}$ (voir TD n°8 exercice 1). Le déterminant de la matrice $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ associée à $x \mapsto 2x$ vaut $2 = 3^2$. Le déterminant de $\left(\begin{smallmatrix} 0 & 3 \\ 1 & 0 \end{smallmatrix}\right)$ associée à $x \mapsto {}^3\!/_x$ vaut $-3 = 2^2$. Ainsi, l'image de $G \hookrightarrow \mathfrak{S}_{\mathbb{P}^1({}^{\mathbb{Z}}\!/_{7\mathbb{Z}})}$ est contenue dans $\mathrm{PSL}_2({}^{\mathbb{Z}}\!/_{7\mathbb{Z}})$ et c'est un isomorphisme par égalité des cardinaux.