Devoir 1. A rendre pour la semaine du 6 octobre.

Pour tout entier $n \geq 1$, on considère le groupe $G_n = (\mathbb{Z}/2^n\mathbb{Z})^\times$ des unités de $\mathbb{Z}/2^n\mathbb{Z}$.

1) Donner un ensemble de représentants dans $\mathbb{Z}$ des éléments du groupe G_n. Quel est l'ordre de G_n?

G_n est le groupe multiplicatif des éléments inversibles pour la loi $\times$ dans $\mathbb{Z}/2^n\mathbb{Z}$. On sait que la classe de x modulo 2^n est inversible si et seulement si x est premier avec 2^n, pour $x \in \mathbb{Z}$. On peut donc prendre comme système de représentants des classes qui sont dans G_n, les nombres entiers impairs m avec $1 \leq m < 2^n$. $|G_n| = 2^{n-1} = \phi(2^n)$, où ϕ est l'indicateur d'Euler.

2) Décrire G_1 et G_2. Montrer que G_3 est isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$G_1 = (\mathbb{Z}/2\mathbb{Z})^\times = \{\overline{1}\}$, $G_2 = (\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\} \simeq \mathbb{Z}/2\mathbb{Z}$ car $3^2 = 9 = 1 \bmod 4$.
$G_3 = (\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, avec $3^2 = 9 = 1 \bmod 8$, $5^2 = 25 = 1 \bmod 8$ et $7^2 = 49 = 1 \bmod 8$. G_3 est donc un groupe d'ordre 4 dont tous les éléments sont d'ordre 2. Donc, $G_3 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

On suppose désormais $n \geq 3$. On note α_n et β_n les classes respectives de -1 et 5 dans $\mathbb{Z}/2^n\mathbb{Z}$ et $\langle\alpha_n\rangle$ et $\langle\beta_n\rangle$ les groupes cycliques engendrés respectivement par α_n et β_n. On va montrer que $G_n \simeq \langle\alpha_n\rangle \times \langle\beta_n\rangle$.
3) Calcul préliminaire. Montrer par récurrence que, pour tout $k \in \mathbb{N}$, on a:

$$5^{2^k} = 1 + 2^{k+2} \bmod(2^{k+3}).$$

Si $k = 0$, $5^{2^k} = 5 = 1 + 2^2 \bmod 2^3$ donc la formule à démontrée est vraie au rang 0.
Supposons la formule vraie au rang k, alors, il existe $a \in \mathbb{Z}$ tel que $5^{2^k} = 1 + 2^{k+2} + 2^{k+3} \times a$. On en déduit que:

$$\begin{aligned} 5^{2^{k+1}} = (5^{2^k})^2 &= (1 + 2^{k+2} + 2^{k+3} \times a)^2 \\ &= 1 + 2^{k+4} + a^2 \times 2^{k+6} + 2^{k+3} + a \times 2^{k+4} + a \times 2^{k+6} \\ &= 1 + 2^{k+3} \bmod 2^{k+4} \end{aligned}$$

Ce qui démontre la formule au rang $k + 1$.

4) En déduire que l'ordre de β_n est 2^{n-2}.

Pour $k = n - 2$, on a $5^{2^{n-2}} = 1 + 2^n \bmod 2^{n+1}$, donc $\beta_n^{2^{n-2}} = \overline{1}$ dans $\mathbb{Z}/2^n\mathbb{Z}$, donc l'ordre de β_n divise 2^{n-2}.
Pour $k = n-3$, on a $5^{2^{n-3}} = 1+2^{n-1} \bmod 2^n$, donc $\beta_n^{2^{n-3}} = \overline{1} + \overline{2^{n-1}} \neq \overline{1}$ dans $\mathbb{Z}/2^n\mathbb{Z}$, donc l'ordre de β_n est exactement 2^{n-2}.

5) Préciser l'ordre de α_n et montrer que α_n ne peut appartenir à $\langle\beta_n\rangle$.

Pour $n \geq 3$, $-1 \neq 1 \bmod 2^n$ et $\alpha_n^2 = 1$ dans $\mathbb{Z}/2^n\mathbb{Z}$. Donc α_n est d'ordre 2.

Le groupe $\langle \beta_n \rangle$ est cyclique d'ordre 2^{n-2}, donc il contient comme seul élément d'ordre 2 l'élément $\beta_n^{2^{n-3}}$.

En, effet si un élément x d'un groupe G est d'ordre m. Alors pour tout $k \in \mathbb{N}$, x^k est d'ordre $m/pgcd(m,k)$.

Or, $5^{2^{n-3}} = 1 + 2^{n-1} \bmod 2^n \neq -1 \bmod 2^n$ car 2^n ne divise pas $2 + 2^{n-1}$.

6) En déduire un isomorphisme entre le groupe produit $\langle \alpha_n \rangle \times \langle \beta_n \rangle$ et le groupe G_n.

Soit $f_n : \begin{array}{ccc} \langle \alpha_n \rangle \times \langle \beta_n \rangle & \to G & \\ (\alpha_n^k, \beta_n^l) & \mapsto & \alpha_n^k \beta_n^l \end{array}$

(α_n^k, β_n^l) est dans le noyau de f_n ssi $\alpha_n^k \beta_n^l = 1_G$, càd, ssi $\alpha_n^k = \beta_n^{-l}$. Mais, on a montré que $\langle \alpha_n \rangle \cap \langle \beta_n \rangle = \{1\}$. Donc, $Ker(f_n) = \{(1_G, 1_G)\}$ et f_n est injective.

D'après 1), l'ordre de G est égal à 2^{n-1}. Par ailleurs,

$$|\langle \alpha_n \rangle \times \langle \beta_n \rangle| = |\langle \alpha_n \rangle| \times |\langle \beta_n \rangle| = 2 \times 2^{n-2} = 2^{n-1}$$

On a donc trouvé un homomorphisme injectif entre 2 groupes finis de même ordre. Donc, f_n est un isomorphisme du produit direct $\langle \alpha_n \rangle \times \langle \beta_n \rangle$ vers G_n.

On sait que l'action de G_n sur lui-même par translation à gauche induit un homomorphisme injectif de groupes $\phi_n : G_n \to \Sigma_{G_n}$, où Σ_{G_n} désigne le groupe des permutations de l'ensemble G_n (théorème de Cayley).

7) Expliciter $\phi_n(\alpha_n)$ et $\phi_n(\beta_n)$ pour $n = 3$ et 4.

Pour tout $g \in G_n$, on note $\phi_n(g)$ l'application de G_n dans G_n définie par $(\phi_n(g))(h) = gh$ pour tout $h \in G_n$. L'application $\phi_n(g)$ est appelée la translation à gauche par g. Cela définit un homomorphisme de groupes injectif $\phi_n : G_n \to \Sigma_{G_n}$.

Pour $n = 3$, $G_3 = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, $\phi_3(\alpha_3) = \begin{pmatrix} \overline{1} & \overline{3} & \overline{5} & \overline{7} \\ \overline{7} & \overline{5} & \overline{3} & \overline{1} \end{pmatrix} = (\overline{1}, \overline{7})(\overline{3}, \overline{5})$

et $\phi_3(\beta_3) = \begin{pmatrix} \overline{1} & \overline{3} & \overline{5} & \overline{7} \\ \overline{5} & \overline{7} & \overline{1} & \overline{3} \end{pmatrix} = (\overline{1}, \overline{5})(\overline{3}, \overline{7})$.

Pour $n = 4$, $G_4 = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{15}\}$,

$\phi_4(\alpha_4) = \begin{pmatrix} \overline{1} & \overline{3} & \overline{5} & \overline{7} & \overline{9} & \overline{11} & \overline{13} & \overline{15} \\ \overline{15} & \overline{13} & \overline{11} & \overline{9} & \overline{7} & \overline{5} & \overline{3} & \overline{1} \end{pmatrix} = (\overline{1}, \overline{15})(\overline{3}, \overline{13})(\overline{5}, \overline{11})(\overline{7}, \overline{9})$

et $\phi_4(\beta_4) = \begin{pmatrix} \overline{1} & \overline{3} & \overline{5} & \overline{7} & \overline{9} & \overline{11} & \overline{13} & \overline{15} \\ \overline{5} & \overline{15} & \overline{9} & \overline{3} & \overline{13} & \overline{7} & \overline{1} & \overline{11} \end{pmatrix} = (\overline{1}, \overline{5}, \overline{9}, \overline{13})(\overline{3}, \overline{15}, \overline{11}, \overline{7})$.