Anneaux et Arithmétique - Feuille 1
L3, semestre 2 (2012-2013)
Université Rennes I

Un peu de théorie des groupes.

Exercice 1.

Soient G_1, G_2 deux groupes, $x \in G_1$ d'ordre fini, $\phi : G_1 \to G_2$ un morphisme de groupes. Montrez que l'ordre de $\phi(x)$ divise celui de x.

Exercice 2.

1) Montrez que $\{(x, y) : x + y = 0 \bmod 2\}$ est un sous-groupe distingué de $\mathbb{Z} \times \mathbb{Z}$ qui n'est pas le produit de deux sous-groupes de $\mathbb{Z}$.
2) Soient G_1, G_2 deux groupes simples non abéliens. Montrez que le produit $G_1 \times G_2$ possède exactement 4 sous-groupes distingués, et dire lesquels.
Indication : on pourra considérer les images et les noyaux des morphismes de projection $p_i : G_1 \times G_2 \to G_i$ et distinguer chaque cas.

Exercice 3.

Soit p un nombre premier, tel qu'il existe un entier $k \geq 1$ tel que $p = 2^k + 1$. Un tel nombre premier est dit *de Fermat*, et les seuls connus sont $p = 3, 5, 17, 257, 65537$. Le but de l'exercice est de démontrer que pour un tel nombre premier de Fermat, k est nécessairement une puissance de 2, c'est à dire qu'en fait $p = 2^{2^n} + 1$ pour un certain $n \geq 0$.

Nos hypothèses sont donc : Soit $k \geq 1$ un nombre entier, tel que $p = 2^k + 1$ est premier.
1. Montrez que l'ordre de $\overline{2}$ dans le groupe multiplicatif $G = (\mathbb{Z}/p\mathbb{Z})^*$ est nécessairement $> k$.
2. Montrez que l'ordre de $\overline{2}$ divise $2k$.
3. Déduisez-en que $\overline{2}$ est d'ordre $2k$.
4. Quel est le cardinal de G ? Déduisez-en que k est une puissance de 2.

Exercice 4.

Soit G un groupe commutatif fini. On s'intéresse au produit

$$\pi = \prod_{g \in G} g.$$

Soit H l'ensemble constitué des éléments de G d'ordre 2 ainsi que du neutre e.
1. Montrez que H est un sous-groupe de G.
2. Montrez que le cardinal de H est nécessairement une puissance de 2.
3. Montrez que

$$\pi = \prod_{g \in H} g,$$

et que si G contient un seul élément s d'ordre 2, alors $\pi = s$.
4. On considère le groupe $G = (\mathbb{Z}/p\mathbb{Z})^*$, où p est un nombre premier. Montrez que -1 est le seul élément d'ordre 2 dans G.
5. Démontrez le *Théorème de Wilson* :
Si p est premier alors $(p-1)! \equiv -1 \mod p$.
6. Soit $n \geq 5$ un entier, montrez que si n n'est pas premier, $(n-1)! \equiv 0 \mod n$. En déduire la réciproque du théorème de Wilson.

Anneaux.

Exercice 5.

Soit $A = C^0([0;1])$ l'ensemble des fonctions continues de $[0,1]$ dans $\mathbb{R}$, muni de l'addition et de la multiplication ponctuelle de fonctions.
a) Montrez que A est un anneau (unitaire).
b) L'anneau A est-il intègre ?
c) Déterminez l'ensemble des éléments nilpotents (càd les $x \in A$ tels que $x^n = 0$ pour un certain $n > 0$)
d) Déterminez l'ensemble des éléments idempotents (càd les $x \in A$ tels que $x^2 = x$)
e) Déterminez l'ensemble des éléments inversibles.
f) Déterminez l'ensemble des diviseurs de zéro.

Exercice 6.

Soit $d > 1$ un entier sans facteurs carrés. On pose

$$\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} \, : \, x, y \in \mathbb{Z}^2\}.$$

1) Montrez que $\mathbb{Z}[\sqrt{d}]$ est un anneau (unitaire), et qu'il est intègre.
2) Montrez que l'écriture $x + y\sqrt{d}$ est unique.
3) Montrez que l'application $\sigma : x + y\sqrt{d} \mapsto x - y\sqrt{d}$ est un automorphisme d'anneau.
4) Montrez que l'ensemble des inversibles est l'ensemble des α tels que

$$|\sigma(\alpha)\alpha| = 1.$$

Donnez un exemple d'inversible d'ordre infini pour $d = 2$.
5) Montrez que si $d \neq d'$, tous deux des nombres entiers sans facteurs carrés, il n'existe pas de morphisme d'anneau de $\mathbb{Z}[\sqrt{d}]$ dans $\mathbb{Z}[\sqrt{d'}]$. (Indication : considérer l'image de $\sqrt{d}$).

Exercice 7. Soit A un anneau unitaire, non nécessairement commutatif. On note $End(A, +)$ l'ensemble des endomorphismes du *groupe* $(A, +)$, muni de l'opération d'addition et de la composition.
a) Montrer que $(End(A, +), +, \circ)$ est un anneau unitaire, non nécessairement commutatif.
b) Si $a \in A$, on pose

$$f_a : A \to A,$$
$$x \mapsto ax,$$

et

$$f : A \to End(A, +),$$
$$a \mapsto f_a.$$

Montrer que f est bien définie, que f est un morphisme unitaire d'anneaux, et que f est injective.
c) Montrer que si $A = \mathbb{Z}$ ou bien $A = \mathbb{Z}/n\mathbb{Z}$, alors f est surjective.
d) Trouver un exemple où A est commutatif, mais pas $End(A, +)$.