Université Paris-Sud 2016-2017
L2/S4 M204 Mathématiques : Algèbre

Feuille d'exercices n°3

Exercice 1
Soient a et b deux entiers.

a) Supposons que a et b soient premiers entre eux. Calculer leur ppcm.

b) On ne suppose plus maintenant que a et b sont premiers entre eux. Calculer le produit PGCD(a,b)PPCM(a,b).

Exercice 2
a) Montrer que dans le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, l'ordre d'une classe $\bar{a}$ est égal à $\dfrac{n}{n \wedge a}$.
b) Montrer que deux classes $\bar{a}$ et $\bar{b}$ engendrent le même sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $n \wedge a = n \wedge b$.
c) En déduire que si p est un nombre premier, les seuls sous-groupes de $\mathbb{Z}/p\mathbb{Z}$ sont $\{\bar{0}\}$ et $\mathbb{Z}/p\mathbb{Z}$.

Exercice 3 *a*) Déterminer les générateurs du groupe multiplicatif $(\mathbb{Z}/13\mathbb{Z})^\times$. Donner une représentation du treillis de ses sous-groupes.

b) Même question pour le groupe additif $\mathbb{Z}/12\mathbb{Z}$.

c) Comparer les deux treillis obtenus.

Exercice 4
Montrer qu'un groupe fini de cardinal un nombre premier est nécessairement cyclique et que tout élément différent de l'élément neutre en est un générateur.

Exercice 5
Parmi les groupes suivants, déterminer (en justifiant à chaque fois) ceux qui sont cycliques.

1. Le groupe $(\mathbb{Z}/7\mathbb{Z})^\times$ des éléments inversibles de $\mathbb{Z}/7\mathbb{Z}$.
2. Le groupe $(\mathbb{Z}/8\mathbb{Z})^\times$ des éléments inversibles de $\mathbb{Z}/8\mathbb{Z}$.
3. Le groupe des racines complexes du polynôme $X^n - 1$ avec $n \geq 1$.
4. Le groupe multiplicatif des matrices de la forme $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ avec $a \in \mathbb{Z}/n\mathbb{Z}$.

Exercice 6
On considère le groupe additif $G := \mathbb{Z}/12\mathbb{Z}$.

1. Déterminer les générateurs de G. Combien y-en-a-t-il?
2. Calculer l'ordre des éléments suivants dans G : $\bar{3}$, $\bar{5}$, $\bar{6}$, $\bar{9}$.

Exercice 7
Soit G un groupe d'ordre 4.

a) Montrer que si G contient un élément d'ordre 4, alors il est cyclique et isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

b) Montrer que si G ne contient aucun élément d'ordre 4, alors il est abélien et isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 8
Pour tout entier $n \geq 1$, on note U_n le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

a) Montrer que les groupes U_2, U_4 et U_5 sont cycliques.

b) Calculer l'ordre du groupe U_{25}. Montrer qu'il est cyclique et déterminer ses générateurs. Déterminer ensuite les générateurs de chacun de ses sous-groupes, donner la liste des dits sous-groupes et en dessiner le treillis.

c) Calculer l'ordre du groupe U_{28}. Montrer que ce n'est pas un groupe cyclique et calculer son exposant.

Exercice 9
Soient G et H deux groupes cycliques d'ordres respectifs m et n. Montrer que le groupe produit $G \times H$ est cyclique si et seulement si m et n sont premiers entre eux. Dans ce cas, exhiber un générateur possible.

Exercice 10 *a*) Soient G, H deux groupes et $f : G \to H$ un homomorphisme de groupes. Montrer que si $x \in G$ est un élément de G d'ordre fini n, alors $f(x)$ est un élément de H d'ordre fini divisant n.

b) Déterminer tous les homomorphismes de groupes $G \to H$ lorsque :

i) $G = \mathbb{Z}/7\mathbb{Z}$ et $H = \mathbb{Z}/13\mathbb{Z}$;
ii) $G = \mathbb{Z}/3\mathbb{Z}$ et $H = \mathbb{Z}/12\mathbb{Z}$;
iii) $G = H = \mathbb{Z}/6\mathbb{Z}$.

Exercice 11
Soient G un groupe monogène et a, b deux générateurs de G.

a) Montrer qu'il existe un unique automorphisme de groupes f de G tel que $f(a) = b$.

b) Montrer que si f est un automorphisme de groupes de G, alors $f(a)$ est encore un générateur de G.

c) Déterminer l'ensemble $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ des automorphismes du groupe $\mathbb{Z}/n\mathbb{Z}$. Montrer que c'est un groupe pour la composition des applications, puis qu'il est isomorphe au groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$.

Exercice 12
On considère la fonction d'Euler ϕ (on rappelle que $\phi(n)$ désigne le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$).

a) Rappeler pourquoi $\phi(nm) = \phi(n)\phi(m)$ lorsque n et m sont deux entiers premiers entre eux.

b) Calculer $\phi(462)$, $\phi(105)$, $\phi(60)$, $\phi(25)$, $\phi(27)$.

c) Calculer le reste de la division euclidienne de 5^{2042} par 462; de 7^{3333} par 60.

Exercice 13

1. Calculer le reste de la division euclidienne de $X^{21} + X^{19} + X^{17}$ par $X^2 - 1$.
2. Calculer le reste de la division euclidienne de $X^{45} - X^{43} + 1$ par $X^2 - 2X + 1$.
3. Calculer le reste de la division euclidienne de $X^{96} - X^{23}$ par $X^2 + 1$.

Exercice 14
Soient $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \in M_2(\mathbb{R})$. Vérifier que $A^2 + A + I = 0$, et en déduire rapidement A^n, pour tout $n \in \mathbb{N}$.

Exercice 15

1. Montrer que l'ensemble des matrices $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ avec $a, b \in \mathbb{R}$ est un anneau.
2. Montrer que l'ensemble des matrices $\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$ avec $a, b, c, d \in \mathbb{R}$ est un anneau.

Exercice 16
Soit A un anneau, on note N l'ensemble des $a \in A$ tels qu'il existe $n \geq 1$, $a^n = 0$ (éléments nilpotents).

1. Démontrer que si $a, b \in N$, alors $a+b \in N$ (et même, $a^p = 0$, $b^q = 0$, alors $(a+b)^{p+q-1} = 0$). Démontrer que si $a \in N$ et $b \in A$, alors $ab \in N$
2. Si $a \in N$, alors $1 + a$ est inversible dans A.
3. Si a est inversible et $b \in N$, alors $a + b$ est inversible

* Si $P(x) \in A[X]$ est nilpotent, démontrer par récurrence descendante sur le degré que tous les coefficients de $P(x)$ sont nilpotents.

* Inversibles de $A[X]$:

(1) si le terme constant est inversible et les autres coefficients nilpotents, alors le polynôme est inversible.

(2) Réciproque ?