Université Paris Diderot — MI4– Année 2014/15
Département de Sciences Exactes — L2 MI4

Feuille d'exercices n°2

GROUPES.

Rappel : l'ordre d'un élément x dans un groupe G est le plus petit entier $d \geq 1$ tel que $x^d = e$ (c'est-à-dire que $x^d = e$ et, si $x^{d'} = e$ alors d divise d').

Exercice 1 [calcul dans les groupes] Soit G un groupe, $a, b \in G$, et $n \in \mathbb{Z}$. Montrer que :

1. $(aba^{-1})^n = ab^n a^{-1}$.
2. $(ab)^{-1} = b^{-1}a^{-1}$.
3. Si $(ab)^n = e$, alors $(ba)^n = e$.
4. Si $ab = ba$, alors $(ab)^n = a^n b^n$. Donner un contre-exemple si $ab \neq ba$.
5. Si $a^{-1}ba = b^{-1}$ et $b^{-1}ab = a^{-1}$, alors $a^2 = b^2$ et $a^4 = b^4 = e$.

Exercice 2 Déterminer toutes les sous-groupes non-triviaux de $\mathbb{Z}$. Montrer que ils sont de la forme $H_m = \{n \in \mathbb{Z} | m \text{ divise } n\}$ avec $m \in \mathbb{N}^*$.

Exercice 3 Soit G un groupe tel que $x^2 = e$ pour tout $x \in G$. Montrer que G est commutatif.

Exercice 4 Soit G un groupe commutatif. On suppose que pour tout $g \in G$ il existe un nombre impair n tel que $g^n = e$. Montrer que l'application $g \mapsto g^2$ est une bijection de G dans lui-même.

Plus généralement si p premier ne divise pas le cardinal de G, montrer que l'application $g \mapsto g^p$ est une bijection de G dans lui-même.

Exercice 5 Soit G un groupe, et soit $a, b \in G$.

1. Montrer que l'ordre de a et l'ordre de a^{-1} sont égaux.
2. Montrer que l'ordre de a et bab^{-1} sont égaux
3. Montrer que l'ordre de ab et l'ordre de ba sont égaux.
4. * On suppose que m l'ordre de a et n l'ordre de b sont premiers entre eux. Si G est commutatif, alors l'ordre de ab est égal à mn.
5. Montrer sur un exemple que la conclusion précédente peut être fausse dans un groupe non commutatif. (Indication : $(123), (12) \in S_6$)

Exercice 6 Soit G un groupe.

1. Quels sont les éléments de G d'ordre 1 ?
2. Soit x un élément de G d'ordre rs avec $r, s \geq 1$. Quel est l'ordre de x^r ?
3. Soit x un élément de G d'ordre n. Soit r un entier strictement positif premier à n, montrer que x^r est d'ordre n.

4. Généralement, soit x un élément de G d'ordre n. Quel est l'ordre de x^r, pour $r \geq 1$?

CONGRUENCES, $\mathbb{Z}/n\mathbb{Z}$

Exercice 7 [générateur de $(\mathbb{Z}/17\mathbb{Z})^*$] Déterminer l'ordre de 2 dans $(\mathbb{Z}/17\mathbb{Z})^*$. Montrer que $(\mathbb{Z}/17\mathbb{Z})^*$ est cyclique, c'est-à-dire qu'il existe $a \in (\mathbb{Z}/17\mathbb{Z})^*$ tel que $\langle a \rangle = (\mathbb{Z}/17\mathbb{Z})^*$. [Indication : on pourra chercher a tel que $a^2 = 2$.]

Il sera vu en cours que $(\mathbb{Z}/p\mathbb{Z})^*$ est toujours cyclique si p est premier.

Exercice 8 Soit n un entier naturel. Montrer que :

1. $2^{3n+5} + 3^{n+1}$ est multiple de 5 mais pas de 10.
2. $3n^5 + 5n^3 + 7n$ est multiple de 15.
3. $n^5 - n$ est multiple de 30.

Exercice 9 [calcul de puissances]

1. Quel est le dernier chiffre de 7777^{7777} ? de 2013^{2013} ?
2. Quels sont les restes des divisions euclidiennes de 900^{2000} et de $101^{102^{103}}$ par 7 ?
3. Quel est le reste de la division euclidienne de $31^{32^{33}}$ par 11 ?

Exercice 10 [diviseurs premiers des nombres de Fermat] Soit $n \in \mathbb{N}$ et $F_n = 2^{2^n}+1$ le n-ieme nombre de Fermat. Soit p un diviseur premier de F_n. Remarquer $2^{2^n} = -1 \mod p$, puis montrer que l'ordre de 2 dans $(\mathbb{Z}/p\mathbb{Z})^*$ est 2^{n+1}. En déduire qu'il existe $k \in \mathbb{N}$ tel que $p = 2^{n+1}k + 1$. Trouver un diviseur de $F_5 = 4\,294\,967\,297$. *Ce fut la démarche d'Euler pour réfuter la conjecture de Fermat, selon laquelle tous les nombres F_n sont premiers.*

Exercice 11 Soit $n > 1$ un entier tel que $2^n = 1 \mod n$. Soit p le plus petit diviseur premier de n.

1. Montrer que $p > 2$.
2. Soit r l'ordre de 2 dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$. Montrer que $r > 1$ et que r divise n et $p - 1$.
3. Conclure qu'il n'existe pas de $n > 1$ tel que $2^n = 1 \mod n$.

Rappel : Équations modulaires linéaires

Soit $n \geq 1$ un entier naturel, et soit $a, b \in \mathbb{Z}/n\mathbb{Z}$. On considère l'équation suivante dans $\mathbb{Z}/n\mathbb{Z}$:

$$ax = b, \quad x \in \mathbb{Z}/n\mathbb{Z}. \tag{1}$$

1. *Soit $d = \text{pgcd}(a, n)$. Alors l'équation (1) admet des solutions si et seulement si $d|b$.*

2. *Soit $u, v \in \mathbb{Z}$ des coefficients de Bézout tels que $au + nv = d$ dans $\mathbb{Z}$. On pose*
$$x_0 = u\frac{b}{d} \mod n.$$
Alors x_0 est solution de l'équation (1).
3. *Soit $x \in \mathbb{Z}/n\mathbb{Z}$ une solution de l'équation (1). Alors x est de la forme :*
$$x_i = x_0 + i\frac{n}{d}, \quad i \in \mathbb{Z}.$$
4. *Donc toutes les solutions de l'équation (1) sont les $x_0, \ldots, x_{d-1}$, et qu'ils sont au nombre de d.*

Exercice 12 Résoudre les équations $6x = 10 \mod 16$ et $7x = 4 \mod 30$.

Exercice 13 [inverses dans $\mathbb{Z}/n\mathbb{Z}$] Rappeler à quelle condition un élément a est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Donner une procédure utilisant l'algorithme d'Euclide-Bézout pour calculer l'inverse d'un élément.

Exercice 14 [Théorème de Wilson] Soit $p > 2$ un nombre premier.

1. Montrer que -1 est le seul élément d'ordre 2 de $(\mathbb{Z}/p\mathbb{Z})^*$.
2. Montrer que $(p-1)! = -1 \mod p$. *Indication :* on pourra regrouper x et x^{-1} dans le produit des x pour $x \in (\mathbb{Z}/p\mathbb{Z})^*$.
3. Que dire de la réciproque : si $(n-1)! = -1 \mod n$, peut-on en conclure que n est premier ?

Exercice 15 Résoudre les sytèmes de congruences :

$$(a) \begin{cases} x = 3 \mod 37 \\ x = 4 \mod 52 \end{cases} \qquad (b) \begin{cases} x = 21 \mod 12 \\ x = 12 \mod 21 \end{cases}$$

Exercice 16 Résoudre les équations :

1. $x^2 + 4x - 1 = 0$ dans $\mathbb{Z}/11\mathbb{Z}$.
2. $x^2 + 7x + 3 = 0$ dans $\mathbb{Z}/11\mathbb{Z}$.
3. $x^2 + 4x - 13 = 0$ dans $\mathbb{Z}/21\mathbb{Z}$.
4. $x^2 + 2x + 6 = 0$ dans $\mathbb{Z}/9\mathbb{Z}$.
5. $2x^2 + 3x + 1 = 0$ dans $\mathbb{Z}/5\mathbb{Z}$.
6. $3x^2 + 4x - 18 = 0$ dans $\mathbb{Z}/77\mathbb{Z}$.