Corrigé de l'examen partiel du 8 mars 2012

Exercice

Soit G un groupe.

1. Pour $a \in G$ et n un entier, on a les équivalences suivantes :

$$a^n = e \Leftrightarrow e = (a^n)^{-1} \Leftrightarrow e = a^{-n} \Leftrightarrow e = (a^{-1})^n \,.$$

On en déduit immédiatement que $ord(a) = ord(a^{-1})$.

2. Soient a et b dans G, et $n > 0$ un entier tel que $(ab)^n = e$. On remarque que

$$(ba)^n = b(ab)^{n-1}a \,.$$

On en déduit que

$$(ba)^n b = b(ab)^{n-1}ab = b(ab)^n = be = b \,,$$

ce qui implique que

$$(ba)^n = (ba)^n bb^{-1} = bb^{-1} = e \,.$$

Comme les rôles de a et de b sont interchangeables, ce qui précède montre aussi que si $m > 0$ est un entier tel que $(ba)^m = e$, alors $(ab)^m = e$. On a donc bien l'égalité $ord(ab) = ord(ba)$.

3. Soient $a, b, c \in G$. On a alors, par une double application de la question précédente :

$$ord(abc) = ord(cab) = ord(bca) \,.$$

4. Posons $a = (1\,2\,3)$, $b = (2\,3)$ et $c = (1\,3)$. On a alors

$$abc = (1\,3\,2) \quad \text{et} \quad bca = c = (1\,3) \,.$$

En particuler, on a donc

$$ord(abc) = 3 \quad \text{et} \quad ord(bac) = 2 \,.$$

5. L'application $\varphi : k \mapsto a^k$ a pour image le sous-groupe $\langle a \rangle$ et pour noyau $m\mathbb{Z}$, où $m = ord(a)$. L'isomorphisme canonique $\mathbb{Z}/\ker(\varphi) \simeq \mathrm{Im}(\varphi)$ s'interprète donc comme un isomorphisme de la forme

$$\mathbb{Z}/m\mathbb{Z} \simeq \langle a \rangle$$

Problème

Partie I

Soit G un groupe fini tel que, pour tout $x \in G$, on ait

$$x^2 = e \,.$$

a) Montrons que G est commutatif. On commence par remarquer que, pour tout $x \in G$, on a

$$x^{-1} = x \,.$$

Pour $x, y \in G$, on a donc

$$yx = (yx)^{-1} = x^{-1}y^{-1} = xy \,.$$

b) Soit $x \in G \setminus \{e\}$. On note $H = \langle x \rangle$ le sous-groupe de G engendré par x. Comme G est commutatif, tout sous-groupe de G est distingué. Il existe une unique structure de groupes sur G/H de sorte que la projection canonique $G \to G/H$ soit un morphisme de groupes. D'autre part, on sait que

$$|G| = |H||G/H|\,.$$

Comme $H = \{e, x\}$, on a $|H| = 2$, de sorte que

$$|G| = 2|G/H|\,.$$

En particulier, l'existence d'un tel élément x implique que G est d'ordre pair. Considérons à présent un élément y du groupe quotient G/H. On peut choisir un élément $x \in G$ de sorte que $y = \overline{x}$, ce qui donne les identifications suivantes :

$$y^2 = \overline{x}^2 = \overline{x^2} = \overline{e} = e$$

(puisque la projection canonique $G \to G/H$, $x \mapsto \overline{x}$ est un morphisme de groupes).

c) Soit m le plus grand entier positif ou nul tel que 2^m divise $|G|$.
Montrons par récurrence sur m que $|G| = 2^m$. Si $m = 0$, alors $|G|$ est impair. Dans ce cas, on doit avoir $G = \{e\}$, car sinon, la question précédente nous dit que $|G|$ est pair, ce qui est absurde. On voit donc bien que $|G| = 1 = 2^0$. Si $m > 0$, on a $|G| > 1$, et donc il existe $x \in G$ tel que $x \neq e$. En posant $H = \langle x \rangle$, on a alors $|G/H| = \frac{|G|}{2}$, et donc le plus grand entier positif ou nul k tel que 2^k divise $|G/H|$ est $k = m - 1$. Il en résulte qu'on peut appliquer l'hypothèse de récurrence à G/H, ce qui nous donne l'égalité $|G/H| = 2^{m-1}$. On en déduit que

$$|G| = 2|G/H| = 2.2^{m-1} = 2^m\,.$$

Partie II

a) Soit $n \geqslant 2$ un entier et $\sigma \in S_n$. Il est clair que tout cycle de longueur k est d'ordre k. Réciproquement, supposons que σ soit d'ordre n. On peut écrire σ comme un produit de cycles dont les supports sont disjoints deux à deux

$$\sigma = \tau_1 \cdots \tau_k\,, \quad k \geqslant 1\,,$$

de sorte que $\tau_i \tau_j = \tau_j \tau_i$ pour tous $1 \leqslant i, j \leqslant k$. On en déduit que

$$ord(\sigma) = \max_{1 \leqslant i \leqslant k} ord(\tau_i)\,.$$

L'un des cycles τ_i doit donc être d'ordre n, et donc doit avoir pour support $\{1, \ldots, n\}$. Cela implique que $k = 1$, et donc que σ est un cycle d'ordre n.

b) Soit E un ensemble fini de cardinal n. On se donne une bijection

$$\alpha : E \to E$$

telle que $\alpha^n = id_E$ et telle que $\alpha^i \neq id_E$ pour $0 < i < n$. Choisissons une bijection

$$\begin{aligned} \{1, \ldots, n\} &\to E \\ i &\mapsto x_i\,. \end{aligned}$$

Il existe alors une unique permutation $\sigma \in S_n$ telle que, pour tout i, $1 \leqslant i \leqslant n$, on ait

$$\alpha(x_i) = x_{\sigma(i)}\,.$$

L'hypothèse faite sur α et la question précédente nous permettent d'affirmer que σ est nécessairement un cycle d'ordre n. Soit $(x, y) \in E^2$. Il existe alors un unique couple (i, j) avec $1 \leqslant i, j \leqslant n$, tel que $x = x_i$ et $y = x_j$. Comme σ est un cycle de support $\{1, \ldots, n\}$, il existe un entier $k \geqslant 1$ tel que $\sigma^k(i) = j$, ce qui signifie précisément que $\alpha^k(x) = y$.

Partie III

a) Soit n un entier positif ou nul, et soit E un ensemble de cardinal $2n + 1$. On suppose donnée bijection $\sigma : E \to E$ telle que $\sigma \circ \sigma = id_E$. Montrons que, pour tout $x \in E$ tel que $\sigma(x) \neq x$, si on pose $F = E \setminus \{x, \sigma(x)\}$, l'application

$$\begin{aligned} F &\to F \\ y &\mapsto \sigma(y) \end{aligned}$$

est bien définie. Il s'agit de prouver que, si $y \notin \{x, \sigma(x)\}$, alors $\sigma(y) \notin \{x, \sigma(x)\}$. Cela résulte du fait que si $\sigma(y) = x$, alors $y = \sigma(\sigma(y)) = \sigma(x)$, et que si $\sigma(y) = \sigma(x)$, alors $y = \sigma(\sigma(y)) = \sigma(\sigma(x)) = x$. Cette application est clairement injective, et comme F est un ensemble fini, elle doit aussi être bijective.
Montrons par récurrence sur n, qu'il existe $x \in E$ tel que $\sigma(x) = x$. Si $n = 0$, alors E n'a qu'un élément, et alors il n'y a rien à vérifier. Supposons que $n > 0$. Dans ce cas, ou bien $\sigma = id_E$, et alors l'assertion est triviale, ou bien $\sigma \neq id_E$. Dans le second cas, on peut donc trouver un élément $x \in E$ tel que $x \neq \sigma(x)$. Si on pose $F = E \setminus \{x, \sigma(x)\}$, on a $|F| = |E| - 2 = 2n + 1 - 2 = 2(n-1) + 1$, et l'application

$$\begin{aligned} F &\to F \\ y &\mapsto \sigma(y) \end{aligned}$$

est bijective. L'hypothèse de récurrence s'applique donc ici, ce qui nous fournit l'existence d'un élément $y \in F$ tel que $\sigma(y) = y$.

b) Soit G un groupe fini non trivial d'ordre pair. Posons $E = G \setminus \{e\}$. Comme l'entier $|E|$ est impair, la question précédente appliquée à la bijection

$$\begin{aligned} E &\to E \\ x &\mapsto x^{-1} \end{aligned}$$

implique qu'il existe $x \in E$ tel que $x = x^{-1}$, se qui s'écrit encore $x^2 = e$.

Partie IV

Soit p un nombre premier impair. On considère un groupe fini G d'ordre $p + 1$. On suppose donné un automorphisme

$$\alpha : G \to G$$

tel que $\alpha^p = id_G$ et $\alpha \neq id_G$.

a) Soit $\mathrm{Aut}(G)$ le groupe des automorphismes de G ; il est clair que α est un élément d'ordre fini de $\mathrm{Aut}(G)$ et que $ord(\alpha)$ divise p. Comme p est un nombre premier, on doit donc avoir $ord(\alpha) = p$, ce qui signifie précisément que $\alpha^i \neq id_G$ pour $0 < i < p$.

b) On pose $E = G \setminus \{e\}$. Le fait que $\alpha(e) = e$ (puisque α est un morphisme de groupes) et que l'application α soit injective implique aussitôt que l'application

$$\begin{aligned} E &\to E \\ x &\mapsto \alpha(x) \end{aligned}$$

est bien définie et injective. Comme E est un ensemble fini, cette dernière application doit aussi être bijective.

c) Il résulte alors de la question II b) que, pour tous $x, y \in E$, il existe un entier k tel que $\alpha^k(x) = y$. D'autre part, en vertu de la question III b), il existe un élément $x_0 \in E$ tel que $x_0^2 = e$. Soit $x \in G$. Si $x \neq e$, il existe donc un entier k tel que $\alpha^k(x_0) = x$. Comme α (et donc aussi α^k) est un morphisme de groupes, on obtient l'équation

$$x^2 = \alpha^k(x_0)^2 = \alpha^k(x_0^2) = \alpha^k(e) = e\,.$$

Par conséquent, la question I c) implique que

$$p + 1 = |G| = 2^m$$

pour un certain entier positif m, de sorte que

$$p = 2^m - 1\,.$$