DEVOIR DE RÉVISIONS

À rendre au plus tard le jeudi 22 mai 2008. Le problème 2 et le problème 4 (sauf la question 5) sont extraits de l'examen de 2004.

Problème 1 — Étant donné un nombre entier naturel $n \geq 2$, on désigne par $\lambda(n)$ le nombre de solutions de l'équation $x^2 - 1 = 0$ dans l'anneau $\mathbb{Z}/n\mathbb{Z}$; de manière équivalente, $\lambda(n)$ est le nombre d'entier naturels $m \in \{0, 1, \ldots, n-1\}$ tels que $m^2 \equiv 1 \pmod{n}$.

Cet exercice a pour objet l'étude de la fonction λ.

1. Calculer explicitement $\lambda(n)$ pour $2 \leq n \leq 8$.

2. Démontrer que la fonction λ est *multiplicative* : pour tous entiers naturels n et n' premiers entre eux,
$$\lambda(nn') = \lambda(n)\lambda(n').$$

3. Montrer que l'on a $\lambda(p^\alpha) = 2$ pour tout nombre premier p *impair* et tout nombre entier $\alpha \geq 1$.

4. (i) Que valent $\lambda(2)$, $\lambda(4)$, $\lambda(8)$ et $\lambda(16)$?

(ii) Soit $\alpha \geq 3$ un nombre entier. Justifier qu'un élément x de $\mathbb{Z}/2^\alpha\mathbb{Z}$ vérifie $x^2 = 1$ si et seulement si c'est la classe d'un nombre entier de la forme $1 + 2y$ avec $y \in \mathbb{Z}$ et $y(y+1) \equiv 0 \pmod{2^{\alpha-2}}$.

(iii) Déduire de ce qui précède que l'on a
$$\lambda(2^\alpha) = \begin{cases} 1 & \text{si } \alpha = 1 \\ 2 & \text{si } \alpha = 2 \\ 4 & \text{si } \alpha \geq 3. \end{cases}$$

5. Donner une formule explicite pour $\lambda(n)$ en fonction de la décomposition de n en produit de facteurs premiers. En guise d'application, déterminer $\lambda(440)$.

Problème 2 — Soit G un groupe fini et soit $x \in \mathrm{G}$ un élément d'ordre n. On désigne par H le sous-groupe de G engendré par x et on pose
$$\mathrm{C} = \{g \in \mathrm{G} \mid gx = xg\}, \quad \mathrm{N} = \{g \in \mathrm{G} \mid g\mathrm{H}g^{-1} = \mathrm{H}\}.$$

1. (i) Pour tout $x \in \mathrm{N}$, montrer qu'il existe un unique nombre entier $\nu(g) \in \{1, \ldots, n-1\}$ premier avec n tel que $gxg^{-1} = x^{\nu(g)}$.

(ii) Démontrer que l'application $\overline{\nu} : \mathrm{N} \to (\mathbb{Z}/n\mathbb{Z})^\times$, $g \mapsto \nu(g) \pmod{n}$ est un homomorphisme de groupes de noyau C.

2. On suppose maintenant que G est un groupe symétrique $\mathfrak{S}_m$.

(i) Soit $c \in \mathrm{G}$ un cycle de longueur ℓ et soit k un nombre entier premier avec ℓ. Démontrer que c^k est également un cycle de longueur ℓ.

(ii) En déduire que si x' est un autre générateur du groupe H, alors x et x' sont conjugués dans G.

(iii) Déduire des questions précédentes que les groupes N/C et $(\mathbb{Z}/n\mathbb{Z})^\times$ sont isomorphes.

(iv) Si l'on suppose en outre que x est un m-cycle, montrer que l'on a $\mathrm{C} = \mathrm{H}$ et calculer l'ordre de N.

Problème 3 (*Simplicité du groupe* $\mathfrak{A}_5$) — Étant donné un nombre entier $n \geq 2$, on rappelle qu'il existe un et un seul homomorphisme de groupes $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ tel que $\varepsilon(\tau) = -1$ pour toute transposition τ ; cet homomorphisme est la *signature* et l'on a $\varepsilon(c) = (-1)^{\text{longueur}(c)-1}$ pour tout cycle $c \in \mathfrak{S}_n$ (cf. Fiche 5, exercice 1). Par définition, le *groupe alterné de degré n* est le noyau de cet homomorphisme ; c'est un sous-groupe distingué de $\mathfrak{S}_n$ d'indice 2, que l'on note $\mathfrak{A}_n$.

1. Pour $n \in \{2,3,4,5\}$, décrire les éléments du groupe $\mathfrak{A}_n$ à partir de leur décomposition en produit de cycles de supports disjoints.

2. (i) Vérifier que le groupe $\mathfrak{A}_3$ est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

(ii) Vérifier que $\mathrm{H} = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ est un sous-groupe distingué de $\mathfrak{A}_4$ et que le groupe quotient $\mathfrak{A}_4/\mathrm{H}$ est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

3. Supposons $n \geq 3$.

(i) Démontrer que le produit de deux transpositions distinctes de $\mathfrak{S}_n$ est un 3-cycle ou le produit de deux trois cycles. (*Indication : considérer d'abord le cas de deux transpositions ayant des supports non disjoints puis celui de deux transpositions ayant des supports disjoints.*)

(ii) En déduire que le groupe alterné $\mathfrak{A}_n$ est engendré par les 3-cycles.

4. L'objet de cette dernière question est de démontrer que le groupe $\mathfrak{A}_5$ est *simple*, c'est-à-dire qu'il ne possède pas de sous-groupe distingué distinct de $\{1\}$ et $\mathfrak{A}_5$. Soit donc N un sous-groupe distingué de $\mathfrak{A}_5$.

(i) En utilisant la question 3, montrer que si N contient un 3-cycle alors $\mathrm{N} = \mathfrak{A}_5$.

(ii) Supposons que N contienne le produit de deux transpositions de supports disjoints, disons $\sigma = (1,2)(3,4)$. Montrer que σ et $\tau = (1,5)(3,4)$ sont conjugués dans $\mathfrak{A}_5$ et en déduire que N contient le 3-cycle $\sigma\tau = (1,2,5)$.

(iii) Supposons que N contienne un 5-cycle, disons $\sigma = (1,2,3,4,5)$. Montrer que le 5-cycle $\tau = (1,3,2,5,4)$ est conjugué à σ dans $\mathfrak{A}_5$ et en déduire que N contient le 3-cycle $\sigma\tau = (1,4,2)$.

(iv) Conclure.

Problème 4 — Soient p et q deux nombres premiers distincts. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps à p éléments et on considère dans $\mathbb{F}_p[\mathrm{X}]$ le polynôme $f(\mathrm{X}) = \mathrm{X}^{q-1} + \mathrm{X}^{q-2} + \ldots + \mathrm{X} + 1$.

1. Vérifier que l'on a $\mathrm{X}^q - 1 = (\mathrm{X}-1)f(\mathrm{X})$ et que $\mathrm{X}-1$ ne divise pas $f(\mathrm{X})$.

Dans ce qui suit, on désigne par $g(\mathrm{X})$ un facteur irréductible de $f(\mathrm{X})$ dans $\mathbb{F}_p[\mathrm{X}]$ et l'on pose $d = \deg(g)$.

2. (i) Expliquer pourquoi l'anneau quotient $\mathrm{K} = \mathbb{F}_p[\mathrm{X}]/(g)$ est un corps.

(ii) Montrer que toute classe dans K contient un unique polynôme de $\mathbb{F}_p[\mathrm{X}]$ de degré au plus $d-1$.

(iii) En déduire que K est de cardinal p^d.

3. Soit x la classe de X dans K.

(i) Montrer que x est un élément d'ordre q dans le groupe multiplicatif $\mathrm{K}^\times$. (*Indication : utiliser la question 1*)

(ii) Prouver que p^d est congru à 1 modulo q.

4. Soit n l'ordre de la classe de p dans le groupe $(\mathbb{Z}/q\mathbb{Z})^\times$.

(i) Prouver que n divise d.

(ii) Vérifier que l'application $\mathrm{F} : \mathrm{K} \to \mathrm{K},\ a \mapsto a^p$ est un automorphisme du corps K.

(iii) Montrer que l'on a $\mathrm{F}^n(x) = x$ puis en déduire que l'on a $\mathrm{F}^n = \mathrm{id}_\mathrm{K}$.

(iv) Déduire de ce qui précède que tout élément de K est racine du polynôme $\mathrm{T}^{p^n} - \mathrm{T}$.

(v) Conclure que l'on a $d = n$.

5. On fixe dans cette dernière question un nombre premier q.

(i) Soit a un nombre entier et supposons que p soit un nombre premier distinct de q qui divise $a^{q-1} + a^{q-2} + \ldots + a + 1$. En utilisant les questions précédentes, démontrer que le polynôme $f(\mathrm{X})$ est scindé dans $\mathbb{F}_p[\mathrm{X}]$ et en déduire que l'on a $p \equiv 1 \pmod{q}$.

(ii) Soit $m \geq 2$ un nombre entier naturel. En utilisant l'identité $(m!)^q - 1 = (m!-1)((m!)^{q-1} + \ldots + m! + 1)$, démontrer que l'on a $p \geq m+1$ pour tout facteur premier p de $(m!)^{q-1} + \ldots + m! + 1$.

(iii) Déduire des deux questions précédentes qu'il existe une infinité de nombres premiers p tels que $p \equiv 1 \pmod{q}$.