Quelques indications de la feuille n°5

Exo. 4.2b Soit $G \subset U$ un groupe *infini*. On se propose de démontrer que $G \subset U$ est alors dense. Rappelons que pour un nombre complexe z de module 1, il existe un *unique* nombre $\theta_z \in [0, 2\pi[$ tel que $z = e^{i\theta_z}$. Notons ensuite

$$\lambda = \inf\{\theta_z : z \in G - \{1\}\} \subset]0, 2\pi[.$$

On va démontrer ce résultat en deux étapes.

- Si $\lambda > 0$. On va prouver que dans ce cas-là, le groupe G est forcément fini, et d'où une contradiction. Pour prouver cette assertion, montrons d'abord que $\lambda = \theta_z$ pour un certain $z \in G - \{1\}$. En effet, si non, comme $\lambda > 0$, on a $\lambda < 2\lambda$. Ainsi, on peut trouver $z_1, z_2 \in G$ tels que $\lambda < \theta_{z_1} < \theta_{z_2} < 2\lambda$. Par suite, on a $\theta_{z_2/z_2} = \theta_{z_2} - \theta_{z_1} \in]0, \lambda[$, ceci nous donne une contradiction avec la définition de λ. Donc, on a forcément $\lambda = \theta_z$ pour un certain $z \in G$.

  Ensuite, montrons que $2\pi/\lambda \in \mathbb{Z}$. Sinon, soit $n = [2\pi/\lambda]$ le plus grand entier $< 2\pi/\lambda$. Alors on a

  $$n\lambda < 2\pi < (n+1)\lambda$$

  Ainsi $z^{n+1} = (e^{i\lambda})^{n+1} = e^{i\cdot(n+1)\lambda} = e^{i\cdot((n+1)\cdot\lambda - 2\pi)}$. Donc $\theta_{z^{n+1}} = (n+1)\lambda - 2\pi \in]0, \lambda[$, ceci nous donne également une contradiction avec la définition de λ. Par suite, on a $2\pi/\lambda$ est un *entier*, noté par n.

  Finalement, quelque soit $u \in G$ un élément, on montre que $\theta_u = e \cdot \lambda$ avec $e \in \mathbb{Z}_{\geq 0}$ un entier. En effet, si non, on peut trouver alors un entier $k \in [0, n-1]$ tel que

  $$k \cdot \lambda < \theta_u < (k+1)\lambda.$$

  Par suite, $\theta_{u/z^k} = \theta_u - k \cdot \lambda \in]0, \lambda[$. Là encore, on obtient une contradiction avec la définition de λ. Donc, $\theta_u = e\lambda$ avec $e \in \mathbb{Z}_{\geq 0}$, ainsi, on trouve que $u = z^e$. C'est-à-dire, $u \in < z >= \mu_n$. Par suite, $G = \mu_n$ est **fini !**. D'où une contradiction !. Par suite, notre hypothèse au départ $\lambda > 0$ n'est pas possible.
- D'après l'étape précédent, on a forcément $\lambda = 0$. Montrons que $G \subset U$ est *dense*. Pour ceci, il suffit de prouver que pour tout interval non vide $]a, b[\subset [0, 2\pi[$, on peut trouver un élément $u \in G$ tel que $\theta_u \in]a, b[$. Or, comme $b - a > 0$, et comme $\lambda = 0$, on peut trouver un élément $g \in G$ tel que $0 < \theta_g < b - a < b$.
  (a) Si $\theta_g > a$, alors il n'y rien à démontrer car $\theta_g \in]a, b[$.
  (b) Si $0 < \theta_g \leq a$. Notons $m = [a/\theta_g]$ le plus grand entier $\leq a/\theta_g$. Alors on a

  $$a < (m+1)\theta_g.$$

  De plus, $(m+1)\theta_g < b$ car $b - (m+1)\theta_g = b - m\theta_g - \theta_g \geq (b-a) - (b-a) = 0$. D'où

  $$a < (m+1)\theta_g < b.$$

  Par suite, $u = g^{m+1}$ vérifie que $\theta_u \in]a, b[$. Ceci achève la preuve.

Exo. 6. Soit G un groupe ayant exactement 2 sous-groupes *propres non triviaux* H et K. Ainsi, G contient exactement 4 sous-groupes : (1), H, K, G. En particulier, le groupe G est *fini*. Dans la suite, on va se distinguer les cas suivants :

1. **Cas où** $H \subset K$ (le cas où $K \subset H$ peut se traiter d'une manière similaire) : On a donc $(1) \subsetneq H \subsetneq K \subsetneq G$. Comme $K \neq G$, soit $g \in G - K$. Alors $< g > \subset G$ est un sous-groupe de G. Par le choix de g, on a

   $$< g > \neq (1), \quad < g > \neq H, \quad < g > \neq K.$$

   Comme G n'a que 4 sous-groupes $(0), H, K, G$, on a donc forcément $G = < g >$. En particulier, G est cyclique. Notons $n = |G|$ l'ordre de G. Si n a au moins deux facteurs premiers *distincts* p, q, alors on peut trouver un sous-groupe d'ordre p, et aussi un sous-groupe d'ordre q. Ainsi, on a ou bien $|H| = p, |K| = q$, ou bien $|H| = q, |K| = p$. En particulier, $(|H|, |K|) = 1$. Ceci nous donne une contradiction car $H \subset G$ est un sous-groupe non trivial. Ainsi l'entier p^e est une puissance de p avec p un premier. Dans ce cas-là,

on sait que G contient alors exactement e+1 sous-groupe. Donc, pour que G contienne exactement 4 sous-groupes, il faut et il suffit que $e+1=4$, autrement-dit, $e=3$. Donc, on a

$$G \simeq \mathbb{Z}/p^3\mathbb{Z}$$

avec p un premier.

2. Supposons maintenant $H \not\subseteq K$ et $K \not\subseteq H$. En particulier, on a

$$H \cap K \subsetneq H, \quad H \cap K \subsetneq K.$$

Par suite, on a forcḿent $H \cap K = (1)$. Encore une fois, comme G n'a que 4 sous-groupes, on en déduit que H et K sont forcément cycliques d'ordre *premier*. Notons $p = |H|$, et $q = |K|$, et soit $h \in H$ (resp. $k \in K$) un générateurs de H (resp. de K). Alors on a

$$H \subsetneq < h, k >, \quad K \subsetneq < h, k > .$$

Ainsi $G =< h, k >$ est engendré par h et k.

Montrons ensuite que $H \subset G$ est *distingué* : en effet, il suffit de regarder kHk^{-1}. Comme H et K sont les seuls sous-groupes propres non triviaux de G, on a donc ou bien $kHk^{-1} = H$, ou bien $kHk^{-1} = K$. Mais la deuxième possibilité est impossible car on aurait alors $H = k^{-1}Kk = K$, ce qui n'est pas possible. Par suite $kHk^{-1} = K$, autrement-dit, $H \subset G$ est *distingué*. De la même manière, on montre que $K \subset G$ est également *distingué*.

Ensuite, montrons que $hk = kh$ de sorte que le groupe G est *commutatif* : en effet, on considère $hkh^{-1}k^{-1} = (hkh^{-1}) \cdot k^{-1}$. Comme $K \subset G$ est distingué, on obtient que $hkh^{-1}k^{-1} \in K$. De la même manière, comme $hkh^{-1}k^{-1} = h \cdot (kh^{-1}k^{-1})$ et comme $H \subset G$ est distingué, on a $hkh^{-1}k^{-1} \in H$. Ainsi, on trouve

$$hkh^{-1}k^{-1} \subset H \cap K = (1).$$

D'où $hk = kh$, par suite, G est commutatif.

Ainsi, on obtient un isomorphisme de groupes

$$H \times K \to G, \quad (h, k) \mapsto hk.$$

Et donc, $G \simeq H \times K \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. Il nous reste à vérifier $p \neq q$. En effet, si non, on aurait un 3-ieme sous-groupe *propre non trivial* d'ordre p de G engendré par hk, ce qui nous donne une contradiction. Donc, on a finalement

$$G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

avec p, q deux premiers *distincts*. Ceci achève la preuve.

Exo. 7. Soient p un premier, et $n \geq 1$ un entier. Notons $G = (\mathbb{Z}/p^n\mathbb{Z})^*$. Rappelons qu'on a $|G| = \varphi(p^n) = p^{n-1}(p-1)$, et pour $n = 1$, le groupe G est cyclique d'ordre $p-1$.

1. **Si p est impair**. Tout d'abord, par récurrence sur k, on montre que pour tout entier $k \geq 1$, on a

$$(1+p)^{p^k} = 1 + a_k p^{k+1}$$

avec a_k un entier convenable *premier* à p. En particulier, ceci montre que l'élément $1+p$ est d'ordre p^{n-1} dans le groupe G.

Ensuite, on considère l'application surjective canonique suivante

$$f : (\mathbb{Z}/p^n\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*.$$

Soit $a \in G$ tel que $f(a) \neq 1$ soit un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^*$. Alors $f(a)$ est d'ordre $p-1$ (car $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p-1$). Par suite, on en déduit que $(p-1)|\mathrm{ord}(a)$: en effet, soit $d = \mathrm{ord}(a)$. Alors $a^d = 1$, puis $f(a)^d = f(a^d) = 1$. Donc $(p-1)|d$. Posons $d' = d/(p-1)$, ainsi, l'élément $b = a^{d'}$ est d'ordre $p-1$.

Maintenant, comme $(p-1, p^{n-1}) = 1$, et comme G est *commutatif*, on trouve que l'élément $b \cdot (1+p) \in G$ est d'ordre $p^{n-1}(1-p) = |G|$. Ainsi, ceci prouve que G est cyclique, engendré par $b \cdot (1+p) \in G$.

2. **Si $p = 2$ est pair.** Remarquons premièrement que pour $n = 1$ ou 2, le groupe $(\mathbb{Z}/2^n\mathbb{Z})^*$ est cyclique d'ordre respectivement 1 et 2. Supposons désormais dans la preuve que $n \geq 3$.

   On montre encore par récurrence que, pour chaque $k \geq 1$, il existe un entier u_k *impair* tel que

$$5^k = 1 + 4 \cdot u_k \cdot 2^k.$$

   Ainsi, la classe de 5 dans $(\mathbb{Z}/2^n\mathbb{Z})^*$ est d'ordre 2^{n-2}. Par suite, cet élément engend un sous-groupe cyclique H d'ordre 2^{n-2}. De plus, si l'on considère

$$g\colon (\mathbb{Z}/2^n\mathbb{Z}) \to (\mathbb{Z}/4\mathbb{Z})^*$$

   On trouve que $\bar{5} \in \ker(g)$. D'autre part, la classe de l'élément -1 dans G est d'ordre 2 (si $n \geq 2$), et on a $g(\overline{-1}) = \overline{-1} \neq 1$ dans le groupe $(\mathbb{Z}/4\mathbb{Z})^*$. Ainsi on trouve que

$$H \cap \overline{-1} \cdot H = \emptyset.$$

   Donc $G = H \cup (\overline{-1}) \cdot H$. Par suite, le morphisme suivant

$$H \times \{\pm 1\} \to (\mathbb{Z}/2^n\mathbb{Z})^*, \quad (h, -1) \mapsto h \cdot overline{-1} \in G.$$

   est bijectif. Donc on a

$$G = (\mathbb{Z}/2^n\mathbb{Z}) \simeq H \times \{\pm 1\} \simeq \mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

   En particulier, G n'est pas cyclique si $n \geq 3$.

Finalement, pour la dernière question de cet exo. on a $(\mathbb{Z}/n\mathbb{Z})^*$ cyclique si et seulement si l'une des conditions suivantes est remplie : (1) $n = p^e$ avec p un premier impair, et $e \geq 0$ un entier ; (2) $n = 2p^e$ avec p premier impair avec $e \geq 0$ un entier ; (3) $n = 2$ ou 4.