Feuille d'exercices 10.
Corrigé de deux exercices.

Exercice 10.19 :

$\diamond$ Remarquons d'abord que G est un groupe abélien, car pour tout $x, y \in G$,
$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.
La solution de cet exercice est en fait une utilisation déguisée des espaces vectoriels, où l'on reproduit la partie de cette théorie qui permet d'aboutir.
$\diamond$ 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 $f(a) = \prod_{i=1}^{m} x_i^{\alpha_i}$.
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, $\prod_{i=1}^{m} x_i^{\alpha_i} = \prod_{i=1}^{m} x_i^{\beta_i}$, 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 $f(a+b) = \prod_{i=1}^{m} x_i^{\alpha_i+\beta_i} = f(a)f(b)$, 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 $1 = f(a) = \prod_{i=1}^{m} x_i^{\alpha_i}$.
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 $x_i = x_i^{-1} = \prod_{\substack{j=1 \\ j \neq i}}^{m} x_j^{\alpha_j} \in H$, 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 $\text{Ker}(f) = \{0\}$, 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.

Exercice 10.21 :

Commençons par définir quelques notations.
◇ On note c le cycle $(1\ 2\ \cdots\ p)$ de $\mathcal{S}_p$.
◇ Si $x = (x_1, \dots, x_p) \in G^p$ et $\sigma \in \mathcal{S}_p$, on pose $\sigma(x) = (x_{\sigma(1)}, \dots, x_{\sigma(p)})$.
On vérifie que, pour tout $x = (x_1, \dots, x_p) \in G^p$ et $\sigma, \sigma' \in \mathcal{S}_p$,
$\sigma(\sigma'(x)) = \sigma(x_{\sigma'(1)}, \dots, x_{\sigma'(p)}) = \sigma(y_1, \dots, y_p)$ où $y_i = x_{\sigma'(i)}$,
donc $\sigma(\sigma'(x)) = (y_{\sigma(1)}, \dots, y_{\sigma(p)}) = (x_{\sigma'(\sigma(1))}, \dots, x_{\sigma'(\sigma(p))})$, donc $\sigma(\sigma'(x)) = (\sigma' \circ \sigma)(x)$.
En particulier, on en déduit que, pour tout $k, h \in \mathbb{Z}$ et $x \in G^p$, $c^k(c^h(x)) = c^{k+k}(x)$.
Ainsi, si $x, y \in G^p$ et $k \in \mathbb{Z}$, $y = c^k(x) \Longrightarrow c^{-k}(y) = x$.
◇ Lorsque $x = (x_1, \dots, x_p) \in G^p$ et $y = (y_1, \dots, y_p) \in G^p$, "$y$ se déduit de x par une permutation circulaire" signifie qu'il existe $k \in \mathbb{Z}$ tel que $y = c^k(x)$.

1°) ◇ Soit $x = (x_1, \dots, x_p) \in E$. Ainsi, $x_1 \cdots x_p = 1$,donc en multipliant par x_p^{-1} à droite, $x_1 \cdots x_{p-1} = x_p^{-1}$, puis en multipliant par x_p à gauche, on obtient que
$x_p x_1 \cdots x_{p-1} = 1$, donc $(x_p, x_1, \dots, x_{p-1}) \in E$, c'est-à-dire $c^{-1}(x) \in E$.
De même, on montre que $x_2 \cdots x_p = x_1^{-1}$, donc $x_2 \cdots x_p x_1 = 1$, ce qui prouve que $c(x) \in E$. Par récurrence, on en déduit que pour tout $k \in \mathbb{Z}$, $c^k(x) \in E$ lorsque $x \in E$.
◇ Lorsque $x, y \in E$, on a donc $x\ R\ y \Longleftrightarrow \exists k \in \mathbb{Z},\ y = c^k(x)$.
Il est alors simple de vérifier que R est réflexive $(\forall x \in E, x\ Rx)$, symétrique
$(\forall x, y \in E,\ x\ R\ y \Longrightarrow y\ R\ x)$ et transitive $(\forall x, y, z \in E,\ (x\ R\ y \wedge y\ R\ z) \Longrightarrow x\ R\ z)$.

2°) Soit $x = (x_1, \dots, x_p) \in E$. La classe d'équivalence de x est
$\overline{x} = \{c^k(x)\ /\ k \in \mathbb{Z}\} = \{c^k(x)\ /\ k \in \{0, \dots, p-1\}\}$, car $c^p = Id_{\mathbb{N}_p}$.
Notons $A = \{k \in \mathbb{N}^*\ /\ c^k(x) = x\}$. $p \in A$ car $c^p = Id_{\mathbb{N}_p}$, donc A est une partie non vide de $\mathbb{N}$. Elle possède ainsi un minimum que l'on notera $q \in \mathbb{N}^*$.
Effectuons la division euclidienne de p par q : $p = q\alpha + r$ où $0 \le r < q$.
Alors $x = c^p(x) = c^r((c^q)^a(x))$, or on montre par récurence sur a que $(c^q)^a(x) = x$, donc $c^r(x) = x$. Si $r \neq 0$, on en déduirait donc que $r \in A$ puis que $r \ge q$, ce qui est faux. Ainsi, $r = 0$, donc $p = q\alpha$. Mais p est supposé premier, donc $q = 1$ ou $q = p$.
Supposons que $q = 1$. Alors $c(x) = x$, donc $\overline{x} = \{x\}$.
Supposons maintenant que $q = p$. Soit $i, j \in \{0, \dots, p-1\}$ tels que $i < j$.
Si $c^i(x) = c^j(x)$, alors $x = c^{j-i}(x)$ et $j - i \ge 1$. C'est impossible car $j - i < p = q$.
Ainsi $\overline{x} = \{c^k(x)\ /\ k \in \{0, \dots, p-1\}\}$ est de cardinal p.

3°) Pour choisir un p-uplet de E, on choisit $x_1, \dots, x_{p-1}$ quelconque dans G, puis on impose $x_p = (x_1 \cdots x_{p-1})^{-1}$, donc $|E| = |G|^{p-1}$. En particulier, $|E| \equiv 0\ [p]$.
Par ailleurs, $|E| = \sum_{c \in E/R} |c|$, donc d'après la question 2, modulo p,

$0 \equiv |E| \equiv \sum_{\substack{c\in E/R \\ |c|=1}} |c| \equiv |\{c \in E/R \ / \ |c| = 1\}|$.

Soit $c \in E/R$ tel que $|c| = 1$. Il existe $x = (x_1, \ldots, x_p) \in E$ tel que $c = \overline{x}$. D'après la question 2, on a $c(x) = x$, donc $(x_2, \ldots, x_p, x_1) = (x_1, \ldots, x_p)$, donc pour tout $i \in \mathbb{N}_p$, $x_i = x_1$. Il existe donc $g \in G$ tel que $x = (g, \ldots, g)$. Alors $g^p = x_1 \cdots x_p = 1$. Réciproquement, si $x = (g, \ldots, g)$ avec $g^p = 1$, il est clair que $x \in E$ et que $\overline{x}$ est de cardinal 1. Ainsi, $\{c \in E/R \ / \ |c| = 1\} = \{(g, \ldots, g) \ / \ g \in G$ avec $g^p = 1\}$
et $|\{c \in E/R \ / \ |c| = 1\}| = |\{g \in G \ / \ g^p = 1\}|$.

On obtient ainsi que $|\{g \in G \ / \ g^p = 1\}| \equiv 0 \ [p]$. Mais $1_G^p = 1_G$, donc il existe $g \in E$ avec $g \neq 1_G$ tel que $g^p = 1_G$. Alors l'ordre de g est supérieur à 2 et il divise p qui est premier : g est donc d'ordre p, ce qu'il fallait montrer.