Groupes, anneaux et arithmétique

Préparation à l'agrégation interne année 2008-09

Séance du mardi 15 septembre

Exercices à chercher en priorité : 1.1 ; 1.2 ; 2.4 ; 2.5 ; 3.3 ; 3.4 ; 3.5 ; 3.6

1 Généralités sur les anneaux

Exercice 1.1 (Corps des fractions d'un anneau)
Soit A un anneau commutatif intègre. Soit S une partie multiplicative de A (c'est-à-dire : $1 \in S$, $0 \notin S$ et si $x, y \in S$ alors $xy \in S$).

1. Démontrer que la relation $\mathcal{R}$ définie ci-dessous sur $A \times S$ est une relation d'équivalence :
$$(a, s)\mathcal{R}(a', s') \iff as' - a's = 0.$$
2. On note $S^{-1}A$ l'ensemble des classes d'équivalences de $\mathcal{R}$ et $\frac{a}{s}$ la classe d'équivalence d'un élément (a, s) de $A \times S$.
   (a) Démontrer que $S^{-1}A$ est un anneau commutatif intègre et qu'il existe un homomorphisme injectif (d'anneaux)noté π de A dans $S^{-1}A$ (On identifie alors$A$ à $\pi(A)$).
   (b) Démontrer qu'il vérifie la propriété (dite universelle) suivante : Si B est un anneau, $\phi \in Hom(A; B)$ et si $\phi(S) \subset B^*$ alors il existe $\overline{\phi} \in Hom(S^{-1}A; B)$ tel que $\overline{\phi} \circ \pi = \phi$.
3. Exemples :
   (a) Si $S = A \setminus \{0\}$ vérifier que $S^{-1}A$ est un corps et qu'on l'appelle corps des fractions de A et on le note $Frac(A)$.
   (b) Si $A = \mathbb{Z}$ et si $S = \{10^k / k \in \mathbb{N}\}$, qui est $S^{-1}A$?

Exercice 1.2
Démontrer que les anneaux $\mathbb{Z}[X]/(3, X)$ et $\mathbb{Z}/3\mathbb{Z}$ sont isomorphes.

Exercice 1.3
Soit A un anneau commutatif.

1. On dit qu'un élément x de A est nilpotent s'il un entier $n > 0$ tel que $x^n = 0$. Démontrer que l'ensemble N des éléments nilpotents de A est un idéal de A.
2. Un élément u de A est dit unipotent s'il existe un élément nilpotent x de A tel que $u = 1 + x$
   (a) Démontrer que tout élément unipotent est inversible et que le produit de deux unipotents est unipotent.
   (b) On suppose que A contient $\mathbb{Q}$ comme sous-anneau.
      i. Soit $x \in N$, pourquoi peut-on définir $\exp(x) = 1 + \frac{x}{1} + ... + \frac{x^n}{n!} + ...$?
      ii. Pour u unipotent, on définit $\ln(u)$ par la formule usuelle. Démontrer que exp et ln sont des isomorphismes réciproques entre le groupe additif N et le groupe multiplicatif U des unipotents de A.

2 Anneaux principaux

Dans tout cette partie, A désigne un anneau commutatif et principal (c'est-à-dire A est commutatif intègre et tout idéal de A est engendré par un élément).// Pour aborder cette partie, il faut revoir les notions d'idéal principal, idéal premier, idéal maximal et surtout la notion d'élément irréductible.
Les deux premiers exercices sont à chercher avec un livre "à portée de main".

Exercice 2.1 (cet exercice ne sera pas corrigé durant la séance)
Démontrer que les propriétés suivantes sont équivalentes :

1. a est irréductible
2. l'idéal $< a >$ est premier.
3. l'idéal $< a >$ est maximal (pour l'inclusion).

Exercice 2.2 (cet exercice ne sera pas corrigé durant la séance)

1. Soit $a, b, c \in A$; on suppose que a est irréductible et que a divise bc, démontrer que a divise b ou c
2. Démontrer que dans un anneau principal toute suite croissante d'idéaux est stationnaire.
3. Si a est un élément non nul et non inversible de A, démontrer qu'il existe u inversible et des éléments irréductibles $\alpha_1, \alpha_2, ..., \alpha_r$ $(r \geq)$ tels que :

$$a = u\alpha_1 ... \alpha_r$$

et de plus r et $\alpha_1, \alpha_2, ..., \alpha_r$ sont uniquement déterminés (à l'ordre près).

Exercice 2.3 (Sous-corps premier d'un corps)

1. Soit n un entier naturel ; Démontrer que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
2. Soit $\mathbb{K}$ un corps commutatif, on définit l'homomorphisme (d'anneaux) ϕ de $\mathbb{Z}$ dans $\mathbb{K}$ en posant :
$$\phi(1) = 1;\ \phi(n) = n.1;\ \phi(-n) = n.(-1)\ \forall n \in \mathbb{N}^*.$$
   (a) Déterminer le noyau de ϕ.
   (b) En déduire que $\mathbb{K}$ contient un plus petit sous-corps.
3. Démontrer que si $\mathbb{K}$ est un corps fini alors son cardinal est de la forme p^n où p est un nombre premier et n un entier naturel non nul.

Exercice 2.4 (Résolution de l'équation (E) : $x^2 + 2 = y^3$)
Partie A : Etude de l'anneau $\mathbb{Z}[i\sqrt{2}]$
On pose $\mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2}/(a, b) \in \mathbb{Z}^2\}$, et pour tout nombre complexe z, $N(z) = z \times \overline{z}$.

1. Vérifier que $\mathbb{Z}[i\sqrt{2}]$ est un sous-anneau de $\mathbb{C}$,que pour tout $z \in \mathbb{Z}[i\sqrt{2}]$ $N(z)$ est entier et enfin que pour tout $(z_1, z_2) \in \mathbb{Z}[i\sqrt{2}]^2$, $N(z_1.z_2) = N(z_1)N(z_2)$ est entier.
2. (a) Démontrer qu'un élément z de $\mathbb{Z}[i\sqrt{2}]$ est inversible si et seulement si $N(z) = 1$.
   (b) Déterminer les éléments inversibles de $\mathbb{Z}[i\sqrt{2}]$.
   (c) L'objectif de cette question est de démontrer que $\mathbb{Z}[i\sqrt{2}]$ est principal.
      i. Démontrer que pour tout $z = x + i\sqrt{2}y$ avec $x, y \in \mathbb{Q}$ il existe γ appartenant $\mathbb{Z}[i\sqrt{2}]$ tel que $N(z - \gamma) < 1$.
      ii. En déduire que pour tous α et β appartenant à $\mathbb{Z}[i\sqrt{2}]$ il existe γ, δ appartenant à $\mathbb{Z}[i\sqrt{2}]$ tels que :
$$\alpha = \beta \times \gamma + \delta \text{ et } N(\delta) < N(\beta)$$
      iii. Démontrer que $\mathbb{Z}[i\sqrt{2}]$ est principal.
3. Démontrer que $i\sqrt{2}$ est irréductible.

Partie B : Résolution de (E) : $x^2 + 2 = y^3$
Soit (x, y) un couple d'entiers relatifs solutions de (E).

1. Démontrer que $x+i\sqrt{2}$ et $x-i\sqrt{2}$ sont premiers entre eux dans $\mathbb{Z}[i\sqrt{2}]$ (Raisonner par l'absurde en considérant un élement irréductible de $\mathbb{Z}[i\sqrt{2}]$ divisant les deux facteurs).
2. Démontrer que $x+i\sqrt{2}$ est le cube d'un élément de $\mathbb{Z}[i\sqrt{2}]$.
3. Résoudre (E).

Remarque : On pourra prolonger cet exercice en travaillant le sujet d'agrégation interne 2006 qui aborde notamment le théorème de Fermat-Wiles pour $n=3$ et $n=4$.

Exercice 2.5 (Anneau non principal)
On pose $\mathbb{Z}[i\sqrt{5}] = \{a+bi\sqrt{5}/(a,b)\in\mathbb{Z}^2\}$, et pour tout nombre complexe z, $N(z)=z.\overline{z}$. On admet que $\mathbb{Z}[i\sqrt{5}]$ est un sous-anneau de $\mathbb{C}$.

1. Démontrer qu'un élément x appartenant à $\mathbb{Z}[i\sqrt{5}]$ est inversible si et seulement si $N(x)=1$ puis déterminer les inversibles de $\mathbb{Z}[i\sqrt{5}]$.
2. Démontrer que $2, 3, 1-i\sqrt{5}, 1+i\sqrt{5}$ sont irréductibles dans $\mathbb{Z}[i\sqrt{5}]$. Qu'en déduit-on ?

3 Arithmétique dans $\mathbb{Z}$

Exercice 3.1 (Petit théorème de Fermat)
1. Soit p un nombre premier et a un entier relatif premier avec p, démontrer que : $a^{p-1}\equiv 1 \pmod p$.
2. Démontrer que pour tout entier relatif a premier avec 561, on a :

$$a^{560}\equiv 1 \pmod{561}.$$

Qu'en conclue-t-on ?

Exercice 3.2 (Nombres de Mersenne)
1. Démontrer que si a^n-1 est premier alors $a=2$ et n est premier. On appelle nombre de Mersenne les nombres $M_p = 2^p-1$ avec p premier.
2. Factorisation des nombres de Mersenne : on suppose p est un nombre premier impair soit q un diviseur premier de M_p.
   (a) Quel est l'ordre de $\overline{2}$ dans $\mathbb{Z}/q\mathbb{Z}$?
   (b) Démontrer que $q\equiv 1 \pmod{2p}$.
   (c) Les nombres M_{17}, M_{19} et M_{23} sont-ils premiers ?
3. Les nombres parfaits pairs : Un entier naturel est dit parfait s'il est somme de ses diviseurs autres que lui-même ; par exemple 6 est parfait car $1+2+3=6$.
   Démontrer qu'un entier pair $n>0$ est parfait si et seulement si il existe un nombre premier p tel que $n=2^{p-1}M_p$ et M_p est premier.

Exercice 3.3 (Résidus quadratiques et symbole de Legendre)
Soit p un nombre premier différent de 2. On pose $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$.

1. Etudier (noyau, image)l'homomorphisme qui à tout élément $\mathbb{F}_p^*$ associe son carré dans $\mathbb{F}_p^*$. En déduire le nombre de carré dans $\mathbb{F}_p^*$.
2. Démontrer que :
   (a) $a\in\mathbb{F}_p^*$ est un carré si et seulement si $a^{\frac{p-1}{2}}\equiv 1 \pmod p$.
   (b) $a\in\mathbb{F}_p^*$ n'est pas un carré si et seulement si $a^{\frac{p-1}{2}}\equiv -1 \pmod p$.
3. Démontrer que -1 est un carré si et seulement si $p\equiv 1 \pmod 4$.
4. Déterminer les carrés de $\mathbb{F}_{17}^*$
5. Soit n un entier. On dit que n est un résidu quadratique modulo p s'il existe un entier a tel que $n\equiv a^2 \pmod p$; de plus on pose :

$$\left(\frac{n}{p}\right) = \begin{cases} 0, & \text{si } n \text{ est divisible par } p\,; \\ 1, & \text{si } n \text{ n'est pas divisible par } p \text{ et est un résidu quadratique modulo } p\,; \\ -1, & \text{si } n \text{ n'est pas divisible par } p \text{ et n'est pas un résidu quadratique modulo } p\,; \end{cases}$$

   (a) Que vaut $\left(\frac{1}{p}\right)$ et $\left(\frac{-3}{17}\right)$?

(b) Démontrer que pour tous entiers n, n', $\left(\frac{nn'}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{n'}{p}\right)$

Remarque : On pourra prolonger cet exercice en travaillant le sujet d'agrégation interne 2000 qui aborde la loi de réciprocité quadratique.

L'objectif des exercices suivant est d'étudier la structure du groupe des inversibles de $\mathbb{Z}/n\,\mathbb{Z}$ (où $n \geq$), noté $(\mathbb{Z}/n\,\mathbb{Z})^*$.

Exercice 3.4 (fonction φ d'Euler)
Pour tout entier n supérieur ou égal à 2, on note $\varphi(n)$ le nombre d'entier q compris entre 1 et n premier avec n. On pose $\varphi(1) = 1$

1. Soient p un nombre premier et α un entier naturel. Démontrer que $\varphi(p^\alpha) = p^\alpha\left(1 - \frac{1}{p}\right)$.
2. **Démontrer que $\forall n \in \mathbb{N}^*$, $\varphi(n) = \#\left(\mathbb{Z}/n\mathbb{Z}\right)^*$. Qu'en déduit-on ?**
3. Démontrer que pour tous entiers m, n supérieurs ou égaux à 2 et premiers entre eux :
$$\varphi(m \times n) = \varphi(m) \times \varphi(n).$$
4. Exprimer $\varphi(n)$ en fonction de n.

Exercice 3.5
Soit G un groupe commutatif fini de cardinal $n \geq 1$. On appelle exposant de G le ppcm des ordres des éléments de G et on le note $\omega(G)$.

1. Montrer que $\omega(G)$ divise n.
2. Soit x, y deux éléments de G d'ordre respectivement p et q que l'on suppose premiers entre eux, démontrer que xy est d'ordre pq.
3. Soit x, y deux éléments de G d'ordre respectivement p et q, démontrer qu'il existe un élément d'ordre $ppcm(p, q)$.
4. En déduire qu'il existe un élément d'ordre $\omega(G)$.
5. *Application :* Soit p un nombre premier, on note s l'exposant du groupe $(\mathbb{Z}/p\,\mathbb{Z})^*$.
   (a) Démontrer que $(\mathbb{Z}/p\,\mathbb{Z})^*$ est d'ordre $p-1$. Démontrer que les éléments $(\mathbb{Z}/p\,\mathbb{Z})^*$ de sont racines de $X^s - 1$.
   (b) En déduire que $(\mathbb{Z}/p\,\mathbb{Z})^*$ est cyclique.

Exercice 3.6
1. Déterminer les générateurs de $(\mathbb{Z}/13\mathbb{Z})^*$.
2. Déterminer les générateurs de $(\mathbb{Z}/17\mathbb{Z})^*$.

Exercice 3.7
Soit p un nombre premier différent de 2 et α un entier supréieur ou égal à 1.

1. Démontrer que pour tout entier naturel k :
$$(p+1)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}}.$$
2. En déduire que $\overline{p+1}$ est d'ordre $p^{\alpha-1}$ $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^*$.
3. Démontrer que $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^*$ est cyclique.

Exercice 3.8
1. Décrire $(\mathbb{Z}/2\mathbb{Z})^*$ et $(\mathbb{Z}/4\mathbb{Z})^*$.
2. Soit α un entier supérieur ou égal à 3.
   (a) Démontrer que pour tout entier naturel k :
$$5^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}}$$
   (b) En déduire l'ordre de $\overline{5}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ et que $\overline{-1}$ n'apprtient pas au sous-groupe engendré par $\overline{5}$.
   (c) En déduire que $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est isomorphe à $\mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.