Exercice 2

Soient $m, n > 0$, on cherche à déterminer $\mathbb{U}_m \cap \mathbb{U}_n$.

Tout d'abord $\mathbb{U}_{m\wedge n} \subseteq \mathbb{U}_m$ et $\mathbb{U}_{m\wedge n} \subseteq \mathbb{U}_n$, alors $\mathbb{U}_{m\wedge n} \subseteq \mathbb{U}_m \cap \mathbb{U}_n$

De plus, pour tout $z \in \mathbb{U}_m \cap \mathbb{U}_n$, on a que l'ordre de z divise à la fois m et n, donc il divise $m \wedge n$, et donc $z \in \mathbb{U}_{m\wedge n}$.

Alors $\mathbb{U}_m \cap \mathbb{U}_n \subseteq \mathbb{U}_{m\wedge n}$.

On a donc montré que $\mathbb{U}_{m\wedge n} = \mathbb{U}_m \cap \mathbb{U}_n$

Autre rédaction :

$$\mathbb{U}_n \cap \mathbb{U}_m = \{z \in \mathbb{C} \mid z^m = z^n = 1\}$$

$$\mathbb{U}_n \cap \mathbb{U}_m = \{z \in \mathbb{U} \text{ d'ordre fini } d \mid d|m \text{ et } d|n\}$$

$$\mathbb{U}_n \cap \mathbb{U}_m = \{z \in \mathbb{U} \text{ d'ordre fini } d \mid d|(m \wedge n)\}$$

$$\mathbb{U}_n \cap \mathbb{U}_m = \{z \in \mathbb{U} \mid s^{m\wedge n}\}$$

$$\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_{m\wedge n}$$

Exercice 3

Soient x et y deux éléments d'un groupe G tels que x soit d'ordre 5 et $xyx^{-1} = y^2$.

On a pour tout n :

$$x^n y x^{-1} = y^{2^n}$$

en effet : $xyx^{-1} = y^2$ et si $x^n y x^{-n} = y^{2^n}$, alors :

$$x^{n+1} y x^{-n-1} = x\left(x^n y x^{-n}\right) x^{-1}$$

$$x^{n+1} y x^{-n-1} = x y^{2^n} x^{-1}$$

$$x^{n+1} y x^{-n-1} = \left(xyx^{-1}\right)^{2^n}$$

$$x^{n+1} y x^{-n-1} = \left(y^2\right)^{2^n}$$

$$x^{n+1} y x^{-n-1} = y^{2\cdot 2^n}$$

$$x^{n+1} y x^{-n-1} = y^{2^{n+1}}$$

On a donc que $x^5 y x^{-5} = y^{32}$, or x étant d'ordre 5, on a donc $y = y^{32}$, c'est-à-dire $y^{31} = e$.

31 est un nombre premier, on peut donc affirmer que l'ordre de y est 31, car aucun diviseur strict d de 31 ne vérifie $y^d = e$ (l'unique diviseur strict étant 1).

Exercice 4

Soient g et h dans G avec $(*)$ $ghg^{-1} = h^n$ pour un certain n fixé.

Montrons par récurrence sur $k \in \mathbb{N}$ que $g^{\alpha_1}h^{\beta_1}...g^{\alpha_k}h^{\beta_k}$ peut être écrit sous la forme $g^{\alpha}h^{\beta}$.

On utilisera le fait que pour tout $x, y \in G$ et pour tout $k \in \mathbb{Z}$, $(**)$ $\left(ghg^{-1}\right)^k = \underbrace{ghg^{-1}ghg^{-1}...ghg^{-1}}_{k \text{ fois}} = gh^kg^{-1}$.

<u>$k = 0$:</u>

Une telle écriture désigne e

<u>$k \geqslant 0$:</u>

Supposons la proposition vraie jusqu'à un certain entier k, et on considère

$$g^{\alpha_1}h^{\beta_1}...g^{\alpha_k}h^{\beta_k}g^{\alpha_{k+1}}h^{\beta_{k+1}}$$

Par hypothèse de récurrence :

$$g^{\alpha_1}h^{\beta_1}...g^{\alpha_k}h^{\beta_k}g^{\alpha_{k+1}}h^{\beta_{k+1}} = g^{\alpha}h^{\beta}g^{\alpha_{k+1}}h^{\beta_{k+1}}$$

$$g^{\alpha_1}h^{\beta_1}...g^{\alpha_k}h^{\beta_k}g^{\alpha_{k+1}}h^{\beta_{k+1}} = g^{\alpha+\alpha_{k+1}}g^{-\alpha_{k+1}}h^{\beta}g^{\alpha_{k+1}}h^{\beta_{k+1}}$$

$$g^{\alpha_1}h^{\beta_1}...g^{\alpha_k}h^{\beta_k}g^{\alpha_{k+1}}h^{\beta_{k+1}} = g^{\alpha+\alpha_{k+1}}\left(g^{-\alpha_{k+1}}h^{\beta}g^{\alpha_{k+1}}\right)h^{\beta_{k+1}}$$

$$g^{\alpha_1}h^{\beta_1}...g^{\alpha_k}h^{\beta_k}g^{\alpha_{k+1}}h^{\beta_{k+1}} = g^{\alpha+\alpha_{k+1}}\left(g^{-\alpha_{k+1}}hg^{\alpha_{k+1}}\right)^{\beta}h^{\beta_{k+1}}, \text{ d'après } (**)$$

$$g^{\alpha_1}h^{\beta_1}...g^{\alpha_k}h^{\beta_k}g^{\alpha_{k+1}}h^{\beta_{k+1}} = g^{\alpha+\alpha_{k+1}}\left(g^{-\alpha_{k+1}+1}h^{n}g^{\alpha_{k+1}-1}\right)^{\beta}h^{\beta_{k+1}}, \text{ d'après } (*)$$

$$g^{\alpha_1}h^{\beta_1}...g^{\alpha_k}h^{\beta_k}g^{\alpha_{k+1}}h^{\beta_{k+1}} = g^{\alpha+\alpha_{k+1}}\left(g^{-\alpha_{k+1}+1}hg^{\alpha_{k+1}-1}\right)^{n\cdot\beta}h^{\beta_{k+1}}, \text{ d'après } (**)$$

$$g^{\alpha_1}h^{\beta_1}...g^{\alpha_k}h^{\beta_k}g^{\alpha_{k+1}}h^{\beta_{k+1}} = g^{\alpha+\alpha_{k+1}}\left(g^{-\alpha_{k+1}+2}h^{n}g^{\alpha_{k+1}-2}\right)^{n\cdot\beta}h^{\beta_{k+1}}, \text{ d'après } (*)$$

$$g^{\alpha_1}h^{\beta_1}...g^{\alpha_k}h^{\beta_k}g^{\alpha_{k+1}}h^{\beta_{k+1}} = g^{\alpha+\alpha_{k+1}}\left(g^{-\alpha_{k+1}+2}hg^{\alpha_{k+1}-2}\right)^{n^2\cdot\beta}h^{\beta_{k+1}}, \text{ d'après } (**)$$

$$...$$

$$g^{\alpha_1}h^{\beta_1}...g^{\alpha_k}h^{\beta_k}g^{\alpha_{k+1}}h^{\beta_{k+1}} = g^{\alpha+\alpha_{k+1}}h^{n^{\alpha_{k+1}}\cdot\beta}h^{\beta_{k+1}}$$

$$g^{\alpha_1}h^{\beta_1}...g^{\alpha_k}h^{\beta_k}g^{\alpha_{k+1}}h^{\beta_{k+1}} = g^{\alpha+\alpha_{k+1}}h^{n^{\alpha_{k+1}}\cdot\beta+\beta_{k+1}}$$

$$g^{\alpha_1}h^{\beta_1}...g^{\alpha_k}h^{\beta_k}g^{\alpha_{k+1}}h^{\beta_{k+1}} = g^{\alpha'}h^{\beta'}$$

Avec $\alpha' = \alpha + \alpha_{k+1}$ et $\beta' = n^{\alpha_{k+1}} \cdot \beta + \beta_{k+1}$.

Exercice 5

1. On considère la relation d'équivalence $\sim$ définie par $x \sim y \Longleftrightarrow f(x) = f(y)$.

   On remarque immédiatement que :

$$x \sim y \Longleftrightarrow f(x^{-1}y) = e$$

$$x \sim y \Longleftrightarrow x^{-1}y \in \ker f$$

$$x \sim y \Longleftrightarrow \left(x^{-1}y\right) \ker f = \ker f$$

$$x \sim y \Longleftrightarrow y \ker f = x \ker f$$

   On a alors, par le théorème du passage au quotient, une injection $\varphi : G/\ker f \longrightarrow G'$ définie par $\varphi(g \ker f) = f(g)$ qui de plus est surjective car f l'est.

   On en déduit

$$\text{Card }(G) = \text{Card }(G') \cdot \text{Card }(\ker f)$$

2. On suppose qu'il existe un élément $g \in G$ tel que son ordre, noté n, est premier à celui de $\ker f$.

   On a toujours que l'ordre de $f(g)$ divise n.

   On sait également que n est premier à l'ordre de $\ker f$, alors pour tout diviseur strict k de n, g^k est d'ordre divisant n donc d'ordre toujours premier à celui de $\ker f$, d'où $g^k \notin \ker f$.

   Ainsi $e \neq f(g^k) = \left(f(g)\right)^k$, n est donc l'ordre de $f(g)$.

Exercice 6

On note pour tout $P \in X$ et tout $g \in G$ $g \cdot P = \{g * x \mid x \in P\}$.

1. Soient $P \in X$ et $g \in G$, on a que $g \cdot P$ est l'image de P par la bijection

$$\varphi_g \ : \ \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & g * x \end{array} \right.$$

   (de bijection réciproque $\varphi_{g^{-1}}$) et donc que P et $g \cdot P$ sont équipotents, d'où $g \cdot P \in X$.

2. Pour tout $g, h \in G$ et tout $P \in X$ on a :

$$g \cdot (h \cdot P) = g \cdot \{h * x \mid x \in\}$$

$$g \cdot (h \cdot P) = \{g * h * x \mid x \in\}$$

$$g \cdot (h \cdot P) = \{(g * h) * x \mid x \in\}$$

$$g \cdot (h \cdot P) = (g * h) \cdot \{x \mid x \in\}$$

$$g \cdot (h \cdot P) = (g * h) \cdot P$$

De plus $e \cdot P = \{e * x \mid x \in P\} = P$

Ainsi, l'application $G \times X \longrightarrow X,\ (g, P) \longmapsto g \cdot P$ est bien une action de groupe.

3. Soit $O_1, ...O_n$ une énumération des orbites et pour tout $k = 1, ...n$ on pose $P_k \in O_k$.

   On a alors :

$$|X| = \sum_{k=1}^{n} \text{Card }(G \cdot P_k) \equiv m \mod p$$

$$\sum_{k=1}^{n} \frac{\text{Card }(G)}{\text{Card }(\text{Stab}_G(P_k))} \equiv m \mod p$$

$$\sum_{k=1}^{n} \frac{p^\alpha m}{\text{Card }(\text{Stab}_G(P_k))} \equiv m \mod p$$

   Or $\text{Stab}_G(P_k)$ est un sous-groupe de G, donc son cardinal est soit de la forme p^β soit $p^\beta m$, avec β éventuellement nul, il existe donc nécessairement un indice k tel que Card $(\text{Stab}_G(P_k))$ soit égal à p^α et on note $P_0 = P_k$.

4. D'après l'équation aux classes :

$$\text{Card }(G \cdot P_0) \cdot \text{Card }(\text{Stab}_G(P_0)) = \text{Card }(G) = p^\alpha m$$

   or p ne divise pas Card $(G \cdot P_0)$, alors nécessairement p^α divise Card $(\text{Stab}_G(P_0))$, d'où Card $(\text{Stab}_G(P_0)) \geqslant p^\alpha$.

5. Pour tout $g \in \text{Stab}_G(P_0)$, $g \cdot P_0 = \{g * y \mid y \in P_0\} = P_0$, en particulier $g * x \in P_0$, ainsi $\text{Stab}_G(P_0)x \subseteq P_0$.

   De plus, pour la même raison qu'en 1 (mais avec la bijection $g \mapsto g * x$), on a que $\text{Stab}_G(P_0)x$ est équipotent à $\text{Stab}_G(P_0)$. On a donc que Card $(\text{Stab}_G(P_0))x \geqslant p^\alpha =$ Card (P_0), alors $\text{Stab}_G(P_0)x$ est maximal dans P_0 (au sens de l'inclusion).

   On a donc montré $\text{Stab}_G(P_0)x = P_0$.

6. $\text{Stab}_G(P_0)$ est équipotent à P_0, donc $\text{Stab}_G(P_0)$ est un sous-groupe d'ordre p^α.