Feuille d'exercices 10.
Corrigé d'un exercice.

Exercice 10.19 :

$\diamond$ Remarquons d'abord que G est un groupe abélien, car pour tout $x, y \in G$,
$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.

$\diamond$ Notons A l'ensemble des entiers $n \in \mathbb{N}$ tels qu'il existe une partie génératrice de G de cardinal n. A est non vide car G est une partie génératrice finie de G. Ainsi, A possède un minimum noté m. Il existe alors m éléments $x_1, \ldots, x_m$ de G tels que $G = Gr(\{x_1, \ldots, x_m\})$.

$\diamond$ Lorsque $a = (\overline{\alpha_1}, \ldots, \overline{\alpha_m}) \in (\mathbb{Z}/2\mathbb{Z})^m$, posons $f(a) = \displaystyle\prod_{i=1}^{m} x_i^{\alpha_i}$.

Soit $a \in (\mathbb{Z}/2\mathbb{Z})^m$. Supposons que $a = (\overline{\alpha_1}, \ldots, \overline{\alpha_m}) = (\overline{\beta_1}, \ldots, \overline{\beta_m})$.
Soit $i \in \mathbb{N}_m$. Il existe $k \in \mathbb{Z}$ tel que $\beta_i = \alpha_i + 2k$, donc $x_i^{\beta_i} = x_i^{\alpha_i}(x^2)^k = x_i^{\alpha_i}$, car $x_i^2 = 1$ par hypothèse. Ainsi, $\displaystyle\prod_{i=1}^{m} x_i^{\alpha_i} = \prod_{i=1}^{m} x_i^{\beta_i}$, donc ce produit ne dépend bien que de a, ce qui prouve que f est une application correctement définie de $(\mathbb{Z}/2\mathbb{Z})^m$ dans G.

$\diamond$ Montrons que f est un isomorphisme de groupes. Ceci prouvera en particulier que G a même cardinal que $(\mathbb{Z}/2\mathbb{Z})^m$, donc que $|G| = 2^m$, ce qu'il fallait démontrer.
Soit $a = (\overline{\alpha_1}, \ldots, \overline{\alpha_m}) \in (\mathbb{Z}/2\mathbb{Z})^m$ et $b = (\overline{\beta_1}, \ldots, \overline{\beta_m}) \in (\mathbb{Z}/2\mathbb{Z})^m$.
Alors $f(a+b) = \displaystyle\prod_{i=1}^{m} x_i^{\alpha_i + \beta_i} = f(a)f(b)$, car G est commutatif. Ainsi f est bien un morphisme de groupes.

Soit $a = (\overline{\alpha_1}, \ldots, \overline{\alpha_m}) \in \mathrm{Ker}(f)$. Ainsi $1 = f(a) = \displaystyle\prod_{i=1}^{m} x_i^{\alpha_i}$.

Supposons que $a \neq 0$. Il existe $i \in \mathbb{N}_m$ tel que $\overline{\alpha_i} \neq 0$. On peut donc supposer que $\alpha_i = 1$.
Alors $x_i = x_i^{-1} = \displaystyle\prod_{\substack{j=1 \\ j \neq i}}^{m} x_j^{\alpha_j} \in H$, où H désigne le groupe engendré par $\{x_1, \ldots, x_m\} \setminus \{x_i\}$.

Alors $\{x_1, \ldots, x_m\} \subset H$, donc $G = Gr(\{x_1, \ldots, x_m\}) \subset H$. Ceci prouve que $H = G$, donc que $\{x_1, \ldots, x_m\} \setminus \{x_i\}$ est une partie génératrice de G, puis que $m - 1 \in A$, ce qui contredit la définition de m. Ainsi, $a = 0$ et $\mathrm{Ker}(f) = \{0\}$, ce qui prouve que f est injective.

Soit $g \in G$. G est engendré par $\{x_1, \dots, x_m\}$ et il est commutatif, donc d'après le cours, il existe $\alpha_1, \dots, \alpha_m \in \mathbb{Z}$ tels que $g = \prod_{i=1}^{m} x_i^{\alpha_i}$, donc $g = f(a)$, où $a = (\overline{\alpha_1}, \dots, \overline{\alpha_m})$. Ainsi, f est surjective. En conclusion, on a bien démontré que f est un isomorphisme.