L3 Algèbre effective - cours-TD

septembre 2019

Ordre d'un élément d'un groupe, groupe cyclique, l'anneau $\mathbb{Z}/n\mathbb{Z}$

On note $\#E$ le cardinal d'un ensemble E, $< g_1, g_2, \dots >$ le sous-groupe d'un groupe G engendré par les éléments $g_1, g_2, \dots$ de G, $\varphi(n)$ le nombre de générateurs du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ ($n > 0$), $m \wedge n$ le pgcd de deux entiers m, n et x $[n]$ la classe d'un entier x modulo un entier n.

On appelle ordre d'un élément g d'un groupe G le cardinal du sous-groupe engendré par g.

On utilise sans cesse le :

Thm de Lagrange : Soient G un groupe fini et H un sous-groupe de G ; alors le cardinal de H divise le cardinal de G

1. Montrer que tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$

(considérer le plus petit élément strictement positif du sous-groupe s'il existe.)

2. Soient k, n deux entiers. Montrer l'équivalence entre :

k est premier avec n

k est inversible pour la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ (le cas $n = 1$ est litigieux)

k engendre $\mathbb{Z}/n\mathbb{Z}$

3. Observer $1 \leq \varphi(n) \leq n-1$ si $n \geq 2$; $\varphi(n) = n-1$ ssi n est premier.

$\varphi(p^k) = p^{k-1}(p-1)$ si p est un nombre premier (déterminer le nombre d'éléments non premier avec p parmi $\{0, \dots, p^k - 1\}$).

$\varphi(pq) = \varphi(p)\varphi(q)$ si p, q sont des nombres premiers (déterminer l'ensemble des éléments non premier avec p ou q parmi ${0,\ldots,pq-1}).

Pouvez vous donner une minoration améliorée de $\varphi(n)$?

4. soient m, n deux entiers premiers entre eux. Montrer que l'homomorphisme $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/mn\mathbb{Z}$, $(x, y) \mapsto nx + my$ est bijectif. Montrer que $nx + my$ est premier avec m et n ssi x est premier avec m et y est premier avec n. En déduire $\varphi(mn) = \varphi(m)\varphi(n)$.

5. On fixe un entier $n > 0$.

Soit $d > 0$ divisant n. Montrer que les éléments de $\mathbb{Z}/n\mathbb{Z}$ d'ordre divisant d dont les éléments du sous-groupe $< \frac{n}{d} >$. Il y a d tels éléments dont $\varphi(d)$ d'ordre exactement d.

En partitionnant $\mathbb{Z}/n\mathbb{Z}$ suivant l'ordre de ses éléments on obtient $n = \sum_{d|n} \varphi(d)$.

Soit ψ une fonction définie sur l'ensemble des diviseurs de n à valeurs dans $\mathbb{N}$ vérifiant $\psi(d) \leq \varphi(d)$ pour tout diviseur d de n et $n = \sum_{d|n} \psi(d)$; alors $\psi(d) = \varphi(d)$ pour tout $d \mid n$, en particulier $\psi(n) > 0$.

Application : soit G un sous-groupe de $\mathbb{Z}/m\mathbb{Z}$ de cardinal n (forcément $n \mid m$!). Pour chaque $d \mid n$ on définit $\psi(d)$ comme le nombre d'éléments de G d'ordre d, alors $\psi(d) \leq \varphi(d)$ puis $\psi(n) > 0$, autrement dit G est cyclique.

Rq : on peut aussi prouver que G est cyclique en considérant l'image réciproque de G par la réduction modulo m :
$\mathbb{Z} \to$\mathbb{Z}/m\mathbb{Z}$.

6. Soient G un groupe, g, g' deux éléments de G d'ordre fini n et n'. On suppose $gg' = g'g$ alors :

Si n et n' sont premiers entre eux alors $< gg' > = < g, g' >$ et est d'ordre nn'.

Sans hypothèse sur n, n', l'ordre maximal d'un élément de $< g, g' >$ est $n \vee n'$ atteint par $g^{n/m} g'^{n'/m'}$ où m, m' sont tels que $m \mid n, m' \mid n', m \wedge m' = 1, mm' = n \vee n'$. L'inclusion $< gg' > \subset < g, g' >$ peut être stricte ou pas.

Application : Soit G un groupe commutatif fini. On suppose que pour tout entier $n \mid \#G$ le nombre d'éléments de G d'ordre divisant n est majoré par n ; alors G est cyclique.

7. Soient A un anneau commutatif intègre, P un polynôme à coefficients dans A et $a_1, \ldots, a_n$ n racines distinctes de P. Montrer que $(X - a_1) \cdots (X - a_n)$ divise P et donc $n \leq \deg(P)$. Que se passe t-il si A n'est pas supposé intègre ?

Soit G un sous groupe fini du groupe $A^\times$ des éléments inversibles de A pour la multiplication. Montrer, sous l'hypothèse A intègre, que G est cyclique.

(Observer que pour tout entier n il y a au plus n éléments de A d'ordre divisant n car de tels éléments sont racines de $X^n - 1$ puis utiliser l'exercice 6.)

8. Soient m, n deux entiers premiers entre eux. Montrer que l'application $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $x \mapsto (x[m], x[n])$ est un isomorphisme d'anneau et qu'elle induit un isomorphisme entre les groupes multiplicatifs $\left(\mathbb{Z}/mn\mathbb{Z}\right)^\times$ et $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$.

Pouvez vous exprimer l'isomorphisme d'anneaux réciproque ?

9. Soit p un nombre premier > 2 et $k > 0$ un entier. Montrer qu'il existe un élément $y \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$ d'ordre $p - 1$. (Observer que la réduction modulo p de y doit être d'ordre $p - 1$ dans $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$; la réciproque n'est pas tout à fait vrai.)

Montrer par récurrence sur n que pour tout entier λ premier à p on a $(1 + \lambda p)^{p^n} = 1 + \mu p^{n+1}$ avec μ premier à p. Que se passe t-il si $p = 2$? Quel est l'ordre de $1 + \lambda p$ dans $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$ ($p > 2$) ?

En déduire que $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$ est cyclique.

Cas $p = 2$: Montrer que l'homomorphisme $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z} \to \left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times$, $(1, 0) \mapsto -1$, $(0, 1) \mapsto 5$ est bijectif.

Pour quels n a t-on $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ cyclique ?