

Les calculatrices ne sont pas autorisées, les documents non plus,
les téléphones portables encore moins

Contrôle du 6 mars 2007
Barème approximatif : sur 20

- (3) **Exercice 1.** Soit d un entier positif. Quel est le développement en fraction continue du nombre $\sqrt{d^2 + 1}$? En déduire que ce nombre est irrationnel.
Résoudre les équations $x^2 - (d^2 + 1)y^2 = 1$ et $x^2 - (d^2 + 1)y^2 = -1$ en entiers x, y positifs.
- (8) **Exercice 2.** On pose $\zeta = e^{i\pi/6}$ et $j = e^{2i\pi/3}$.
a) Décomposer le polynôme $X^{12} - 1$ en facteurs irréductibles sur \mathbf{Q} .
b) Pour chacun des douze nombres complexes

$$1, \zeta, -j^2, i, j, j\zeta, -1, -\zeta, j^2, -i, -j, -j\zeta,$$

donner son polynôme irréductible sur \mathbf{Q} .

- c) Soit G le groupe de Galois de $\mathbf{Q}(\zeta)$ sur \mathbf{Q} . Pour chacun des éléments de G , dire quelle est l'image de ζ, i et j .
d) Quels sont les sous-corps de $\mathbf{Q}(\zeta)$? Quels sont les entiers $d > 0$ tels que $\mathbf{Q}(\sqrt{d})$ soit contenu dans $\mathbf{Q}(\zeta)$?

- (9) **Exercice 3.**
a) On note $f_1(X)$ le polynôme $X^4 + 4$ et $K_1 \subset \mathbf{C}$ son corps de décomposition sur \mathbf{Q} . Quelles sont les racines de f_1 dans \mathbf{C} ? Quel est le degré de K_1 sur \mathbf{Q} ? Quel est le groupe de Galois de K_1 sur \mathbf{Q} ?
b) On note $f_2(X)$ le polynôme $X^3 - 2$ et $K_2 \subset \mathbf{C}$ son corps de décomposition sur \mathbf{Q} . Quelles sont les racines de f_2 dans \mathbf{C} ? Quel est le degré de K_2 sur \mathbf{Q} ? Quel est le groupe de Galois de K_2 sur \mathbf{Q} ? Quels sont les sous-corps quadratiques de K_2 ?
On rappelle la terminologie : un corps quadratique est une extension de \mathbf{Q} de degré 2.
c) Quelle est l'intersection de K_1 et K_2 ?
Soit $K \subset \mathbf{C}$ le corps de décomposition sur \mathbf{Q} du produit $f_1 f_2$. Quel est le degré de K sur \mathbf{Q} ?
d) Trouver tous les sous-corps quadratiques de K .
e) Donner un exemple d'élément primitif de l'extension K/\mathbf{Q} , c'est-à-dire un élément $\gamma \in K$ tel que $K = \mathbf{Q}(\gamma)$.

Contrôle du 6 mars 2007
Corrigé

Exercice 1. Les inégalités

$$d^2 < d^2 + 1 < (d + 1)^2$$

montrent que la partie entière du nombre $t = \sqrt{d^2 + 1}$ est d . On écrit

$$\sqrt{d^2 + 1} = d + \frac{1}{x}$$

et on trouve

$$x = \frac{1}{\sqrt{d^2 + 1} - d} = d + t,$$

donc

$$t = d + \frac{1}{d + t}.$$

On aurait pu aussi obtenir ce résultat en écrivant $(t - d)(t + d) = t^2 - d^2 = 1$.

Alors

$$t = d + \frac{1}{2d + \frac{1}{d + t}}$$

et le développement en fraction continue de t est

$$[d; 2d, 2d, \dots] = [d; \overline{2d}].$$

Comme ce développement est infini, t est irrationnel.

Une solution de l'équation

$$x^2 - (d^2 + 1)y^2 = -1$$

est $(x_1, y_1) = (d, 1)$. On obtient toutes les solutions (x_k, y_k) ($k = 1, 2, \dots$) en entiers x, y positifs de l'équation $x^2 - (d^2 + 1)y^2 = \pm 1$ en écrivant

$$x_k + y_k \sqrt{d^2 + 1} = (d + \sqrt{d^2 + 1})^k \quad (k \geq 0).$$

Pour k pair on obtient les solutions de l'équation $x^2 - (d^2 + 1)y^2 = 1$:

$$(x_0, y_0) = (1, 0), \quad (x_2, y_2) = (2d^2 + 1, 2d)$$

et

$$x_{2h} + y_{2h} \sqrt{d^2 + 1} = (2d^2 + 1 + 2d\sqrt{d^2 + 1})^h \quad (h \geq 0).$$

Pour k impair on obtient les solutions de l'équation $x^2 - (d^2 + 1)y^2 = -1$: par exemple

$$(x_1, y_1) = (d, 1), \quad (x_3, y_3) = (4d^3 + 3d, 4d^2 + 1).$$

Exercice 2.

a) Les diviseurs de 12 sont 1, 2, 3, 4, 6 et 12. Le polynôme $X^{12} - 1$ est donc facteur de 6 polynômes irréductibles sur \mathbf{Q} qui sont les polynômes cyclotomiques

$$\begin{aligned} \Phi_1(X) &= X - 1, & \Phi_2(X) &= X + 1, & \Phi_3(X) &= X^2 + X + 1, \\ \Phi_4(X) &= X^2 + 1, & \Phi_6(X) &= X^2 - X + 1, & \Phi_{12}(X) &= X^4 - X^2 + 1. \end{aligned}$$

b) Les douze nombres $1, \zeta, -j^2, i, j, j\zeta, -1, -\zeta, j^2, -i, -j, -j\zeta$ sont les racines 12èmes de l'unité dans l'ordre

$$\{1, \zeta, \zeta^2, \dots, \zeta^{11}\} = \{\zeta^k ; k = 0, 1, \dots, 11\}.$$

Ce sont donc les racines du polynôme $X^{12} - 1$ et

1 est racine de Φ_1 ,

-1 est racine de Φ_2 ,

j et j^2 sont les racines de Φ_3 ,

i et $-i$ sont les racines de Φ_4 ,

$-j$ et $-j^2$ sont les racines de Φ_6 ,

$\zeta, j\zeta, -\zeta$ et $-j\zeta$ sont les racines de Φ_{12} : ce sont les racines primitives 12èmes de l'unité

$$\zeta, \zeta^5, \zeta^7, \zeta^{11}$$

car les classes de 1, 5, 7 et 11 sont les éléments inversibles de l'anneau $\mathbf{Z}/12\mathbf{Z}$.

On peut aussi dire que, comme i et $-i$ sont d'ordre 4 dans le groupe multiplicatif \mathbf{C}^\times , que j et j^2 sont d'ordre 3 et que 3 et 4 sont premiers entre eux, chacun des produits $ij, -ij, ij^2, -ij^2$ est d'ordre 12. On a en effet

$$\zeta = -ij, \quad \zeta^5 = -ij^2, \quad \zeta^7 = ij, \quad \zeta^{11} = ij^2 = \bar{\zeta} = \zeta^{-1}.$$

On voit aussi que $\mathbf{Q}(\zeta) = \mathbf{Q}(i, j)$.

b) Le groupe G est isomorphe au groupe multiplicatif $(\mathbf{Z}/12\mathbf{Z})^\times$ des entiers premiers avec 12. On peut noter ses 4 éléments σ_1 (qui est l'identité), σ_5, σ_7 et σ_{11} , avec $\sigma_k(\zeta) = \zeta^k$.

Comme $\sigma_5(\zeta) = \zeta^5 = j\zeta$ et que $i = \zeta^3, j = \zeta^4$, on trouve

$$\sigma_5(i) = (j\zeta)^3 = i, \quad \sigma_5(j) = (j\zeta)^4 = j^2.$$

Comme $\sigma_7(\zeta) = \zeta^7 = -\zeta$ on trouve de même

$$\sigma_7(i) = (-\zeta)^3 = -i, \quad \sigma_7(j) = (-\zeta)^4 = j.$$

Enfin σ_{11} est le composé $\sigma_5 \circ \sigma_7$, il vérifie $\sigma_{11}(\zeta) = \zeta^{11} = \bar{\zeta}$ et

$$\sigma_{11}(i) = -i, \quad \sigma_{11}(j) = j^2.$$

d) Le groupe G est abélien d'ordre 4, non cyclique, il admet donc trois sous-groupes d'ordre 2, ce qui fait que $\mathbf{Q}(\zeta)$ possède trois sous-corps quadratiques (donc cinq sous-corps en tout, en comptant \mathbf{Q} et $\mathbf{Q}(\zeta)$).

Comme $\zeta^3 = i$ est fixé par σ_5 le sous-corps de $\mathbf{Q}(\zeta)$ fixé par le sous-groupe $\{1, \sigma_5\}$ de G est $\mathbf{Q}(i)$. De même le sous-corps de $\mathbf{Q}(\zeta)$ fixé par le sous-groupe $\{1, \sigma_7\}$ de G est $\mathbf{Q}(j)$. Enfin σ_{11} est la conjugaison complexe, le sous-corps fixé par $\{1, \sigma_{11}\}$ est le sous-corps réel maximal de $\mathbf{Q}(\zeta)$ (intersection de $\mathbf{Q}(\zeta)$ avec \mathbf{R}). Comme $\mathbf{Q}(j) = \mathbf{Q}(i\sqrt{3})$ on a $\mathbf{Q}(\zeta) = \mathbf{Q}(i, \sqrt{3})$ et le sous-corps fixé par σ_{11} est $\mathbf{Q}(\sqrt{3})$.

On peut aussi écrire $\sqrt{3} = i(j^2 - j)$ et utiliser les relations

$$\sigma_{11}(i) = -i, \quad \sigma_{11}(j) = j^2, \quad \sigma_{11}(j^2) = j$$

pour vérifier $\sigma_{11}(\sqrt{3}) = \sqrt{3}$.

Le seul sous-corps quadratique réel de $\mathbf{Q}(\zeta)$ est $\mathbf{Q}(\sqrt{3})$, donc les entiers $d > 0$ tels que $\mathbf{Q}(\zeta)$ contienne $\mathbf{Q}(\sqrt{d})$ sont les carrés a^2 (avec a entier positif) et les produits $3a^2$ de 3 par un carré.

Exercice 3.

a) On trouve les racines complexes de $f_1(X) = X^4 + 4$ en posant $Y = X/\sqrt{2}$: les racines du polynôme $Y^4 + 1 = \Phi_8(Y)$ sont les racines primitives 8èmes de l'unité $(\pm 1 \pm i)\sqrt{2}/2$. Par conséquent celles de f_1 sont $\pm 1 \pm i$. Comme ce sont quatre nombres quadratiques sur \mathbf{Q} , le polynôme f_1 est produit de deux polynômes irréductibles de degré 2, à savoir $X^4 + 4 = (X^2 + 2X + 2)(X^2 - 2X + 2)$ (ce que l'on vérifie trivialement bien entendu). Le corps de décomposition sur \mathbf{Q} de f_1 est donc $K_1 = \mathbf{Q}(i)$, il est de degré 2 sur \mathbf{Q} , de groupe de Galois le groupe cyclique à 2 éléments $\{1, \tau\}$ où τ est la conjugaison complexe.

b) Les trois racines complexes de $f_2(X) = X^3 - 2$ sont $\alpha = \sqrt[3]{2}$, $j\alpha$ et $j^2\alpha$, quand j désigne une racine du polynôme $X^2 + X + 1$ (c'est-à-dire que j est une racine primitive cubique de l'unité). Le corps de décomposition sur \mathbf{Q} de f_2 est $K_2 = \mathbf{Q}(j, \sqrt[3]{2})$, il est de degré 6 sur \mathbf{Q} , de groupe de Galois le groupe symétrique \mathfrak{S}_3 sur 3 lettres. Le groupe G a, comme \mathfrak{S}_3 , un unique sous-groupe H d'ordre 3 (et d'indice 2), donc K_2 possède un unique sous-corps quadratique qui est $K_2^H = \mathbf{Q}(j)$.

c) Le corps K_1 est quadratique et n'est pas contenu dans K_2 , donc l'intersection de K_1 et K_2 est un sous-corps de K_1 distinct de K_1 : c'est donc \mathbf{Q} . Le compositum de K_1 et K_2 est $K = \mathbf{Q}(i, j, \alpha)$, c'est une extension de degré 2 de K_2 (puisque K_1 n'est pas contenu dans K_2), donc $[K : \mathbf{Q}] = 12$.

d) Soit G le groupe de Galois de K sur \mathbf{Q} , d'ordre 12. On peut utiliser le fait que les corps K_1 et K_2 sont galoisiens sur \mathbf{Q} et ont pour intersection \mathbf{Q} , donc leur compositum K est galoisien sur \mathbf{Q} et a pour groupe de Galois le produit direct $G_1 \times G_2$. Cela permet de vérifier que G a un unique sous-groupe d'ordre 3, celui qui fixe le corps quartique $\mathbf{Q}(i, j)$ (quartique = de degré 4 sur \mathbf{Q}). On peut aussi le vérifier en donnant la liste de tous les sous-groupes de G (voir ci-dessous).

Un sous-corps quadratique de K est fixé par un sous-groupe de G d'ordre 6. Un groupe d'ordre 6 contient un unique sous-groupe d'ordre 3. Le seul sous-groupe d'ordre 3 de G est celui qui fixe $\mathbf{Q}(i, j)$. Remarquons que $\mathbf{Q}(i, j)$ est le corps cyclotomique $\mathbf{Q}(\zeta)$ de la question précédente. Les sous-corps quadratiques de K sont donc ceux de $\mathbf{Q}(i, j)$, qui sont, comme nous l'avons vu, $\mathbf{Q}(i)$, $\mathbf{Q}(j)$ et $\mathbf{Q}(\sqrt{3})$.

Remarque. Bien que la question ne soit pas posée, on peut compléter la description de tous les sous-corps de K . Par la théorie de Galois cela revient à décrire les sous-groupes de G .

Un élément de G est déterminé par les images de α , i et j . L'image d'un nombre algébrique par un automorphisme est un conjugué de ce nombre. Donc l'image de α est α , $j\alpha$ ou $j^2\alpha$, celle de i est i ou $-i$, celle de j est j ou j^2 . Cela donne les $3 \times 2 \times 2 = 12$ triplets possibles et les 12 éléments du groupe de Galois.

Notons ϱ l'élément de G d'ordre 3 qui fixe i et j et qui envoie α sur $j\alpha$. Notons ensuite σ_1 celui qui fixe α et i et qui envoie j sur j^2 . Notons enfin σ_2 celui qui fixe α et j et qui envoie i sur $-i$.

On peut alors donner la liste des 12 éléments de G en précisant les images de α , i et j . On donne aussi leur ordre dans G :

| G | α | i | j | ordre |
|-----------------------------|-------------|------|-------|-------|
| 1 | α | i | j | 1 |
| ϱ | $j\alpha$ | i | j | 3 |
| ϱ^2 | $j^2\alpha$ | i | j | 3 |
| σ_1 | α | i | j^2 | 2 |
| σ_2 | α | $-i$ | j | 2 |
| $\sigma_1\sigma_2$ | α | $-i$ | j^2 | 2 |
| $\varrho\sigma_1$ | $j\alpha$ | i | j^2 | 2 |
| $\varrho\sigma_2$ | $j\alpha$ | $-i$ | j | 6 |
| $\varrho\sigma_1\sigma_2$ | $j\alpha$ | $-i$ | j^2 | 2 |
| $\varrho^2\sigma_1$ | $j^2\alpha$ | i | j^2 | 2 |
| $\varrho^2\sigma_2$ | $j^2\alpha$ | $-i$ | j | 6 |
| $\varrho^2\sigma_1\sigma_2$ | $j^2\alpha$ | $-i$ | j^2 | 2 |

Les relations entre ϱ , σ_1 et σ_2 se déduisent des suivantes :

$$\varrho^3 = \sigma_1^2 = \sigma_2^2 = 1, \quad \sigma_1\sigma_2 = \sigma_2\sigma_1, \quad \sigma_1\varrho = \varrho^2\sigma_1, \quad \sigma_2\varrho = \varrho\sigma_2.$$

Noter que σ_2 est dans le centre de G (il commute avec tous les éléments de G) et que $\sigma_1\sigma_2$ est la conjugaison complexe.

• Il y a 7 éléments d'ordre 2 (et donc 7 sous-groupes d'ordre 2 dans G avec autant de sous-corps de K de degré 6 sur \mathbf{Q}) :

- σ_1 qui fixe $\mathbf{Q}(\alpha, i)$,
- σ_2 qui fixe $\mathbf{Q}(\alpha, j) = K_2$ (la restriction de σ_2 à K_1 est la conjugaison complexe),
- $\sigma_1\sigma_2$, la conjugaison complexe, qui fixe le sous-corps réel maximal $\mathbf{Q}(\alpha, \sqrt{3})$,
- $\varrho\sigma_1$ qui fixe $\mathbf{Q}(j^2\alpha, i)$,
- $\varrho^2\sigma_1$ qui fixe $\mathbf{Q}(j\alpha, i)$,
- $\varrho\sigma_1\sigma_2$ qui fixe $\mathbf{Q}(j^2\alpha, \sqrt{3})$,
- $\varrho^2\sigma_1\sigma_2$ qui fixe $\mathbf{Q}(j\alpha, \sqrt{3})$.

• Il y a trois sous-groupes d'ordre 4, (aucun n'est cyclique puisqu'il n'y a pas d'élément d'ordre 4 dans G) :

- $\{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$, qui fixe le corps cubique $\mathbf{Q}(\alpha)$,
- $\{1, \sigma_2, \varrho\sigma_1, \varrho\sigma_1\sigma_2\}$, qui fixe le corps cubique $\mathbf{Q}(j\alpha)$,
- $\{1, \sigma_2, \varrho^2\sigma_1, \varrho^2\sigma_1\sigma_2\}$, qui fixe le corps cubique $\mathbf{Q}(j^2\alpha)$.

• Il y a un unique sous-groupe d'ordre 3, à savoir $\{1, \varrho, \varrho^2\}$, qui est le sous-groupe fixant $\mathbf{Q}(\zeta) = \mathbf{Q}(i, j)$.

• Il y a trois sous-groupes d'ordre 6, comme nous l'avons vu :

- $\{1, \varrho, \varrho^2, \sigma_2, \varrho\sigma_2, \varrho^2\sigma_2\}$, cyclique, qui fixe le corps $\mathbf{Q}(j)$,
- $\{1, \varrho, \varrho^2, \sigma_1, \varrho\sigma_1, \varrho^2\sigma_1\}$, isomorphe à \mathfrak{S}_3 , qui fixe le corps $K_1 = \mathbf{Q}(i)$,
- $\{1, \varrho, \varrho^2, \sigma_1\sigma_2, \varrho\sigma_1\sigma_2, \varrho^2\sigma_1\sigma_2\}$, isomorphe à \mathfrak{S}_3 , qui fixe le corps $\mathbf{Q}(\sqrt{3})$.

Le sous-groupe $G_1 = \{1, \sigma_2\}$ de G s'identifie au groupe de Galois de K_1 sur \mathbf{Q} . De même les restrictions à K_2 des éléments du sous-groupe $G_2 = \{1, \varrho, \varrho^2, \sigma_1, \varrho\sigma_1, \varrho^2\sigma_1\}$ sont les 6 automorphismes de K_2 . Le groupe G est le produit direct de G_1 et de G_2 .

e) Un élément primitif de K sur \mathbf{Q} est $\zeta + \alpha$ (il y en a bien d'autres!) car ses 12 images sous l'action des éléments de G sont distinctes.