Lycée Louis-Le-Grand, Paris
MPSI 4 – Mathématiques
A. Troesch

Pour le 21/03/2019

DM n° 15 : Anneaux, arithmétique

Problème 1 –

- *Un pseudo-anneau A est un ensemble muni de deux lois de composition interne notées $+$ et $\times$, telles que $(A,+)$ soit un groupe abélien, et telle que $\times$ soit associative et distributive sur $+$. En revanche, il n'existe pas nécessairement d'élément neutre pour la loi $\times$.*
- *Un anneau est donc un pseudo-anneau admettant un élément neutre 1_A pour la loi $\times$.*
- *Une partie I de A est appelée* idéal bilatère *de A si I est un sous-groupe additif de $(A,+)$, et si pour tout $x \in I$ et $y \in A$, $xy \in I$ et $yx \in I$.*
- *Le centre $C(A)$ d'un pseudo-anneau A est : $C(A) = \{x \in A \mid \forall y \in A,\ xy = yx\}$.*
- *On dit qu'un pseudo-anneau A est commutatif si la loi $\times$ est commutative, ce qui revient à dire que $C(A) = A$.*

1. Soit A un pseudo-anneau
   (a) Montrer que $C(A)$ est un sous-groupe additif de $(A,+)$.
   (b) Montrer que tout idéal bilatère I de A est un pseudo-anneau.
2. Soit A un pseudo-anneau vérifiant : $\forall x \in A,\ \ x^2 - x \in C(A)$.
   (a) En considérant $x+y$, montrer que pour tout $(x,y) \in A^2$, $xy + yx \in C(A)$.
   (b) En déduire que A est commutatif.

Dans la suite, A désigne un anneau *tel que pour tout $x \in A$, $x^3 = x$. On veut prouver que A est commutatif.*

3. Prouver l'égalité $6 = 0$, où 6 désigne $6 \cdot 1_A$.
4. On note $2A = \{2 \cdot a \mid a \in A\}$ et $3A = \{3 \cdot a \mid a \in A\}$. Prouver les assertions suivantes :
   (a) $3A \cap 2A = \{0\}$
   (b) $3A$ et $2A$ sont des idéaux bilatères de A
   (c) Tout élément de A s'écrit de façon unique comme somme d'un élément de $3A$ et d'un élément de $2A$.
   (d) $\forall x \in 3A,\ \forall y \in 2A,\ xy = yx = 0$.
5. (a) Prouver que pour tout $x \in 3A$, $2x = 0$ et $x^2 = x$.
   (b) En déduire que pour tout $(x,y) \in (3A)^2$, $xy = yx$
6. Soit x et y dans $2A$. En développant $(x+y)^3$ et $(x-y)^3$, montrer que $xy = yx$.
7. Montrer que A est commutatif.

Problème 2 – **Nombres de Carmichael**

Le but de ce problème est d'étudier certaines propriétés des nombres de Carmichael, nombres composées qui satisfont tout de même la propriété du petit théorème de Fermat. Notre but est notamment de donner une caractérisation des nombres de Carmichael en fonction de l'indicateur de Carmichael $\lambda(G)$, défini comme l'exposant du groupe $(\mathbb{Z}/n\mathbb{Z})^*$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$, donc comme le ppcm des ordres des éléments de ce groupe. Pour étudier cet indicateur de Carmichael, nous commençons par l'étude des groupes $(\mathbb{Z}/n\mathbb{Z})^*$, éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Partie I – Structure du groupe $(\mathbb{Z}/p\mathbb{Z})^*$

Soit p un nombre premier. On montre dans cette partie que le groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ des éléments inversibles du corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est cyclique d'ordre $p-1$, donc isomorphe à $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$ ou encore à $(\mathbb{U}_{p-1}, \times)$. Un générateur de ce

groupe est appelé racine primitive modulo p. On admettra dans cette partie que si P est un polynôme à coefficients dans un corps $\mathbb{K}$ et si r est une racine de P, alors P est divisible par $(X-r)$: autrement dit, il existe un polyôme Q tel que $P(X) = (X-r)Q(X)$.

1. Soit $(G, \times)$ un groupe abélien fini, et x et y deux éléments de G d'ordre a et b. Montrer qu'il existe deux éléments x' et y' d'ordre a' et b' tels que $a' \wedge b' = 1$ et $a'b' = a \vee b$.
2. En considérant $x'y'$, en déduire l'existence d'un élément d'ordre $a \vee b$.
3. Soit $\omega(G)$ le ppcm des ordres de tous les éléments de G. Montrer qu'il existe un élément $g \in G$ d'ordre $\omega(G)$. En déduire que
$$\omega(G) = \min\{k \in \mathbb{N}^* \mid \forall g \in G,\ g^k = 1, \}$$
où 1 désigne le neutre de G.
4. Soit $G = ((\mathbb{Z}/p\mathbb{Z})^*, \times)$. Justifier que l'ordre de G est $p-1$.
5. Soit $P \in \mathbb{F}_p[X]$ le polynôme à coefficients dans $\mathbb{F}_p$ défini par :
$$P(X) = X^{\omega(G)} - 1.$$
Montrer que pour tout $\xi \in G$, $P(\xi) = 0$, et en déduire que $P(X)$ est divisible par $\prod_{\xi \in G}(X - \xi)$
6. En déduire que $p - 1 \leqslant \omega(G)$, puis que $\omega(G) = p - 1$.
7. Montrer que G est cyclique d'ordre $p-1$.

On peut remarquer que la preuve ci-dessus s'adapte sans difficulté pour montrer plus généralement que pour tout corps fini K, K^* est un groupe cyclique, formé des racines du polynôme $X^{n-1} - 1$, n étant l'ordre de K.

Partie II – Stucture des groupes $(\mathbb{Z}/p^n\mathbb{Z})^*$

Soit p un entier premier impair et $n \in \mathbb{N}^*$, $n \geqslant 2$. On généralise le résultat de la partie I en montrant dans cette partie que le groupe $((\mathbb{Z}/p^n\mathbb{Z})^*, \times)$ des éléments inversibles de l'anneau $\mathbb{Z}/p^n\mathbb{Z}$ est cyclique.

1. Soit $k \in \mathbb{Z}$, et $\overline{k}$ son représentant dans $\mathbb{Z}/p^n\mathbb{Z}$. Montrer que $\overline{k}$ est inversible si et seulement si k n'est pas divisible par p.
2. En déduire que $(\mathbb{Z}/p^n\mathbb{Z})^*$ est d'ordre $p^{n-1}(p-1)$.
3. Montrer que pour tout $a \in \mathbb{Z}$, et tout $m \in \mathbb{N}^*$, $(1 + p^m a)^p \equiv 1 + p^{m+1}a\ [p^{m+2}]$.
4. En déduire que pour tout $a \in \mathbb{Z}$, et tout $m \in \mathbb{N}$, $(1 + pa)^{p^m} \equiv 1 + p^{m+1}a\ [p^{m+2}]$.
5. Montrer que $1 + p$ est d'ordre p^{n-1} dans $(\mathbb{Z}/p^n\mathbb{Z})^*$
6. En considérant une racine primitive modulo p, montrer qu'il existe un élément d'ordre $p-1$ dans $(\mathbb{Z}/p^n\mathbb{Z})^*$.
7. En déduire que $(\mathbb{Z}/p^n\mathbb{Z})^*$ est cyclique d'ordre $p^{n-1}(p-1)$.

Partie III – Cas des $(\mathbb{Z}/2^n\mathbb{Z})^*$

On termine cette étude avec le cas $p = 2$.

1. On suppose $n \geqslant 3$. On note $G = (\mathbb{Z}/2^n\mathbb{Z})^*$, H l'ensemble des classes modulo 2^n des entiers k congrus à 1 modulo 4, et et $K = (\{-1, +1\}, \times)$.
   (a) Montrer que H est un sous-groupe de G. Quel est son ordre ?
   (b) Exhiber un isomorphisme de $H \times K \longrightarrow G$
   (c) Montrer que $5^{2^{n-3}} \equiv 1 + 2^{n-1}\ [2^n]$, et en déduire que l'ordre de 5 dans H est 2^{n-2}.
   (d) En déduire que le groupe multiplicatif G est isomorphe au groupe additif $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-2}\mathbb{Z})$. Est-il cyclique ?

2. Décrire les groupes $(\mathbb{Z}/2^n\mathbb{Z})^*$ pour $n \in \{1, 2\}$.

Partie IV – Nombres de Carmichael et indicateur de Carmichael

On appelle nombre de Carmichael un nombre composé n tel que pour tout entier a premier avec n, on ait $a^{n-1} \equiv 1\ [n]$. On rappelle que l'exposant d'un groupe abélien fini G est le ppcm de l'ordre de tous les éléments du groupe G, et que la question III-2 permet de justifer l'existence d'un élément $x \in G$ dont l'ordre est égal à l'exposant de G. On définit l'indicateur $\lambda(n)$ de Carmichael d'un entier $n > 1$ comme étant égal à l'exposant de $((\mathbb{Z}/n\mathbb{Z})^*, \times)$. On rappelle enfin que pour tout $n \geqslant 1$, $\varphi(n)$ est le nombre d'entiers premiers avec n dans $[\![1, n]\!]$.

1. Justifier que pour tout $n \geqslant 2$, $\lambda(n)$ divise $\varphi(n)$, avec égalité si et seulement si $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique.
2. Justifier que n est un nombre de Carmichael si et seulement si $\lambda(n)$ divise strictement $n - 1$.
3. Montrer que pour tout $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ avec $\alpha_i \geqslant 1$ et $k \geqslant 1$, on a
$$\lambda(n) = \lambda(p_1^{\alpha_1}) \vee \lambda(p_2^{\alpha_2}) \vee \cdots \vee \lambda(p_k^{\alpha_k}).$$
4. En déduire une expression explicite de $\lambda(n)$ en fonction des facteurs premiers de n, en distinguant suivant que 8 divise n ou non (on ne cherchera pas à expliciter les ppcm intervenant dans cette formule)
5. À l'aide des questions précédentes, montrer que n est un nombre de Carmichael si et seulement si n est composé, sans facteur multiple (*i.e.* $v_p(n) = 0$ ou 1 pour tout p premier), et pour tout facteur premier p de n, $p - 1$ divise $n - 1$.
6. Montrer que 561 est un nombre de Carmichael.
7. Montrer que n est de Carmichael si et seulement si n est composé, et pour tout $a \in \mathbb{Z}$, $a^n \equiv a[n]$.