

## Correction du devoir maison

### Partie I : Théorème de Lagrange.

1. Montrons que  $\sim$  est une relation d'équivalence sur  $G$ .

- Pour tout  $g \in G$ ,  $g^{-1}g = e \in H$ , donc  $g \sim g$  :  $\sim$  est réflexive.
- Soient  $(g, g') \in G^2$  tels que  $g \sim g'$ . Alors  $g^{-1}g' \in H$  et donc  $(g^{-1}g')^{-1} = g'^{-1}g \in H$  (car  $H$  stable par passage à l'inverse en tant que sous-groupe). Et donc  $g' \sim g$ , de sorte que  $\sim$  est symétrique.
- Soient  $g_1, g_2, g_3$  trois éléments de  $G$  tels que  $g_1 \sim g_2$  et  $g_2 \sim g_3$ . Alors  $g_1^{-1}g_2 \in H$  et  $g_2^{-1}g_3 \in H$ . Et donc  $g_1^{-1}g_2g_2^{-1}g_3 = g_1^{-1}g_3$  appartient à  $H$  (car  $H$  stable par produit). Par conséquent,  $g_1 \sim g_3$ , donc  $\sim$  est transitive.

Comme annoncé,  $\sim$  est une relation d'équivalence sur  $G$ .

2. Soit  $g \in G$ . Pour tout  $g' \in G$  :

$$g \sim g' \Leftrightarrow g^{-1}g' \in H \Leftrightarrow \exists h \in H, g^{-1}g' = h \Leftrightarrow \exists h \in H, g' = gh \Leftrightarrow g' \in gH.$$

Et donc la classe d'équivalence de  $g$  est  $gH$ .

3. Soit  $g \in G$ . Alors l'application  $\varphi_g : \begin{matrix} H & \longrightarrow & gH \\ h & \longmapsto & gh \end{matrix}$  est surjective par définition de  $gH$ . Elle est injective car si  $gh_1 = gh_2$ , alors  $h_1 = h_2$ .

Donc  $\varphi_g$  est une bijection de  $H$  sur  $gH$ , qui ont donc le même cardinal.

4. Nous savons que les classes d'équivalence de  $\sim$  forment une partition de  $G$ . Notons  $n$  le nombre de classes d'équivalence distinctes, et soient  $E_1, \dots, E_n$  les différentes classes d'équivalence, de sorte que :

$$G = \bigcup_{i=1}^n E_i \text{ et } E_i \cap E_j = \emptyset \text{ si } i \neq j.$$

Alors, le cardinal de  $G$  est égal à la somme des cardinaux des  $E_i$ . Or, chacun des  $E_i$  a même cardinal que  $G$ , donc  $\text{Card}(G) = n \text{Card}(H)$ . Ainsi, l'ordre de  $H$  divise bien l'ordre de  $G$ .

### Partie II : Ordre d'un élément.

5. Puisque  $G$  est fini, le sous-ensemble  $\{g^k, k \in \mathbb{Z}\}$  de  $G$  l'est aussi, et il existe  $k_1, k_2 \in \mathbb{Z}$  tels que  $k_1 < k_2$  et  $g^{k_1} = g^{k_2}$ . Mais alors  $k = k_2 - k_1 \in \mathbb{N}^*$  et satisfait  $g^k = g^{k_2 - k_1} = g^{k_2} * g^{-k_1} = e$ .

L'ensemble  $E = \{k \in \mathbb{N}^* \mid g^k = e\}$  est donc une partie non vide de  $\mathbb{N}^*$  : elle admet un plus petit élément, qu'on appelle l'ordre de  $g$ , et qu'on notera  $o(g)$ .

6. Soit  $k \in \mathbb{Z}$ .

$\Leftarrow$  Si  $o(g)$  divise  $k$ , il existe  $u \in \mathbb{Z}$  tel que  $k = uo(g)$ . Alors :

$$g^k = g^{uo(g)} = \underbrace{(g^{o(g)})^u}_{\text{assoc. de } *} = e^u = e.$$

$\Rightarrow$  Supposons que  $g^k = e$ , et notons  $q$  et  $r$  le quotient et le reste de la division euclidienne de  $k$  par  $o(g)$ , de sorte que :

$$k = qo(g) + r \text{ avec } 0 \leq r < o(g).$$

Calculons :

$$e = g^k = g^{qo(g)+r} = \underbrace{(g^{o(g)})^q}_{\text{assoc. de } *} * g^r = e^q * g^r = g^r.$$

Par minimalité de l'entier  $k$ ,  $r = 0$  et  $k = qo(g)$  est un multiple de  $o(g)$ .

Ainsi,  $g^k = e$  si, et seulement si,  $o(g)$  divise  $k$ .

7. L'inclusion  $\{g^k, k \in \llbracket 0, o(g) - 1 \rrbracket\} \subset \langle g \rangle$  est immédiate. Pour l'inclusion réciproque, soit  $k \in \mathbb{Z}$ . En notant  $q$  et  $r$  le quotient et le reste de  $k$  par  $o(g)$ , on obtient  $g^k = g^r$  en reprenant les calculs effectués dans la question précédente. D'où le résultat puisque  $r \in \llbracket 0, o(g) - 1 \rrbracket$ .

Ainsi,  $\langle g \rangle = \{g^k, k \in \llbracket 0, o(g) - 1 \rrbracket\}$ .

**Remarque.** Notons de plus que les éléments de  $\{g^k, k \in \llbracket 0, o(g) - 1 \rrbracket\}$  sont deux à deux distincts. En effet, si  $k_1, k_2 \in \llbracket 0, o(g) - 1 \rrbracket$  sont tels que  $g^{k_1} = g^{k_2}$ , alors  $g^{k_2 - k_1} = e$ . Par la question précédente,  $o(g)$  divise  $k_2 - k_1 \in \llbracket -o(g) + 1, o(g) - 1 \rrbracket$ , ce qui impose  $k_2 - k_1 = 0$ , et donc  $k_1 = k_2$ .

8. Montrons que  $\varphi$  est bien définie. Soient pour cela  $k, k'$  tels que  $\zeta^k = \zeta^{k'}$ . Alors  $e^{\frac{2ik\pi}{p}} = e^{\frac{2ik'\pi}{p}}$ , d'où  $\frac{2k\pi}{p} \equiv \frac{2k'\pi}{p} [2\pi]$  par propriété de l'exponentielle complexe. Ainsi,  $k \equiv k' [p]$  et  $p$  divise  $k - k'$ . Par la question 6,  $g^{k-k'} = e$ , ce qui se récrit  $g^k = g^{k'}$ .

L'application  $\varphi$  est donc bien définie.

Montrons que  $\varphi$  est un morphisme de groupes. Soient pour cela  $k, k' \in \mathbb{Z}$ . Calculons :

$$\varphi(\zeta^k \times \zeta^{k'}) = \varphi(\zeta^{k+k'}) = g^{k+k'} = g^k * g^{k'} = \varphi(\zeta^k) * \varphi(\zeta^{k'}).$$

Donc  $\varphi$  est un morphisme de groupes de  $(\mathbb{U}_p, \times)$  sur  $(G, *)$ .

Montrons que  $\varphi$  est injective. Soit pour cela  $z \in \mathbb{U}_p$  tel que  $\varphi(z) = e$ . La connaissance de  $\mathbb{U}_p$  assure l'existence d'un entier  $k \in \mathbb{Z}$  tel que  $z = \zeta^k$ . D'où  $e = \varphi(z) = g^k$ , et par la question 6, il existe  $u \in \mathbb{Z}$  tel que  $k = up$ . Ainsi,  $z = \zeta^k = (\zeta^p)^u = 1^u = 1$ . Le noyau de  $\varphi$  est donc réduit à l'élément neutre :  $\varphi$  est injective.

Enfin,  $\varphi$  est évidemment surjective, car pour tout  $h \in \langle g \rangle$ , il existe  $k \in \mathbb{Z}$  tel que  $h = g^k = \varphi(\zeta^k)$  avec  $\zeta^k \in \mathbb{U}_p$ .

Finalement,  $\varphi$  est un isomorphisme de  $\mathbb{U}_p$  dans  $\langle g \rangle$ .

**Remarque.** Si  $G$  est un groupe cyclique d'ordre  $p$ , il existe  $g \in G$  tel que  $G = \langle g \rangle$ . Ce qui précède montre que  $g$  est d'ordre fini, nécessairement égal à  $p$  puisque  $\langle g \rangle = \{g^k, k \in \llbracket 0, o(g) - 1 \rrbracket\}$  est de cardinal  $p$ . On vient alors de montrer que  $G$  est isomorphe à  $\mathbb{U}_p$ . Ainsi, il existe à isomorphisme près un unique groupe cyclique d'ordre  $p$ , et tout groupe cyclique d'ordre  $p$  est isomorphe à  $(\mathbb{U}_p, \times)$  (ou à  $(\mathbb{Z}/p\mathbb{Z}, +)$  puisqu'on a vu en cours que ces deux groupes sont isomorphes).

9.  $\langle g \rangle$  est un sous-groupe de  $G$  de cardinal (ou d'ordre)  $o(g)$ . Par le théorème de Lagrange,  $o(g)$  divise  $|G|$ .

Par la question 6, on obtient  $|g^G| = e$ .

**Remarque.** Nous avons obtenu ce résultat en TD dans le cas d'un groupe commutatif fini.

10. Soit  $p$  un nombre premier. Alors nous savons que  $(\mathbb{Z}/p\mathbb{Z}, +, \times)$  est un corps. Son groupe des inversible est donc  $\mathcal{U}(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$  qui est de cardinal  $p - 1$ .

Soit  $x \in \mathbb{Z}$ . Distinguons deux cas :

- Si  $p$  divise  $x$ , alors  $x \equiv 0 [p]$ , et donc  $x^p \equiv x [p]$ .
- Si  $p$  ne divise pas  $x$ , alors  $x$  et  $p$  sont premiers entre eux (car  $p$  premier). Par conséquent,  $\bar{x}$  appartient à  $\mathcal{U}(\mathbb{Z}/p\mathbb{Z})$  (vu en cours). D'après la question précédente,  $\bar{x}^{p-1} = \bar{1}$ , ce qui se récrit  $x^{p-1} \equiv 1 [p]$ . On obtient l'identité voulue en multipliant par  $x$ .

Dans tous les cas, on retrouve le petit théorème de Fermat : pour tout  $x \in \mathbb{Z}$ ,  $x^p \equiv x [p]$ .

### Partie III : Réciproque du théorème de Lagrange pour les groupes cycliques.

11. Notons pour commencer que  $\zeta = e^{\frac{2i\pi}{n}}$  est un élément d'ordre  $n$  puisque  $\zeta^n = 1$  et que pour tout  $k \in \llbracket 1, n - 1 \rrbracket$ ,  $\zeta^k \neq 1$ . Par conséquent,  $(\zeta^d)^r = \zeta^r d = \zeta^n = 1$  et  $(\zeta^d)^k = \zeta^{kd} \neq 1$  pour tout  $k \in \llbracket 1, r - 1 \rrbracket$  (car  $kd \in \llbracket 1, n - 1 \rrbracket$ ). Ainsi,  $\zeta^d$  est d'ordre  $r$ .

L'ensemble  $H = \langle \zeta^d \rangle$  est le sous-groupe de  $\mathbb{U}_n$  engendré par  $\zeta^d$ , d'ordre  $r$  car  $\zeta^d$  est d'ordre  $r$ .

12. (a) L'ensemble  $\{k \in \mathbb{N}^* \mid \zeta^k \in H'\}$  est une partie de  $\mathbb{N}^*$ , non vide car elle contient  $n$  (puisque  $\zeta^n = 1 \in H'$ ). Elle admet donc un plus petit élément qu'on notera  $k$ .

Montrons que  $H' = \langle \zeta^k \rangle$ .

$\supseteq$  Puisque  $\zeta^k$  appartient à  $H'$  et que  $H'$  est un groupe,  $\langle \zeta^k \rangle$  est inclus dans  $H'$  en tant que plus petit sous-groupe contenant  $\zeta^k$ .

$\subseteq$  Soit  $h \in H'$ . Puisque  $h \in \mathbb{U}_n$ , il existe  $p \in \mathbb{Z}$  tel que  $h = \zeta^p$ . Notons alors  $q \in \mathbb{Z}$  et  $r \in \llbracket 0, k-1 \rrbracket$  le quotient et le reste de la division euclidienne de  $p$  par  $k$ . Alors,  $h = \zeta^p = \zeta^{kq+r} = (\zeta^k)^q \zeta^r$ , ce qui se récrit :

$$\zeta^r = h \times (\zeta^k)^{-q} \in H'$$

car  $h, \zeta^k \in H'$ . Mais par minimalité de  $k$ , cela impose que  $r = 0$ , et donc que  $p = kq$ . Par conséquent,  $h = \zeta^{kq} = (\zeta^k)^q$  appartient à  $\langle \zeta^k \rangle$ .

Ainsi,  $H' = \langle \zeta^k \rangle$ .

- (b) Puisque  $H'$  est d'ordre  $r$  et que  $\zeta^k$  appartient à  $H'$ , il suit que  $\zeta^{kr} = (\zeta^k)^r = 1$  par la question 9. Par la question 6,  $o(\zeta) = n$  divise  $kr$ . Il existe donc  $u \in \mathbb{Z}$  tel que  $kr = un = udr$ , d'où  $k = ud$  (puisque  $r \neq 0$ ). Ainsi,  $d$  divise  $k$ .

En conservant les notations introduites,  $\zeta^k = (\zeta^d)^u \in H$  qui est un sous-groupe, donc  $H' = \langle \zeta^k \rangle \subset H$ . Enfin, puisque  $H$  et  $H'$  sont des ensembles finis de même cardinal  $r$ ,  $H = H'$ .

Résumons :

- on a montré que si  $r$  est un diviseur de  $n$ , l'ordre du groupe  $\mathbb{U}_n$ , alors  $\mathbb{U}_n$  admet un sous-groupe  $H$  d'ordre  $r$ . De plus, ce sous-groupe est unique, c'est le sous-groupe engendré par  $\zeta^d$  avec  $d = \frac{n}{r}$ .
- Puisque tout groupe cyclique d'ordre  $n$  est isomorphe à  $\mathbb{U}_n$ , ce résultat vaut aussi tous les groupes cycliques.

Ainsi, la réciproque du théorème de Lagrange est vraie **pour les groupes cycliques**.



**Mise en garde.**

La réciproque du théorème de Lagrange est fautive en général : le premier contre-exemple pourra être donné lorsqu'on aura étudié plus précisément le groupe symétrique. Le groupe alterné  $\mathfrak{A}_4$  est d'ordre 12, mais n'admet pas de sous-groupe d'ordre 6 bien que 6 divise 12.

13. Par ce qu'on vient d'établir, l'unique sous-groupe d'ordre 4 de  $\mathbb{U}_{32}$  est le sous-groupe engendré par  $\zeta^d$  avec  $d = \frac{32}{4} = 8$ , soit  $\langle \zeta^8 \rangle = \{1, \zeta^8, \zeta^{16}, \zeta^{24}\}$ .

**Remarque.** De même, l'unique sous-groupe de  $(\mathbb{Z}/32\mathbb{Z}, +)$  est  $\langle \bar{8} \rangle = \{\bar{0}, \bar{8}, \bar{16}, \bar{24}\}$ .

**Partie IV : Un peu de botanique des groupes.**

14. Soit  $G$  un groupe fini d'ordre  $p$  premier. Prenons  $g \in G$  différent de l'élément neutre  $e$ . L'ordre du sous-groupe  $\langle g \rangle$  de  $G$  divise l'ordre  $p$  de  $G$ . Il est donc égal à 1 ou à  $p$ .

Si  $\langle g \rangle$  est d'ordre 1, il ne contient qu'un seul élément qui est nécessairement l'élément neutre. Mais alors  $g \in \langle g \rangle = \{e\}$ , ce qui contredit  $g \neq e$ .

Donc  $\langle g \rangle$  est d'ordre  $p$ . Puisque  $\langle g \rangle \subset G$  et que ces deux ensembles sont de même cardinal  $p$ , ils sont donc égaux. Ainsi,  $G = \langle g \rangle$ ,  $G$  est un groupe cyclique à  $p$  éléments. Par la question 8,  $G$  est donc isomorphe à  $\mathbb{U}_p$ .

Soit  $p$  un nombre premier. Montrer que si  $G$  est un groupe fini d'ordre  $p$ , alors  $G$  est isomorphe à  $\mathbb{U}_p$ .

15. Dans cette question, on cherche à déterminer tous les groupes finis d'ordre 4 à isomorphisme près.

- (a) Rappelons que  $\mathbb{U}_4 = \{1, i, -1, -i\}$  et  $\mathbb{U}_2 \times \mathbb{U}_2 = \{(1, 1), (-1, 1), (1, -1), (-1, -1)\}$ . Donnons les tables de ces groupes.

$\times$	1	$i$	-1	$-i$
1	1	$i$	-1	$-i$
$i$	$i$	-1	$-i$	1
-1	-1	$-i$	1	$i$
$-i$	$-i$	1	$i$	-1

$\times$	(1, 1)	(-1, 1)	(1, -1)	(-1, -1)
(1, 1)	(1, 1)	(-1, 1)	(1, -1)	(-1, -1)
(-1, 1)	(-1, 1)	(1, 1)	(-1, -1)	(1, -1)
(1, -1)	(1, -1)	(-1, -1)	(1, 1)	(-1, 1)
(-1, -1)	(-1, -1)	(1, -1)	(-1, 1)	(1, 1)

- (b) Soit  $G$  un groupe d'ordre 4. Nous avons établi dans ce DM que tout élément  $g \in G$  est d'ordre fini, et que son ordre divise 4. Ainsi,  $o(g)$  est égal à 1 (auquel cas  $g = e$ ), 2 ou 4.

Deux cas se présentent :

- S'il existe un élément  $g \in G$  d'ordre 4. Alors  $\langle g \rangle$  est un sous-ensemble de  $G$  de cardinal 4. Puisque  $|G| = 4$ ,  $G = \langle g \rangle$  et  $G$  est un groupe cyclique à 4 éléments. Par ce qu'on a établi,  $G$  est donc isomorphe à  $\mathbb{U}_4$ .
- Sinon, supposons que tous les éléments de  $G$  différents de l'élément neutre sont d'ordre 2. Notons  $G = \{e, a, b, c\}$ , où  $e$  est l'élément neutre de  $G$ , et  $a, b, c$  les trois autres éléments de  $G$ . Par hypothèse,  $a^2 = e = b^2 = c^2$ , et  $a, b$  et  $c$  sont leur propre inverse. Déterminons le produit  $a * b$  :
  - Si  $a \times b = e$ , alors en multipliant par  $a$  à gauche, on obtient  $b = a$ , ce qui est faux car  $a$  et  $b$  sont supposés distincts.
  - Si  $a \times b = a$ , alors en multipliant de nouveau par  $a$  à gauche, on obtient  $b = e$ , ce qui là aussi est faux car  $b \neq e$ . On montre de même que  $a \times b \neq b$ .

Ainsi,  $a \times b = c$ . On montre de même que  $b \times a = c$ ,  $a \times c = c \times a = b$  et que  $b \times c = c \times b = a$ . On peut alors dresser la table de ce groupe :

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

On observe que cette table est « identique » à celle du groupe  $\mathbb{U}_2 \times \mathbb{U}_2$  (quitte à renommer ses éléments). Donc  $G$  est isomorphe au groupe  $\mathbb{U}_2 \times \mathbb{U}_2$ .

On vient ainsi de montrer qu'à isomorphisme près, il existe exactement deux groupes finis à 4 éléments, à savoir  $\mathbb{U}_4$  et  $\mathbb{U}_2 \times \mathbb{U}_2$ . Un corollaire de cette étude est qu'un groupe fini à 4 éléments est nécessairement abélien.

**Remarque.** Par les résultats obtenus en cours et dans ce DM, nous avons montré qu'à isomorphisme près :

- il existe un unique groupe d'ordre 1, qui est  $\mathbb{U}_1 = \{1\}$  ;
- il existe un unique groupe d'ordre 2, qui est  $\mathbb{U}_2 = \{1, -1\}$  ;
- il existe un unique groupe d'ordre 3, qui est  $\mathbb{U}_3 = \{1, j, j^2\}$  ;
- il existe deux groupes d'ordre 4, qui sont  $\mathbb{U}_4$  et  $\mathbb{U}_2 \times \mathbb{U}_2$  ;
- il existe un unique groupe d'ordre 5 (car 5 est premier), qui est  $\mathbb{U}_5 = \{e^{\frac{2ik\pi}{5}}, k = 0, 1, 2, 3, 4\}$ .

On pourrait prolonger cette étude. On trouverait que (mais cela nécessite des outils un peu plus élaborés) :

- il existe deux groupes d'ordre 6,  $\mathbb{U}_6$  qui est abélien, et  $\mathfrak{S}_3$  qui ne l'est pas.
- il existe un unique groupe d'ordre 7 (car 7 est premier), qui est  $\mathbb{U}_7$ .
- il existe trois groupes **abéliens** d'ordre 8, qui sont  $\mathbb{U}_8$ ,  $\mathbb{U}_4 \times \mathbb{U}_2$  et  $\mathbb{U}_2 \times \mathbb{U}_2 \times \mathbb{U}_2$ .