Université Pierre et Marie Curie 2006–2007

LM220 Maths-Info groupes 1, 2 et 5

Devoir maison 1

L'objectif du devoir est de caractériser les entiers $n \geqslant 2$ pour lesquels le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique. On admet le fait que, pour p premier, $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique. En effet, on sait que $\mathbf{Z}/p\mathbf{Z}$ est un corps, et il sera démontré plus loin dans le cours (corollaire 6 p. 97) que le groupe multiplicatif d'un corps fini est cyclique.

1 Préliminaires

Soit $n \geqslant 2$ un entier. On considère sa décomposition en facteurs premiers $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, où les p_i sont des premiers distincts et les α_i des entiers non nuls.

1.1 Montrer par récurrence sur r que l'on a un isomorphisme de groupes :

$$(\mathbf{Z}/n\mathbf{Z})^\times \approx \prod_{i=1}^{r} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times \ .$$

(*Indication* : utiliser le théorème chinois.)

On va donc dans les deux sections suivantes étudier chaque facteur du membre de droite, c'est-à-dire les groupes de la forme $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$, en distinguant les cas $p = 2$ et p impair. Avant de commencer cette étude, on établit un résultat utile de théorie des groupes.

1.2 Soit G un groupe abélien, noté multiplicativement. On considère deux éléments x et y, d'ordres respectifs a et b. Montrer que si a et b sont premiers entre eux, leur produit xy est d'ordre ab. (*Indication* : si $(xy)^d = 1$, montrer que a et b divisent d en élevant cette égalité à la puissance b ou a.)

2 Le cas $p \neq 2$

On suppose dans toute cette section que p est un nombre premier impair, et α un entier supérieur ou égal à 2. On va montrer que $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ est cyclique.

2.1 Calculer l'ordre de $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$. Justifier par ailleurs que $(1+p) \in (\mathbf{Z}/p^\alpha\mathbf{Z})^\times$.

2.2 Montrer que, si i est un entier compris entre 1 et $p-1$, alors p divise le coefficient binomial C_p^i. En déduire que si $i \geqslant 2$, alors p^3 divise $C_p^i p^i$.

2.3 Montrer qu'il existe un entier $u \in \mathbf{N}^*$ tel que $(1+p)^p = 1 + p^2(1+up)$.

2.4 En déduire par récurrence que pour tout entier $k \geqslant 1$, il existe un entier λ (dépendant de k), premier à p, tel que $(1+p)^{p^k} = 1+\lambda p^{k+1}$. (*Indication* : si $(1+p)^{p^k} = 1+\lambda p^{k+1}$, on pourra montrer qu'il existe $u \in \mathbf{N}^*$ tel que $(1+p)^{p^{k+1}} = 1 + p^{k+2}(\lambda + up)$.)

2.5 Déduire de la question précédente que $(1+p)^{p^{\alpha-1}} \equiv 1 \bmod p^\alpha$ et que $(1+p)^{p^{\alpha-2}} \not\equiv 1 \bmod p^\alpha$. En déduire que $1+p$ est d'ordre $p^{\alpha-1}$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$.

2.6 On considère à présent l'application

$$\begin{aligned} \pi : (\mathbf{Z}/p^\alpha\mathbf{Z})^\times &\longrightarrow (\mathbf{Z}/p\mathbf{Z})^\times \\ x \bmod p^\alpha &\longmapsto x \bmod p \end{aligned}$$

dont on admet qu'elle est bien définie et constitue un morphisme de groupes surjectif. Montrer qu'il existe $x \in (\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ tel que $\pi(x)$ soit d'ordre $p-1$.

2.7 Montrer qu'alors l'ordre de x est multiple de $p-1$ et qu'il existe un entier k tel que $y = x^k$ soit d'ordre exactement $p-1$.

2.8 En utilisant le résultat des questions 2.5 et 1.2, calculer l'ordre de $y(1+p)$ et conclure.

3 Le cas $p = 2$

L'objectif de cette section est de montrer que $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times$ *est cyclique si et seulement si* $\alpha = 1$ *ou* $\alpha = 2$.

3.1 Expliciter $(\mathbf{Z}/2\mathbf{Z})^\times$ et $(\mathbf{Z}/4\mathbf{Z})^\times$ et vérifier qu'ils sont cycliques.

On supposera pour la suite de la section que $\alpha \geqslant 3$.

3.2 Calculer l'ordre de $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times$.

3.3 En s'inspirant des questions 2.3 et 2.4, montrer que pour tout $k \in \mathbf{N}^*$, il existe un entier impair λ (dépendant de k) tel que $5^{2^k} = 1 + \lambda 2^{k+2}$. (*Indication* : $5 = 1+4$.)

3.4 En déduire comme à la question 2.5 que 5 est d'ordre $2^{\alpha-2}$ dans $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times$.

3.5 On note μ_2 le groupe multiplicatif à deux éléments $\{1,-1\}$. On rappelle que le produit $\mu_2 \times \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$ est un groupe dont la loi est donnée par $(\varepsilon, a)\cdot(\varepsilon', a') = (\varepsilon\varepsilon', a+a')$. On considère l'application

$$\begin{aligned} f : \mu_2 \times \mathbf{Z}/2^{\alpha-2}\mathbf{Z} &\longrightarrow (\mathbf{Z}/2^\alpha\mathbf{Z})^\times \\ (\varepsilon, a) &\longmapsto \varepsilon \cdot 5^a \end{aligned}$$

Montrer que f est un morphisme de groupes.

3.6 Soit $a \in \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$. Montrer que dans $(\mathbf{Z}/2^{\alpha}\mathbf{Z})^{\times}$ on a $5^a = 1$ si et seulement si $a = 0$ dans $\mathbf{Z}/2^{\alpha-2}\mathbf{Z}$. Montrer par ailleurs que pour tout $a \in \mathbf{Z}$, on a $5^a \neq -1$ dans $\mathbf{Z}/2^{\alpha}\mathbf{Z}$. (*Indication* : on pourra au choix réduire 5^a modulo 4 ou utiliser le résultat de 3.3.)

3.7 En déduire que l'application f de la question 3.5 est injective, en vérifiant que $\ker f = \{(1, 0)\}$. Prouver alors que f est un isomorphisme en utilisant la question 3.2.

3.8 Montrer que tous les éléments de $(\mathbf{Z}/2^{\alpha}\mathbf{Z})^{\times}$ sont d'ordre divisant $2^{\alpha-2}$ et conclure.

4 Conclusion

4.1 Soient a et b deux entiers non nuls. Montrer que si a et b ne sont pas premiers entre eux, alors $\mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z}$ n'est pas cyclique.

4.2 Déduire des questions précédentes que le groupe $(\mathbf{Z}/n\mathbf{Z})^{\times}$ est cyclique si et seulement si n vaut 2 ou 4 ou est de la forme p^{α} ou $2p^{\alpha}$, avec p premier et α entier non nul.