Université Claude Bernard Lyon 1 — L3 Mathématiques : Groupes
Automne 2023

CORRIGÉ DU CONTRÔLE PARTIEL
Mercredi 25 octobre 2023 – Durée : 1h30 (08h00 - 09h30)

Les documents, écrans, téléphones portables et calculettes ne sont pas autorisés.

Exercice 1. Choisir la réponse A ou B. On justifiera toute réponse par un argument clair ou un contre-exemple.

1. Tout groupe dont l'ordre est un nombre premier est abélien.

A. Vrai

Preuve. Soit G avec $|G| = p$ premier et $g \in G \setminus \{e\}$. Par le théorème de Lagrange, $|\langle g\rangle|$ divise p. Comme p est premier, $|\langle g\rangle| = p$ et donc $G = \langle g\rangle$. Ainsi G est cyclique et donc abélien.

2. Si deux sous-groupes H et K d'un groupe G, d'ordre m et n vérifient $\text{pgcd}(m, n) = 1$, alors $H \cap K = \{e\}$.

A. Vrai

Preuve. $|H \cap K|$ divise m et n (par le théorème de Lagrange) et comme $pgcd(m, n) = 1$ on a $|H \cap K| = 1$ et donc $H \cap K = \{e\}$.

3. Soit le cycle $c = (12345678)$ dans le groupe des permutations S_8. La liste L des ordres de c^l, $l \in [1, 7]$, est $L = (8, 4, 8, 2, 8, 4, 8)$.

A. Vrai

Preuve. On a $ord(c) = 8$ et $ord(c^l) = 8/pgcd(8, l)$. D'où

$$ord(c^1) = 8/pgcd(8,1) = 8,\ ord(c^2) = 8/pgcd(8,2) = 4,\ ord(c^3) = 8/pgcd(8,3) = 8,$$

$$ord(c^4) = 8/pgcd(8,4) = 2,\ ord(c^5) = 8/pgcd(8,5) = 8,\ ord(c^6) = 8/pgcd(8,6) = 4,$$

$$ord(c^7) = 8/pgcd(8,7) = 8.$$

4. Soit G un groupe et $H \leq G$ un sous-groupe distingué d'indice n. Alors quel que soit $g \in G$, $g^n \in H$.

A. Vrai

Preuve. Soit $\pi : G \to G/H$ la projection canonique. Alors $|G/H| = [G : H] = n$ et donc $\pi(g)^n = 1$ pour tout $g \in G$. Or $\pi(g)^n = \pi(g^n)$ et donc $g^n \in Ker(\pi) = H$.

5. Soit $f : G \to H$ un morphisme de groupes et soit x un élément de G d'ordre fini. Alors l'ordre de x divise l'ordre de $f(x)$.

B. Faux

Contre-exemple. Soit $f : \mathbf{Z}/2\mathbf{Z} \to \{1\}$ le morphisme trivial et a un générateur de $\mathbf{Z}/2\mathbf{Z}$. Alors $ord(a) = 2$, $ord(f(a))) = 1$ et 2 ne divise pas 1 [Remarquons que d'une façon générale, si $n = ord(x)$ alors $f(x^n) = f(x)^n = e$ et donc $ord(f(x))$ divise $ord(x)$].

6. Soit G un groupe abélien fini et p un nombre premier ne divisant pas $|G|$. Alors l'application $G \to G : x \mapsto x^p$ est un automorphisme de G.

A. Vrai

Preuve. Posons $\pi : G \to G, \pi(x) = x^p$. Comme G est abélien, π est bien définie et est un morphisme. Si $ker(\pi) \neq \{1\}$ on aurait un élément d'ordre p, contradiction avec le théorème de Lagrange. Donc $ker(\pi) = \{1\}$ et donc π est injectif. Comme G est fini, on a π est surjectif.

7. L'ordre maximal d'une permutation de S_5 vaut 5.

B. Faux

Contre-exemple. Posons $\sigma = (12)(345)$. Alors $ord(\sigma) = ppcm(2, 3) = 6$.

Exercice 2. On dit de deux éléments a, b d'un groupe G qu'ils sont *conjugués* s'il existe $g \in G$ tel que $g^{-1}ag = b$. Soit G un groupe.

1. Montrer que si deux éléments de G sont conjugués alors ils ont le même ordre.

Soit $a, b, c \in G$ tels que $c^{-1}ac = b$. Si $ord(a) = n$ alors $b^n = c^{-1}a^nc = 1$ et donc b est d'ordre fini divisant n. Par symétrie (puisque $a = cbc^{-1}$), $ord(a)$ divise $ord(b)$. Donc si a (resp. b) est d'ordre fini, il en est de même de b (resp. a) et $ord(a) = ord(b)$. Si $ord(a) = \infty$, par ce qui précède $ord(b) = \infty$.

2. Déterminer deux éléments dans $\mathbb{Z}/3\mathbb{Z}$ qui ont le même ordre mais qui ne sont pas conjugués.

On utilise la notation additive. On a $G = \mathbb{Z}/3\mathbb{Z} = \{e, a, -a\}$, où on peut prendre $a = \bar{1}$. Alors $ord(a) = ord(-a) = 3$ et pour tout $g \in G$, $-g + a + g = a \neq -a$ et donc a n'est pas conjugué à $-a$.

3. Déterminer tous les groupes abéliens G qui vérifient : deux éléments sont conjugués si et seulement si ils ont le même ordre.

Comme G est abélien cela devient : deux éléments sont identiques si et seulement si ils ont le même ordre. Supposons $G \neq \{e\}$ et soit $g \in G \setminus \{e\}$. Alors $ord(g) = ord(g^{-1})$ et donc $g = g^{-1}$. D'où $g^2 = e$ et $ord(g) = 2$. Donc n'importe quels deux éléments non triviaux sont identiques. D'où $|G| = 2$ et $G = \mathbf{Z}/2\mathbf{Z}$. Donc les seuls groupes abéliens qui vérifient la propriété énoncée sont le groupe trivial et $\mathbf{Z}/2\mathbf{Z}$.

4. Est-ce que n'importe quels deux éléments de S_3 sont conjugués si et seulement si ils ont le même ordre ?

Posons $e = Id, \sigma = (123), \sigma^2 = (132), \alpha = (12), \beta = (23), \ \gamma = (31)$. On a $ord(\sigma) = ord(\sigma^2) = 3$, $ord(\alpha) = ord(\beta) = ord(\gamma) = 2$ et

$$\beta\sigma\beta^{-1} = \sigma^2, \ \sigma\alpha\sigma^{-1} = \beta, \ \sigma\beta\sigma^{-1} = \gamma.$$

Donc S_3 vérifie bien la propriété énoncée.

Exercice 3. Soit G un groupe dont l'élément neutre est noté e et de loi $(a, b) \mapsto ab$. Pour un entier naturel $n \geq 2$, on pose

$$G_n = \{g \in G, \ g^n = e\}.$$

On souhaite décrire l'ensemble $Hom(\mathbf{Z}/n\mathbf{Z}, G)$ des morphismes $\varphi : \mathbf{Z}/n\mathbf{Z} \to G$ du groupe $(\mathbf{Z}/n\mathbf{Z}, +)$ vers G. Pour $\varphi \in Hom(\mathbf{Z}/n\mathbf{Z}, G)$, on notera $\varphi(\overline{1}) = \hat{\varphi}$.

1. Montrer que $\hat{\varphi} \in G_n$.

On a $\hat{\varphi}^n = \varphi(\overline{1})^n = \varphi(n\overline{1}) = \varphi(\overline{n}) = \varphi(\overline{0}) = e$ *et donc* $\hat{\varphi} \in G_n$.

On considère l'application

$$\begin{array}{rcl} \Psi : Hom(\mathbf{Z}/n\mathbf{Z}, G) & \to & G_n \\ \varphi & \mapsto & \Psi(\varphi) = \hat{\varphi} \end{array}$$

2. Montrer que Ψ est injective.

Si $\hat{\varphi} = \hat{\varphi'}$, *alors pour tout entier* m, $\varphi(\overline{m}) = \hat{\varphi}^m = \hat{\varphi'}^m = \varphi'(\overline{m})$.

3. Soit $g \in G_n$.
   (a) Montrer que l'application $f : \mathbf{Z} \to G : l \mapsto g^l$ est un morphisme et $n\mathbf{Z} \leq Ker f$.

   Morphisme : $f(l+l') = g^{l+l'} = g^l g^{l'} = f(l)f(l')$. *On a* $f(nl) = g^{nl} = (g^n)^l = e$ *et donc* $n\mathbf{Z} \leq Ker\, f$.

   (b) En déduire qu'il existe un morphisme $\varphi : \mathbf{Z}/n\mathbf{Z} \to G$ tel que $\hat{\varphi} = g$.

   À la main : si $a \equiv b[n]$ *alors* $f(a) = f(b + ln) = g^{b+ln} = g^b = f(b)$, *i.e.* f *est constante sur les classes de congruence modulo* n. *Ceci nous permet de définir* $\varphi : \mathbf{Z}/n\mathbf{Z} \to G$ *comme suit : si* $C = \overline{a}$, *alors* $\varphi(C) = f(a) = g^a$. φ *est un morphisme :* $\varphi(\overline{a} + \overline{b}) = \varphi(\overline{a + b}) = f(a + b) = f(a)f(b) = \varphi(\overline{a})\varphi(\overline{b})$. *On a bien* $\varphi(\overline{1}) = g$. *On peut aussi se servir du théorème d'isomorphisme.*

4. Conclure que Ψ est bijective.

   Par 3 (b), Ψ *est surjective et par 2.* Ψ *est injective.*

5. On suppose ici que G est le groupe U_m des racines $m-$ièmes de l'unité dans $\mathbf{C}$. On rappelle que $U_m = \langle \zeta \rangle$ où $\zeta = e^{\frac{2\pi i}{m}}$.
   (a) Montrer que $(\zeta^k)^n = 1$ ssi $\frac{m}{\text{pgcd}(n,m)}$ divise k.

   Si $1 = (\zeta^k)^n = \zeta^{kn}$, *alors* $m = ord\ (\zeta)$ *divise* nk, *i.e.* $\frac{m}{m\wedge n} | \frac{n}{m\wedge n} k$ *et par Gauss* $\frac{m}{m\wedge n} | k$, *i.e.* $k = d\frac{m}{m\wedge n}, d \in \mathbf{Z}$.

   (b) En déduire la valeur du cardinal $|Hom(\mathbf{Z}/n\mathbf{Z}, U_m)|$.

   Par division euclidienne $d = q(m \wedge n) + r, 0 \leq r \leq m \wedge n - 1$ *et*

   $$\zeta^{d\frac{m}{m\wedge n}} = \zeta^{r\frac{m}{m\wedge n}}.$$

   Il y a donc $m \wedge n$ *morphismes : pour* $r \in [0, m \wedge n - 1]$, *le morphisme s'écrit*

   $$\varphi_r(\overline{a}) = (\zeta^{r\frac{m}{m\wedge n}})^a.$$

   (c) A titre d'exemple établir la liste des morphismes de $\mathbf{Z}/4\mathbf{Z} \to U_6$.

   $4 \wedge 6 = 2$ *:* $\varphi_0(\overline{a}) = 1$ *et* $\varphi_1(\overline{a}) = (\zeta^3)^a = (-1)^a$.