Corrigé de l'examen du 12 novembre 2019

Ex 1

1.] On note $f(x) = ax+b$ et $g(x) = cx+d$

Alors $f\circ g(x) = a(cx+d)+b = (ac)x + (ad+b)$

$g\circ f(x) = c(ax+b)+d = (ac)x + (cb+d)$

en général $ad+b \neq cb+d$, donc la loi de composition n'est pas commutative.

2.] $f(x) = x$ est le neutre ($a=1, b=0$), car.

$f\circ g = g\circ f = g \quad \forall g \in G$.

3.] Je faut résoudre l'équation $f\circ g(x) = x$

$\Leftrightarrow \begin{cases} ac = 1 \\ ad+b = 0 \end{cases}$ (notation du (1)).

$\Leftrightarrow c = \frac{1}{a} \quad d = -\frac{b}{a}$.

Donc l'inverse de $f(x) = ax+b$ est la fonction.

$g(x) = \frac{1}{a}\cdot x - \frac{b}{a}$.

4.] G est un groupe, car (i) associatif $f\circ(g\circ h) = (f\circ g)\circ h$

(ii) G admet un neutre (2)

(iii) tout $f \in G$ admet un inverse (3)

5.] H est un sous-groupe de G, car

(i) neutre $f(x) = x \in H$ ($b=0$)

(ii) si $f, g \in H$, alors $f\circ g \in H$.

(iii) si $f \in H$, alors $f^{-1}(x) = x - b \in H$.

Ex 2 1.] Il faut vérifier que

- $(A,+)$ est un groupe.
  - $\frac{m}{n} + \frac{m'}{n'} = \frac{n'm+nm'}{nn'} \in A$, car si n et n' sont impairs, alors nn' est impair.
  - inverse de $\frac{m}{n} = \frac{-m}{n}$.
  - neutre $= \frac{0}{1} \in A$.
- $(A,\cdot)$ $\frac{m}{n} \cdot \frac{m'}{n'} = \frac{mm'}{n \cdot n'} \in A$, car si n et n' sont impairs, alors $n \cdot n'$ est impair.

2.] oui, A est unitaire.
d'unité $\frac{1}{1} \in A$.

3.] Si $r = \frac{m}{n}$ est inversible, alors il existe $q = \frac{m'}{n'}$ tel que.

$$r \cdot q = 1 \iff \frac{mm'}{nn'} = 1 \iff mm' = n \cdot n'$$

Comme n et n' sont impairs, on conclut que m et m' sont aussi impairs.
Inversément si m est impair, $\frac{m}{n}$ est inversible, d'inverse $\frac{n}{m}$

Conclusion : $A^* = \left\{ r \in A \; ; \; r = \frac{m}{n}, \; m \text{ et } n \text{ impairs} \right\}$.

Ex 3 1.] L'algorithme d'Euclide donne PGCD(18, 49) = 1.
Donc $\overline{18}$ inversible dans $\mathbb{Z}/49\mathbb{Z}$.
L'algorithme d'Euclide étendu donne la relation. $1 = 7 \cdot 49 - 19 \cdot 18$.

Donc l'inverse de $\overline{18}$ est $-\overline{19} = \overline{30}$ dans $\mathbb{Z}/497\mathbb{Z}$

2.] L'algorithme d'Euclide donne $PGCD(42, 135) = 3$
donc $\overline{42}$ n'est pas inversible dans $\mathbb{Z}/135\mathbb{Z}$.

Ex 4 Il faut calculer l'inverse de $\overline{7}$ dans $\mathbb{Z}/37\mathbb{Z}$.
Par l'algorithme d'Euclide étendu on obtient

$$1 = -3 \cdot 37 + 16 \cdot 7.$$

Donc l'inverse de $\overline{7}$ est $\overline{16}$.

Donc $x = \overline{2} \cdot \overline{16} = \overline{32}$.

Ex 5 1.] $G = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}\}$.

2.] $\langle \overline{1} \rangle = \{\overline{1}\}$
$\langle \overline{3} \rangle = \{\overline{1}, \overline{3}, \overline{9}, \overline{7}\}$.
$\langle \overline{7} \rangle = \{\overline{1}, \overline{7}, \overline{9}, \overline{3}\}$.
$\langle \overline{9} \rangle = \{\overline{1}, \overline{9}\}$.
$\langle \overline{11} \rangle = \{\overline{1}, \overline{11}\}$.
$\langle \overline{13} \rangle = \{\overline{1}, \overline{13}, \overline{9}, \overline{17}\}$.
$\langle \overline{17} \rangle = \{\overline{1}, \overline{17}, \overline{9}, \overline{13}\}$.
$\langle \overline{19} \rangle = \{\overline{1}, \overline{19}\}$.

3.] NON, il n'existe pas de $a \in G$ tel que
$\langle a \rangle = G$ d'après les calculs faits dans (2)

4.] Par exemple $a = \overline{3}$ et $b = \overline{11}$.