Université Claude Bernard Lyon 1

MASTER M1G

Algèbre

Correction Exercice 2 Fiche 1

Exercice 2*Automorphismes de $\mathbb{Z}/n\mathbb{Z}$ (suite et fin)*

Le but de l'exercice est de décomposer en groupes cycliques le groupe des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ (qui est abélien par l'exercice précédent). Dans un esprit de modération nous allons nous limiter au cas où $n = p^k$.

1. Trouver un élément d'ordre 6 dans $(\mathbb{Z}/7\mathbb{Z})^*$, un élément d'ordre 12 dans $(\mathbb{Z}/13\mathbb{Z})^*$. Pouvait-on être certain de leur existence ?
2. On veut montrer que $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, c'est-à-dire qu'il existe un élément d'ordre $(p-1)$ dans $(\mathbb{Z}/p\mathbb{Z})^*$.
   (a) Montrer que sur $(\mathbb{Z}/p\mathbb{Z})^*$, le nombre d'éléments d'ordre d est inférieur ou égal à $\varphi(d)$.
   (b) A l'aide de l'égalité $n = \sum_{d|n} \varphi(d)$ (que signifie cette égalité ?), conclure qu'il existe forcément un élément d'ordre $p-1$.
3. On suppose que p est premier impair et on veut montrer que $(\mathbb{Z}/p^k\mathbb{Z})^*$ est cyclique.
   (a) Montrer qu'il existe λ_k, pour tout k premier à p tel que
   $$(1+p)^{p^k} = 1 + \lambda p^{k+1}.$$
   (b) Montrer qu'il existe un élément d'ordre $p-1$ dans $(\mathbb{Z}/p^k\mathbb{Z})^*$.
   (c) Montrer qu'il existe un élément d'ordre $p^{k-1}(p-1)$. Conclure.
4. Où s'est-on servi du fait que p était impair ?

Soluce

1. Pour le premier, on trouve 3. Il est très clair qu'un tel élément se devait d'exister : l'ordre du groupe est 6 et donc le groupe est d'ordre 6 et abélien ; il n'y en a qu'un et il est cyclique.

   Pour le second, on trouve 2. L'existence a priori demande tout de même le théorème du cours qui dit que le groupe multiplicatif d'un corps fini est cyclique [1].

1. Plus généralement, tout sous-groupe fini du groupe multiplicatif d'un corps (non nécessairement fini) est cyclique

2. (a) Le groupe $\mathbb{Z}/p\mathbb{Z}$ se réalise dans le groupe multiplicatif $\mathbb{C}^*$ comme le sous-groupe des racines p-ièmes de l'unité. S'il n'y a pas d'élément d'ordre d, c'est ok. S'il y en a un, alors, il engendre, dans $\mathbb{C}^*$, un groupe à d éléments qui vérifient tous $x^d = 1$. Or, il y a au plus d éléments dans $\mathbb{C}^*$ qui peuvent vérifier cette équation, et c'est le groupe des racines d-ièmes de l'unité. Parmi eux, seuls $\varphi(d)$ racines sont d'ordre d, ce sont les racines primitives d-ièmes de l'unité. En fait, on a une réponse un peu plus précise que l'énoncé : le nombre d'élements d'ordre d est, soit 0, soit $\varphi(d)$.

   (b) L'égalité signifie que l'on peut partitionner $\mathbb{Z}/n\mathbb{Z}$ en éléments d'ordre d pour chaque diviseur d de n, et qu'il y a exactement $\varphi(d)$ éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$.

   Il y a $p-1$ éléments dans $(\mathbb{Z}/p\mathbb{Z})^*$. Supposons qu'il n'y ait pas d'élément d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^*$. Alors, en partitionant $(\mathbb{Z}/p\mathbb{Z})^*$ en éléments d'ordre d (qui divise nécessairement $p-1$), on obtient, d'après ce qui précède :

$$p - 1 = \sum_{d|p-1, d<p-1} \varphi(d) < \sum_{d|p-1} \varphi(d) = p - 1,$$

   ce qui est absurde.

3. (a) On fait une récurrence sur k. L'initialisation pour $k = 1$ est laissée au lecteur consciencieux.

   On suppose par récurrence $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$, avec λ^k premier avec p et $k \geq 1$. Alors, en prenant la puissance p-ième :

$$(1+p)^{p^{k+1}} = 1 + p\lambda_k p^{k+1} + p^{2k+2}\nu,$$

   pour un ν entier. On a donc :

$$(1+p)^{p^{k+1}} = 1 + \lambda_{k+1} p^{k+2},$$

   avec $\lambda_{k+1} = \lambda^k + p^k\nu$, qui est clairement premier avec p. Ce qui prouve notre récurrence.

   (b) Comme $(1+p)$ est premier avec p^k (il n'a aucun diviseur premier commun !), sa classe est bien dans $(\mathbb{Z}/p^k\mathbb{Z})^*$.

   D'après ce qui précède, on a, dans $(\mathbb{Z}/p^k\mathbb{Z})^*$

$$(1+p)^{p^{k-1}} = 1, \text{ et } (1+p)^{p^{k-2}} = 1 + \lambda_{k-2} p^{k-1}.$$

   L'ordre de $(1+p)$ divise p^{k-1} et s'il le divisait strictement, on aurait $1 = (1+p)^{p^{k-2}} = 1 + \lambda_{k-2}p^{k-1}$ et donc $\lambda_{k-2}p^{k-1} = 0$ λ serait multiple de p dans $\mathbb{Z}$, absurde. D'où la conclusion que $(1+p)$ est d'ordre p^{k-1} dans $(\mathbb{Z}/p^k\mathbb{Z})^*$.

   (c) On construit le morphisme canonique de $\mathbb{Z}$ sur $\mathbb{Z}/p\mathbb{Z}$. Puis, comme $p^k\mathbb{Z} \subset p\mathbb{Z}$ qui est le noyau du morphisme, on a, par passage au quotient, un morphisme $\mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, qui reste surjectif. Or, la classe d'un entier a dans $\mathbb{Z}/p^k\mathbb{Z}$ est inversible si et seulement si p ne divise pas a, et donc si et seulement si la classe

de a dans $\mathbb{Z}/p\mathbb{Z}$ est inversible. Le morphisme que l'on a construit se resteint donc en un morphisme (de groupes multiplicatifs !) $\pi : (\mathbb{Z}/p^k\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$, qui reste surjectif.

Soit g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$ et soit h un antécédent de g. Comme l'ordre d'un élément est multiple de l'ordre de son image par un morphisme, on a que l'ordre m de h est multiple de $p-1$. Le sous-groupe de $(\mathbb{Z}/p^k\mathbb{Z})^*$ engendré par h est cyclique d'ordre m, et donc, il contient un élément d'ordre $p-1$.

(d) Si a et b ont des ordres premiers entre eux dans un groupe abélien, respectivement s et t, dans un groupe multiplicatif abélien, alors l'ordre de ab vaut le produit des ordres de a et de b. Effectivement, $ab^{st} = a^{st}b^{st} = 1$. De plus, si $ab^u = 1$, alors $a^u = b^{-u}$. Comme, par Lagrange, l'intersection de $\langle a\rangle$ et $\langle b\rangle$ est triviale, on a $a^u = 1$ et $b^u = 1$. Donc, u est multiple de s et de t, donc de st.

Conclusion, comme $p^{k-1}(p-1)$ sont premiers entre eux, on construit ainsi un élément d'ordre $p^{k-1}(p-1)$. Comme on a justement $p^{k-1}(p-1) = \varphi(p^k) = \#(\mathbb{Z}/p^k\mathbb{Z})^*$, ce groupe est cyclique.

4. Ah-Aaaah ! Oui, où s'en est-on servi de cette hypothèse ? Pourtant le théorème est faux pour p pair puisque l'on trouve dans le Perrin que

$$(\mathbb{Z}/2^k\mathbb{Z})^* \simeq \mathbb{Z}/2^{k-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ k \geq 3.$$

Si vous êtes le lecteur consciencieux qui a vérifié l'initialisation, alors vous avez remarqué que $(1+2)^2 = 1+8$, et donc, l'initialisation est fausse pour p pair. C'est un très bel exemple de récurrence qui marche très bien au niveau de l'hérédité, mais pas pour l'initialisation. Etonnant, non ?