Université de Bordeaux **Algèbre 3**
Licence de Sciences et Technologies
2014-2015

Corrigé du devoir surveillé

Exercice 1

1. (a) Clairement, si u et v sont dans U_6, alors $(uv^{-1})^6 = u^6v^{-6} = 1$, ce qui signifie que uv^{-1} est dans U_6. Ainsi, U_6 est bien un sous-groupe de $\mathbb{C}^*$, en vertu du critère vu en cours.
   Par ailleurs, si $z = re^{i\theta}$ est un nombre complexe non nul ($r = |z| > 0$ et $\theta \in [0, 2\pi[$), alors $z^6 = 1$ si et seulement si $r^6 = 1$ et $6\theta \equiv 0 \mod 2\pi$, c'est-à-dire si $r = 1$ et $\theta = \dfrac{k\pi}{3}$ avec $k \in \{0, 1, \dots, 5\}$. Par conséquent, en posant $\rho = e^{i\frac{\pi}{3}}$, on constate que
   $$U_6 = \left\{1, \rho, \rho^2 : \rho^3, \rho^4, \rho^5\right\} = \langle\rho\rangle$$
   est bien cyclique d'ordre 6.

   (b) En examinant un à un les éléments de U_6, on constate que
   - 1 est d'ordre 1,
   - ρ et ρ^5 sont d'ordre 6,
   - ρ^2 et ρ^4 sont d'ordre 3,
   - ρ^3 est d'ordre 2.

   En particulier, il n'y a pas d'élément d'ordre n pour $n \notin \{1, 2, 3, 6\}$, comme prévu par le théorème de Lagrange...

2. (a) La transposition τ est d'ordre 2, car $\tau^2 = \mathrm{Id}$ et $\tau \neq \mathrm{Id}$ et le cycle γ est d'ordre 3 puisque $\gamma^3 = \mathrm{Id}$, $\gamma^2 \neq \mathrm{Id}$ et $\gamma \neq \mathrm{Id}$.

   (b) Les éléments de S_3 sont :
   - l'identité, d'ordre 1,
   - les transpositions $(1, 2)$, $(1, 3)$ et$(2, 3)$, d'ordre 2,
   - les 3-cycles $(1, 2, 3)$ et $(1, 3, 2)$, d'ordre 3.

3. Les deux groupes ne sont pas isomorphes, par exemple parce que les répartitions de leurs éléments selon leur ordre ne sont pas identiques (le premier contient des élements d'ordre 6 et pas le second). Un autre argument possible est de remarquer que l'un est abélien mais pas l'autre.

Exercice 2

1. D'après le théorème de Lagrange, les ordres possibles pour les éléments de G sont 1, 2, 3 et 6.
2. (a) Comme G est d'ordre 6, et que l'ordre de tout élément d'un groupe divise l'ordre du groupe, on peut déjà affirmer que $(xy)^6 = e$ (on peut aussi le vérifier directement : puisque x et y commutent on a : $(xy)^6 = x^6y^6 = (x^2)^3(y^3)^2 = e$). Pour vérifier que xy est bien d'ordre 6, il reste à vérifier que ni xy, ni $(xy)^2$, ni $(xy)^3$ n'est égal à l'élément neutre.
   - Si $xy = e$, alors $x = y^{-1}$, ce qui est absurde puisque l'un est d'ordre 2 et l'autre d'ordre 3.
   - Si $(xy)^2 = e$, alors, en utilisant le fait que x et y commutent, on conclut que $x^2y^2 = e$, c'est-à-dire $y^2 = e$ (puisque x est d'ordre 2), mais cela est absurde puisque y est d'ordre 3.
   - De même, si $(xy)^3 = e$, on conclut que $x^3 = e$, c'est-à-dire $x = e$ (puisque $x^2 = e$) ce qui est absurde.

   (b) i. Le sous-groupe H est d'ordre 3, par construction. De plus l'application $h \mapsto xh$ induit une bijection de H sur xH. Par conséquent

   $$|H| = |xH| = 3$$

   et pour conclure que G est réunion disjointe de H et de xH, il suffit de vérifier que les deux sous-ensembles ne s'intersectent pas, ce qui est bien le cas car si un élément h appartient à $H \cap xH$, alors il existe $k \in H$ tel que $h = xk$, d'où il résulte que $x = hk^{-1}$ appartient à H, ce qui est impossible car H ne contient pas d'élément d'ordre 2.
   Il s'ensuit que l'élement $z = xyx^{-1}$ appartient à H ou à xH. Dans le second cas ($z \in xH$), on concluerait que $yx^{-1} \in H$, puis que $x^{-1} \in H$ (puisque $y \in H$), ce qui est absurde comme on l'a déjà vu. Par conséquent z appartient à H, ce qui donne trois possibilités que l'on va traiter successivement, par élimination.
   - Si $z = e$, c'est-à-dire $xyx^{-1} = e$, alors $y = x^{-1}\left(xyx^{-1}\right)x = x^{-1}ex = e$, ce qui est absurde.
   - Si $z = y$, c'est-à-dire $xyx^{-1} = y$, alors $xy = yx$, ce qu'on a exclu.
   - Il reste donc la seule possibilité que $z = y^2 = y^{-1}$.

   ii. La partition $G = H \sqcup xH$ permet d'écrire G en extension sous la forme

   $$\begin{aligned} G &= \left\{e, y, y^2, x, xy, xy^2\right\} \\ &= \left\{x^iy^j,\, 0 \le i \le 1,\, 0 \le j \le 2\right\} \end{aligned} \qquad (1)$$

   L'application $\varphi : G \to S_3$ définie par

   $$\varphi(x^iy^j) = \tau^i\gamma^j,\, 0 \le i \le 1,\, 0 \le j \le 2$$

   est clairement injective car

   $$\tau^i\gamma^j = \tau^{i'}\gamma^{j'} \Leftrightarrow \tau^{i-i'} = \gamma^{j'-j}$$

   ce qui n'est possible que si $i \equiv i' \mod 2$ et $j \equiv j' \mod 3$ puisque les sous-groupes engendrés par τ et γ s'intersectent trivialement (leurs ordres sont premiers entre eux), auquel cas $x^iy^j = x^{i'}y^{j'}$.

Comme G et S_3 ont même cardinal, on conclut que φ est une bijection. Il reste à justifier que c'est un morphisme de groupes. Remarquons tout d'abord que la relation $xyx^{-1} = y^2$ établie à la question précédente équivaut, compte tenu des égalités $x = x^{-1}$ et $y^2 = y^{-1}$, à

$$xy = y^{-1}x. \tag{2}$$

Le fait que φ soit un morphisme en résulte presque immédiatement. Pour le vérifier proprement, on peut utiliser l'écriture $G = \{e, y, y^2, x, xy, xy^2\}$ et constater que

- $\varphi(y^i y^j) = \varphi(y^{i+j})\gamma^{i+j} = \gamma^i\gamma^j = \varphi(y^i)\varphi(y^j)$,
- $\varphi(xy^i xy^j) = \varphi(y^{-i}y^j) = \gamma^{-i}\gamma^j = \tau\gamma^i\tau\gamma^j = \varphi(xy^i)\varphi(xy^j)$,
- $\varphi(xy^i y^j) = \varphi(xy^{i+j}) = \tau\gamma^{i+j}\gamma^j = \tau\gamma^i\gamma^j = \varphi(xy^i)\varphi(y^j)$ et
- $\varphi(y^i xy^j) = \varphi(xy^{-i}y^j) = \tau\gamma^{-i}\gamma^j = \gamma^i\tau\gamma^j = \varphi(y^i)\varphi(xy^j)$.

Remarque : on peut également, et c'est aussi rapide, dresser à partir de la relation (2) la table de G et constater qu'elle est identique à celle de S_3, ce qui garantit l'existence d'un isomorphisme de G sur S_3.

3. (a) Si G ne contient pas d'élément d'ordre 3, alors il ne contient pas non plus d'élement d'ordre 6, car le carré d'un tel élément serait d'ordre 3. En vertu du théorème de Lagrange, les seuls ordres possibles pour les éléments de G sont donc 2 et 1 ; les éléments de $G \setminus \{e\}$ sont donc d'ordre 2. En particulier, on a $x^2 = e$ pour tout $x \in G$, c'est-à-dire $x = x^{-1}$ (tout élément est son propre inverse). Par suite, si x et y sont deux éléments quelconques de G on a

$$xyx^{-1}y^{-1} = xyxy = (xy)^2 = e$$

donc

$$xy = yx$$

ce qui signifie que G est abélien. Si x et y sont deux éléments de $G \setminus \{e\}$, le groupe $H = \langle x, y\rangle$ qu'ils engendrent est alors égal à $\{e, x, y, xy\}$ (on utilise ici le fait que x et y commutent). En particulier H est d'ordre 4, qui ne divise pas 6, ce qui contredit le théorème de Lagrange.

(b) Si $H = \langle y\rangle$ et $K = \langle z\rangle$ avec y et z d'ordre 3, alors $H \cap K$ est un sous-groupe commun de H et de K. Son ordre vaut donc 1 ou 3, grâce au théorème de Lagrange. Dans le premier cas $H \cap K = \{e\}$ et dans le second $H = K$. Les éléments d'ordre 3 se rangent donc par paires deux à deux disjointes $\{x, x^{-1}\}$ appartenant à un même sous-groupe d'ordre 3. Leur nombre est donc divisible par 2, et comme $|G \setminus \{e\}| = 5$, il existe par conséquent dans $G \setminus \{e\}$ au moins un élément z qui n'est pas d'ordre 3, donc d'ordre 2 ou 6. Dans le second cas, z^3 est d'ordre 2, et on peut donc conclure qu'il existe toujours un élément d'ordre 2.