Corrigé de l'examen "Groupes"

I - Une action de groupe.

1. L'action est bien définie car $gxH = gyH$ implique (appliquer g^{-1} à gauche des deux côtés de l'égalité) $xH = yH$.

   On vérifie directement que pour tous $g_1, g_2 \in G$ on a $g_1(g_2xH) = g_1g_2xH$, et de plus $1.xH = xH$ ainsi les deux axiomes pour une action de groupe sont bien satisfaits.

   Le stabilisateur d'une classe xH est l'ensemble des $g \in G$ tels que $gxH = xH$, ce qui équivaut à $x^{-1}gxH = H$ ou encore $x^{-1}gx \in H$. Finalement $\mathrm{Stab}(xH) = xHx^{-1}$.

2. Si x_iH, $i = 1, \cdots, p$ est un système de représentants pour les classes modulo H, en définissant σ par $gx_iH = x_{\sigma(i)}H$ on obtient un morphisme de groupe $\varphi : G \to S_p$. En effet si $\varphi(g) = \sigma$ et $\varphi(g') = \sigma'$ alors pour tout i on a

   $$g'(gx_iH) = g'x_{\sigma(i)}H = x_{\sigma'\circ\sigma(i)}H$$

   ce qui donne $\varphi(g'g) = \sigma' \circ \sigma$ comme attendu.

   Le morphisme φ ne peut être trivial : en effet H est d'indice $p \geq 2$ donc est un sous-groupe strict, et si $g \in G \setminus H$ alors $g \cdot H \neq H$, en particulier $g \notin \ker\varphi$.

3. Par le théorème de passage au quotient on a $G/\ker(\varphi)$ isomorphe à un sous-groupe F de S_p (l'image de φ), donc $|G| = |\ker(\varphi)|.|F|$. On a $|F|$ qui divise $p!$, donc les facteurs premiers de $|F|$ sont inférieurs ou égaux à p; mais ce sont aussi des facteurs de $|G|$, on en déduit que p est le seul facteur premier de $|F|$. Finalement comme p ne divise pas $(p-1)!$, ou bien $|F| = 1$: mais ceci est exclu car φ n'est pas trivial, ou bien $|F| = p$, autrement dit $\ker(\varphi) \subset G$ est d'indice p.

4. On remarque que si $gH = H$ on a $g \in H$, donc $\ker(\varphi) \subset H$. On a inclusion entre deux sous-groupes de même cardinal, donc $\ker(\varphi) = H$ et H est donc distingué (car un noyau est toujours un sous-groupe distingué).

5. Soit $H \subset G$ un sous-groupe d'indice 2. Soit $x \in G$, on veut montrer que $xH = Hx$. Si $x \in H$, c'est clair (ces deux classes sont égales à H), donc supposons maintenant $x \notin H$. Le groupe G est l'union disjointe de ses deux classes à gauche, qui sont H et xH. Mais G est aussi l'union disjointe de ses deux classes à droite, qui sont H et Hx. Par différence, on en déduit que $xH = Hx$, comme attendu.

II - Groupes d'ordre 12.

Les groupes abéliens.

1. Comme $12 = 2^2 \cdot 3$, on a deux possibilités pour un groupe abélien d'ordre 12 :

   $$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3,$$
   $$\mathbb{Z}/4 \times \mathbb{Z}/3.$$

   La liste est complète et non redondante d'après le théorème qui dit que tout groupe abélien fini s'écrit de façon unique (à l'ordre des facteurs près) comme un produit direct de facteurs cycliques d'ordre une puissance d'un nombre premier.

(NB : une autre façon est d'utiliser le théorème de classification en terme de facteurs cycliques dont les ordres se divisent successivement, on obtient alors une autre façon d'écrire les deux groupes ci-dessus :

$$\mathbb{Z}/6 \times \mathbb{Z}/2 \quad \text{et} \quad \mathbb{Z}/12.)$$

Le groupe alterné.

2. Il y a 4 classes de conjugaison dans A_4, qui sont l'identité, les trois double-transpositions, et deux classes de 3-cycles (chacune de cardinal 4 : en effet le stabilisateur d'un 3-cycle est d'ordre exactement 3, puisque c'était déjà le cas dans S_4).

   Comme tous sous-groupe distingué doit être une union de classes de conjugaison, et avoir son ordre qui divise 12, on obtient exactement 3 sous-groupes distingués dans A_4 : $\{1\}$, A_4 et V_4 le sous-groupe d'ordre 4 contenant les double-transpositions.

3. Un sous-groupe d'ordre 6 de A_4 serait d'indice 2, donc distingué car de façon générale tout sous-groupe d'indice 2 est distingué (voir Question I.5). On conclut par la question précédente que A_4 n'admet aucun sous-groupe d'ordre 6.

4. Le groupe A_4 contient donc le groupe distingué V_4, ainsi que le sous-groupe d'ordre 3 $H = \langle(123)\rangle$. Le quotient A_4/V_4 est d'ordre 3, et la classe de (123) en est un générateur, ce qui montre que $A_4 = V_4 \rtimes H$. Ce produit n'est pas direct car sinon A_4 serait abélien (comme produit direct de sous-groupes abéliens), or par exemple (123) ne commute pas avec (124).

Le groupe diédral.

5. Le groupe D_6 contient trois classes de conjugaison d'éléments d'ordre 2 :

   - Les trois symétries d'axe passant par des sommets opposés de l'hexagone;
   - Les trois symétries d'axe passant par des milieux d'arêtes opposées;
   - La symétrie centrale (qui engendre le centre de D_6).

   Les autres éléments sont l'identité, deux rotations d'ordre 3, deux rotations d'ordre 6.

   On conjugue les symétries à l'intérieur d'une même classe via les rotations d'ordre 3.

6. Considérons l'hexagone régulier comme ayant ses sommets sur les racines 6èmes de l'unité. Soit H le sous-groupe de D_6 engendré par la rotation d'angle $2i\pi/3$ et par la symétrie le long de l'axe des réels : le groupe H est isomorphe à S_3, car il s'agit du groupe des isométries du plan préservant le triangle équilatéral de sommets les racines cubiques de l'unité (un dessin est apprécié).

   H étant d'indice 2 il est distingué, et la classe de la symétrie centrale s engendre le groupe quotient.

   Ainsi D_6 est le produit direct (car H et $\langle s\rangle$ sont tous deux distingués, ici il est crucial de ne pas avoir pris s une symétrie axiale...) de $H \simeq S_3$ et $\langle s\rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

7. Soit s la symétrie par rapport à l'axe des réels, et r la rotation d'angle $2i\pi/6$. Le groupe engendré par r est d'indice 2 donc distingué, et la classe de s engendre le quotient, donc $D_6 = \langle r\rangle \rtimes \langle s\rangle \simeq \mathbb{Z}/6\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. De plus ce produit n'est pas direct car D_6 n'est pas abélien (on a vu qu'il contenait une copie de S_3).

Un troisième larron.

8. On a $I^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, donc I est d'ordre 4, et d'autre part J est d'ordre 3. De plus

$$IJI = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} j & 0 \\ 0 & j^2 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -j^2 & 0 \\ 0 & -j \end{smallmatrix}\right) = -J^2 = I^2J^2.$$

   Autrement dit $JI = IJ^2$. On en déduit que les éléments de G s'écrivent de façon unique I^aJ^b avec $0 \leq a \leq 3$, $0 \leq b \leq 2$, ainsi $|G| = 12$.

9. - A_4 et D_6 ne sont pas isomorphes car on a vu que D_6 contient un groupe d'ordre 6, mais pas A_4.
   - A_4 et G ne sont pas isomorphes car G contient un groupe d'ordre 6 (celui engendré par J et I^2), ce qui n'est pas le cas pour A_4.
   - D_6 et G ne sont pas isomorphes, car G contient des éléments d'ordre 4 (I par exemple), et on a vu que ce n'était pas le cas pour D_6.

III - Quizz.

1. On calcule $\sigma_1 = (123)\circ(215) = (153)$, donc $\sigma_1 = (153)(2)(4)$ et $\sigma_2 = (542)(1)(3)$ sont conjuguées, par exemple par $\alpha = (15432)$.

2. Le groupe alterné A_5 contient 5 classes de conjugaison :

   - celle du neutre, de cardinal 1;
   - celle des 3-cycles, de cardinal 20;
   - celle des double-transpositions, de cardinal 15;
   - une première classe de 5-cycles, de cardinal 12;
   - une deuxième classe de 5-cycles, de cardinal 12.

   Les 24 5-cycles ne peuvent former une seule classe de conjugaison (24 ne divise pas 60), et on trouve qu'une classe de 5-cycle contient exactement 12 éléments (car le centralisateur d'un 5-cycles est égal au groupe engendré par le 5-cycle, puisque c'était déjà le cas dans S_5).

3. Le groupe multiplicatif $(\mathbb{Z}/11\mathbb{Z})^*$ est cyclique, puisque c'est le groupe multiplicatif du corps fini $\mathbb{Z}/11\mathbb{Z}$. La classe de 2 est un générateur, en effet $2^5 = 32 \equiv -1 \mod 11$, donc $\bar{2}$ est bien d'ordre 10 dans $(\mathbb{Z}/11\mathbb{Z})^*$.

4. Chaque $A \in \mathrm{GL}_2(\mathbb{F}_2)$ correspond à une bijection linéaire de $(\mathbb{F}_2)^2$, et donc à une permutation des trois vecteurs non nuls $v_1 = (1,0)$, $v_2 = (0,1)$, $v_3 = (1,1)$. Autrement dit il existe $\sigma_A \in S_3$ tel que $A(v_i) = v_{\sigma_A(i)}$. L'application qui a $A \in \mathrm{GL}_2(\mathbb{F}_2)$ fait correspondre $\sigma_A \in S_3$ est l'isomorphisme cherché.

5. Le groupe $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ est de cardinal 2, il s'identifie à $(\mathbb{Z}/4\mathbb{Z})^\times$ qui est égal à $\{\bar{1}, \bar{3}\}$.

   Concernant la seconde partie de cette question, je me suis planté dans l'énoncé : je voulais demander le cardinal de $(\mathbb{F}_4)^\times$, et attendait la réponse : "$(\mathbb{F}_4)^\times$ est de cardinal 3 car tous les éléments non nuls sont inversibles dans un corps". Mais comme je l'ai formulé en terme de $\mathrm{Aut}(\mathbb{F}_4)$, qui ne peut guère avoir d'autre sens que "les automorphismes **de corps** de $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1) = \{\bar{0}, \bar{1}, \bar{X}, \overline{X+1}\}$", la réponse devenait "le groupe $\mathrm{Aut}(\mathbb{F}_4)$ est de cardinal 2, engendré par la permutation de $\bar{X}$ et $\overline{X+1}$".

6. Il est faux que le cardinal de G est toujours supérieur ou égal au cardinal de $\mathrm{Aut}(G)$: prendre par exemple $G = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$, le groupe d'automorphisme s'identifie à $\mathrm{GL}_3(\mathbb{Z}/2)$ qui est d'ordre 168.

   Un autre exemple vu en cours est celui du groupe S_6, qui se plonge strictement dans $\mathrm{Aut}(S_6)$ comme sous-groupe des automorphismes intérieurs.

7. Si on identifie le groupe S_4 avec les isométries directes de $\mathbb{R}^3$ préservant un cube, le sous-groupe alterné A_4 s'interprète comme le sous-groupe préservant un coloriage des sommets par deux couleurs, de façon à ce que deux sommets reliés par une arête ne soit pas de même couleur (et donc également comme le sous-groupe préservant le tétraèdre dont les sommets sont d'une couleur donnée : la figure 1 montre les deux choix possibles). En effet, ce groupe est clairement d'indice 2, et A_4 est l'unique sous-groupe d'indice 2 dans S_4.

Figure 1: Les deux tétraèdres partageant les mêmes sommets qu'un cube : réalisation géométrique de $A_4 \subset S_4$, puisqu'on visualise $\mathrm{Isom}^+(\text{tétraèdre}) \subset \mathrm{Isom}^+(\text{cube})$

8. Dans S_{10}, l'ordre maximal d'un élément est 30, comme par exemple $(1\,2\,3\,4\,5)(6\,7\,8)(9\,10)$. Pas vraiment de méthode pour cette question à part un tatonnement facile (mais qui deviendrait impraticable pour S_n avec n grand...)