Université de Bretagne Occidentale
UFR Sciences et Techniques
L3 DE MATHEMATIQUES

GROUPES ET GEOMETRIE

Examen terminal, le 14 mai 2019, 15h45-18h45

CORRIGE et BAREME

Exercice 1. a(i). D'après le cours, l'ordre du sous-groupe engendré $\langle g\rangle$ est égal à l'ordre de g qui vaut n. Du coup, $\langle g\rangle$ est cyclique d'ordre n et est donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$. **(0,5 pt)**

a(ii). Soit $S \subseteq \mathbb{C}$ l'ensemble des racines dans $\mathbb{C}$ du polynôme $X^n - 1$. On doit montrer que $H \subseteq S$. Soit $h \in H$. Comme H est d'ordre n, l'ordre de h divise n, d'après le Théorème de Lagrange. On a, en particulier, $h^n = 1$ dans S^1 ou encore, $h^n - 1 = 0$ dans $\mathbb{C}$. Cela veut dire que h est racine dans $\mathbb{C}$ du polynôme $X^n - 1$. D'où $h \in S$. **(0,5 pt)**

a(iii). Rappelons que les racines du polynôme $X^n - 1$ dans $\mathbb{C}$ sont les nombres complexes $e^{\frac{2ik\pi}{n}}$, $k = 0, \dots, n-1$. En particulier, $|S| = n$. Comme $H \subseteq S$ et $|H| = n$, on a $H = S$. En particulier $g \in H$, et même $\langle g\rangle \subseteq H$. Comme g est d'ordre n et $|H| = n$, on a $\langle g\rangle = H$. **(0,5 pt)**

a(iv). Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les éléments de la forme $\bar{a}$, avec $\mathrm{pgcd}(a, n) = 1$. Il suit du a(i) que les générateurs de H sont g^a où $\mathrm{pgcd}(a, n) = 1$ et $0 \leq a \leq n-1$. **(0,5 pt)**

b(i). D'après le a(iii), on a

$$\langle g\rangle = \langle e^{\frac{2i\pi}{m}}\rangle \quad \text{et} \quad \langle h\rangle = \langle e^{\frac{2i\pi}{n}}\rangle.$$

Comme $d|m$ et $d|n$, il existe des entiers naturels non nuls m' et n' tels que $m = m'd$ et $n = n'd$. Du coup,

$$j = (e^{\frac{2i\pi}{m}})^{m'} \in \langle e^{\frac{2i\pi}{m}}\rangle = \langle g\rangle,$$

et de même pour $j \in \langle h\rangle$. **(0,5 pt)**

b(ii). L'intersection $\langle g\rangle \cap \langle h\rangle$ est à la fois un sous-groupe de $\langle g\rangle$ et de $\langle h\rangle$. D'après Lagrange, son ordre divise m et n, et divise donc d. **(0,5 pt)**

b(iii). Comme $j \in \langle g\rangle \cap \langle h\rangle$, on a $\langle j\rangle \subseteq \langle g\rangle \cap \langle h\rangle$. Or, j est d'ordre d, donc $\langle j\rangle$ est un sous-groupe de $\langle g\rangle \cap \langle h\rangle$ d'ordre d. D'après le b(ii), $\langle j\rangle = \langle g\rangle \cap \langle h\rangle$. **(0,5 pt)**

b(iv). On applique le deuxième Théorème d'isomorphisme au groupe $\langle g, h\rangle$ et ses deux sous-groupes $\langle g\rangle$ et $\langle h\rangle$. Remarquons que tous les sous-groupes de $\langle g, h\rangle$ sont distingués, S^1 étant commutatif. On a donc un isomorphisme

$$\langle g, h\rangle/\langle h\rangle \cong \langle g\rangle/(\langle g\rangle \cap \langle h\rangle).$$

En particulier,

$$\frac{|\langle g, h\rangle|}{|\langle h\rangle|} = \frac{|\langle g\rangle|}{|\langle g\rangle \cap \langle h\rangle|}.$$

Comme $|\langle h\rangle| = n$, $|\langle g\rangle| = m$ et $|\langle g\rangle \cap \langle h\rangle| = d$, on obtient que $|\langle g, h\rangle| = \frac{mn}{d}$. **(1 pt)**

b(v). Comme $gh \in \langle g, h\rangle$, l'ordre de gh divise l'ordre de $\langle g, h\rangle$ qui vaut $\frac{mn}{d} = \mathrm{ppcm}(m, n)$. **(0,5 pt)**

b(vi). Prenons $g = h = -1 \in S^1$. Le produit $gh = 1$ est d'ordre $1 \neq \mathrm{ppcm}(2, 2) = 2$. **(0,5 pt)**

b(vii). On a $g = e^{\frac{2ai\pi}{m}}$ et $h = e^{\frac{2bi\pi}{n}}$ avec $\mathrm{pgcd}(a, m) = \mathrm{pgcd}(b, n) = 1$. Comme

$$gh = e^{\frac{2ai\pi}{m}} e^{\frac{2bi\pi}{n}} = e^{2i\pi\frac{an+bm}{mn}},$$

il suffit de montrer que $an+bm$ est premier avec mn. Par l'absurde. Soit p un nombre premier divisant $an + bm$ et mn. Comme p est premier, $p|m$ ou $p|n$. Si $p|m$, on a $p|an$. Comme m et n sont premiers entre eux, $p \not| n$. Donc $p|a$ ce qui contredit le fait que a et m sont premiers entre eux. On obtient de même une contradiction lorsque $p|n$. Par conséquence, $an + bm$ et mn sont premiers entre eux. **(0,5 pt)**

c. L'élément $e^{2i\sqrt{2}\pi} \in S^1$ n'est pas d'ordre fini. Sinon, il existerait un entier naturel non nul n tel que $n\sqrt{2} \in \mathbb{Z}$ ce qui impliquerait que $\sqrt{2} \in \mathbb{Q}$ ce qui est absurde comme on sait bien. **(1 pt)**

Exercice 2. a. On a

$$(1\ 2\ 3\ 5)^{-1}(1\ 2\ 3\ 4) = (1)(2)(3\ 4\ 5) = (3\ 4\ 5). \quad \textbf{(0,5 pt)}$$

b. Soit $(i\ j\ k) \in S_5$, avec i, j, k distincts bien-sûr. Soit $\sigma \in S_5$ telle que $\sigma(3) = i$, $\sigma(4) = j$ et $\sigma(5) = k$. On a alors

$$\begin{aligned}(i\ j\ k) = (\sigma(3)\ \sigma(4)\ \sigma(5)) = \sigma(3\ 4\ 5)\sigma^{-1} = \sigma(1\ 2\ 3\ 5)^{-1}(1\ 2\ 3\ 4)\sigma^{-1} = \\ (\sigma(1\ 2\ 3\ 5)\sigma^{-1})^{-1}\sigma(1\ 2\ 3\ 4)\sigma^{-1} = \\ (\sigma(1)\ \sigma(2)\ \sigma(3)\ \sigma(5))^{-1}(\sigma(1)\ \sigma(2)\ \sigma(3)\ \sigma(4)),\end{aligned}$$

ce qui montre que $(i\ j\ k)$ appartient à $\langle S\rangle$. **(1 pt)**

c. On a

$$(1\ 2\ 3)^{-1}(1\ 2\ 3\ 4) = (1)(2)(3\ 4) = (3\ 4). \quad \textbf{(0,5 pt)}$$

d. Soit $(i\ j) \in S_5$ où $i \neq j$. Soit $\sigma \in S_5$ telle que $\sigma(3) = i$ et $\sigma(4) = j$. On a alors

$$\begin{aligned}(i\ j) = (\sigma(3)\ \sigma(4)) = \sigma(3\ 4)\sigma^{-1} = \sigma(1\ 2\ 3)^{-1}(1\ 2\ 3\ 4)\sigma^{-1} = \\ (\sigma(1\ 2\ 3)\sigma^{-1})^{-1}\sigma(1\ 2\ 3\ 4)\sigma^{-1} = \\ (\sigma(1)\ \sigma(2)\ \sigma(3))^{-1}(\sigma(1)\ \sigma(2)\ \sigma(3)\ \sigma(4)) \in \langle S\rangle\end{aligned}$$

d'après le b. **(1 pt)**

e. Soit $T \subseteq S_5$ le sous-ensemble des transpositions. D'après le d, on a $T \subseteq \langle S\rangle$. Du coup, $\langle T\rangle \subseteq \langle S\rangle$. D'après le cours $\langle T\rangle = S_5$. Il suit que $\langle S\rangle = S_5$. **(1 pt)**

f. En prenant $\sigma = (1\ 3)(2\ 4) \in S_5$ dans le d ci-dessus, on a

$$(1\ 2) = (3\ 4\ 1)^{-1}(3\ 4\ 1\ 2).$$

En prenant $\sigma = (1\ 5) \in S_5$ dans le b ci-dessus, on a

$$(3\ 4\ 1) = (5\ 2\ 3\ 1)^{-1}(5\ 2\ 3\ 4).$$

Du coup,

$$(1\ 2) = ((5\ 2\ 3\ 1)^{-1}(5\ 2\ 3\ 4))^{-1}(3\ 4\ 1\ 2) = \\ (5\ 2\ 3\ 4)^{-1}(5\ 2\ 3\ 1)(3\ 4\ 1\ 2) = (4\ 3\ 2\ 5)(5\ 2\ 3\ 1)(3\ 4\ 1\ 2). \quad \textbf{(1 pt)}$$

g. Supposons que $(1\ 2) = \sigma_1 \cdots \sigma_n$ est une décomposition de σ en permutations cycliques d'ordre 4. On a alors

$$-1 = \varepsilon(1\ 2) = \varepsilon(\sigma_1) \cdots \varepsilon(\sigma_n) = (-1)^n$$

et donc n est impair. **(1 pt)**

Exercice 3. a. On a $e \in N$ car $eH = H = He$. Si $g, g' \in N$, on a $(gg')H = g(g'H) = g(Hg') = (gH)g' = (Hg)g' = H(gg')$, et donc $gg' \in N$. Si $g \in N$, on a $gH = Hg$, et donc aussi $g^{-1}(gH)g^{-1} = g^{-1}(Hg)g^{-1}$ ce qui donne $Hg^{-1} = g^{-1}H$, et $g^{-1} \in N$. **(0,5 pt)**

b. Comme $hH = H = Hh$ quel que soit $h \in H$, on a bien $H \subseteq N$. **(0,5 pt)**

c. Par définition de N, on a $gH = Hg$ quel que soit $g \in N$. Le sous-groupe H de N est bien distingué. **(0,5 pt)**

d. Soit $M \subseteq G$ un sous-groupe contenant H dans lequel H est distingué. On a donc $gH = Hg$ quel que soit $g \in M$. Il s'ensuit que $M \subseteq N$. **(0,5 pt)**

e. Soit $g \in K$. Comme $g \in N$, on a $gH = Hg$. Il s'ensuit que H est distingué dans K. **(0,5 pt)**

Exercice 4. a. L'ordre de H est égal à l'ordre de σ. Comme σ est une permutation cyclique de longueur 5, l'ordre de σ est égal à 5. **(0,5 pt)**

b. On a

$$\tau\sigma\tau^{-1} = (\tau(1)\ \tau(2)\ \tau(3)\ \tau(4)\ \tau(5)) = (1\ 3\ 5\ 2\ 4) = \sigma^2. \quad \textbf{(0,5 pt)}$$

c. Soit $N \subseteq S_5$ le normalisateur de H dans S_5. On a donc

$$N = \{\rho \in S_5 \,|\, \rho H \rho^{-1} \subseteq H\}.$$

D'après le b, $\tau\sigma\tau^{-1} \in H$ et donc aussi $\tau\sigma^i\tau^{-1} \in H$ quel que soit $i \in \mathbb{Z}$. Il s'ensuit que $\tau \in N$. Comme $\sigma \in H$ et $H \subseteq N$, on a $\sigma \in N$. Du coup $K = \langle \sigma, \tau \rangle \subseteq N$. D'après le 3e, H est distingué dans K. **(1,5 pt)**

d. Comme K/H est le quotient de K, il est engendré par $\bar{\sigma}, \bar{\tau}$. Or, $\bar{\sigma} = \bar{\mathrm{id}}$ dans K/H. Le groupe quotient K/H est donc monogène et engendré par $\bar{\tau}$. Comme $\tau^4 = \mathrm{id}$, on a $\bar{\tau}^4 = \bar{\mathrm{id}}$. Afin de montrer que $\bar{\tau}$ est d'ordre 4, il suffit de montrer que $\bar{\tau}^2 \neq \bar{\mathrm{id}}$. Or, $\tau^2 = (2\ 5)(3\ 4)$ est d'ordre 2 et ne peut appartenir à H qui est d'ordre 5. Du coup, $\bar{\tau}^2 \neq \bar{\mathrm{id}}$ dans K/H. **(1,5 pt)**

e. On a $|K| = |K/H| \cdot |H| = 4 \cdot 5 = 20$ d'après le a et le d. **(0,5 pt)**