Exercice 1

Soient $a \geq 1$ $\quad b \geq 1$ $\quad a \wedge b = 1$

$c := (a-b)^2$ $\quad d := a^2 - ab + b^2$

(a) Soit $p \in \mathbb{P}$, $p \geq 2$ et $p \mid c$ et $p \mid d$

$(p \mid c$ et $p \mid d) \Rightarrow p \mid (uc + vd)$ $\quad \forall u, v$

Alors $p \mid (-c + d)$ $\quad -c + d = -a^2 + 2ab - b^2 + a^2 - ab + b^2$
$= ab$

$\Rightarrow p \mid ab$

(b) On sait que $p \mid c \Leftrightarrow p \mid a^2 - 2ab + b^2$ et $p \mid ab$
$\Leftrightarrow ab \equiv 0 \mod p$

$\Leftrightarrow p \mid (a-b)(a-b) \Rightarrow p \mid (a-b)$

d'après le théorème d'Euclide ($p \mid n_1 \dots n_2 \Rightarrow$
$p \mid n_1$ ou $p \mid n_2$ ou ...
ou $p \mid n_2$)

(c) $p \mid (a-b) \Rightarrow p \mid (a-b)b \Rightarrow p \mid ab - b^2$

$(p \mid a^2 - ab + b^2$ et $p \mid (ab - b^2)) \Rightarrow p \mid a^2$

(d) $p \mid d \Rightarrow d \equiv 0 \mod p \Leftrightarrow a^2 - ab + b^2 \equiv 0 \mod p$

d'après (c) et (a) $a^2 \equiv 0 \mod p$ et $ab \equiv 0 \mod p$

d'où $\underline{a}_0^2 - \underline{a}_0 b + b^2 \equiv 0 \mod p$
$\Leftrightarrow b^2 \equiv 0 \mod p \Rightarrow p \mid b^2$

(e) Si $\operatorname{pgcd}(c,d) > 1$, donc $\operatorname{pgcd}(c,d) \mid a^2$ et $\operatorname{pgcd}(c,d) \mid b^2$

$\Rightarrow \operatorname{pgcd}(c,d) \mid a$ et $\operatorname{pgcd}(c,d) \mid b$, mais par hypothèse
$a \wedge b = 1$ donc $\operatorname{pgcd}(c,d) = 1$.

Exercice 2

Soient $m \geq 2$ et $n \geq 2$ et C_m, C_n groupes cycliques avec $|C_m| = m$ et $|C_n| = n$

(a) D'après le théorème du cours, si G est un groupe cyclique avec $|G| = p$
donc $G \cong (\mathbb{Z}/p\mathbb{Z}, +)$ D'où $C_m \cong (\mathbb{Z}/m\mathbb{Z}, +)$
et $C_n \cong (\mathbb{Z}/n\mathbb{Z}, +)$

(b) D'après (a) On a montré que

$$C_m \cong (\mathbb{Z}/m\mathbb{Z}, +) \quad \text{et} \quad C_n \cong (\mathbb{Z}/n\mathbb{Z}, +)$$

D'après le cours si $m \wedge n = 1$, donc

$$(\mathbb{Z}/m\mathbb{Z}, +) \times (\mathbb{Z}/n\mathbb{Z}, +) \cong (\mathbb{Z}/nm\mathbb{Z}, +)$$ les anneaux dont cardinal est $m \cdot n$

donc pour les groupes de l'addition.

Or $(\mathbb{Z}/nm\mathbb{Z}, +)$ est cyclique engendré par $\bar{1}$ et isomorphe aux $(\mathbb{Z}/m\mathbb{Z}, +) \times (\mathbb{Z}/n\mathbb{Z}, +)$ qui sont isomorphes aux C_m et C_n

D'où $C_m \times C_n$ est cyclique

(c) Soit $m \wedge n > 1$
Supposons par l'absurde que $C_m \times C_n$ soit cyclique, ce qui par (a) implique que $C_m \times C_n$ est isomorphe à $(\mathbb{Z}/mn\mathbb{Z}, +)$ qui est cyclique.
Donc il doit exister un élément $(x, y) \in (\mathbb{Z}/m\mathbb{Z}, +) \times (\mathbb{Z}/n\mathbb{Z}, +)$ qui engendre additivement $(\mathbb{Z}/m\mathbb{Z}, +) \times (\mathbb{Z}/n\mathbb{Z}, +)$
i.e $\{(0,0), (x,y), \ldots, (kx, ky), \ldots, ((mn-1)x, (mn-1)y)\} = (\mathbb{Z}/m\mathbb{Z}, +) \times (\mathbb{Z}/n\mathbb{Z}, +)$
Soit $d = pgcd(n, m) \Rightarrow ppcm(m, n) = dn'm' < dn'dm' = mn$
où $m' = \frac{m}{d}$ et $n' = \frac{n}{d}$
les élément du groupe doivent être 2 à 2 distincts, ce qui n'est pas vrai, car si $k = dm'n' \leq mn - 1$
donc $(kx, ky) = (mn'x, m'ny) = (0,0) \in (\mathbb{Z}/m\mathbb{Z}, +) \times (\mathbb{Z}/n\mathbb{Z}, +)$
Donc contradiction. Donc $C_m \times C_n$ n'est pas cyclique si $m \wedge n > 1$.

Exercice 3

On doit montrer que $(\mathbb{R}^3, *)$ est un groupe

avec $(a,b,c) * (a',b',c') \longmapsto (a+a', b+b'+ac', c+c')$

(a) Montrons l'associativité :

Soit (a,b,c), (a',b',c'), $(a'',b'',c'') \in (\mathbb{R}^3, *)$

$$\big((a,b,c) * (a',b',c')\big) * (a'',b'',c'') = (a+a', b+b'+ac', c+c') * (a'',b'',c'')$$

$$= (a+a'+a'', b+b'+ac'+b''+(a+a')c'', c+c'+c'') = (a+a'+a'', b+b'+b''+ac'+ac''+a'c'', c+c'+c'')$$

$$(a,b,c) * \big((a',b',c') * (a'',b'',c'')\big) = (a,b,c) * (a'+a'', b'+b''+a'c'', c'+c'')$$

$$= (a+a'+a'', b+b'+b''+a'c''+a(c'+c''), c+c'+c'')$$
$$= (a+a'+a'', b+b'+b''+ac'+ac''+ac'', c+c'+c'')$$

D'où la loi est associative.

(b) Montrons que $(0,0,0)$ est un élément neutre

$$(a,b,c) * (0,0,0) = (a+0, b+0+a\cdot 0, c+0) = (a,b,c)$$
$$(0,0,0) * (a',b',c') = (0+a', 0+b'+0\cdot c', 0+c') = (a',b',c')$$

D'où $(0,0,0)$ est un élément neutre.

(c) Cherchons un inverse (a',b',c') de (a,b,c)

tq $(a,b,c) * (a',b',c') = (0,0,0) = (a',b',c') * (a,b,c)$

$$(a+a', b+b'+ac', c+c') = (0,0,0) \Leftrightarrow \begin{cases} a+a' = 0 \\ b+b'+ac' = 0 \\ c+c' = 0 \end{cases} \Leftrightarrow \begin{cases} a' = -a \\ b' = -b - a\cdot(-c) = -b+ac \\ c' = -c \end{cases}$$

D'où $(a',b',c') = (-a, -b+ac, -c)$

Vérifions: $(-a, -b+ac, -c)$

$$(a,b,c) * (-a, -b+ac, -c) = (a-a, b-b+ac-ac, c-c)$$
$$= (0,0,0)$$
$$(-a, -b+ac, -c) * (a,b,c) = (-a+a, -b+ac+b-ac, -c+c)$$
$$= (0,0,0)$$

De plus $-a \in \mathbb{R}$, $-c \in \mathbb{R}$ et $(-b+ac) \in \mathbb{R}$

d'où $(-a, -b+ac, -c) \in (\mathbb{R}^3, *)$

Donc $(-a, -b+ac, -c) = (a', b', c')$ est une inverse de (a,b,c).

(d) $(a,b,c) * (a',b',c') = (a+a', b+b'+ac', c+c')$ **

$(a',b',c') * (a,b,c) = (a+a', b+b'+a'c, c+c')$

donc le groupe n'est pas commutatif.

Exercice 4

$$(ED) \quad 5x^3 + 11y^3 + 13z^3 = 0$$

(a) $\mathbb{Z}/13\mathbb{Z}$

$\bar{1}^3 = \bar{1} \mod 13$

$\bar{2}^3 = \bar{8} \mod 13$

$\bar{3}^3 = \bar{1} \mod 13$

$\bar{4}^3 = \bar{12} \mod 13$

$\bar{5}^3 = \bar{8} \mod 13$

$\bar{6}^3 = \bar{8} \mod 13$

b) $\bar{12}^3 = \overline{3\cdot 4}^3 = \bar{3}^3 \cdot \bar{4}^3 = \bar{1} \cdot \bar{12} = \bar{12} \mod 13$

$\bar{11}^3 = -\bar{2}^3 = -\bar{8} = \bar{5} \mod 13$

$\bar{10}^3 = \overline{2\cdot 5}^3 = \bar{2}^3 \cdot \bar{5}^3 = \bar{8}\cdot\bar{8} = \bar{64} = \bar{12} \mod 13$ 39 52

$\bar{9}^3 = \bar{3}^{2\cdot 3} = \bar{3}^6 = \bar{1}^2 = 1 \mod 13$

$\bar{8}^3 = -\bar{5}^3 = -\bar{8} = \bar{5} \mod 13$

$\bar{7}^3 = -\bar{6}^3 = \bar{5} \mod 13$

(c) $5\alpha + 13\beta = 1$ On utilise la méthode de division euclidienne.

$13 = 5 \cdot 2 + 3$

$5 = 3 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 2 \cdot 1 + 0$

$1 = 3 - 2$

$= 3 - (5-3)$

$= 2 \cdot 3 - 5$

$= 2 \cdot (13 + (-2) \cdot 5) - 5$

$= 2 \cdot 13 - 4 \cdot 5 - 5$

$= (-5) \cdot 5 + 2 \cdot 13 = 25 + 26 = 1$

d'où $\alpha = -5$, $\beta = 2$

d) $5x^3 + 11y^3 + 13z^3 = 0$

$\equiv 0 \mod 13 \qquad 13z^3 \equiv 0 \mod 13$

$\Leftrightarrow 5x^3 + 11y^3 \equiv 0 \mod 13$

$\Leftrightarrow \left| 5x^3 \equiv -11y^3 \equiv 0 \mod 13 \right| \quad -5$

$x^3 \equiv 55y^3 \equiv 0 \mod 13$

$\Leftrightarrow x^3 \equiv 3y^3 \mod 13$

(e) D'après (a) et (b) On a trouvé que 4 éléments distincts de $\{\bar{1}^3, \bar{2}^3, \ldots, \overline{12}^3\}$ sont: $\bar{1}, \bar{5}, \bar{8}, \overline{12}$

On ajoute $\bar{0}^3 = \bar{0}$ dans cet ensemble d'où on obtient: $\{\bar{0}, \bar{1}, \bar{5}, \bar{8}, \overline{12}\}$

$\bar{3} \cdot \bar{0} = \bar{0}$

$\bar{3} \cdot \bar{1} = \bar{3}$

$\bar{3} \cdot \bar{5} = \bar{2}$

$\bar{3} \cdot \bar{8} = \overline{24} = \overline{-2} = \overline{11}$

$\bar{3} \cdot \overline{12} = \overline{36} = \overline{-3} = \overline{10}$

D'où $F = \{\bar{0}, \bar{2}, \bar{3}, \overline{10}, \overline{11}\}$

D'après [d] $x^3 \equiv 3y^3 \bmod 13$

D'après [e] on a multiplié tous les élément puissance cube mod 13 par $\bar{3}$ et le seul élément qui est égal à un autre est: $\bar{0}$ mod 13

d'où $x \equiv \bar{0} \bmod 13$ et $\bar{y} \equiv 0 \bmod 13$

g) d'après (f) $x = 13x'$ et $y = 13y'$

$$\begin{aligned} \text{D'où } & 5x^3 + 11y^3 + 13z^3 = 0 \\ \Leftrightarrow\ & 13z^3 = -5x^3 - 11y^3 \\ & = 13^3(-5x'^3 - 11y'^3) \\ \Leftrightarrow\ & z^3 = 13^2(-5x'^3 - 11y'^3) \end{aligned}$$

D'où $z^3 \equiv 0 \bmod 13 \Rightarrow z \equiv 0 \bmod 13$

h) Soit $d = \text{pgcd}(x, y, z)$

$$0 = 5x^3 + 11y^3 + 13y^3 \qquad \begin{aligned} x &= dx' \\ y &= dy' \\ z &= dz' \end{aligned}$$

$$\begin{aligned} 0 &= 5(dx')^3 + 11(dy')^3 + 13(dz')^3 \\ &= d^3[5x'^3 + 11y'^3 + 13z'^3] \end{aligned}$$

On pose $d = 1$ et donc $(x', y', z') \neq (0,0,0)$ est une solution de (ED)

i) Par (h) par absurd on a trouvé que $\exists (x,y,z) \neq (x',y',z') \neq (0,0,0)$ tq x', y', z' sont n'ont aucun multiple commun par contre dans (e) et (g) on a montré que les solutions (x,y,z) doivent être divisés par 13. Contradiction. Donc $(0,0,0)$ est la seule solution de (ED)

Exercice 5

$(\mathbb{Z}/17\mathbb{Z})^\times \qquad (\mathbb{Z}/17\mathbb{Z}, +, \times)$

$17 - 1 = 2^4$

$\bar{3}^1 = \bar{3} \mod 17$

$\bar{3}^2 = 9$

$\equiv -\bar{8} \mod 17$ $\qquad 34$ $\qquad 68$

$\bar{3}^4 = \bar{9}^2 = -\bar{8}^2 = \bar{64} = -\bar{4}$

$\bar{3}^8 = -\bar{4}^2 = \bar{16} = -\bar{1}$

a) $\bar{3}^{16} = \bar{3}^{8+8} = \bar{3}^8 \cdot \bar{3}^8 = (-\bar{1})(-\bar{1}) = \bar{1}$

b) $n \in \mathbb{N} \qquad n = \min\{k \in \mathbb{N} : \bar{3}^k = \bar{1}\}$

$|(\mathbb{Z}/17\mathbb{Z})^\times| = 16$

$\langle \bar{3} \rangle \subset |(\mathbb{Z}/17\mathbb{Z})^\times|$ car $\bar{3}$ génère $(\mathbb{Z}/17\mathbb{Z})^\times$

$|\langle \bar{3} \rangle| = o(\bar{3}) = n$

Par le théorème de Lagrange $|H| \mid |G|$

d'où $n \mid 16$

c) Supposons par l'absurde que $n \mid 8$

d'où $|\langle \bar{3} \rangle| = 1$ ou 2 ou 4 ou 8

par le théorème de Lagrange.

Mais $\bar{3}^1 = \bar{3} \neq \bar{1} \qquad \bar{3}^2 = -\bar{8} \neq \bar{1}$

$\bar{3}^4 = -\bar{4} \neq \bar{1}$ et $\bar{3}^8 = -\bar{1} \neq 1$

D'où n n'est pas l'ordre de 3

et n'est pas ss-gpe de $(\mathbb{Z}/17\mathbb{Z})^\times$

contradiction. Donc $n \nmid 8$

f) Le dernier diviseur est 16
$16 | 16$ et $\bar{3}^{16} = \bar{1}$ D'après (a)
D'où 16 est le plus petit nombre que $\bar{3}^n = \bar{1}$
d'où $o(\bar{3}) = 16$

e) D'après le théorème du cours cardinal du groupe est égal à l'ordre d'élément qui engendre ce groupe.
On a trouvé que $o(\bar{3}) = 16$ et $\bar{3}$ engendre $(\mathbb{Z}/17\mathbb{Z})^\times$
d'où $|(\mathbb{Z}/17\mathbb{Z})^\times| = 16$

f) Soit un morphisme $f : (\mathbb{Z}, +) \longrightarrow ((\mathbb{Z}/17\mathbb{Z})^\times, \times)$
$k \longmapsto \bar{3}^k =: f(k)$

Supposons par l'absurde que $\exists\ 1 \leq i < j \leq 16$
$\bar{3}^i \equiv \bar{3}^j \mod 17$
$\Leftrightarrow \bar{3}^{i-j} \equiv \bar{1} \mod 17$

Donc $k = i - j \in \{1, \dots, 15\}$ $\bar{3}^k = \bar{1}$ ce qui contredit à ce qu'on a établi dans (d)

Donc $\bar{3}^1, \dots, \bar{3}^{16}$ sont 2 à 2 distincts et
f est surjective.

g) $\ker f = \{i \in \mathbb{Z} : \bar{3}^i = \bar{1}\}$

On sait que $\langle 3 \rangle$ est cyclique avec $o(16)$
donc $\bar{3}^i$ est périodique de période 16, d'où

$\forall i \in \mathbb{Z}$, $\bar{3}^{16i} = \bar{1}$, d'où $\ker f = 16\mathbb{Z}$

h) On sait que $f: \mathbb{Z} \longrightarrow ((\mathbb{Z}/17\mathbb{Z})^\times, \times)$
est un morphisme
avec $\ker f = 16\mathbb{Z}$
d'après le théorème de factorisation,

$\bar{f}: (\mathbb{Z}/\ker f) = (\mathbb{Z}/16\mathbb{Z}) \longrightarrow (\mathbb{Z}/17\mathbb{Z}, \times)$
est injective. De plus $|\mathbb{Z}/16\mathbb{Z}| = |(\mathbb{Z}/17\mathbb{Z})^\times|$

donc $\bar{f}$ est bijective.

Exercice 6

(a) $3^{n+3} - 4^{4n+2} \equiv$
$3^3 3^n - (4^4)^n \cdot 4^2 \equiv$
$27\,3^n - 16(16\cdot 16)^n \equiv$
$53^n - 5(5\cdot 5)^n \equiv$
$5\cdot 3^n - 5(3)^n \equiv 0 \mod 17$
$= 0 \equiv 0 \mod 11$

Exercice 7

Soit G un groupe avec $2 \leq \text{card } G < \infty$
avec la loi multiplicative $e = 1_G \in G$
$\forall g \in G,\ g^2 = e$

(a) $\forall g \in G,\ g^2 = e \iff g^2 \cdot g^{-1} = g^{-1} = g = g^{-1}$

D'où
Soit $g' \in G$. $\quad gg'(g'g)^{-1} = gg'g^{-1}g'^{-1} = gg'gg' = (gg')^2 = e$

$\Rightarrow gg' = g'g$

D'où G est commutatif

(6) Soit $g \in G \setminus \{e\}$ on sait que $g^2 = e$

d'où $g^{-1} = g$ $g^{-2} = e$ donc $\langle g \rangle \subset G$

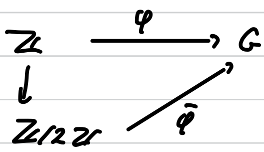
et $o(g) = 2 = |\mathbb{Z}/2\mathbb{Z}| = 2$

Introduisons $\varphi : \mathbb{Z} \longrightarrow G$ application

avec $\underset{\varphi(2)}{\underset{\shortparallel}{\varphi(0)}} = e \neq g = \varphi(1)$

Clairement $\mathrm{Ker}\, f = 2\mathbb{Z}$

Grace à la théorème factorisation



où $\bar{\varphi}$ est un isomorphisme.