1 Exercices

Exercice 1.1 Soit A un anneau commutatif.

- On dit que $x \in A$ est nilpotent ssi il existe un entier k tel que $x^k = 0$
- On dit que $x \in A$ est idempotent ssi $x^2 = x$

1. Déterminer le nombre d'éléments inversibles de $\mathbb{Z}/p^n\mathbb{Z}$.
2. Déterminer le nombre d'idempotents de $\mathbb{Z}/p^n\mathbb{Z}$.
3. Déterminer le nombre d'éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$ où n est un entier quelconque.
   Dans toute la suite de l'exercice, p désigne un nombre premier.
4. On note $GL_2(\mathbb{Z}/p\mathbb{Z})$ l'ensemble des matrices 2×2 à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ (qui est un corps)
   Déterminer le cardinal de $GL_2(\mathbb{Z}/p\mathbb{Z})$. Généraliser à $GL_n(\mathbb{Z}/p\mathbb{Z})$

Exercice 1.2 Soit p un nombre premier. Soit x un entier, on note $\overline{x}$ la classe de $x \bmod p$

1. Calculer les sommes $\sum_{k=1}^{p-1} \overline{k}$ et $\sum_{k=1}^{p-1} \overline{k}^2$
2. Soit $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Montrer que l'application $\overline{x} \mapsto \overline{ax}^{-1}$ est une bijection de $(\mathbb{Z}/p\mathbb{Z})^\times$ sur lui-même.
3. Soit $p \geqslant 5$ un entier naturel premier et $N \in \mathbb{N}$ défini par : $\sum_{k=1}^{p-1} \frac{1}{k^2} = \frac{N}{(p-1)!^2}$.
   Montrer que p divise N

Exercice 1.3 Déterminer les polynômes $P \in \mathbb{C}[X]$ tels que P' divise P dans $\mathbb{C}[X]$.
Qu'en est-il si $P \in k[X]$ et P' divise P dans $k[X]$ lorsque k est un sous-corps de $\mathbb{C}$?

Exercice 1.4 Soit p un nombre premier Soit G un groupe fini de cardinal p^k.

1. Montrer que si $k = 1$ alors G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$
2. Si on suppose en outre que G est commutatif et $k = 2$, montrer alors G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z})^2$.

2 Indications

Indication pour l'exercice 1.1 :

1. Se rappeler que a est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi a est premier à n
2. Se ramener à $\overline{x(x-1)} = 0 \bmod p^n$ et calculer le pgcd de x et $x-1$ puis appliquer Gauss.
3. Ecrire la décomposition de n en produit de facteurs premiers et utiliser le théorème de Gauss ($p \mid a_1 \cdots a_r$ alors p divise l'un des a_k)
4. Une matrice est inversible ssi ses vecteurs colonnes sont linéairement indépendants.
   En particulier, si $n = 2$ alors le premier vecteur est presque quelconque et le second ne peut être un multiple du premier.
   Dans le cas général, le troisième vecteur ne peut être une combinaison linéaire des deux premiers (il faut donc compter le nombre de vecteurs qui sont combinaisons linéaires des deux premiers), etc..

Indication pour l'exercice 1.2 :

1. Revoir les sommes classiques $\sum_{k=1}^{p-1} k$ et $\sum_{k=1}^{p-1} k^2$ dans $\mathbb{N}$ et justifier que 2 et 3 sont inversibles en général dans $\mathbb{Z}/p\mathbb{Z}$ puis traiter les cas manquants.
2. Résoudre l'équation $\overline{y} = \overline{ax}^{-1}$
3. Considérer $(p-1)!^2 \sum_{k=1}^{p-1} \frac{1}{k^2}$ et montrer que $(p-1)!^2$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$

Indication pour l'exercice 1.3 : Ecrire en terme d'égalité la relation de divisibilité et donner le degré du polynôme quotient. Considérer ensuite une racine ζ de P de multiplicité donné et factoriser P. En utilisant la multiplicité de ζ dans P', obtenir une autre égalité puis montrer que ζ est la racine du polynôme quotient.
Tout polynôme de $k[X]$ peut être vu comme un polynôme de $\mathbb{C}[X]$ et la condition de divisibilité est conservée.

Indication pour l'exercice 1.4 :

1. Montrer qu'il existe nécessaire un élément distinct de l'identité et utiliser le théorème de Lagrange (le cardinal d'un sous-groupe divise le cardinal du groupe)
2. S'il existe un élément d'ordre p^2 montrer que G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$.
   Sinon, en utilisant la notation additive, justifier que tout élément distinct de 0 est d'ordre p puis vérifier que l'application $\overline{k}.x = kx$, $\overline{k} \in \mathbb{Z}/p\mathbb{Z}$ et $x \in G$ muni G d'une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension fini.

3 Corrections

Correction de l'exercice 1.1 : Rappelons pour commencer que nous disposons de l'égalité $\mathbb{Z}/n\mathbb{Z} = \{\overline{k}, \quad k \in [\![0, n-1]\!]\}$

1. Notons $(\mathbb{Z}/p^n\mathbb{Z})^\times$ l'ensemble des inversibles de $\mathbb{Z}/p^n\mathbb{Z}$ (ce dernier ensemble étant de cardinal p^n). Un élément $\overline{x}$ appartient à $(\mathbb{Z}/p^n\mathbb{Z})^\times$ ssi x est premier à p^n (caractérisation des inversibles de $\mathbb{Z}/N\mathbb{Z}$) ce qui équivaut à dire que x est premier à p (si $p \mid a$ alors, puisque $p \mid p$, on a $p \mid \text{pgcd}(a, p^n) = 1$). Par conséquent, $\overline{x} \notin (\mathbb{Z}/p^n\mathbb{Z})^\times \Leftrightarrow p \mid x$. Puisque l'on peut supposer $x \in [\![0, p^n - 1]\!]$, la condition $p \mid x$ équivaut à ce que $x = pk$ avec

$$x = pk \leqslant p^n - 1 \Leftrightarrow pk < p^n \Leftrightarrow k < p^{n-1} \Leftrightarrow k \leqslant p^{n-1} - 1.$$

Nous en déduisons que le complémentaire de $(\mathbb{Z}/p^n\mathbb{Z})^\times$ dans $\mathbb{Z}/p^n\mathbb{Z}$ est l'ensemble $\{p\overline{k}, \quad k \in [\![0, p^{n-1} - 1]\!]\}$ dont le cardinal est p^{n-1} donc $\text{card}(\mathbb{Z}/p^n\mathbb{Z})^\times = p^n - p^{n-1} = p^n(1 - \dfrac{1}{p})$

2. Notons F l'ensemble des idempotents de $\mathbb{Z}/p^n\mathbb{Z}$.

$$\overline{x} \in F \Leftrightarrow \overline{x}^2 = \overline{x} \bmod p^n \Leftrightarrow \overline{x}^2 - \overline{x} = 0 \bmod p^n \Leftrightarrow \overline{x(x-1)} = 0 \bmod p^n \Leftrightarrow p^n \mid x(x-1)$$

Les entiers x et $x-1$ étant premier entre eux (si d divise x et $x-1$, il divise $x-(x-1) = 1$ donc $d = 1$), le lemme de Gauss montrer que $p^n \mid x$ ou $p^n \mid x-1$ ce qui signifie que $\overline{x} = 0 \bmod p^n$ ou $\overline{x} = 1 \bmod p^n$. Réciproquement, si $\overline{x} = 0 \bmod p^n$ ou $\overline{x} = 1 \bmod p^n$, il est évident que $\overline{x}^2 = \overline{x} \bmod p^n$ donc $\overline{x} \in F$, ce qui montrer que $F = \{0 \bmod p^n, 1 \bmod p^n\}$ et $\text{card}\, F = 2$.

3. Soit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ la décomposition de n en produit de nombres premiers distincts (avec $r \in \mathbb{N}$ et $\forall i \in [\![1, r]\!]$, $\alpha_i \in \mathbb{N}^\times$ et p_i est un nombre premier pour tous les entiers i). Considérons un élément $\overline{x}$ nilpotent dans $\mathbb{Z}/n\mathbb{Z}$. Alors $\overline{x}^k = 0 \bmod n$ pour un certain entier k, ce qui signifie qu'il existe un entier N (non nécessairement premier aux p_i) tel que

$$x^k = nN = \left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) N$$

. Il est dès lors immédiat que x^k est divisible par tous les p_i, $i \in [\![1, r]\!]$. Pour $i \in [\![1, r]\!]$ fixé, le nombre premier p_i divise $x^k = \underbrace{x \times x \times \cdots \times x}_{k \text{ foix}}$ et le lemme de Gauss montre alors que p_i divise x (p_i divise x ou x ou ... x). Ainsi, chaque facteur premier de n est un facteur premier de x donc l'entier $\prod_{i=1}^{r} p_i$ divise x. Réciproquement, si $\prod_{i=1}^{r} p_i$ divise x alors $x = \left(\prod_{i=1}^{r} p_i\right) x'$ pour un certain entier x' et $x^{\alpha_1+\alpha_2+\cdots+\alpha_r}$ est clairement divisible par $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ donc

$$x^{\alpha_1+\alpha_2+\cdots+\alpha_r} = 0 \bmod n.$$

On en déduit que l'ensemble des éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble $E = \{\overline{x}, \quad x \in [\![0, n-1]\!]$ et $\prod_{i=1}^{r} p_i \mid x\}$ (autrement dit, c'est l'ensemble des classes $\bmod n$ des multiples de $\prod_{i=1}^{r} p_i$).Un élément x de E est de la forme $x = \left(\prod_{i=1}^{r} p_i\right) M$ avec $M \in \mathbb{N}$ et $x \in [\![0, n-1]\!]$ ce qui implique que

$$\left(\prod_{i=1}^{r} p_i\right) M \leqslant n-1 \Leftrightarrow \left(\prod_{i=1}^{r} p_i\right) M < n \Leftrightarrow M < \frac{n}{\prod_{i=1}^{r} p_i} \in \mathbb{N}.$$

Réciproquement, si $M < \dfrac{n}{\prod_{i=1}^{r} p_i}$ alors $\left(\prod_{i=1}^{r} p_i\right) M \in E$ donc $E = \{\left(\prod_{i=1}^{r} p_i\right) M, \quad M \in [\![0, \dfrac{n}{\prod_{i=1}^{r} p_i} - 1]\!]$, ce qui démontre que $\text{card}\, E = \dfrac{n}{\prod_{i=1}^{r} p_i}$

4. Rappelons ce point d'algèbre linéaire : une matrice A est inversible ssi l'ensemble de ses vecteurs colonnes forment une famille libre.(une famille libre de cardinal n sur un espace vectoriel de dimension n est une base)
Notons également que l'espace vectoriel $(\mathbb{Z}/p\mathbb{Z})^2$ est de cardinal p^2.
Soit $g = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in GL_2(\mathbb{Z}/p\mathbb{Z})$. Si l'on note $e_1 = \begin{pmatrix} a \\ b \end{pmatrix}$ et $e_2 = \begin{pmatrix} c \\ d \end{pmatrix}$ alors $g \in GL_2(\mathbb{Z}/p\mathbb{Z})$ ssi (e_1, e_2) est une famille

libre de l'espace vectoriel $(\mathbb{Z}/p\mathbb{Z})^2$. Cette condition est équivalente à ce que e_1 soit un vecteur non nul de $(\mathbb{Z}/p\mathbb{Z})^2$ et e_2 soit un vecteur non colinéaire à e_1. L'espace $(\mathbb{Z}/p\mathbb{Z})^2$ étant de cardinal p^2 et puisqu'il n'existe qu'un seul vecteur nul (sic), on en déduit que l'on a p^2-1 choix pour le vecteur e_1. Les vecteurs colinéaires au vecteur e_1 étant de la forme $\overline{x}e_1$, $\overline{x}\in\mathbb{Z}/p\mathbb{Z}$, (remarquons que le vecteur nul est colinéaire à e_1) on en déduit qu'il existe p vecteurs colinéaires de e_1. On peut choisir alors pour e_2 n'importe quel vecteur parmi les p^2-p vecteurs non colinéaires de e_1 dans $(\mathbb{Z}/p\mathbb{Z})^2$. Nous en déduisons que $\operatorname{card} GL_2(\mathbb{Z}/p\mathbb{Z}) = (p^2-1)(p^2-p)$
Si $g\in GL_n(\mathbb{Z}/p\mathbb{Z})$, on note e_i le $i^{ième}$ vecteur colonne de g. L'espace vectoriel $(\mathbb{Z}/p\mathbb{Z})^n$ étant de cardinal p^n, on a donc p^n-1 vecteurs non nul possibles pour e_1. On poursuit par itération : supposons avoir choisit les k ($k\leqslant n-1$) premiers vecteurs libres $e_1,..,e_k$. Le choix du vecteur e_{k+1} doit se faire parmi les vecteurs n'appartenant pas à l'espace engendré par $e_1,..,e_k$, qui est de cardinal p^k puisque l'application

$$(\overline{x_1},..,\overline{x_k})\in(\mathbb{Z}/p\mathbb{Z})^k\mapsto \overline{x_1}e_1+\cdots+\overline{x_k}e_k$$

est une bijection de $(\mathbb{Z}/p\mathbb{Z})^k$ sur $\operatorname{Vect}(e_1,..,e_k)$ (la famille $(e_1,..,e_k)$ étant libre) Nous avons donc p^n-p^k choix pour le vecteur e_k, ce qui nous donne

$$\operatorname{card} GL_n(\mathbb{Z}/p\mathbb{Z}) = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = \prod_{k=0}^{n-1}(p^n-p^k)$$

Correction de l'exercice 1.2 :

1. Dans $\mathbb{N}$, nous avons les égalités suivantes $2\sum_{k=1}^{p-1}k = p(p-1)$ et $6\sum_{k=1}^{p-1}k^2 = p(p-1)(2p-1)$ donc on a

$$2\sum_{k=1}^{p-1}k = 0\bmod p \quad\text{et}\quad 6\sum_{k=1}^{p-1}k^2 = 0\bmod p$$

Si $p\geqslant 5$ (donc différent de 2 et 3), les deux nombres 2 et $6(=2\times 3)$ sont premiers à p donc ils sont inversibles dans $\mathbb{Z}/p\mathbb{Z}$ et l'on a :

$$\sum_{k=1}^{p-1}k = 0\bmod p \quad\text{et}\quad \sum_{k=1}^{p-1}k^2 = 0\bmod p$$

Si $p=3$ alors 2 est inversible dans $\mathbb{Z}/3\mathbb{Z}$ donc $\sum_{k=1}^{2}k = 0\bmod 3$ et $\sum_{k=1}^{2}k^2 = 5\bmod 3 = 2\bmod 3$.

Si $p=2$ alors $\sum_{k=1}^{1}k = 1\bmod 2$ et $\sum_{k=1}^{1}k^2 = 1\bmod 2$

2. Puisque $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe, l'application $\overline{x}\mapsto\overline{ax}^{-1}$ est bien une application de $(\mathbb{Z}/p\mathbb{Z})^\times$ dans lui-même. Les ensembles de départ et d'arrivée étant finis et de même cardinal, pour montrer que cette application est bijective, il suffit de montrer qu'elle est injective, ce qui découle du calcul suivant : $\overline{ax}^{-1}=\overline{ay}^{-1}\Leftrightarrow\overline{x}^{-1}=\overline{y}^{-1}\Leftrightarrow\overline{x}=\overline{y}$.

3. Nous avons par définition

$$N=(p-1)!^2\sum_{k=1}^{p-1}\frac{1}{k^2}=\sum_{k=1}^{p-1}\frac{(p-1)!^2}{k^2}=\sum_{k=1}^{p-1}\left(\frac{(p-1)!}{k}\right)^2 \tag{1}$$

Remarquons ensuite que pour tout entier $k\in[\![1,p-1]\!]$, le nombre $\dfrac{(p-1)!}{k}=1\times...\times\widehat{k}\times..\times(p-1)$ est entier et que

$$\overline{k}\times\overline{\frac{(p-1)!}{k}}=\overline{k\times\frac{(p-1)!}{k}}=\overline{(p-1)!} \tag{2}$$

Puisque p est un nombre premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps donc tous ces éléments non nuls sont les inversibles de $\mathbb{Z}/p\mathbb{Z}$, c'est-à-dire $(\mathbb{Z}/p\mathbb{Z})^\times=\{\overline{k},\quad k\in[\![1,p-1]\!]\}$. En particulier, pour $k\in[\![1,p-1]\!]$, les éléments $\overline{k}$, $\overline{\dfrac{(p-1)!}{k}}$ et $\overline{(p-1)}=\overline{1}\times\overline{2}\times...\times\overline{p-1}$ sont inversibles dans $\mathbb{Z}/p\mathbb{Z}$. L'égalité (2) montre alors que

$$\forall k\in[\![1,p-1]\!],\quad \overline{\frac{(p-1)!}{k}}=\overline{(p-1)!}\times\overline{k}^{-1}.$$

En écrivant l'égalité (1) dans $\mathbb{Z}/p\mathbb{Z}$, on obtient alors

$$N=\sum_{k=1}^{p-1}\left(\frac{(p-1)!}{k}\right)^2\bmod p=\sum_{k=1}^{p-1}\left[\overline{(p-1)!}\times\overline{k}^{-1}\right]^2\bmod p \tag{3}$$

La question 2 montre que l'application $\overline{k} \mapsto \overline{(p-1)!}\overline{k}^{-1}$ est une bijection de $(\mathbb{Z}/p\mathbb{Z})^\times$ sur lui-même. En effectuant le changement de variable $\overline{x} = \overline{(p-1)!} \times \overline{k}^{-1}$ dans l'égalité (3), on en déduit que $N = \sum_{k=1}^{p-1} \overline{x}^2 \bmod p$. En utilisant le fait que p est un nombre premier plus grand que 5 ainsi que la question 1, on aboutit à $N = 0 \bmod p$ autrement dit p divise N

Correction de l'exercice 1.3 : Soit $P \in \mathbb{C}[X]$ tel que $P' \mid P$, c'est-à-dire qu'il existe un polynôme $R \in \mathbb{C}[X]$ tel que $P = RP'$.
Si le polynôme P est constant alors P' est nul donc P est nul.
Si P est un polynôme non constant de degré n alors P' est de degré $n-1$ et R est alors de degré 1 donc on a l'égalité

$$P = \alpha(X - z_0)P' \tag{4}$$

où α et z_0 sont deux complexes, avec $\alpha \neq 0$. Puisque P est un polynôme à coefficients complexes, on est assuré qu'il admet une ou plusieurs racines dans $\mathbb{C}$ (il est même scindé sur $\mathbb{C}$). Soit ζ une racine de P de multiplicité $k \in [\![1, n]\!]$ alors

$$P = (X - \zeta)^k Q, \text{ avec } Q \in \mathbb{C}[X] \text{ et } Q(\zeta) \neq 0 \tag{5}$$

En outre, ζ est une racine de P' de multiplicité $k-1$ (cf. cours sur les polynômes) donc il existe un polynôme T tel que

$$P' = (X - \zeta)^{k-1} T, \text{ avec } T \in \mathbb{C}[X] \text{ et } T(\zeta) \neq 0 \tag{6}$$

La combinaison des égalités (4), (5) et (6) fournit l'égalité suivante

$$(X - \zeta)^k Q = \alpha(X - z_0)(X - \zeta)^{k-1} T, \text{ avec } Q(\zeta) \neq 0 \text{ et } T(\zeta) \neq 0,$$

d'où l'on en déduit

$$(X - \zeta)Q = \alpha(X - a)T$$

En évaluant cette dernière égalité en $X = \zeta$ et utilsant que $T(\zeta) \neq 0$, on en déduit que $\zeta = z_0$. Nous venons de montrer que toute racine de P est égale à z_0 donc P admet une unique racine dans $\mathbb{C}$ ce qui implique que P est de la forme $\beta(X - z_0)^n$ (P est scindé sur $\mathbb{C}$) Réciproquement, tout polynôme P de la forme $P = \beta(X - z_0)^n$, où $\beta \neq 0$ et z_0 sont deux complexes, vérifie bien la condition $P' \mid P$.un complexe.
Ainsi les seuls polynômes appartenant à $\mathbb{C}[X]$ satisfaisant à la condition souhaitée sont soit le polynôme nul soit les polynômes admettant une unique racine.
Si $P \in k[X]$ avec $k \subset \mathbb{C}$ et $P' \mid P$ dans $k[X]$ alors $P \in \mathbb{C}[X]$ et $P' \mid P$ dans $\mathbb{C}[X]$ (l'égalité $P = RP'$ étant valable dans $k[X]$, elle reste valable dans $\mathbb{C}[X]$). Le raisonnement ci-dessu montre que P est de la forme $P = 0$ ou $P = \beta(X - z_0)^n$ où $n = \deg P \geqslant 1$, β et z_0 étant deux complexes.
Si $P = 0$ alors P appartient bien à $k[X]$ et vérifie $P' \mid P$ dans $k[X]$.
Si $P \neq 0$, le coefficient dominant a_n de P étant par définition dans k et le coefficient dominant de $\beta(X - z_0)^n$ étant β, on en déduit que $\beta = a_n \in k$. D'autre part, le coefficient a_{n-1} de X^{n-1} dans P étant également dans k et le coefficient de X^{n-1} dans $\beta(X - z_0)^n$ étant $-\beta n z_0$, on obtient $a_{n-1} = -\beta n z_0 \Leftrightarrow z_0 = -\dfrac{a_{n-1}}{\beta n} \in k$ donc le polynôme $P = \beta(X - z_0)^n$ appartient également à $k[X]$.
Ainsi les seuls polynômes appartenant à $k[X]$ satisfaisant à la condition souhaitée sont soit le polynôme nul soit les polynômes scindés sur k et admettant une unique racine.

Correction de l'exercice 1.4 :

1. Puisque $\operatorname{card} G = p$ est un nombre premier, il est d'ordre au moins 2 donc il admet un élément $x \neq 1$. Le groupe $< x >$ engendré par x est donc de cardinal au moins 2 et son ordre divise celui de G qui est premier. On en déduit que $\operatorname{card} < x >= 1$ ou $\operatorname{card} < x >= p$. La première égalité étant impossible, on en déduit que $\operatorname{card} < x >= p$ et puisque $\operatorname{card} G = p$ et $< x > \subset G$, on a donc $G =< x >$. Le groupe G étant monogène et fini d'ordre p, on en déduit qu'il est isomorphe) $\mathbb{Z}/p\mathbb{Z}$.
   Rappel sur la dernière assertion : il suffit de considérer l'application $k \bmod p \to x^k$ de $\mathbb{Z}/p\mathbb{Z}$ dans G. Elle est bien définie car si $k \bmod p = r \bmod p$ alors $k = r + qp$ avec $q \in \mathbb{Z}$ donc $x^k = x^{r+qp} = x^r(x^p)^q = x^r(1)^q = x^r$. Cette application étant clairement surjective entre deux ensembles finis de même cardinal, on en déduit qu'elle est bijective. Le fait qu'il s'agisse d'un morphisme est laissé au lecteur

2. Soit x un élément de G. L'ordre $o(x)$ de x étant par définition le cardinal du groupe $< x >$ engendré par x, le théorème de Lagrange montrer que l'ordre de x divise $\operatorname{card} G = p^2$, ce qui signifie que $o(x) = 1$ ou $o(x) = p$ ou $o(x) = p^2$. Le groupe G étant distinct du groupe trivial, on est assuré de l'existence d'un élément $x \neq 1$ donc d'ordre différent de 1.
   Supposons qu'il existe un élement $x \in G$ d'ordre p^2 alors par le raisonnement tenu à la question 1, on en déduit que $G =< x >$ et l'application $k \bmod p^2 \to x^k$ de $\mathbb{Z}/p^2\mathbb{Z}$ dans G est un isomorphisme (je laisse au lecteur la vérification en

tout point semblable à la question 1).
Supposons qu'aucun élément de G soit d'ordre p^2. Cela implique que tout élément $x \neq 1$ de G est d'ordre p. En particulier, $\forall x \in G, \quad x^p = 1$ ou si nous utilisons la notation additive (autrement, la loi de G est notée $+$ au lieu de $\times$), $\forall x \in G, \quad px = 0$. Montrons que G est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. G. Le groupe $(G, +)$ étant additif, il suffit de définir la loi externe. Pour $\overline{k} \in \mathbb{Z}/p\mathbb{Z}$ et $x \in G$, on note $\overline{k}.x = kx$. Vérifions que cette loi est bien définie (qu'elle ne dépend pas de k mais de sa classe modulo p). Si $k \bmod p = q \bmod p$ alors il existe un entier $r \in \mathbb{Z}$ tel que $k = q + rp$ et l'on a

$$kx = (q + rp)x = qx + r(\underbrace{px}_{=0}) = qx$$

donc la loi . est bien définie. Nous avons également

$$\overline{k}.(x + y) = k(x + y) = kx + ky = \overline{k}.x + \overline{k}.y$$

(puis G est commutatif) et

$$\overline{k}.\overline{q}.x = \overline{k}.(qx) = k(qx) = kqx = \overline{kq}.x$$

Par conséquent, G est bien un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. G étant fini, il est nécessairement de dimension finie. Si n désigne sa dimension alors G est isomorphe (en tant que $\mathbb{Z}/p\mathbb{Z}$-espace espace vectoriel) à $(\mathbb{Z}/p\mathbb{Z})^n$ donc son cardinal est p^n et l'on sait déjà que son cardinal est p^2. On en déduit que $n = 2$, c'est-à-dire qu'il existe une $\mathbb{Z}/p\mathbb{Z}$ base (e_1, e_2) de G. En particulier, pour tout élément x de G, il existe un et un seul couple d'éléments $(\overline{k_1}, \overline{k_2}) \in (\mathbb{Z}/p\mathbb{Z})^2$ tel que

$$x = \overline{k_1}.e_1\overline{+k_2}.e_2.$$

Il est dès lors clair que l'application $(\overline{k_1}, \overline{k_2}) \mapsto \overline{k_1}.e_1\overline{+k_2}.e_2$ est une bijection de $(\mathbb{Z}/p\mathbb{Z})^2$ sur G et je laisse le lecteur vérifié qu'il s'agit d'un morphisme de groupe. Nous venons donc de montrer que G est isomorphe en tant que groupe à $(\mathbb{Z}/p\mathbb{Z})^2$.