Master Training Program : Royal Academy of Cambodia/CIMPA

Corrigé de l'examen écrit: 26 octobre 2006

mise à jour: 30/10/2006

Énoncé

1. On rappelle que le développement en fraction continue d'un nombre réel irrationnel t, à savoir

$$t = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

avec $a_j \in \mathbf{Z}$ pour tout $j \geq 0$ et $a_j \geq 1$ pour $j \geq 1$, est noté $[a_0; a_1, a_2, a_3, \dots]$.

Soit t le nombre réel dont le développement en fraction continue est $[1; 3, 1, 3, 1, 3, 1, \dots]$, ce qui signifie $a_{2n} = 1$ et $a_{2n+1} = 3$ pour $n \geq 0$. Écrire un polynôme quadratique à coefficients rationnels qui s'annule en t.

Solution

Le nombre t vérifie

$$t = 1 + \frac{1}{3 + \dfrac{1}{t}}\cdot$$

Un calcul facile montre qu'il est racine du polynôme $3X^2 - 3X - 1$.

Énoncé

2. Résoudre l'équation $y^2 - y = x^2$

a) dans $\mathbf{Z} \times \mathbf{Z}$,

b) dans $\mathbf{Q} \times \mathbf{Q}$.

Solution

a) Il y a deux solutions évidentes $(x, y) = (0, 0)$ et $(x, y) = (0, 1)$. S'il y avait une autre solution dans $\mathbf{Z} \times \mathbf{Z}$, elle aurait $x^2 \geq 1$ et $|y| \geq 2$. Dans ce cas les deux nombres $|y|$ et $|y - 1|$ sont consécutifs, donc premiers entre eux. Si le produit de deux nombres premiers entre eux est un carré, alors chacun d'eux est un carré. Mais il n'existe pas deux carrés positifs consécutifs. Donc dans $\mathbf{Z} \times \mathbf{Z}$ il n'y a que les deux solutions évidentes.

b) L'idée géométrique consiste à couper la courbe par une droite passant par un point rationnel, par exemple $(0, 0)$. Soit $(x, y) \in \mathbf{Q} \times \mathbf{Q}$ une solution avec $x \neq 0$.

Posons $t = y/x$. On remarque déjà que $t \neq \pm 1$ car $y = \pm x$ ne donne pas de solution quand $x \neq 0$. On substitue tx à y dans l'équation et on simplifie par x qui n'est pas nul. On trouve

$$x = \frac{t}{t^2 - 1} \quad \text{et} \quad y = \frac{t^2}{t^2 - 1}. \tag{1}$$

On peut remarquer que pour $t = 0$ ces formules (1) donnent la solution $(x, y) = (0, 0)$, mais ces formules (1) ne donnent pas la solution $(x, y) = (0, 1)$.

Inversement, si t est un nombre rationnel différent de 1 et -1, alors le couple (x, y) donné par (1) est solution de l'équation. Finalement (1) donne toutes les solutions rationnelles à l'exception de $(0, 1)$.

Énoncé
3. Résoudre l'équation $x^{15} = y^{21}$ dans $\mathbf{Z} \times \mathbf{Z}$.

`Solution`
On remarque d'abord que l'équation $15a = 21b$ en entiers rationnels $(a, b) \in \mathbf{Z} \times \mathbf{Z}$ est équivalente à $5a = 7b$. Comme 5 et 7 sont premiers entre eux, la solution générale est $(a, b) = (7c, 5c)$ avec $c \in \mathbf{Z}$.

En décomposant x et y en facteurs premiers, on en déduit que la solution générale de l'équation $x^{15} = y^{21}$ dans $\mathbf{Z} \times \mathbf{Z}$ est donnée par $(x, y) = (t^7, t^5)$ avec t dans $\mathbf{Z}$.
`Remarque.` *Comme les exposants* 15 *et* 21 *sont impairs, x et y ont le même signe. Les $t > 0$ donnent les solutions positives (x, y), tandis que les $t < 0$ donnent les solutions négatives.*

Énoncé
4. Soit $A = \mathbf{Z}[1/2]$ le sous-anneau de $\mathbf{Q}$ engendré par $1/2$.
a) Est-ce que A est un $\mathbf{Z}$–module de type fini?
b) Quelles sont les unités de A?

`Solution`
a) Rappelons qu'un $\mathbf{Z}$–module M est de type fini s'il est engendré par un nombre fini d'éléments, ce qui signifie qu'il existe un ensemble fini $\{\gamma_1, \ldots, \gamma_m\}$ d'éléments de M tel que

$$M = \mathbf{Z}\gamma_1 + \cdots + \mathbf{Z}\gamma_m.$$

Rappelons aussi que le second membre désigne l'ensemble des combinaisons linéaires des γ_j à coefficients dans $\mathbf{Z}$:

$$\mathbf{Z}\gamma_1 + \cdots + \mathbf{Z}\gamma_m = \big\{a_1\gamma_1 + \cdots + a_m\gamma_m \ ; \ (a_1, \ldots, a_m) \in \mathbf{Z}^m\big\}.$$

D'autre part le sous–anneau $A = \mathbf{Z}[1/2]$ de $\mathbf{Q}$ engendré par $1/2$ est l'ensemble des nombres rationnels $\ell/2^n$ avec $\ell \in \mathbf{Z}$ et n entier ≥ 0.

Maintenant si $\gamma_1, \ldots, \gamma_m$ sont des éléments de $A = \mathbf{Z}[1/2]$ alors chacun d'eux s'écrit $\ell_j/2^{n_j}$. Soit n le plus grand des n_j. Toute combinaison linéaire de $\gamma_1, \ldots, \gamma_m$ à coefficients entiers est un nombre rationnel r tel que $2^n r$ soit entier. Par exemple

$1/2^{n+1}$ est un élément de A qui n'est pas dans le $\mathbf{Z}$-module $\mathbf{Z}\gamma_1 + \cdots + \mathbf{Z}\gamma_m$. On en déduit que A n'est pas un $\mathbf{Z}$-module de type fini.

Le fait que l'anneau A ne soit pas un $\mathbf{Z}$–module de type fini résulte aussi d'un théorème du cours et du fait que $1/2$ n'est pas entier sur $\mathbf{Z}$.

b) Un élément $x = \ell/2^n$ de A est inversible si et seulement s'il existe $x' = \ell'/2^{n'} \in A$ tel que le produit xx' soit égal à 1, ce qui s'écrit $\ell\ell' = 2^{n+n'}$. Ainsi ℓ et ℓ' sont des puissances de 2, multipliés éventuellement par -1. Inversement toute puissance de 2 avec un exposant entier positif ou négatif est une unité: $2^j \cdot 2^{-j} = 1$ pour tout $j \in \mathbf{Z}$, et les deux facteurs 2^j, 2^{-j} sont dans A.

En conclusion les unités de A sont les nombres $\pm 2^j$, $j \in \mathbf{Z}$.

Énoncé

5. Quels sont les sous–$\mathbf{Z}$–modules de type fini du groupe additif $\mathbf{Q}$?

`Solution`

Montrons que ce sont exactement les sous-groupes de $\mathbf{Q}$ engendrés par un élément. Dans un sens si γ est un nombre rationnel alors $\mathbf{Z}\gamma$ est un $\mathbf{Z}$–sous–module de $\mathbf{Q}$ de type fini. Ce qu'il faut démontrer est la réciproque.

Soient $\gamma_1, \ldots, \gamma_m$ des nombres rationnels. Si les γ_i sont tous nuls le $\mathbf{Z}$–module qu'ils engendrent est $\{0\}$ et le résultat est clair avec $\gamma = 0$. Sinon désignons par q le plus petit dénominateur positif commun des γ_i et posons $p_i = q\gamma_i$. Ainsi les nombres $q, p_1, \ldots, p_m$ sont des entiers positifs ayant un pgcd égal à 1. Soit p le pgcd de $p_1, \ldots, p_m$, de sorte que $\mathbf{Z}p = \mathbf{Z}p_1 + \cdots + \mathbf{Z}p_m$. Alors p et q sont premiers entre eux et le $\mathbf{Z}$–module engendré par $M = \mathbf{Z}\gamma_1 + \cdots + \mathbf{Z}\gamma_m$ est $\mathbf{Z}\gamma$ avec $\gamma = p/q$.

Énoncé

6. Quelles sont les racines rationnelles du polynôme $X^7 - X^6 + X^5 - X^4 - X^3 + X^2 - X + 1$?

`Solution`

On rappelle que si p/q est une racine rationnelle avec $\mathrm{pgcd}(p, q) = 1$ d'un polynôme $a_0X^n + \cdots + a_n$ à coefficients dans $\mathbf{Z}$ ayant $a_0a_n \neq 0$, alors p divise a_n et q divise a_0. Ici a_0 et a_n valent 1, les seules valeurs à tester sont 1 et -1 qui sont toutes deux racines.

Énoncé

7. Soit k le corps de nombres $\mathbf{Q}(i, \sqrt{2})$.

a) Quel est le degré de k sur $\mathbf{Q}$? Donner une base de k sur $\mathbf{Q}$. Trouver un élément $\gamma \in k$ tel que $k = \mathbf{Q}(\gamma)$. Quels sont les conjugués de γ sur $\mathbf{Q}$?

b) Montrer que k est une extension galoisienne de $\mathbf{Q}$. Quel est le groupe de Galois? Quels sont les sous-corps de k?

`Solution`

a) Le corps k est le corps engendré par i et $\sqrt{2}$ sur $\mathbf{Q}$, il contient donc $\sqrt{2}$ et i.

Comme le corps $\mathbf{Q}(\sqrt{2})$ est contenu dans celui des nombres réels, il ne contient pas i. Donc k est une extension de degré 2 de $\mathbf{Q}(\sqrt{2})$ et par conséquent une extension de degré 4 de $\mathbf{Q}$.

Une base de $\mathbf{Q}(\sqrt{2})$ sur $\mathbf{Q}$ (comme $\mathbf{Q}$–espace vectoriel) est $\{1, \sqrt{2}\}$, une base de k sur $\mathbf{Q}(\sqrt{2})$ est $\{1, i\}$, donc une base de k sur $\mathbf{Q}$ est obtenue en prenant les 4 produits $\{1, \sqrt{2}, i, i\sqrt{2}\}$.

Un exemple (parmi beaucoup d'autres!) de générateur de k sur $\mathbf{Q}$ (ici il s'agit d'un générateur pour l'extension de corps: on cherche γ tel que $k = \mathbf{Q}(\gamma)$) est $\gamma = i + \sqrt{2}$, car ses quatre conjugués sur $\mathbf{Q}$ sont distincts: ce sont

$$i + \sqrt{2}, \quad i - \sqrt{2}, \quad -i + \sqrt{2}, \quad -i - \sqrt{2}.$$

b) Le corps k est le corps de décomposition sur $\mathbf{Q}$ du polynôme $(X^2-2)(X^2+1)$ - c'est d'ailleurs aussi le corps de décomposition sur $\mathbf{Q}$ du polynôme unitaire irréductible de γ qui est, avec notre choix de γ,

$$(X - i - \sqrt{2})(X - i + \sqrt{2})(X + i - \sqrt{2})(X + i + \sqrt{2}) = X^4 - 2X^2 + 9.$$

Ainsi k est une extension normale de $\mathbf{Q}$ (c'est le corps de décomposition d'un polynôme) et séparable (le polynôme n'a pas de racines multiples – de toutes façons ici la caractéristique est nulle!).

Le groupe de Galois G de k sur $\mathbf{Q}$ est le groupe des automorphismes de k. Un tel automorphisme est déterminé par sa valeur en $\sqrt{2}$ et en i. Sa valeur en $\sqrt{2}$ est un conjugué de $\sqrt{2}$, donc c'est $\sqrt{2}$ ou $-\sqrt{2}$. De même sa valeur en i est un conjugué de i, donc i ou $-i$. Cela donne les quatre automorphismes. Si on désigne par σ l'automorphisme non trivial de k qui fixe i et par τ celui qui fixe $\sqrt{2}$ alors τ est la conjugaison complexe et $G = \{1, \sigma, \tau, \sigma\tau\}$ (ici 1 désigne l'élément neutre de G, qui est l'automorphisme identité de k). Ainsi G est le groupe d'ordre 4 qui n'est pas cyclique, il est abélien de type $(2, 2)$ ce qui veut dire qu'il est isomorphe à $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$, et il possède exactement 5 sous–groupes: deux de ces sous–groupes sont les sous–groupes triviaux $\{1\}$ et G, les trois autres sont d'ordre 2:

$$\{1, \sigma\}, \quad \{1, \tau\}, \quad \{1, \sigma\tau\}.$$

Il en résulte que k a exactement 5 sous–corps, deux sont les sous–corps triviaux k (dont le groupe de Galois sur k est $\{1\}$) et $\mathbf{Q}$ (le groupe de Galois de k sur $\mathbf{Q}$ est G), les trois autres sont les sous–corps fixés par chacun des trois sous–groupes d'ordre 2, ce sont les trois sous–corps de k quadratiques sur $\mathbf{Q}$:

$$\mathbf{Q}(i), \quad \mathbf{Q}(\sqrt{2}), \quad \mathbf{Q}(i\sqrt{2}).$$

On vérifie par exemple que $i\sqrt{2}$ est fixé par $\sigma\tau$, puisque $\sigma\tau(i) = \sigma(-i) = -i$ et $\sigma\tau(\sqrt{2}) = \sigma(\sqrt{2}) = -\sqrt{2}$. Le groupe de Galois de k sur $\mathbf{Q}(i\sqrt{2})$ est donc bien $\{1, \sigma\tau\}$.

Énoncé

8. Soit $\zeta \in \mathbf{C}$ un nombre complexe qui satisfait $\zeta^5 = 1$ et $\zeta \neq 1$. Soit $K = \mathbf{Q}(\zeta)$.
a) Quel est le polynôme unitaire irréductible de ζ sur $\mathbf{Q}$? Quels sont les conjugués de ζ sur $\mathbf{Q}$? Quel est le groupe de Galois G de K sur $\mathbf{Q}$? Quels sont les sous–groupes de G?
b) Montrer que K contient un unique sous-corps L qui est de degré 2 sur $\mathbf{Q}$. Quel est l'anneau des entiers de L? Quel est le discriminant? Quel est le groupe des unités?

Solution

a) Le polynôme unitaire irréductible de ζ sur $\mathbf{Q}$ est $X^4 + X^3 + X^2 + X + 1$. Les conjugués de ζ sur $\mathbf{Q}$ sont les quatre racines de ce polynôme, ce sont les quatre racines primitives cinquième de l'unité. Si ζ est l'une d'entre elles, les autres sont $\zeta^2, \zeta^3, \zeta^4$. Le groupe de Galois de K sur $\mathbf{Q}$ a quatre éléments, qui sont les quatre automorphismes de K. Chacun d'eux est déterminé par l'image de ζ, on peut donc les noter $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ avec $\sigma_j(\zeta) = \zeta^j$. Ce groupe G est cyclique, un générateur est σ_2: en effet

$$\sigma_2^2(\zeta) = \sigma_2(\zeta^2) = \zeta^4, \quad \sigma_2^3(\zeta) = \sigma_2(\zeta^4) = \zeta^8 = \zeta^3,$$

donc $\sigma_2^2 = \sigma_4$, $\sigma_2^3 = \sigma_3$ et $G = \{1, \sigma_2, \sigma_2^2, \sigma_2^3\}$. Un autre générateur est σ_2^3 (cela provient du fait que l'exposant 3 est premier avec l'ordre du groupe 4).

b) Le groupe G est cyclique d'ordre 4, il possède donc exactement 3 sous-groupes, deux sont les sous-groupes triviaux $\{1\}$ et G, le troisième est l'unique sous-groupe H d'ordre 2 engendré par l'unique élément d'ordre 2, à savoir σ_2^2. Comme $\sigma_2^2(\zeta) = \zeta^4$ est le conjugué complexe de ζ (rappelons que $\zeta^5 = 1$, $|\zeta|^2 = \zeta\bar{\zeta} = 1$ et donc $\zeta^4 = \zeta^{-1} = \bar{\zeta}$), le sous–corps L de K fixé par H est l'intersection de K et $\mathbf{R}$.

Posons $\alpha = \zeta + \bar{\zeta}$, de sorte que $\alpha \in K \cap \mathbf{R}$. Comme

$$\alpha^2 = (\zeta + \bar{\zeta})^2 = \zeta^2 + \bar{\zeta}^2 + 2 \quad \text{et que} \quad 1 + \zeta + \zeta^2 + \bar{\zeta}^2 + \bar{\zeta} = 0,$$

on a $\alpha^2 + \alpha - 1 = 0$. La partie réelle de ζ étant positive, il en résulte que α est le nombre d'or $(1 + \sqrt{5})/2$. Le corps L est le corps $\mathbf{Q}(\sqrt{5})$, son anneau d'entiers est $\mathbf{Z} + \mathbf{Z}\alpha$, son discriminant est 5, le groupe des unités est $\{\pm\alpha^m \ ; \ m \in \mathbf{Z}\}$.