Exercice 6 $H \subset G$ sous-groupe strict.

Trouver $\langle G\setminus H \rangle$ le sous-groupe engendré par $G\setminus H$.

$H \neq G$.

Nous savons que si $H_1, H_2 \subset G$ des sous-groupes $H_1 \cup H_2$ est un sous-groupe ssi $H_1 \subset H_2$ ou $H_2 \subset H_1$.

On $G\setminus H \subset \langle G\setminus H \rangle$ d'où

$$H \cup \langle G\setminus H \rangle = G$$ et donc :

$$H \subset \langle G\setminus H \rangle = G$$ ou $\langle G\setminus H \rangle \subset H = G$

impossible car H strict.

Et donc $< G \setminus H > = G$.

<u>Exercice 7</u> : $x \in G$ x d'ordre p
$y \in G$ y d'ordre q

G abélien
Montrer que (xy) est d'ordre au plus pq.

L'ordre de x c'est le nombre d'éléments de $<x>$

On a vu que c'est aussi le plus petit entier k dans $\mathbb{N}^*$ tel que $x^k = e$.

On calcule $(xy)^{pq} \underset{\text{abélien}}{=} (x^p)^q (y^q)^p = ee = e$

On a montré que l'ordre xy est au plus pq.

2) $(1\,2) \in S_n$ $\qquad (1\,2)^2 = id$.

ordre de $(1\,2)$ vaut 2

$< (1\,2) > = \{ id, (1\,2) \}$ abélien :

$(1\,2)$ d'ordre 2 $\qquad (1\,2)^2$ est-il d'ordre 4 ?

l'ordre de id est $\underline{1}$ donc on peut avoir une égalité stricte.

Mais on peut avoir égalité ;

Soit $G = \mathbb{U} = \{ z, |z| = 1 \}$, $\times$ groupe abélien.

(-1) est d'ordre 2.

$j = \exp \frac{2i\pi}{3}$ $\quad j^3 = 1 \quad j^2 = \exp \frac{4i\pi}{3} = \bar{j}$

j est d'ordre 3.

De plus $(-j)$, $(-j)^2 = j^2 = \bar{j}$, $(-j)^3 = -1$,

$(-j)^4 = j \quad (-j)^5 = -j^2 = -\bar{j} \quad (-j)^6 = 1$

donc l'ordre de $(-j)$ vaut 2×3.

3/ $f : (m,n) \longmapsto (-n, m) \qquad g : (m,n) \longmapsto (n, -m-n)$

$f, g \in \mathrm{Bij}(\mathbb{Z} \times \mathbb{Z}) \qquad f, g : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$

$f \circ f(m,n) = f(-n,m) = (-m,-n) = -id$

d'où $f^4 = f \circ f \circ f \circ f = id$

f est d'ordre 4 $\langle f \rangle = \{ id, f, f \circ f, f \circ f \circ f \}$

et $g(m,n) = (n, -m-n)$, $(g \circ g)(m,n) =$

$(-m-n, m)$ / $g^3(m,n) = g(-m-n, n) = (n, m)$

$g^3 = id$, $\langle g \rangle = \{ id, g, g \circ g \}$

g est d'ordre 3

De plus $f \circ g(m,n) = (m+n, n)$

$(f\circ g)^k(1,0) = (k,0)$. $(f\circ g)^k \neq id$.

ordre de $f\circ g$ est <u>infini</u>.

$f\circ g \neq g\circ f$.

Exercice 8 $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2},\ a,b \in \mathbb{Z}\}$.

$(\mathbb{Z}[\sqrt{2}], +) < (\mathbb{Z}, +)$.

i) $\mathbb{Z}[\sqrt{2}] \neq \emptyset$ car $0 = 0 + 0\sqrt{2}$

donc $0 \in \mathbb{Z}[\sqrt{2}]$.

ii) $\forall\ a+b\sqrt{2},\ a'+b'\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$

calculons $a+b\sqrt{2} - (a'+b'\sqrt{2})$

$= (a-a') + (b-b')\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$

Conclusion $(\mathbb{Z}[\sqrt{2}], +)$ est un sous-groupe.

2) $(a+b\sqrt{2}) \times (a'+b'\sqrt{2})$

$= (aa'+2bb') + (ba'+ab')\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$

et donc $(\mathbb{Z}[\sqrt{2}] \setminus \{0\}, \times)$ est stable;

1 est l'élément neutre : $1 = 1 + 0.\sqrt{2}$

$\sqrt{2} = 0 + 1.\sqrt{2}$; l'inverse ;

$\frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2} = a + b\sqrt{2}$

$\sqrt{2} = 2a + b\sqrt{2} \Rightarrow (1-b)\sqrt{2} = 2a$

$\sqrt{2} = \frac{2a}{1-b}$ $\sqrt{2}$ n'est pas un rationnel.

Donc $\sqrt{2}$ n'est pas inversible.

3) $N(a+b\sqrt{2}) = a^2 - 2b^2$.

$x = a + b\sqrt{2}$ $\quad y = a' + b'\sqrt{2}$

$xy = aa' + 2bb' + \sqrt{2}(ab' + a'b)$.

$N(xy) = (aa' + 2bb')^2 - 2(ab' + a'b)^2$ *

$\boxed{N(x)N(y) = (a^2 - 2b^2)(a'^2 - 2b'^2)}$.

$= (aa')^2 + 4(bb')^2 - 2a^2b'^2 - 2a'^2b^2$

$= *$

On a vérifié $N(xy) = N(x)N(y)$;

$N(x) \in \mathbb{Z}$

4) Supposons x inversible et $x^{-1} = y$.

$N(xy) = N(1) = 1$

$=$

$N(x)N(y)$ $\Longrightarrow N(x) = \pm 1$.

$\in \mathbb{Z} \quad \in \mathbb{Z}$

$\Longleftrightarrow a^2 - 2b^2 = \pm 1$

Si $N(x) = \pm 1$ $\quad x = a + \sqrt{2}\, b = \dfrac{a^2 - 2b^2}{a - \sqrt{2}\, b}$

$$x^{-1} = \frac{a}{a^2-2b^2} - \frac{\sqrt{2}\,b}{a^2-2b^2} \in \mathbb{Z}[\sqrt{2}] \text{ car } a^2-2b^2=\pm 1$$

<u>Conclusion</u> : x est inversible ssi

$$N(x) = \pm 1 .$$