Algèbre – Interrogation I

Exercice 1. Énoncer et démontrer le théorème de factorisation pour un morphisme de groupes finis $f : G \to G'$. Rappeler le lien entre $\#\mathrm{Ker}(f)$ et celui de $\#\mathrm{Im}(f)$.

Solution. Soient G et G' deux groupes ainsi que $f : G \to G'$ un morphisme de groupes. On a alors que f passe au quotient en un isomorphisme

$$\tilde{f} : G/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}(f).$$

En effet, par le cours, $\mathrm{Ker}(f)$ est un sous-groupe distingué de G et $f : G \to \mathrm{Im}(f)$ est surjective par définition. On note alors $\pi : G \to G/\mathrm{Ker}(f)$ la surjection canonique qui est un morphisme de groupes. On pose alors

$$\tilde{f} : \left\{ \begin{array}{ccc} G/\mathrm{Ker}(f) & \longrightarrow & \mathrm{Im}(f) \\ \pi(g) & \longmapsto & f(g). \end{array} \right.$$

L'application est bien à valeurs dans $\mathrm{Im}(f)$ et est bien définie car si $\pi(g) = \pi(g')$, alors il existe un élément $h \in \mathrm{Ker}(f)$ tel que $g = g'h$ de sorte que $f(g) = f(g')f(h)$ (car f est un morphisme de groupes) et puisque h est dans le noyau, $f(g) = f(g')$. On a alors que $\tilde{f}$ est surjective par surjectivité de f à valeurs dans $\mathrm{Im}(f)$. On a un morphisme de groupes car pour tous $g, g' \in G$ on a

$$\tilde{f}(\pi(g)\pi(g')) = \tilde{f}(\pi(gg')) = f(gg') = f(g)f(g') = \tilde{f}(\pi(g))\tilde{f}(\pi(g'))$$

car π et f sont des morphismes de groupes. Enfin, $\tilde{f}(\pi(g)) = e$ implique que $f(g) = e$ soit $g \in \mathrm{Ker}(f)$ et $\pi(g) = \pi(e)$ ce qui établit l'injectivité. On a donc obtenu que $\tilde{f}$ est un isomorphisme de groupes et en particulier

$$\#\left(G/\mathrm{Ker}(f)\right) = \#\mathrm{Im}(f) \quad \text{soit si } G \text{ est fini} \quad \#G = \#\mathrm{Ker}(f) \times \#\mathrm{Im}(f).$$

Exercice 2. Soient p un nombre premier et n un entier naturel tels que $p > n$. On considère G un groupe d'ordre pn et H un sous-groupe de G d'ordre p.

1. Justifier que H est un p-Sylow de G.
2. Démontrer que H est un sous-groupe distingué de G.

Solution.

1. Comme $p \nmid n$, par définition, un p-Sylow de G est de cardinal p et H est un p-Sylow.
2. Les théorèmes de Sylow fournissent que, si n_p dénote le nombre de p-Sylow de G, $n_p \equiv 1 \pmod{p}$ et $n_p \mid n$. Mais, puisque $n < p$, on a que tout diviseur $d \neq 1$ de n vérifie $d < p$ et $d \equiv d \not\equiv 1 \pmod{p}$ de sorte que nécessairement, $n_p = 1$ et comme tous les p-Sylow sont conjugués, cela implique que l'unique p-Sylow est distingué. Comme H est un p-Sylow, on obtient le résultat !

Exercice 3.

1. Soient n un entier naturel plus grand que 2 et $\varphi : \mathfrak{S}_n \longrightarrow \{\pm 1\}$ un morphisme de groupes. Montrer que toutes les transpositions ont la même image et décrire tous les morphismes φ possibles.
2. Rappeler ce que vaut $Z(\mathfrak{S}_3)$ et donner une partie génératrice de $\mathfrak{S}_3$. Montrer que

$$f : \left\{ \begin{array}{ccc} \mathfrak{S}_3 & \longrightarrow & \mathtt{Aut}(\mathfrak{S}_3) \\ \sigma & \longmapsto & [\mu \mapsto \sigma\mu\sigma^{-1}] \end{array} \right.$$

   est un isomorphisme de groupes.
2. Décrire toutes les actions de groupes de $\mathbb{Z}/7\mathbb{Z}$ sur $\mathfrak{S}_3$ par automorphismes.
   On rappelle que si G et X sont deux groupes et que G agit sur X, on dit que G agit sur X *par automorphismes* si pour tout $g \in G$, $x \mapsto g \cdot x$ est un automorphisme de X.
3. Soient n un entier naturel supérieur ou égal à 2 et $n_1, \ldots, n_k$ des entiers naturels non nuls tels que $n = n_1 + n_2 + \cdots + n_k$. En utilisant le théorème de Lagrange pour un sous-groupe bien choisi, montrer que

$$\prod_{i=1}^{k} (n_i)! \,\Big|\, n!.$$

Solution.

1. Soit φ un tel morphisme et τ une transposition. On suppose que $\varphi(\tau) = \varepsilon$ pour $\varepsilon \in \{\pm 1\}$. On sait alors que toutes les transpositions de $\mathfrak{S}_n$ sont conjuguées[1] et ainsi si τ' est une autre transposition, il existe $\sigma \in \mathfrak{S}_n$ tel que $\tau' = \sigma\tau\sigma^{-1}$. On a alors (puisque φ est un morphisme de groupes et que le groupe d'arrivée est **abélien**)

$$\varphi(\tau') = \varphi(\sigma)\varphi(\tau)\varphi(\sigma)^{-1} = \varphi(\sigma)\varphi(\sigma)^{-1}\varphi(\tau) = \varphi(\tau).$$

Ainsi soit $\varphi(\tau) = 1$ pour toutes les transpositions mais alors puisque les transpositions engendrent $\mathfrak{S}_n$, il vient que pour tout $\sigma \in \mathfrak{S}_n$, $\varphi(\sigma) = 1$ **ou** $\varphi(\tau) = -1$ pour toutes les transpositions mais alors puisque les transpositions engendrent $\mathfrak{S}_n$, on obtient que pour tout $\sigma \in \mathfrak{S}_n$, $\varphi(\sigma)$ vaut $(-1)^r$ où r est le nombre de transpositions dans la décomposition de σ en produit de transpositions. On reconnaît alors la signature !

2. On rappelle[2] que pour tout $n \geqslant 3$, $Z(\mathfrak{S}_n)) = \{e\}$. Notons $i_\sigma : \mathfrak{S}_3 \to \mathfrak{S}_3$ définie par $i_\sigma(\mu) = \sigma\mu\sigma^{-1}$. On a alors que f est un morphisme de groupes car pour tous $\sigma, \sigma' \in \mathfrak{S}_3$, on a

$$\forall \mu \in \mathfrak{S}_3, \quad f(\sigma'\sigma)(\mu) = (\sigma'\sigma)\mu(\sigma'\sigma)^{-1} = \sigma'\sigma\mu\sigma^{-1}\sigma'^{-1}$$

tandis que

$$i_{\sigma'} \circ i_\sigma(\mu) = i_{\sigma'}\left(\sigma\mu\sigma^{-1}\right) = \sigma'\sigma\mu\sigma^{-1}\sigma'^{-1}$$

ce qui montre bien que $f(\sigma'\sigma) = f(\sigma') \circ f(\sigma)$. Par ailleurs, $\sigma \in \mathrm{Ker}(f)$ si, et seulement si, $i_\sigma = \mathrm{Id}$ soit si, et seulement si, pour tout $\mu \in \mathfrak{S}_3$, $\sigma\mu\sigma^{-1} = \mu$ soit $\sigma\mu = \mu\sigma$ et $\sigma \in Z(\mathfrak{S}_3) = \{e\}$. On en déduit que f est injective. Enfin, on sait que $\mathfrak{S}_3$ est engendré[3] par $\tau = (1\,2)$ et $\sigma = (1\,2\,3)$. Or, un automorphisme de groupe envoie un élément d'ordre d sur un élément d'ordre d. Ainsi, un automorphisme de $\mathfrak{S}_3$ est déterminé par l'image de τ (qui doit être un élément d'ordre 2 donc une transposition, ce qui laisse 3 choix) et par l'image de σ (qui doit être un élément d'ordre 3 donc une 3-cycle, ce qui laisse 2 choix). Finalement, on en déduit que $\#\mathtt{Aut}(\mathfrak{S}_3) \leqslant 6$ mais on a obtenu un morphisme de groupe injectif d'un groupe de cardinal 6 dans $\mathtt{Aut}(\mathfrak{S}_3)$. Il s'agit donc nécessairement d'un isomorphisme et $\#\mathtt{Aut}(\mathfrak{S}_3) = 6$.

3. Cela revient à dénombrer les morphismes de groupes $g : \mathbb{Z}/7\mathbb{Z} \to \mathtt{Aut}(\mathfrak{S}_3) \cong \mathfrak{S}_3$. Mais comme $\mathbb{Z}/7\mathbb{Z}$ est cyclique, un tel morphisme est déterminé par l'image de la classe de 1 qui doit être un élément de $\mathtt{Aut}(\mathfrak{S}_3)$ d'ordre divisant 7. Par Lagrange, puisque le cardinal de $\mathfrak{S}_3$ est premier à 7, cela impose que cet ordre soit 1 et que $g(\overline{1}) = \mathrm{Id}$ et g est trivial. Il n'y a donc que l'action triviale $\overline{k} \cdot \sigma = \sigma$ pour $\overline{k} \in \mathbb{Z}/7\mathbb{Z}$ et $\sigma \in \mathfrak{S}_3$.

4. On partitionne $\{1, \ldots, n\} = N_1 \sqcup N_2 \sqcup \cdots \sqcup N_k$ où $N_1 = \{1, \ldots, n_1\}$, $N_2 = \{n_1+1, \ldots, n_1+n_2\}$, $\ldots$, $N_k = \{1+n_1+\cdots+n_{k-1}, \ldots, n\}$ qui sont respectivement de taille $n_1, n_2, \ldots, n_k$. On prend alors l'ensemble des permutations $\sigma \in \mathfrak{S}_n$ qui stabilisent chacun des N_i. On vérifie immédiatement qu'il s'agit d'un sous-groupe de $\mathfrak{S}_n$ isomorphe à $\prod_{i=1}^{k} \mathfrak{S}_{n_i}$ et on conclut par le théorème de Lagrange !

Exercice 4.

1. Soient p un nombre premier, G un p-groupe et X un ensemble fini sur lequel G agit. On note

$$X^G := \{x \in X \,:\, \forall g \in G,\, g \cdot x = x\}.$$

Montrer que $\left|X^G\right| \equiv |X| \pmod p$.

2. Que pouvez-vous en déduire si $|X|$ n'est pas divisible par p ?

La suite de l'exercice est un **bonus** à traiter *uniquement* si vous avez terminé le reste ! On considère p un nombre premier congru à 1 modulo 4 et on souhaite montrer que p est somme de deux carrés. On note

$$X = \left\{(x, y, z) \in \mathbb{N}^3 \,:\, x^2 + 4yz = p\right\}.$$

On pose alors $i : X \longrightarrow X$ définie par

$$(x, y, z) \longmapsto \begin{cases} (x + 2z, z, y - x - z) \text{ si } x < y - z \\ (2y - x, y, x - y + z) \text{ si } y - z < x < 2y \\ (x - 2y, x - y + z, y) \text{ si } x > 2y. \end{cases}$$

3. Vérifier que i est bien définie et est une involution, c'est-à-dire que $i \circ i = \mathrm{Id}_X$. En déduire une action de $\mathbb{Z}/2\mathbb{Z}$ sur X.

4. Montrer que i a un unique point fixe.

1. Voir l'exercice 4 du TD sur les groupes, cela découle du fait que deux transpositions ont le même type de décomposition en produit de cycles à supports disjoints.
2. Je vous renvoie au premier TD, exercice 4 dernière question pour une démonstration.
3. Pour le voir, il suffit de reprendre l'exercice de classification des groupes d'ordre 6. Mais de façon plus générale, $\mathfrak{S}_n$ est engendré par $(1\,2)$ et $(1\,2\,3\,\cdots\,n)$. Je vous renvoie par exemple au Perrin pour cela. Attention que cela ne fonctionne pas avec n'importe quel transposition et n'importe quel cycle ! Par exemple, vous pouvez démontrer (c'est un classique à l'oral de l'agreg !) que si $1 \leqslant a < b \leqslant n$, alors $\mathfrak{S}_n$ est engendré par $(a\,b)$ et $(1\,2\,3\,\cdots\,n)$ si, et seulement si, $\mathrm{pgcd}(b - a, n) = 1$.

5. Établir que $|X|$ est impair.
6. Montrer que l'application $j : X \longrightarrow X$ définie par $j(x, y, z) = (x, z, y)$ est une involution et en déduire qu'elle admet un point fixe. Conclure !

Solution.

1. On note Ω l'ensemble des orbites. On utilise l'équation aux classes et on sépare les orbites selon celles de cardinal 1 et les autres
$$|X| = \sum_{\omega \in \Omega} |\omega| = \left|X^G\right| + \sum_{\substack{\omega \in \Omega \\ |\omega|>1}} |\omega|.$$
On sait alors que $|\omega| = |G|/|\mathrm{Stab}_G(x_\omega)|$ pour tout $x_\omega \in \omega$. Pour une orbite de cardinal au moins 2, on a que $|G|/|\mathrm{Stab}_G(x_\omega)|$ est un diviseur de $|G|$ différent de 1. Comme G est un p-groupe, cela implique que pour tout orbite $\omega \in \Omega$ telle que $|\omega| > 1$, on a $p \mid |\omega| = |G|/|\mathrm{Stab}_G(x_\omega)|$. On a alors en passant modulo p le résultat voulu !
2. Si $p \nmid |X|$, alors $|X| \not\equiv 0 \pmod p$. Il vient que $X^G \neq \emptyset$.
3. On peut commencer par constater que puisque $p \equiv 1 \mod 4$, il existe z entier tel que $p = 1 + 4z$ et ainsi $(1, 1, z) \in X$ qui est non vide. On a également que X est fini car $yz \neq 0$ car p n'est pas un carré et ainsi $x, y, z \leqslant p$. Noter qu'on a également toujours $y - z < 2y$ et que $x \neq y - z$ sinon
$$p = (y - z)^2 + 4yz = (y + z)^2$$
ce qui est absurde et $x \neq 4y$ sinon $p = 4y(y + z)$ ce qui est absurde. On a donc bien une disjonction de cas exhaustive et il suffit de vérifier que
$$(x+2z)^2+4(y-x-z)z = x^2+4yz = p, \quad (2y-x)^2+4(x-y+z)y = x^2+4yz = p, \quad (x-2y)^2+4(x-y+z)y = x^2+4yz = p.$$
Ainsi, i est bien définie et si on pose $E_1 = \{(x, y, z) \in X : x < y - z\}$, $E_2 = \{(x, y, z) \in X : y - z < x < 2y\}$ et
$$E_3 = \{(x, y, z) \in X : 2y < x\},$$
on constate que i échange E_1 et E_3 et stabilise E_2. On vérifie alors par le calcul que si $x < y-z$, alors $i(x, y, z) = (x+2z, z, y-x-z) = (X, Y, Z)$ avec
$$X > 2Y \iff x + 2z > 2z \iff x > 0.$$
On a alors
$$i \circ i(x, y, z) = (X - 2Y, X - Y + Z, Y) = (x + 2z - 2z, x + 2z - z + y - x - z, z) = (x, y, z).$$
On traite tous les autres cas de la même façon et on a bien que i est une involution. On définit alors l'action suivante
$$\forall \overline{k} \in \mathbb{Z}/2\mathbb{Z}, \forall (x, y, z) \in X, \quad \overline{k} \cdot (x, y, z) = i^k(x, y, z).$$
On vérifie que cette action est bien définie et est bien une action de groupe.
4. Un point fixe est donc nécessairement dans E_2. On cherche donc un triplet qui vérifie $y - z < x < 2y$, $p = x^2 + 4yz$ et $x = 2y - x$, $z = x - y + z$. On a donc $x = y$ et $p = y(y + 4z)$. Par primalité de p, cela implique $x = y = 1$ ou $x = y = p$ mais si $x = y = p$, $1 = p + 4z$ avec z non nul ce qui est absurde. Ainsi $(x, y, z) = (1, 1, z)$ avec $p = 1 + 4z$ ce qui fournit bien une unique solution puisque $p \equiv 1 \pmod 4$.
5. Posons $G = \mathbb{Z}/2\mathbb{Z}$. On constate que i a un point fixe si, et seulement s'il existe $(x, y, z) \in X$ tel que $i(x, y, z) = (x, y, z)$ soit tel que $\overline{1} \cdot (x, y, z) = (x, y, z)$. On cherche donc un élément de X^G (puisque $\overline{1} \cdot (x, y, z) = (x, y, z)$ est toujours vérifié). Par la question **2.** et la question précédente, il vient que $\left|X^G\right| = 1 \not\equiv 0 \pmod 2$ et par conséquent $|X| \equiv 1 \pmod 2$.
6. On vérifie immédiatement qu'il s'agit d'une involution. Comme $|X|$ est impair, il vient de la question **2.** qu'elle admet un point fixe (car elle donne lieu à une action de $\mathbb{Z}/2\mathbb{Z}$ sur X comme ci-dessus). Un tel point fixe est un triplet $(x, y, z) \in X$ tel que $(x, y, z) = (x, z, y)$ soit de la forme (x, y, y) avec $p = x^2 + 4yz = x^2 + 4y^2 = x^2 + (2y)^2$ et on a bien obtenu que p s'écrit comme somme de deux carrés !

Cette démonstration est due au mathématicien Don Zagier et parue en 1990. La preuve usuelle (et classique au programme de l'agrégation) est en général celle du Perrin utilisant les propriétés de l'anneau $\mathbb{Z}[i]$. Mais pour cela, rendez-vous au TD 2 !