Théorie des groupes

Corrigé feuille 9

Exercice 1 $200 = 2^3.5^2$.

D'après les théorèmes de Sylow: $n_5 \equiv 1[5]$ et $n_5 \mid 8$. Donc $n_5 = 1$. Par théorème de Sylow, il existe donc un unique 5-Sylow qui est d'ordre 25 et distingué. Donc G n'est pas simple.

Exercice 2

1. Par théorème de Sylow, $n_q \equiv 1[q]$ et $n_q \mid p < q$, donc $n_q = 1$.

2. Soit P un p-Sylow. P est d'ordre p premier donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

   Q est d'ordre q premier donc isomorphe à $\mathbb{Z}/q\mathbb{Z}$.

   Par ordre des éléments, $P \cap Q = \{e\}$.

   Montrons que $QP = G$:

   -QP est un groupe: Soient $q, q' \in Q$ et $p, p' \in P$. $pq'^{-1}p^{-1} = q_0 \in Q$ car $Q \lhd G$.

   Donc $qpq'^{-1}p'^{-1} = qpq'^{-1}p^{-1}pp'^{-1} = qq_0pp'^{-1} \in QP$. QP est donc un groupe.

   -QP est un groupe contenant Q et P, donc de cardinal $> p$ et q. Comme $|PQ|$ divise $|G| = pq$, on doit avoir $|PQ| = |G|$ et donc $QP = G$.

   Par théorème de produit semi-direct, $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\alpha \mathbb{Z}/p\mathbb{Z}$.

3. $\alpha : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. Donc $ord(\alpha(1)) \mid p$ et $ord(\alpha(1)) = 1$ ou p.

   De plus, $\alpha(1) \mid |\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})|$.

   Comme q est premier, $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^\star$, donc $|\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})| = q - 1$. p ne divise pas $q - 1$ par hypothèse, donc $\alpha(1)$ est d'ordre 1, donc est trivial. Comme 1 génère $\mathbb{Z}/p\mathbb{Z}$, α est le morphisme trivial et le produit est direct.

   Donc G est abélien isomorphe à $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Exercice 3 (Théorème de Wilson)

1. Un p-cycle est d'ordre p.

   Réciproquement, soit $\sigma \in \mathfrak{S}_p$ d'ordre p. σ se décompose en produit de cycles à supports disjoints: $\sigma = \gamma_1 \cdots \gamma_n$.

   $ord(\sigma) = ppcm(ord(\gamma_1), \ldots, \gamma_n)$, Comme pour tout i, $ord(\gamma_i) \leq p$, il doit y avoir un élément d'ordre p dans la décomposition, c'est à dire un p-cycle γ. Les γ_i sont à supports disjoints et $supp(\gamma) = [\![1, p]\!]$, donc $\sigma = \gamma$ est un p-cycle.

2. p est un facteur premier apparaissant à l'exposant 1 dans la décomposition de σ. Donc les p-Sylow sont des groupes cycliques d'ordre p, engendré par un p-cycle (d'après question précédente).

   L'intersection de deux p-Sylow distincts est réduite à l'identité (sinon ils ont un générateur commun donc sont égaux).

   Chaque élément d'ordre p est donc contenu dans un unique p-Sylow et chaque p-Sylow contient $(p - 1)$ éléments d'ordre p.

   Donc: $n_p = \frac{\text{nombre d'éléments d'ordre } p}{p-1}$.

   Il y a $(p - 1)!$ p-cycles dans $\mathfrak{S}_p$, donc $n_p = (p - 2)!$.

3. Par théorème de Sylow, $n_p \equiv 1[p]$, soit $(p - 2)! \equiv 1[p]$.

   En multipliant par $p - 1 = -1$, on obtient le théorème de Wilson.

Exercice 4 $175 = 5^2.7$.

Théorèmes de Sylow:
$n_5 \equiv 1[5]$ et $n_5 \mid 7$ donc $n_5 = 1$ et il existe unique 5-Sylow distingué H_5.
$n_7 \equiv 1[7]$ et $n_7 \mid 25$ donc $n_7 = 1$ et il existe unique 7-Sylow distingué H_7.
$H_5 \cap H_7 = \{e\}$ car les éléments de l'intersection ont un ordre divisant 5^2 et 7.
Pour $x \in H_5$, $y \in H_7$, $xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} \in H_7 = x(yx^{-1}y^{-1}) \in H_5$. Donc x et y commutent.
Donc H_5H_7 est un sous-groupe contenant un sous-groupe d'ordre 25 et un d'ordre 7, donc est G.
Par théorème de produit direct, $G \cong H_5 \times H_7$.
H_7 est abélien car cyclique. H_5 est abélien car d'ordre 5^2.
Donc G abélien.

Exercice 5

1. p, q, r apparaissent avec un exposant 1 dans l'ordre de G. Donc les sous-groupes de Sylow qui leurs sont associés sont cycliques.

   $k \in \{p, q, r\}$. L'intersection de deux k-Sylow distincts est réduite à l'identité (sinon ils ont un générateur commun donc sont égaux).

   Chaque élément d'ordre k est donc contenu dans un unique k-Sylow et chaque k-Sylow contient $(k-1)$ éléments d'ordre k.

   Le nombre d'éléments d'ordre k est donc $n_k(k-1)$. En ajoutant qu'il y a un élément d'ordre 1, on obtient qu'il y a au moins $1 + n_p(p-1) + n_q(q-1) + n_r(r-1)$ éléments dans G.

2. Par théorèmes de Sylow:

   $n_p \equiv 1[p]$ et $n_p \mid qr$. $n_p > 1$, et les seuls diviseurs de qr sont $q < p$, $r < p$ et qr. Le seul qui convient est donc $n_p = qr$.

   $n_q \equiv 1[q]$ et $n_p \mid pr$. $n_q > 1$ et n_q ne peut pas être r car $r < q$, donc $n_q \geq p$.

   $n_r \mid pq$. $n_q > 1$ donc $n_r \geq q$.

3. Si G est simple, on est dans le cas de la question précédente. En appliquant la question 1:

$$pqr \geq qr(p-1) + p(q-1) + q(r-1) + 1$$
$$0 \geq -qr + pq - p + qr - q + 1$$
$$0 \geq (p-1)(q-1)$$

   Ceci est absurde. Donc G n'est pas simple.

Exercice 6 (Simplicité de $\mathfrak{A}_5$...)

1. Montrons que tous les 3-cycles sont conjugués à (123) dans $\mathfrak{A}_5$.

   Soit $(ijk) \in \mathfrak{A}_5$. Alors, il existe $\sigma \in \mathfrak{S}_5$ telle que $(123) = \sigma(ijk)\sigma^{-1}$.

   Si $\sigma \in\in \mathfrak{A}_5$, c'est fini, sinon, on pose $\sigma' = (45)\sigma$. $\sigma' \in \mathfrak{A}_5$ (car une décomposition en transpositions en contient exactement une de plus qu'une décomposition de σ.

   Alors $\sigma'(ijk)\sigma'^{-1} = (45)\sigma(ijk)\sigma^{-1}(45) = (45)(123)(45) = (123)$.

   Donc tout 3-cycle est conjugué à (123) $\mathfrak{A}_5$.

2. Montrons que toutes les doubles transpositions sont conjuguées à $(12)(34)$ dans $\mathfrak{A}_5$.

   Soit $(ij)(kl) \in \mathfrak{A}_5$ une double transposition. Alors, il existe $\sigma \in \mathfrak{S}_5$ telle que $(123) = \sigma(ijk)\sigma^{-1}$.

   Si $\sigma \in\in \mathfrak{A}_5$, c'est fini, sinon, on pose $\sigma' = (12)\sigma$. $\sigma' \in \mathfrak{A}_5$ (car une décomposition en transpositions en contient exactement une de plus qu'une décomposition de σ.

   Alors $\sigma'(ij)(kl)\sigma'^{-1} = (12)\sigma(ij)(kl)\sigma^{-1}(12) = (12)(12)(34)(12) = (34)(12) = (12)(34)$.

   Donc toute double transposition est conjuguée à $(12)(34)$ dans $\mathfrak{A}_5$.

3. Soient σ et γ deux 5-cycles.

   $\mathfrak{A}_5$ est d'ordre $60 = 2^2.3.5$.

   $< \sigma >$ et $< \gamma >$ sont des 5-Sylow de $\mathfrak{A}_5$ donc sont conjugués.

4. Soit H un sous-groupe distingué dans $\mathfrak{A}_5$.

   H est stable par conjugaison. Comme tous les 3-cycles sont conjugués, si H en contient H les contient tous. (De même pour les doubles transpositions).

   Si H contient un 5-cycle σ, alors H contient $< \sigma >$. H stable par conjugaison, donc d'après la question précédente, contient tous les 5-cycles.

   Enfin, l'élément neutre est le seul de son type.

5. Il y a $4! = 24$ 5-cycles. (4 possibilités pour a l'image de 1, puis 3 pour b l'image de a, puis 2 pour c l'image de b, et ensuite on a plus le choix).

   Il y a $\binom{5}{1} = 5$ façons de choisir le point fixe d'une double transfo, puis 3 doubles transpositions possibles sur les 4 points bougés. Soit 15 doubles transpositions.

   Il y a $\binom{5}{2} = 10$ façons de choisir les 2 points fixes d'un 3-cycle, puis 2 3-cycles possibles sur les 3 points bougés. Soit 20 3-cycles.

   Soit $H \lhd G$. Par la question précédente, H contient e, et pour chacun des trois autres types d'éléments, soit les contient tous, soit n'en contient aucun.

   Supposons que H contient exactement un type d'éléments non triviaux. Alors $|H| \in \{1+15, 1+20, 1+24\} = \{16, 21, 25\}$. Aucun de ces nombres n'est un diviseur de 60, donc c'est absurde.

   Supposons que H ne contient exactement deux types d'éléments non triviaux. Alors $|H| \in \{1+15+20, 1+20+24, 1+24$ $\{36, 45, 40\}$. Aucun de ces nombres n'est un diviseur de 60, donc c'est absurde.

   Donc H contient soit aucun élément non trivial soit tous les éléments non triviaux.

   Donc $\mathfrak{A}_5$ est simple.

Exercice 7 (...qui est d'ailleurs le seul groupe simple d'ordre 60) 1. (a) Par théorèmes de Sylow, $n_5 \equiv 1[5]$ et $n_5 \mid 12$. Comme de plus on a supposé G simple, on a $n_5 \neq 1$ (sinon, l'unique Sylow serait distingué). La seule possibilité est donc $n_5 = 6$.

   (b) On fixe une numérotation des 5-Sylow. Cela donne un morphisme $\alpha : G \to \mathfrak{S}_6$. $\ker(\alpha) \lhd G$, comme G est simple, $\ker(\alpha) = G$ ou $\{e\}$. Comme tous les Sylow sont conjugués, l'action n'est pas triviale, donc $\ker(\alpha) = \{e\}$.

   Par le premier théorème d'isomorphisme, $G \simeq Im(\alpha)$, qui est un sous-groupe de $\mathfrak{S}_6$.

   (c) $\mathfrak{A}_6 \lhd \mathfrak{S}_6$ donc $\alpha^{-1}(\mathfrak{A}_6) \lhd G$, d'où $\alpha^{-1}(\mathfrak{A}_6) = G$ ou $\{e\}$.
   Si $\alpha^{-1}(\mathfrak{A}_6) = \{e\}$: Pour tout g dans G, $\alpha(g^2) \in \mathfrak{A}_6$, Donc $g^2 \in \alpha^{-1}(\mathfrak{A}_6)$ et $g^2 = e$. Donc G est abélien, ce qui est absurde car d'ordre non-premier.
   Donc $\alpha^{-1}(\mathfrak{A}_6) = G$. Par injectivité, $\alpha(G) = \mathfrak{A}_6$.

2. (a) $|\mathfrak{A}_6/H| = \frac{|\mathfrak{A}_6|}{|H|} = 6$.

   (b) En numérotant les 6 classes à gauche, l'action donne un morphisme $\varphi : \mathfrak{A}_6 \to \mathfrak{S}_6$. $\ker(\varphi) \lhd \mathfrak{A}_6$qui est simple, donc $\ker(\varphi) = \mathfrak{A}_6$ ou $\{e\}$. Comme l'action n'est pas triviale $\ker(\varphi) = \{e\}$ et donc φ est injective.
   $\mathfrak{A}_6 \lhd \mathfrak{S}_6$ donc $\varphi^{-1}(\mathfrak{A}_6) \lhd \mathfrak{A}_6$, d'où $\varphi^{-1}(\mathfrak{A}_6) = \mathfrak{A}_6$ ou $\{e\}$.
   Si $\varphi^{-1}(\mathfrak{A}_6) = \{e\}$: Pour tout g dans $\mathfrak{A}_6$, $\alpha(g^2) \in \mathfrak{A}_6$, Donc $g^2 \in \alpha^{-1}(\mathfrak{A}_6)$ et $g^2 = e$. Donc $\mathfrak{A}_6$ est abélien, ce qui est absurde.
   Donc $\varphi^{-1}(\mathfrak{A}_6) = \mathfrak{A}_6$. Par injectivité, la corestriction de φ à son image nous donne un isomorphisme $\phi : \mathfrak{A}_6 \to \mathfrak{A}_6$.

   (c) Un élément $x \in \mathfrak{A}_6$ fixe la classe neutre $e.H$ par l'action de translation à gauche si et seulement si $x \in H$. Donc $\phi(H) = Stab_{\mathfrak{A}_6}(H)$.

   (d) Le stabilisateur dans $\mathfrak{A}_6$ d'un élément dans $[\![1, 6]\!]$ est l'ensemble des permutation ayant cet élément comme point fixe, donc est isomorphe à $\mathfrak{A}_5$, donc $\phi(H) = \mathfrak{A}_5$.

   (e) On a montré que $G \cong \phi(\alpha(G)) = \phi(H) = \mathfrak{A}_5$. Donc tout groupe simple d'ordre 60 est isomorphe à $\mathfrak{A}_5$.