VI. Considérons le groupe $G = (\mathbf{Z}/15\mathbf{Z})^*$ et son sous-groupe $H = \langle \overline{2} \rangle$.

(a) Quels sont les membres de G et de H ? Quels sont les ordres $|G|$ et $|H|$?

(b) Quel est l'ordre de chaque élément de G ?

(c) Les groupes G et H sont-ils cycliques ?

(d) i. Quelles sont les classes (à gauche) pour H dans G ?

ii. Combien de membres y a-t-il dans chaque classe ?

iii. Combien de classes y a-t-il ?

iv. Quelle est l'indice $[G : H]$?

a). $G = \{1 ; 2 ; 4 ; 7 ; 8 ; 11 ; 13 ; 14\}$.

. $|G| = \varphi(15) = 8$

. $H = \langle \bar{2} \rangle$

$\langle g \rangle = \{e_G ; g ; \underbrace{g^2}_{g * g} ; g^3 ; \dots\}$

$\langle \bar{2} \rangle = \{1 ; 2 ; 4 ; 8\}$

donc $|H| = 4$.

b) $o(1) = 1$ $\quad o(8) = 4$

$o(2) = 4$ $\quad o(11) = 2$

$o(4) = 2$ $\quad o(13) = 4$

$o(7) = 4$ $\quad o(14) = 2$

$\{2 ; 4\}$

$\boxed{o(g) \mid |G|}$

c) • G n'est pas cyclique car il n'a pas d'éléments d'ordre 8

• H est cyclique par définition

d) $\boxed{gH = \{ g * h : h \in H \}}$.

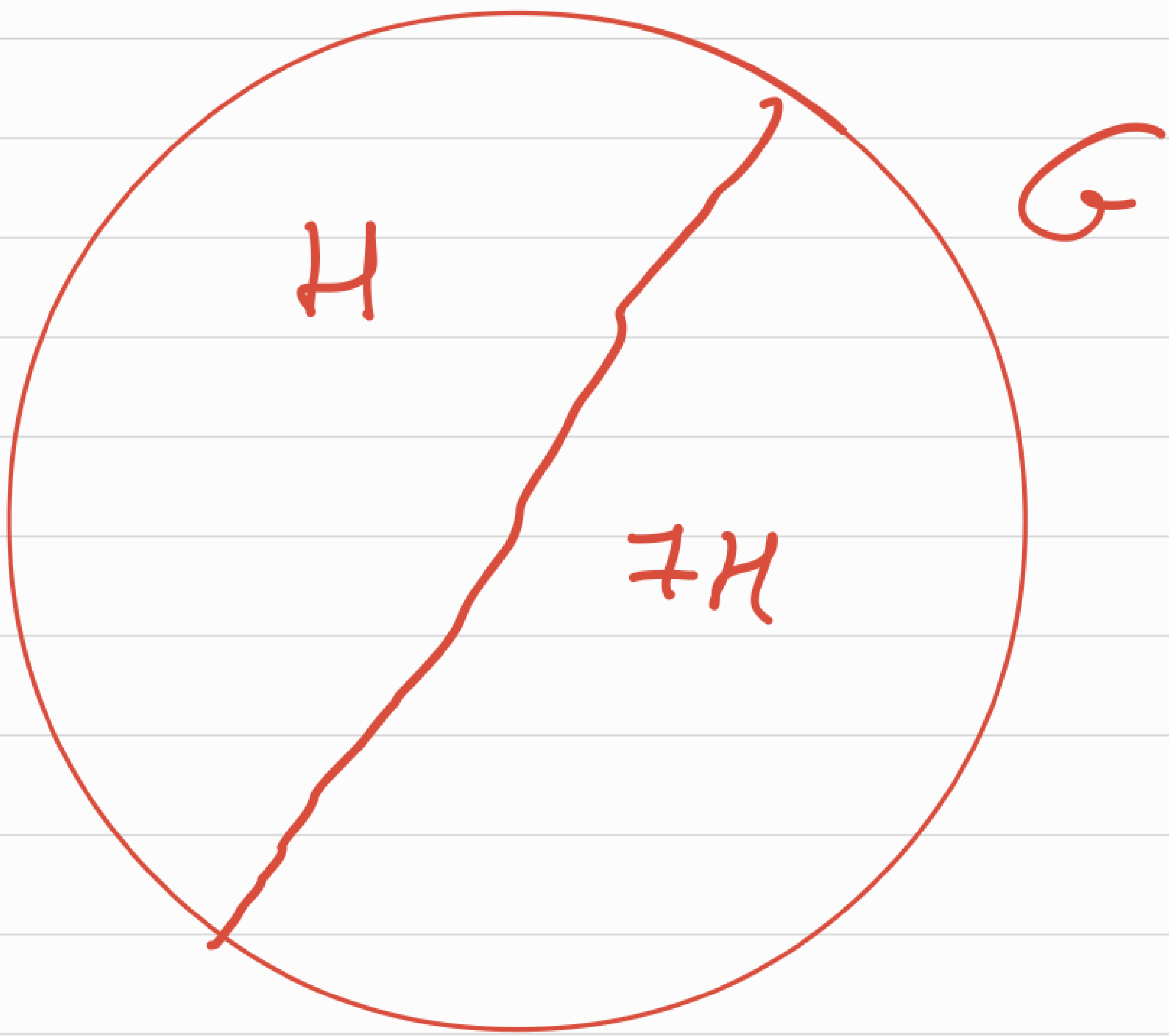
i)

• $H = \{ 1 ; 2 ; 4 ; 8 \}$

• $7H = \{ 7 \times 1 ; 7 \times 2 ; 7 \times 4 ; 7 \times 8 \}$

$= \{ 7 ; 14 ; 13 ; 11 \}$

comme $\begin{cases} H \cap 7H = \emptyset \\ H \cup 7H = G \end{cases}$ alors 7H et H sont les classes à gauche



ii) chaque classe contient 4 membres.

iii) il y a deux classes à gauches.

iv) $[G:H] = \dfrac{|G|}{|H|} = 2$.

$$\# \text{classes} = \frac{|G|}{|H|}$$

VII. Soit m et n deux entiers premiers entre eux. Démontrer à partir de résultats antérieurs que pour tous entiers a, b il existe un entier x avec

$$\begin{cases} x \equiv a \pmod{m}, \\ x \equiv b \pmod{n}. \end{cases}$$

V. Quel est le reste de la division euclidienne de $13^{13^{13}} + 17^{17^{17}}$ par 11 ?

$$13^{13^{13}} \equiv 2^{13^{13}} \mod 11$$

Le petit théorème de Fermat :

$$2^{10\,p-1} \equiv 1 \mod 11_p$$

donc comme $13 \equiv 3 \mod 10$

et $3^1 \equiv 3 \mod 10$

$3^2 \equiv 9 \mod 10$

$3^3 \equiv 7 \mod 10$

$3^4 \equiv 1 \mod 10$

donc : $13^{13} \equiv 3^{13} \mod 10$

or $13 \equiv 1 \mod 4$.

donc : $13^{13} \equiv 3^{1} \mod 10$

Donc :

$$13^{13^{13}} \equiv 2^{13^{13}} \equiv 2^{3^{1}} \equiv 8 \mod 11$$

$$17^{17^{17}} \equiv 6^{17^{17}} \mod 11$$

Fermat : $6^{\overset{p-1}{10}} \equiv 1 \mod \underset{p}{11}$

on cherche $17^{17} \mod 10$

or $17 \equiv 7 \mod 10$

$7^1 \equiv 7 \mod 10$

$7^2 \equiv 9 \mod 10$

$7^3 \equiv 3 \mod 10$

$7^4 \equiv 1 \mod 10$

donc $17^{17} \equiv 7^{17} \mod 10$

et $17 \equiv 1 \mod 4$

Ains $17^{17} \equiv 7^1 \mod 10.$

Donc :

$17^{17^{17}} \equiv 6^{17^{17}} \equiv 6^{7^1} \mod 11$

$\equiv 8 \mod 11$

$6 \equiv 6 \mod 11$

$6^2 \equiv 3 \mod 11$

$6^3 \equiv 7 \mod 11$

$6^4 \equiv 9 \mod 11$

$6^5 \equiv 10 \mod 11$

$6^6 \equiv 5 \mod 11$

$6^7 \equiv 8 \mod 11$

Donc :

$$13^{13^{13}} + 17^{17^{17}} \equiv 8 + 8 \equiv 5 \mod 11.$$

VI. Soit $U = \{z \in \mathbf{C}^* \mid |z| = 1\}$.

(a) Donner un morphisme de groupes de la forme $f \colon \mathbf{C}^* \to G$ tel que U soit le noyau de f.

(b) Dans le plan $\mathbf{C}$, dessiner les classes à gauche suivantes : (i) U, (ii) $2U$, (iii) $(1+2i)U$.

(c) Soit $w \in \mathbf{C}^*$. Donner une description géométrique de la classe à gauche $wU \subset \mathbf{C}^*$.

a) on pose $f : \mathbb{C}^* \longrightarrow \mathbb{R}_+^*$
$z \longmapsto |z|$

$\ker(f) = \mathcal{U} = \{z \in \mathbb{C}^* : |z| = 1\}$

$x \in G : f(x) = e_H\}$

b) . $\mathcal{U} = \{z \in \mathbb{C}^* : |z| = 1\}$

↳ cercle centre O et de rayon 1

. $2\mathcal{U} = \{2u : u \in \mathcal{U}\}$

$|u| = 1$ car $u \in \mathcal{U}$

$|2u| = 2|u| = 2$

donc $2\mathcal{U} = \{ z \in \mathbb{C}^* : |z| = 2 \}$

↳ cercle centre O et de rayon 2.

- $(1+2i)\mathcal{U} = \{ (1+2i)u : u \in \mathcal{U} \}$

$|u| = 1$ car $u \in \mathcal{U}$

$|(1+2i)u| = \boxed{|1+2i|}\,|u|$

$= \sqrt{5} \times 1 = \sqrt{5}$

$\hookrightarrow \sqrt{1^2+2^2} = \sqrt{5}$

donc $(1+2i)\mathcal{U} = \{z \in \mathbb{C}^* : |z| = \sqrt{5}\}$

↳ cercle centre 0 et de rayon $\sqrt{5}$.

c) $\omega\mathcal{U} = \{z \in \mathbb{C}^* : |z| = |\omega|\}$

↳ cercle centre 0 et de rayon $|\omega|$.