Théorie des groupes

Corrigé feuille 7

Exercice 1 $\sigma = (1478)(265)(39)$.

L'ordre de σ est le $ppcm$ des ordres des cycles à supports disjoints. $ordre(\sigma) = ppcm(4, 3, 2) = 6$.

$\varepsilon(\sigma) = \varepsilon(1478)\varepsilon(265)\varepsilon(39) = (-1)(1)(-1) = 1$.

$\sigma = (18)(17)(14)(25)(26)(38)$.

$\sigma^{100} = (1478)^{100}(265)^{100}(39)^{100} = (265)$ car $2 \mid 100$, $4 \mid 100$ et $1 \equiv 100[3]$.

Exercice 2 Soit σ un élément d'ordre 14 dans $\mathfrak{S}_{10}$. On note $\gamma_1\gamma_2 \dots \gamma_r$ sa décomposition en produit de cycles disjoints (ordonnés par taille décroissante puis par premier élément croissant à longueur égale).

on sait que $ordre(\sigma) = ppcm(\text{ordre}(\gamma_1), ordre(\gamma_2), \dots, ordre(\gamma_r))$.

Il n'y a pas de 14-cycle dans $\mathfrak{S}_{10}$, donc $ordre(\gamma_1) = 7$.

L'ordre de γ_2 ne peut pas être 1 (sinon σ est un 7-cycle) ou 7 (car son support est disjoint de celui de γ_2), donc c'est 2.

Si $r > 2$, $ordre(\gamma_3) \neq 1$, ce qui est absurde car son support doit être disjoint avec ceux de γ_1 et γ_2 mais contenu dans $[\![1, 10]\!]$.

D'où $\sigma = \gamma_1\gamma_2$ avec γ_1 un 7-cycle et γ_2 une transposition à support disjoint de γ_1.

Nombre de 7-cycles : Choix de 3 points fixes : $\binom{10}{3}$ possibilités. Nombre de 7-cycles sur les 7 autres points : 6! possibilités.

Nombre de transpositions sur les 3 points restants : choix de 1 point fixe parmi 3.

D'où, le nombre d'éléments d'ordre 14 dans $\mathfrak{S}_{10}$:

$$3\binom{10}{3}6! = \frac{3.10.9.8.6!}{6} = \frac{10!}{14} = 259200.$$

Exercice 3 (Quelques ensembles générateurs)

1. On note $\mu = (\sigma(j_1), \sigma(j_2) \dots \sigma(j_r))$. On cherche à montrer que $\sigma\gamma = \mu\sigma$.
   Remarquons que $Supp(\mu) = \{\sigma(j_1), \dots, \sigma(j_r)\} = \sigma(Supp(\mu))$.
   Soit $m \in [\![1, n]\!]$.
   Si $m \notin Supp(\gamma)$, alors $\sigma(\gamma(m)) = \sigma(m) = \mu(\sigma(m))$ car $\sigma(m) \notin Supp(\mu)$.
   Si $m \in Supp(\gamma)$, alors $m = j_k$ pour un certain k. $\sigma(\gamma(j_k)) = \sigma(j_{k+1}) = \mu(\sigma(j_k)) = \mu(\sigma(m))$.
   Donc $\sigma\gamma = \mu\sigma$.
2. Par récurrence, $\rho_1^k\tau\rho_1^{-k} = (k + 1, k + 2)$. Donc $\{(i, i + 1)\} \subset < \tau, \rho_1 >$.
   $\mathfrak{S}_n \subset < \tau, \rho_1 > \subset \mathfrak{S}_n$, donc $\mathfrak{S}_n = < \tau, \rho_1 >$.
3. $\tau\rho_2 = \rho_1$ donc $\mathfrak{S}_n = < \tau, \rho_1 > \subset < \tau, \rho_2 >$. D'où $< \tau, \rho_2 > = \mathfrak{S}_n$.
4. $(1jk) = (1k)(1j)$ pour tout triplet $1, j, k$ distincts.
   Soit $\sigma \in A_n$, alors il peut se décomposer comme un produit de transpositions de la forme $(1i)$ de longueur paire. $\sigma = (1i_1)(1i_2) \dots (1i_{2k}) =$. On peut supposer que pour tout i_j, $1 \neq i_j \neq i_{j+1}$. Alors $\sigma = (1i_1i_2)(1i_3i_4) \dots (1i_{2k-1}i_{2k}) \in < (1ij) \mid 1 \neq i \neq j \neq 1 >$.

Exercice 4 (Une application combinatoire) On numérote les sièges de 1 à n et les personnes de mêmes. Asseoir tout le monde autour de la table revient donc à choisir une permutation de $\mathfrak{S}_n$ qui a un siège attribue le numéro de la personne qui y est.

On définit la relation d'équivalence sur $\mathfrak{S}_n$: $\sigma \cong \gamma$ si $\forall k, l \in [\![1, n]\!]$, $[\sigma(k) = \gamma(l)] \Rightarrow [\{\sigma(k+1)\sigma(k-1)\} = \{\gamma(l + 1)\gamma(l - 1)\}]$ avec la convention $0 = n$.

Comptons les permutations équivalentes à σ quelconque.

Voyons à présent les n personnes assises à la table ronde comme les n sommets d'un n-gone régulier. Alors D_n, le groupe d'isométrie du n-gone, préserve tous les voisins (car isométries). En effet, D_n est engendré par une rotation de la table d'angle $\frac{2\pi}{n}$ et par une symétrie passant par le centre de la table et le siège 1, les deux étant des transformations qui préservent les voisins. Il y a donc au moins $|D_n| = 2n$ permutation équivalentes à σ.

Il ne peut y en avoir plus. En effet, une fois que l'on a déterminé le nouveau siège de la personne 1 et si on inverse ou pas ses deux voisins, il n'y a qu'une façon de placer les autres convives pour obtenir une permutation équivalente à σ.

Il y a donc $\frac{|\mathfrak{S}_n|}{|D_n|} = \frac{(n-1)!}{2}$ façons de places les n convives à permutation préservant les voisins près.

Exercice 5 On note $N =< r >$ et $H =< s >$. On alors que $N \cong \mathbb{Z}/n\mathbb{Z}$ et $H \cong \mathbb{Z}/2\mathbb{Z}$.

N est un sous-groupe d'indice 2 de D_n donc $N \lhd D_n$.

On a clairement que $D_n =< r >< s >$.

$< r > \cap < s >= \{e\}$.

Par théorème de produit semi-direct, on a que $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$.

$\varphi :< s >\to Aut(\mathbb{Z}/n\mathbb{Z})$ est défini par $\varphi(0) = Id$ et $\varphi(1) = -Id$.

Exercice 6 Soit τ une transposition de $\mathfrak{S}_n$. On note H le groupe $< \tau >$, isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

$\mathfrak{A}_n \ker \epsilon$ donc $\mathfrak{A}_n \lhd G$.

$\mathfrak{A}_n\tau$ est un ensemble de $n!/2$ transpositions distinctes de signature -1. On a donc $\mathfrak{S}_n = \mathfrak{A}_n \sqcup \mathfrak{A}_n\tau = \mathfrak{A}_n H$.

Enfin, τ étant de signature -1, $\mathfrak{A}_n \sqcup H = \{e\}$.

Par théorème de produit semi-direct, $\mathfrak{S}_n \cong \mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$.

Exercice 7 On note H le sous-groupe de $\mathrm{GL}_n(k)$ des matrices diagonales de la forme $E_\lambda = diag(\lambda, 1, \ldots, 1)$, où λ parcourt k^*. Il est clair que $H \cong k^*$ et que H est un sous-groupe de $\mathrm{GL}_n(k)$.

$\mathrm{SL}_n(k) = \ker \det$ donc $\mathrm{SL}_n(k) \lhd \mathrm{GL}_n(k)$.

Soit $M \in \mathrm{GL}_n(k)$. Alors $M = ME_{(\det M)^{-1}}E_{\det M)}$, avec $ME_{(\det M)^{-1}} \in \mathrm{SL}_n(k)$ et $E_{(\det M)} \in H$. Donc $\mathrm{GL}_n(k) = \mathrm{SL}_n(k)H$.

$SL_n(k) \cap H = \{Id\}$ trivialement.

Par théorème de produit semi-direct, $\mathrm{GL}_n(k) \cong \mathrm{SL}_n(k) \rtimes k^*$

Exercice 8 (Les groupes d'ordre 8)

1. L'ordre de tout élément divise 8. G a un unique élément d'ordre 1. G n'a pas d'élément d'ordre 8, sinon il serait cyclique et donc abélien. Si G n'a que des éléments d'ordre 2, il est également abélien. Donc G contient au moins un élément d'ordre 4.
2. Si il existe x d'ordre 2 dans $G\backslash N$. Alors, comme $< i >$ est distingué, $xix \in< i >$. De plus par conservation de l'ordre, $xix = i$ ou i^3.

   Si $xix = i$, alors x, i commutent. Comme $< x, i >= G$ (Car $< x, i >$ contient $< x >$ et i, donc est de cardinal au moins 5 et son cardinal doit diviser 8), G commute. Absurde.

   Donc $xix = i^3$ et $ixix = e$. D'où G isomorphe à D_4 par la proposition de l'exo 5 feuille 6.
3. j^2 et k^2 sont d'ordre 2. Le seul élément d'ordre 2 étant -1, on a $i^2 = j^2 = k^2 = -1$.

   On vérifie facilement que $j, -j, k, -k$ sont tous distincts. Donc $G = \{1, -1, i, -i, j, -j, k, -k\}$.

   D'où $j^3 = -j$ et $k^3 = -k$.

   Pour tout x dans G, $(x(-1)x^{-1})^2 = e$, c'est à dire que le conjugué de -1 par x est d'ordre divisant 2. Ca ne peut pas être e, donc c'est -1. On déduit que pour tout $x \in G$, $x(-1)x^{-1} = (-1)$, et donc $x(-1) = (-1)x$.

   D'où $-1 \in Z(G)$.

   $ij = k$, donc $ijk = k^2 = -1$.

   On peut retrouver tous les produits ainsi. Par exemple $ik = -(ki) = -(kijkk^{-1}j^{-1}) = -(k(-1)k^{-1}(-j)) = -j$. Donc il n'y a qu'une seule table possible. et $G \cong \mathcal{Q}_8$.
4. Soit G abélien d'ordre 8.

   Si G contient un élément d'ordre 8, alors il est cyclique et donc isomorphe à $\mathbb{Z}/8\mathbb{Z}$.

   Sinon : Si G contient x un élément d'ordre 4. $G\backslash < x >$ contient forcément un élément d'ordre 2. En effet, supposons que ce ne soit pas le cas : Alors $G\backslash < x >$ ne contient que des éléments d'ordre 4 dont le carré est x^2 (puisque c'est le seul élément d'ordre 2 de G). Soit y un tel élément. Alors $xy \notin< x >$ (Sinon $y \in< x >$, ce qui serait absurde). Et $(xy)^2 = x^2y^2 = x^4 = e$. Donc $xy \in< x >$. Absurde, donc $G\backslash < x >$ contient un élément z d'ordre 2.

   $< x >\lhd G$ et $< z >\lhd G$ car G abélien.

$< x >< z > = < z >< x >$ car G abélien.

$< x >< z >$ est un sous-groupe d'ordre au moins 5 (contient e, x, x^2, x^3, z) donc est G tout entier.

Par théorème du produit direct : $G \cong < x > \times < z > \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

SINON : G ne contient que des éléments d'ordre 2. On peut donc le munir d'une structure de $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel. En notant $(b_1, \dots, b_n)$ une $\mathbb{Z}/2\mathbb{Z}$, base de G il existe un unique isomorphisme d'espace vectoriel entre G et $(\mathbb{Z}/2\mathbb{Z})^n$. Cela force $n = 3$ (par cardinaux) et fournit un isomorphisme de groupes entre G et $(\mathbb{Z}/2\mathbb{Z})^3$.

Tout groupe d'ordre 8 non-abélien est soit isomorphe à D_4, soit à $\mathcal{Q}_8$. Un moyen facile de les distinguer est de compter les éléments d'ordre 2.

Exercice 9 1. On montre le résultat par récurrence sur n.

$n = 1$: le graphe à un sommet sans arrêtes est connexe.

Supposons n fixé et que tout graphe connexe a n sommets à au moins $n - 1$ arrêtes. Soit T un graphe connexe à $n + 1$ sommets, numérotés de 1 à $n + 1$.

Si tous les sommets ont au moins deux arrêtes, on a alors directement que A contient au moins $n+1$ arrêtes.

Sinon, il existe k un sommet de A dont part une seule arrête (k, j). On note A' le graphe de A privé du sommet k et de l'arrête (k, j). Alors A' est un graphe connexe à n sommets. Par hypothèse de récurrence, il contient au moins $n - 1$ arrêtes. Donc A contient au moins n arrêtes.

Le résultat est montré par récurrence.

2. Soit H un ensemble de transpositions engendrant $\mathfrak{S}_n$. On considère le graphe $G = (\llbracket 1, n \rrbracket, \{(i, j) \mid (ij) \in H\})$.

   Soit $i \in \llbracket 1, n \rrbracket$.

   Les sommets à distance 1 de i sont les images possibles de i après une transposition par un élément de H.

   Les sommets à distance inférieure à 2 sont les images possibles de i après au plus deux transpositions par un élément de H.

   Par récurrence, on peut montrer que les sommets qui sont dans la même composante connexe que i sont tous les sommets accessibles après un nombre fini de transpositions de H.

   D'où : Si H engendre $\mathfrak{S}_n$, alors tous les sommets sont accessibles à i après un nombre fini de transpositions de H, donc la composante connexe de i est G, c'est à dire que G est connexe.

   Par la question 1, G a au moins $n - 1$ arrêtes, c'est à dire que H a au moins $n - 1$ éléments.