FEUILLE N° 7

LU3MA270 – 2023/24

Exercice 1. (a) On a $n_q \mid p$ et $n_q \equiv 1 \mod q$. Donc $n_q \in \{1, p\}$, puis puisque $p < q$, $n_q = 1$. La taille du q-Sylow est q. Comme le nombre q est premier, tout groupe d'ordre q est cyclique, par le théorème de Lagrange.

(b) Un p-Sylow de G est de taille p, qui est premier, donc c'est un groupe cyclique.

(c) On a $S \simeq \mathbb{Z}/q\mathbb{Z}$, donc $\mathrm{Aut}(S) \simeq \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/q\mathbb{Z})^*$. Il y a $\varphi(q) = q - 1$ automorphismes de S. Pour tout $t \in T$ le morphisme de conjugaison par T se restreint au sous-groupe stable S. On obtient un morphisme $T \to \mathrm{Aut}(S)$. L'image de T est un sous-groupe de $\mathrm{Aut}(S)$ donc son cardinal divise $q - 1$. Par le théorème d'isomorphisme de Noether ce cardinal divise aussi celui de T qui est p. Donc il divise $\mathrm{pgcd}(p, q - 1)$, qui vaut 1 par hypothèse. C'est donc le sous-groupe trivial $\{\mathrm{id}\}$. En conclusion T agit trivialement sur S par conjugaison.

(d) En particulier si $S = \langle x \rangle$ et $T = \langle y \rangle$, alors x et y commutent donc xy est d'ordre $\mathrm{ppcm}(p, q) = pq$. On en déduit que $G = \langle xy \rangle$ est cyclique.

Exercice 2. (a) Le nombre q étant premier, le groupe $(\mathbb{Z}/q\mathbb{Z})^*$ est cyclique, isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$. L'élément $(q-1)/p \in \mathbb{Z}$ est d'ordre p dans $\mathbb{Z}/(q-1)\mathbb{Z}$. On considère un antécedent a par l'isomorphisme, qui est aussi d'ordre p.

(b) –

(c) Si $f_{\lambda,b} = f_{\mu,c}$ alors pour tout $x \in \mathbb{Z}/q\mathbb{Z}$:

$$(\lambda - \mu)x = (c - b).$$

Pour $x = 0$, on trouve $b = c$, puis pour $x = 1$, on trouve $\lambda = \mu$.

(d) On a $f_{\lambda,b} \circ f_{\mu,c}(x) = \lambda\mu x + \lambda c + b$. Si $c = -\lambda^{-1}b$ et $\mu = \lambda^{-1}$, on trouve l'identité. On a alors $f_{\mu,c} \circ f_{\lambda,b}(x) = \mu\lambda x + \mu b + c = x$. Donc $f_{\lambda,b}$ est inversible d'inverse $f_{1/\lambda,-b/\lambda}$.

(e) On a $f_{\lambda,b} \circ f_{\mu,c}(x) = f_{\lambda\mu,b+\lambda c}$.

(f) On a vérifié la stabilité par passage à l'inverse et par produit du sous-ensemble non-vide $G \subseteq S_{\mathbb{Z}/q\mathbb{Z}}$ des bijections de la forme $f_{\lambda,b}$. C'est donc un sous-groupe. L'ensemble G est l'image du produit $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ par une application injective. L'ensemble de départ est de cardinal pq, donc $|G| = pq$.

(g) Le groupe G est isomorphe au produit $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ muni de la loi

$$(\lambda, b)(\mu, c) = (\lambda\mu, b + \lambda c).$$

On a donc

$$(\lambda, b)(\mu, c) - (\mu, c)(\lambda, b) = (0, (1 - \mu)b + (\lambda - 1)c).$$

En particulier

$$(a, 1)(a, 0) - (a, 0)(a, 1) = (0, (1 - a)).$$

Comme a est d'ordre p, on a $1 - a \neq 0$. Le groupe G n'est donc pas abélien.

(h) On considère l'application d'évaluation $\varphi\colon f_{\lambda,b} \mapsto f_{\lambda,b}(1-b/\lambda) = \lambda$. C'est une application surjectif $G \to \langle a \rangle$. De plus, on a $f_{\lambda,b} \circ f_{\mu,c}(x) = f_{\lambda\mu,b+\lambda c}$, donc φ est un morphisme de groupes.

(i) Le noyau de φ est formé des translations de $\mathbb{Z}/q\mathbb{Z}$. Ce sous-groupe est isomorphe à $\mathbb{Z}/q\mathbb{Z}$ via l'application d'évaluation $t \mapsto t(0)$.

(j) On a une suite de composition :

$$\{0\} \trianglelefteq \ker(\varphi) \trianglelefteq G.$$

Les quotients successifs sont $\ker(\varphi) \simeq \mathbb{Z}/q\mathbb{Z}$, qui est abélien, et $G/\ker(\varphi) \simeq \varphi(G) = \langle a \rangle \simeq \mathbb{Z}/p\mathbb{Z}$, qui est aussi abélien. Le groupe G est donc résoluble.

Exercice 3. (a) Si $n = 0$ ou $n = 1$, il n'y a pas de transpositions, et il n'y a que des automorphismes intérieurs.

(b) Si $n = 2$, $S_2 = \{\mathrm{id}, (1,2)\}$. Donc f fixe tous les éléments de S_2. On en déduit que $f = \mathrm{id}$ est intérieur.

(c) On a :

$$\sigma = f((1,2))f((1,3)) = f((1,2)(1,3)) = f((2,1,3)).$$

La permutation $(2,1,3)$ est d'ordre 3 donc σ est d'ordre 1 ou 3. Mais σ est le produit de deux transposition distinctes puisque f est injective. Donc σ ne peut pas être l'identité. On en déduit que σ est d'ordre 3. Autrement dit c'est un 3-cycle. On en déduit que le support des transpositions $f(1,2)$ et $f(1,3)$ doit s'intersecter en exactement un point.

(d) Pour $i \geq 4$, on a

$$(12)(1,i)(13) = (1,3,i,2).$$

Par ailleurs, on a

$$f((12)(1,i)(13)) = (e_1,e_2)f((1,i))(e_1,e_3).$$

Si $f((1,i)) = (e_2,e_3)$, on obtient le 2-cycle (e_2,e_3). Mais f est un isomorphisme donc il préserve l'ordre. Il ne peut donc pas envoyer un 4-cycle sur un 2-cycle.

On a donc $f((1,i)) \neq (e_2,e_3)$. Par le raisonnement de la question (c), le support de $f((1,i))$ intersecte lui de $f(1,2)$ et celui de $f(1,3)$ en exactement un point. Si e_1 n'est pas dans le support, alors le support est $\{e_2,e_3\}$, ce qui est exclu. On a donc $f((1,i)) = (e_1,e_i)$, pour un certain élément e_i.

(e) Par le raisonnement de la question (c), les supports de $f((1,i)) = (e_1,e_i)$ et de $f((1,j)) = (e_1,e_j)$ doivent s'intersecter en exactement un point pour $i \neq j$. Donc $e_i \neq e_j$.

(f) On considère la permutation donnée par $\tau(i) = e_i$. Par la formule de conjugaison des cycles, pour toute transposition $(1,i)$, on a $f((1,i)) = \tau(1,i)\tau^{-1}$. Mais les transpositions $(1,i)$ engendrent S_n : par la formule de conjugaison des cycles, on a

$$(i,j) = (1,i)(1,j)(1,i),$$

et les transpositions engendrent S_n. On a donc

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

L'automorphisme f est intérieur.

Exercice 4. (a) On a

$$x = \sigma(x) \iff \Phi(x) = \Phi\sigma(x) \iff \Phi(x) = \Phi\sigma\Phi^{-1}(\Phi(x)).$$

(b) On a $n_5 \mid 4! = 24$ donc $n_5 \in \{1,2,3,4,6,8,12;24\}$ et $n_5 \equiv 1 \mod 5$, donc $n_5 \in \{1,6\}$. Si $n_5 = 1$, tous les conjugués d'un 5-Sylow H, qui sont des 5-Sylow, doivent être égaux à H, donc H est distingué. Mais il n'y a pas de sous-groupe distingué d'indice 24 dans S_5 : ses sous-groupes distingués sont $\{\mathrm{id}\}$, A_5 et S_5. Finalement $n_5 = 6$.

darondeau@imj-prg.fr

(c) L'action de S_5 sur E par conjugaison est transitive. Le stabilisateur de chaque élément de E est donc de cardinal $|S_5|/\#E = 120/6 = 20$. Le noyau de l'action $S_5 \to S_E$ est distingué dans S_5 donc c'est $\{\mathrm{id}\}$, A_5 ou S_5. Ce noyau est l'intersection des stabilisateurs de tous les éléments, donc son cardinal divise 20. Or $|A_n| = 60$ et $|S_n| = 120$. La seul possibilité est donc

$$\ker(S_n \to S_E) = \{\mathrm{id}\},$$

ce qui signifie que le morphisme est injectif.

(d) On a déjà dit que l'action de S_5 sur E est transitive, donc il n'ya qu'une seule orbite, de taille $\#E = n_5 = 6$. En particulier, il n'y a pas d'orbite de taille 1 (c'est à dire de point fixe).

(e) Par définition, si $\sigma \in f(S_5)$ et $x \in E$, on a :

$$g(\sigma) \cdot \Phi(x) = \Phi(\sigma(x)).$$

Les orbites de $G = g(f(S_5))$ sont donc l'image par la bijection Φ des orbites de $f(S_5)$ par E. Il n'y en a qu'une, qui est $g(E) = \{1, \dots, 6\}$. En particulier, l'action est transitive et n'a pas de points fixes.

(f) Si $\sigma \in \ker(h)$, alors pour tout élément $\tau \in S_6$, on a $[\tau] == \sigma \cdot [\tau] = [\sigma\tau]$. En particulier pour $\tau = \mathrm{id}$, on obtient $[\sigma] = [\mathrm{id}]$. Autrement dit $\sigma \in G$. On en conclut que $\ker(h) \subseteq G$. Le noyau du morphisme h est un sous-groupe distingué de S_6, c'est donc $\{\mathrm{id}\}$, A_6 ou S_6. Pour des raisons de cardinal, ça ne peut-être que $\{\mathrm{id}\}$. Le morphisme h est un morphisme injectif entre deux groupes finis de même cardinal, donc c'est un isomorphisme.

(g) Pour tout $g \in G$, On a $G \cdot g \in G$, car G est un sous-groupe. En passant au quotient, on en déduit que le neutre $G \in S_6/G$ est un point fixe de $h(G)$.

(h) Comme précédemment, les orbites de $k(h(G))$ sont les images par la bijection Ψ des orbites de $h(G)$. Une bijection préserve le cardinal donc il y a une orbite de taille 1, c'est-à-dire un point fixe.

(i) Le groupe G agit sans point fixe sur $\{1, \dots, 6\}$ tandis que le groupe $k \circ h$ admet un point fixe. Si $k \circ h$ était intérieur, il serait de la forme $\sigma \mapsto \tau\sigma\tau^{-1}$. Soit $\tau(x)$ un point fixe de $k \circ h(G)$. Cela signifie que c'est un point fixe pour tout $\tau\sigma\tau^{-1}$, $\sigma \in G$. Alors par la question préliminaire, x est un point fixe pour tout $\sigma \in G$, c'est-à-dire un point fixe de G. C'est une contradiction donc $k \circ h \in \mathrm{Aut}(S_6)$ n'est pas un isomorphisme intérieur.

darondeau@imj-prg.fr