Corrigé de devoir non surveillé

Exercice 1 : Groupes de racines de l'unité

1

a Fait en TD.

b Notons n l'ordre de G. D'après la question précédente, pour tout $x \in G$, $x^n = 1$ (car le groupe G est abélien), donc $G \subset \mathbb{U}_n$. Comme ces ensembles ont même cardinal n, $G = \mathbb{U}_n$.

2

a Supposons que m divise n : $n = mk$ pour un certain entier k. Soit $x \in \mathbb{U}_m$: $x^n = x^{mk} = (x^m)^k = 1$, donc $x \in \mathbb{U}_n$, puis $\mathbb{U}_m \subset \mathbb{U}_n$.

Réciproquement, supposons $\mathbb{U}_m \subset \mathbb{U}_n$. En particulier, $e^{2i\pi/m} \in \mathbb{U}_n$, *i.e.* $e^{2i\pi n/m} = 1$, donc m divise n.

b Comme $m \wedge n$ divise m et n, on a $\mathbb{U}_{m\wedge n} \subset \mathbb{U}_m \cap \mathbb{U}_n$.

Réciproquement, soit $x \in \mathbb{U}_m \cap \mathbb{U}_n$, *i.e.* $x^m = x^n = 1$. Soit $mu + nv = m \wedge n$ une relation de Bézout pour (m, n). Il vient :

$$x^{m\wedge n} = x^{mu+nv} = (x^m)^u (x^n)^v = 1,$$

i.e. $x \in \mathbb{U}_{m\wedge n}$, d'où l'inclusion réciproque, puis l'égalité.

c $m \vee n$ étant un multiple commun à m et à n, $\mathbb{U}_{m\vee n}$ contient à la fois $\mathbb{U}_m$ et $\mathbb{U}_n$. C'est aussi un sous-groupe de $\mathbb{U}$. Soit G un sous-groupe de $\mathbb{U}$ contenant $\mathbb{U}_m$ et $\mathbb{U}_n$. Soit $x \in \mathbb{U}_{m\vee n}$, *i.e.* $x^{m\vee n} = 1$. Écrivons $m = (m \wedge n)m'$ et $n = (m \wedge n)n'$, où m' et n' sont des entiers premiers entre eux. On a $m'n = mn' = m \vee n$.

Soit $um' + vn' = 1$ une relation de Bézout entre m' et n'. On a

$$(x^{m'})^n = x^{m'n} = x^{m\vee n} = 1,$$

soit $x^{m'} \in \mathbb{U}_n$ et, de même, $x^{n'} \in \mathbb{U}_m$: $x^{m'}$ et $x^{n'}$ sont des éléments du groupe G, donc $x = x^{um'+vn'}$ aussi.

$\mathbb{U}_{m\wedge n}$ est bien le sous-groupe engendré par $\mathbb{U}_m \cup \mathbb{U}_n$.

Remarque : bien sûr, pour ces deux dernières questions, on pouvait utiliser 1.b et 2.a, en s'assurant au préalable que les sous-groupes considérés étaient bien finis.

3

a G_p est bien sûr une partie non vide de $\mathbb{U}$. Soit $g, h \in G_p$, $n, m \in \mathbb{N}$ tels que $g \in \mathbb{U}_{p^m}$ et $h \in \mathbb{U}_{p^n}$. En posant $k = \max(m, n)$, on a $g, h \in \mathbb{U}_{p^k}$, donc $gh^{-1} \in \mathbb{U}_{p^k} \subset G_p$.

G_p est bien un sous-groupe de $\mathbb{U}$.

b Soit $n \in \mathbb{N}$. G_p contient $\mathbb{U}_{p^n}$ et a donc au moins p^n éléments. Ceci valant pour tout entier naturel n, G_p est infini.

Soit H un sous-groupe propre de G_p : il existe un élément w de G_p que H ne comprend pas. Soit n_0 un entier tel que $w^{p^{n_0}} = 1$.

Soit $h \in H$, et n_1 le plus petit entier tel que $h^{p^{n_1}} = 1$. On a $\mathbb{U}_{p^{n_1}} \subset H$, par minimalité de n_1. Or, w n'appartenant pas à H, $\mathbb{U}_{p^{n_0}}$ n'est pas inclus dans $\mathbb{U}_{p^{n_1}}$, donc $n_0 > n_1$. Ceci prouve l'inclusion de H dans $\mathbb{U}_{p^{n_0-1}}$, et, partant, le fait qu'il soit fini.

c Soit H un sous-groupe propre de G_p. D'après la question précédente, H est fini, inclus dans un sous-groupe $\mathbb{U}_{p^n}$, et donc strictement inclus dans le sous-groupe propre $\mathbb{U}_{p^{n+1}}$: H n'est pas maximal.

G_p n'admet pas de sous-groupe (propre) maximal.