Licence de mathématiques L3 14 janvier 2010
Université Claude Bernard (Lyon 1)
Département de Mathématiques - U.F.R. Sciences et technologies

Algèbre et théorie des nombres - Corrigé Examen

I - Arithmétique (4 points)

La comète A qui est visible exactement tous les 26 ans a été observée il y a 4 ans. La comète B qui est visible exactement tous les 14 ans a été observée il y a 10 ans. Dans combiens d'années pourra-t-on observer simultanément les comètes A et B ?
Soit $n \in \mathbb{Z}$. Les comètes peuvent(ou ont pu) être observées simultanément dans n années (il y a $-n$ années) si et seulement si

$$\begin{cases} n & \equiv & -4 & \pmod{26} \\ n & \equiv & -10 & \pmod{14} \end{cases}$$

Par le théorème des restes chinois, la première équation est équivalente à

$$\begin{cases} n & \equiv & -4 \equiv 9 & \pmod{13} \\ n & \equiv & -4 \equiv 0 & \pmod{2} \end{cases}$$

et la seconde à

$$\begin{cases} n & \equiv & -10 \equiv 4 & \pmod{7} \\ n & \equiv & -10 \equiv 0 & \pmod{2} \end{cases}$$

Le système est donc équivalent à

$$\begin{cases} n & \equiv & 9 & \pmod{13} \\ n & \equiv & 4 & \pmod{7} \\ n & \equiv & 0 & \pmod{2} \end{cases}$$

En utilisant l'identité $7 \times 2 - 13 = 1$ et le théorème des restes chinois, il suit que le système des deux premères équations est équivalent à $n \equiv 9 \times 14 - 4 \times 13 \pmod{91}$, c'est-à-dire $n \equiv 74 \pmod{91}$. A nouveau à l'aide du théorème des restes chinois, le système de départ est équivalent à $n \equiv 74 \pmod{182}$.
Les comètes A et B pourront donc être (à nouveau) observées simultanément dans 74 ans.

II - Opération de groupe (12 points).

1. Soit G un groupe fini agissant sur un ensemble fini X. Soit n le nombre d'orbites.
   (a) Démontrer la formule de Burnside (à l'aide de la formule des classes) :

$$n = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

où $X^g = \{x \in X; g \cdot x = x\}$.
Soit

$$D = |\{(g, x) \in G \times X; g \cdot x = x\}|.$$

D'une part

$$|D| = \sum_{g \in G} |\{(g, x) G\times \in X; g \cdot x = x\}| = \sum_{g \in G} |X^g|.$$

D'autre part

$$|D| = \sum_{x \in X} |\{(g,x)G\times \in X; g \cdot x = x\}| = \sum_{x \in X} |\mathrm{Stab}_G(x)|.$$

On utilse la formule des classes $|\mathrm{Stab}_G(x)| = |G|/|\Omega(x)|$ *pour chaque* $x \in X$ *et on obtient,*
D'où

$$|D| = |G| \times \sum_{x \in X} \frac{1}{|\Omega(x)|} = |G| \times \sum_{i=1}^{n} \left(\sum_{x \in \Omega_i} \frac{1}{|\Omega(x)|} \right) = |G| \times n$$

où les Ω_i *sont les* n*-orbites.*

(b) Montrer que si g_1 et g_2 sont deux éléments conjugués de G alors

$$|X^{g_1}| = |X^{g_2}|.$$

Soit $h \in G$ *tel que* $g_2 = hg_1h^{-1}$*. Soit* $x \in X$*. Alors* $x \in X^{g_2}$ *si et seulement si* $g_2 \cdot x = x$ *si et seulement si* $hg_1h^{-1} \cdot x = x$ *ssi* $g_1h^{-1} \cdot x = h^{-1} \cdot x$ *si et seulement si* $h^{-1} \cdot x \in X^{g_1}$*. Par conséquent la multiplication par* h *définit une bijection de* X^{g_1} *sur* X^{g_2}*.*

2. Soit $\mathcal{P}$ un pentagone régulier $ABCDE$. On note G le groupe des isométries de ce pentagone et S l'ensemble $\{A, B, C, D, E\}$ des sommets de $\mathcal{P}$. Déterminer l'orbite de A sous l'action de G sur S. Déterminer le stabilisateur de A. En déduire l'ordre de G.
En utilisant la rotation de centre l'isobarycentre O *du pentagone régulier et d'angle* $2\pi/5$ *on passe d'un sommet à un autre sommet adjacent. Il suit que l'oribite d'un sommet est l'ensemble des sommets du pentagone. Une isométrie du pentagone régulier fixe* O *et donc si cette isométrie fixe de plus* A *elle fixe la droite* (OA)*. Le stabilisateur de* A *est donc constitué de l'identité et de la symétrie par rapport à la droite* (OA)*. Par la formule des classes, on a*

$$|G| = 5 \times 2 = 10.$$

3. Donner un ensemble de générateurs de G constitué de deux éléments. Expliciter un isomorphisme de G vers un sous-groupe de S_5.
La rotation r *d'angle* $2\pi/5$ *est d'ordre* 5*. La symétrie d'axe* (OA) *n'est pas engendré par* r*. Donc le sous-groupe de* G *engendré par* r *et* s *contient au moins* 6 *élements et comme son ordre divise* 10*, ce sous-groupe est tout* G*. Les éléments de* G *sont déterminés par leur action sur les sommets du pentagone et donc par les permutations de ceux-ci correspondant. On peut donc envoyer* r *sur le* 5*-cycle* (12345) *de* S_5 *et* s *sur la permtutation* (25)(34)*. On obtient ainsi un isomorphisme de* G *sur le sous-groupe de* S_5 *engendré par* (12345) *et* (25)(34)*.*

4. On se propose de colorier les côtés de $\mathcal{P}$ à l'aide de m couleurs. On considère que deux coloriages sont identiques s'il existe un élément de G qui envoie l'un sur l'autre. En utilisant la première question, montrer que le nombre de coloriages possibles est égal à

$$\frac{m^5 + 5m^3 + 4m}{10}.$$

On fait agir G *sur l'ensemble* X *des pentagones coloriés avec* m *couleurs et on utilise la formule de Burnside pour calculer le nombre d'orbites par cette action. Notons que* G *a trois classes de conjugaisons, la classe de l'identité qui a un seul élément, la classe de conjugaison de* r *qui contient les quatre rotations, et la classe de conjugaison de* s *qui contient les cinq symétries. On a alors* $|X^{id}| = m^5$*,* $|X^r| = m$ *et* $|X^s = m^3|$*. On en déduit que le nombre d'orbites est* $(m^5 + 4m + 5m^3)/10$*.*

III - Questions de cours (6 points)

1. Montrer qu'un anneau euclidien est principal.
   voir cours
2. Soit A un anneau. Montrer que $A[X]$ est principal si et seulement si A est un corps.
   voir cours
3. Donner un exemple d'anneau factoriel qui n'est pas principal.
   $\mathbb{Z}[X]$ *est factoriel car anneau de polynômes sur* $\mathbb{Z}$ *qui est factoriel (car principal). Par contre* $\mathbb{Z}[X]$ *n'est pas principal* $\mathbb{Z}$ *n'est pas un corps.*

IV - Polynômes(18 points)

Soient

$$P = X^4 + 5X^3 + 7X^2 + 3X + 5,$$
$$Q = X^4 + 7X^3 + 7X^2 + 5X + 7 \text{ et}$$
$$R = X^4 + 7X^3 + 7X^2 + 3X + 5$$

trois polynômes de $\mathbb{Z}[X]$.

1. Montrer que $X^2 + X + \bar{1}$ est l'unique polynôme irréductible de degré 2 de $\mathbb{Z}/2\mathbb{Z}[X]$.
   $X^2 + X + \bar{1}$ *est de degré* 2 *et n'a pas de racines dans* $\mathbb{Z}/2\mathbb{Z}$*, il est donc irréductible. Les autres polynômes de degré* 2 *sont* $X^2 + X$ *et* $X^2 + \bar{1}$ *qui ont tous deux une racine.*
2. Calculer $(X^2 + X + \bar{1})^2$ dans $\mathbb{Z}/2\mathbb{Z}[X]$.
   $(X^2 + X + \bar{1})^2 = (X^4 + X^2 + \bar{1})$.
3. En déduire que $X^4 + X^3 + X^2 + X + \bar{1}$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$.
   $X^4 + X^3 + X^2 + X + \bar{1}$ *n'a pas de racines dans* $\mathbb{Z}/2\mathbb{Z}$ *et est différent de* $(X^2 + X + \bar{1})^2$*. Or* $X^2 + X + \bar{1}$ *étant le seul polynôme irréductible de degré* 2 *de* $\mathbb{Z}/2\mathbb{Z}[X]$*, il suit qu'on ne peut factoriser* $X^4 + X^3 + X^2 + X + \bar{1}$*.*
4. Déduire de la question précédente que P, Q et R sont des polynômes irréductibles de $\mathbb{Q}[X]$.
   Les réductions modulo 2 *de ces trois polynômes valent* $X^4 + X^3 + X^2 + X + \bar{1}$ *qui est irréductibles dans* $\mathbb{Z}/2\mathbb{Z}[X]$*. Par le théorème de réduction modulo* 2*, on déduit que ces trois polynômes sont irréductibles dans* $\mathbb{Q}[X]$*.*

   Pour la suite, on note $\bar{P}$, $\bar{Q}$ et $\bar{R}$ les polynômes de $\mathbb{Z}/3\mathbb{Z}[X]$ obtenus par réduction modulo 3 des polynômes P, Q, R. On note A, B et C les anneaux $\mathbb{Z}/3\mathbb{Z}[X]/(\bar{P})$, $\mathbb{Z}/3\mathbb{Z}[X]/(\bar{Q})$ et $\mathbb{Z}/3\mathbb{Z}[X]/(\bar{R})$.

5. Combien y-a-t-il d'éléments dans chacun des anneaux A, B et C ?
   Les anneaux A, B et C étant les quotients de $\mathbb{Z}/3\mathbb{Z}[X]$ par des idéaux ezngendré par des polynômes de degré 4, chacun de ces anneaux à 3^4 éléments.
6. Décomposer $\bar{P}$ en facteurs irréductibles.
   $\bar{P} = (X - \bar{1})^2(X^2 + X - \bar{1})$
7. Montrer qu'il existe un élément non nul a de A tel que $a^2 = 0$.
   Prenons pour a la classe de $(X - \bar{1})(X^2 + X - \bar{1})$ modulo $(\bar{P})$. Alors $a \neq 0$ (car a est la classe d'un polynôme de degré 3) mais $a^2 = 0$ (car a^2 est la classe de $(X-\bar{1})^2(X^2+X-\bar{1})^2$ qui est divisible par $\bar{P}$.
8. Décomposer $\bar{Q}$ en facteurs irréductibles.
   $\bar{Q} = (X - \bar{1})(X + \bar{1})(X^2 + X - \bar{1})$
9. Les anneaux A et B sont-ils isomorphes ?
   Remarquons que si $b \in B$ a un carré nul, alors b est la classe d'un polynôme T dont le carré est divisible par $\bar{Q}$, mais comme la décomposition de $\bar{Q}$ est formé du produit de trois polynômes irréductibles premiers entre-eux, on en déduit que T est lui-même divisible par $\bar{Q}$, c'est-à-dire b est nul. On a vu par contre qu'il existait un élément non nul a de A de carré nul. On déduit que a et b ne sont pas isomorphes.
10. Montrer que A et C sont isomorphes. On pourra utiliser le morphisme ϕ défini par

$$\begin{array}{rccc} \phi : & \mathbb{Z}/3\mathbb{Z}[X] & \to & \mathbb{Z}/3\mathbb{Z}[X] \\ & S(X) & \mapsto & S(-X) \end{array} .$$

    Remarquons que ϕ est un isomorphisme. En composant ϕ par la projection de $\mathbb{Z}/3\mathbb{Z}[X]$ sur C, on obtient un morphisme surjectif ψ de $\mathbb{Z}/3\mathbb{Z}[X]$ sur C. Le noyau de ψ est alors égal à $\phi^{-1}((\bar{R}))$. Or $\bar{R}(X) = \bar{P}(-X)$, donc $\phi^{-1}((\bar{R})) = (\bar{P})$. Par passage au quotient, ψ induit un isomorphisme de A sur C.
11. Déterminer l'idéal I engendré par $\bar{P}$ et $\bar{Q}$, puis l'idéal J engendré par $\bar{R}$ et $\bar{Q}$. Les anneaux $\mathbb{Z}/3\mathbb{Z}[X]/I$ et $\mathbb{Z}/3\mathbb{Z}[X]/J$ sont-ils isomorphes ?
    $PGCD(\bar{P}, \bar{Q}) = (X - \bar{1})(X^2 + X - \bar{1})$, donc $I = ((X - \bar{1})(X^2 + X - \bar{1}))$. On a $\bar{R} = (X+\bar{1})^2(X^2-X-\bar{1})$ donc $PGCD(\bar{R}, \bar{Q}) = (X+\bar{1})$ et $J = (X+\bar{1})$. Les anneaux quotients ne sont pas isomorphes car le premier a 3^3 éléments alors que le second en à seulement 3.