Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
http://www.math.jussieu.fr/∼miw/

Master de sciences et technologies 1ère année -
Spécialité : Mathématiques Fondamentales

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

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

Examen du jeudi 24 Mai 2007
Barême approximatif : sur 34

Exercices.

(1) 1) Donner un exemple d'une extension finie qui n'est pas normale et préciser sa clôture normale.

(2) 2) Quels sont les degrés des facteurs irréductibles de $X^{33} - 1$ sur $\mathbf{F}_3$?

(2) 3) Existe-t-il des nombres algébriques de norme 1 qui ne sont pas des unités ? Si oui en donner un exemple, si non démontrer qu'il n'en existe pas.

(4) 4) On désigne par φ la fonction d'Euler.

a) Montrer qu'il existe deux constantes positives c et κ telles que, pour tout $n \geq 1$, on ait

$$\varphi(n) \geq cn^{\kappa}$$

Dans la suite, s désigne un nombre réel $> 1/\kappa$.

b) Montrer que quand p est un nombre premier on a

$$\sum_{a\geq 0} \varphi(p^a)^{-s} = 1 + \frac{1}{(p-1)^s(1-p^{-s})}.$$

c) On pose

$$G(s) = \prod_p (1 + (p-1)^{-s} - p^{-s})$$

où le produit est étendu à l'ensemble des nombres premiers. Vérifier

$$\sum_{n\geq 1} \varphi(n)^{-s} = \zeta(s)G(s)$$

où ζ est la fonction zêta de Riemann.

Problème. Soient p un nombre premier impair, $\zeta \in \mathbf{C}$ une racine primitive p-ième de l'unité, $k = \mathbf{Q}(\zeta)$ le corps cyclotomique engendré par les racines p-ièmes de l'unité et $\mathbf{Z}_k$ l'anneau des entiers de k.

(13) **I** On va démontrer $\mathbf{Z}_k = \mathbf{Z}[\zeta]$. Quelle est l'inclusion évidente ?

On pose $\pi = \zeta - 1$.

1) Quel est le polynôme irréductible de ζ sur $\mathbf{Q}$? Quel est le degré de k sur $\mathbf{Q}$? Quels sont les conjugués de ζ ? Quelle est la norme de ζ ? Quel est la trace de ζ ?
2) Quels sont les automorphismes de k ?
3) Quel est le polynôme irréductible de π sur $\mathbf{Q}$? Quels sont les conjugués de π ? Quelle est la norme de π ? Quel est la trace de π ?
4) Montrer que

$$\{1,\ \zeta,\ \zeta^2, \ldots,\ \zeta^{p-2}\}, \quad \{\zeta,\ \zeta^2, \ldots,\ \zeta^{p-2},\ \zeta^{p-1}\}, \quad \{1,\ \pi,\ \pi^2, \ldots,\ \pi^{p-2}\}$$

sont trois bases de k sur $\mathbf{Q}$ et aussi de $\mathbf{Z}[\zeta]$ sur $\mathbf{Z}$.

5) Montrer que si π' est un conjugué de π sur $\mathbf{Q}$, alors les deux idéaux principaux $\pi\mathbf{Z}[\zeta]$ et $\pi'\mathbf{Z}[\zeta]$ de l'anneau $\mathbf{Z}[\zeta]$ coïncident.
6) Montrer que π^{p-1}/p est une unité de l'anneau $\mathbf{Z}[\zeta]$.
7) Soit $n \in \mathbf{Z}$. Montrer que n appartient à l'idéal $\pi\mathbf{Z}[\zeta]$ si et seulement si n est multiple de p.
8) Montrer que l'idéal $\pi\mathbf{Z}[\zeta]$ est maximal. Quel est le quotient $\mathbf{Z}[\zeta]/\pi\mathbf{Z}[\zeta]$?
9) Soit $\alpha \in \mathbf{Z}_k$.

a) On écrit

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$$

avec $a_0,\ a_1,\ \ldots,\ a_{p-2}$ dans $\mathbf{Q}$. Montrer que $pa_0 \in \mathbf{Z}$.
`Indication :` *On pourra considérer la trace de* $\pi\alpha$.
Montrer que $pa_i \in \mathbf{Z}$ pour $1 \leq i \leq p-2$.

b) Montrer qu'on peut écrire

$$p\alpha = b_0 + b_1\pi + \cdots + b_{p-2}\pi^{p-2}$$

avec $b_i \in \mathbf{Z}$ pour $0 \leq i \leq p-2$. Montrer que π divise b_0 dans $\mathbf{Z}[\zeta]$. En déduire que p divise b_0. Montrer ensuite que p divise $b_1,\ \ldots,\ b_{p-2}$.

c) En déduire $\mathbf{Z}_k = \mathbf{Z}[\zeta]$.

(12) **II** On suppose maintenant $p = 23$. On veut montrer que l'anneau $\mathbf{Z}_k$ des entiers de k n'est pas principal.

On note $\zeta = e^{2i\pi/23}$ et $k = \mathbf{Q}(\zeta)$. Le but de ce problème est de montrer que l'anneau $\mathbf{Z}_k$ n'est pas principal.

1) 2 est-il un carré modulo 47 ? En déduire que 47 divise $2^{23} - 1$.
2) Par le calcul montrez que $2^{23} - 1$ n'est pas divisible par 47^2.
3) Calculez $\mathrm{N}_{k/\mathbf{Q}}(\zeta - 2)$.
4) On note $\mathfrak{a}$ l'idéal de $\mathbf{Z}_k$ engendré par 47 et $\zeta - 2$. Montrer que, pour tout élément β de $\mathfrak{a}$, 47 divise $\mathrm{N}_{k/\mathbf{Q}}(\beta)$.
5) On suppose que $\mathfrak{a}$ est principal, engendré par α. Montrer que la norme $\mathrm{N}_{k/\mathbf{Q}}(\alpha)$ divise 47^{22} et $\mathrm{N}_{k/\mathbf{Q}}(\zeta - 2)$. Calculer $\mathrm{N}_{k/\mathbf{Q}}(\alpha)$.
6) Montrer que k contient un corps K quadratique sur $\mathbf{Q}$ et un seul. Montrer que $K = \mathbf{Q}(\sqrt{-23})$.
7) Posons $\omega = \mathrm{N}_{k/K}(\alpha)$. Montrer que ω est un entier de K et que sa norme est 47.
8) Montrer que K ne contient pas d'entier de norme 47, et conclure.

Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
http://www.math.jussieu.fr/∼miw/

Master de sciences et technologies 1ère année -
Spécialité : Mathématiques Fondamentales

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Examen du jeudi 24 Mai 2007
Corrigé

Exercice 1. L'exemple habituel est $\mathbf{Q}(\sqrt[3]{2})$ dont la clôture normale est $\mathbf{Q}(\sqrt[3]{2}, j)$ où j est une racine primitive cubique de l'unité : $j^2 + j + 1 = 0$.

Exercice 2. En caractéristique 3 on a $X^{33} - 1 = (X^{11} - 1)^3$. Comme 11 est premier on a $X^{11} - 1 = (X - 1)\Phi_{11}(X)$ avec

$$\Phi_{11}(X) = X^{10} + X^9 + X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1.$$

Il reste à décomposer le polynôme $\Phi_n(X)$ sur $\mathbf{F}_q$ avec $n = 11$, $q = 3$ et la caractéristique $p = 3$ ne divise pas n. On sait par le cours que $\Phi_n(X)$ est produit de r polynômes irréductibles, tous de degrés $\varphi(n)/r$, où r est l'ordre de q modulo n. Ici $\varphi(11) = 10$ et $r = 5$ car 3 est d'ordre 5 modulo 11 :

$$3^2 \equiv -2 \pmod{11}, \qquad 3^5 \equiv 4 \times 3 \equiv 1 \pmod{11}.$$

Donc $\Phi_{11}(X)$ est produit de 2 facteurs irréductibles de degrés 5. Finalement pour répondre à la question, sur $\mathbf{F}_3$ le polynôme $X^{33} - 1$ est produit de 15 facteurs irréductibles (en comptant les multiplicités), trois sont distincts, un des facteurs irréductibles est de degré 1 et a pour multiplicité 3, les deux autres ont degré 5 et multiplicité 6.
`Remarque`. *On peut aussi écrire* $X^{33} - 1 = \Phi_1\Phi_3\Phi_{11}\Phi_{33}$. *On vérifie alors que* $\Phi_3 = \Phi_1^2$ *et* $\Phi_{33} = \Phi_{11}^2$ *dans* $\mathbf{F}_3[X]$. *En général en caractéristique* p *on a*

$$\Phi_{p^\alpha m} = \Phi_m^{\varphi(p^\alpha)}$$

si p *ne divise pas* m.

Exercice 3. Un théorème du cours affirme qu'un *entier* algébrique non nul est une unité si et seulement s'il est de norme 1. Ici il n'est pas précisé que le nombre algébrique est entier, donc ce théorème ne s'applique pas. Un exemple (donné dans le cours) de nombre algébrique α de norme 1 qui n'est pas une unité est

$$\frac{-1 + i\sqrt{15}}{4},$$

racine du polynôme $2X^2 + X + 2$.
On peut prendre un nombre quadratique non réel β (dans le cas présent $3 + i\sqrt{15}$) et le diviser par son conjugué complexe $\overline{\beta}$ (il faut juste éviter que le quotient ne soit une racine de l'unité). Un autre exemple avec $\beta = 1 + i\sqrt{2}$ on a

$$\alpha = \frac{\beta}{\overline{\beta}} = \frac{-1 + 2i\sqrt{2}}{3}$$

qui est racine du polynôme $3X^2 + 2X + 3$.
On peut aussi construire de tels α en prenant une racine d'un polynôme $aX^2 + bX + c \in \mathbf{Q}[X]$ ayant un discriminant $b^2 - 4ac$ négatif avec $c = \pm a$.

Exercice 4.

a) La minoration

$$\varphi(n) \geq n^{1/2}$$

est vraie si n est une puissance d'un nombre premier et $n \neq 2$: en effet pour $p \geq 3$ on a $p - 1 > \sqrt{p}$ et

$$p^k - p^{k-1} > p^{k-(1/2)} \geq p^{k/2}.$$

Pour $p = 2$ cette minoration est encore valable dès que $k \geq 2$. En décomposant n en facteurs premiers on en déduit $\varphi(n) \geq \sqrt{n/2}$ (le coefficient $1/2$ n'apparaît que quand n est congru à 2 modulo 4). Ceci démontre le résultat demandé avec $c = \kappa = 1/2$.
`Remarque`. *En étant plus soigneux on démontre que pour tout $\epsilon > 0$ il existe un entier $N > 0$ tel que pour tout $n \geq N$ on ait*

$$\varphi(n) > n^{1-\epsilon}.$$

*C'est équivalent à dire (*le démontrer !*) qu'on peut choisir pour κ n'importe quel nombre réel positif < 1.*

b) Comme $\varphi(p^a) = (p-1)p^{a-1}$ pour $a \geq 1$ et que $\varphi(1) = 1$, on a

$$\sum_{a \geq 0} \varphi(p^a)^{-s} = 1 + \sum_{k \geq 0} (p-1)^{-s} p^{-ks} = 1 + \frac{1}{(p-1)^s(1-p^{-s})}.$$

c) On écrit

$$1 + \frac{1}{(p-1)^s(1-p^{-s})} = \frac{1 + (p-1)^{-s} - p^{-s}}{1 - p^{-s}}.$$

Quand on fait le produit sur les nombres premiers p, on trouve à droite $\zeta(s)G(s)$. En utilisant le fait que la fonction φ est multiplicative, on vérifie qu'on trouve à gauche

$$\sum_{n \geq 1} \varphi(n)^{-s}.$$

Pour cela on écrit d'abord le produit sur les nombres premiers $\leq X$ et la somme sur n est restreinte aux entiers dont tous les facteurs premiers sont majorés par X, puis on fait tendre X vers l'infini, comme dans le cours. La convergence est assurée par la minoration de $\varphi(n)$ démontrée dans la question a).

Problème.

I. L'inclusion évidente est $\mathbf{Z}[\zeta] \subset \mathbf{Z}_k$ car $\zeta \in \mathbf{Z}_k$.

1) Le polynôme irréductible de ζ sur $\mathbf{Q}$ est

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1 = (X - \zeta)(X - \zeta^2) \cdots (X - \zeta^{p-1}).$$

Le corps $k = \mathbf{Q}(\zeta)$ a donc pour degré 10 sur $\mathbf{Q}$, les conjugués de ζ sur $\mathbf{Q}$ sont ζ, ζ^2, $\dots \zeta^{p-1}$. La norme de ζ sur $\mathbf{Q}$ est le produit de ces conjugués,

$$\mathrm{N}_{k/\mathbf{Q}}(\zeta) = \prod_{h=1}^{p-1} \zeta^h = \zeta^{p(p-1)/2} = 1.$$

Plus simplement, cette norme est le terme constant de Φ_p (avec le même signe car le degré $p-1$ de Φ_p est pair), à savoir $\Phi_p(0) = 1$. De même la trace est la somme des conjugués

$$\mathrm{Tr}_{k/\mathbf{Q}}(\zeta) = \sum_{h=1}^{p-1} \zeta^h = \frac{\zeta^p - \zeta}{\zeta - 1} = -1$$

et c'est aussi $-a_{p-2}$ où $a_{p-2} = 1$ est le coefficient de X^{p-2} dans Φ_p.

2) Le corps k est une extension galoisienne de $\mathbf{Q}$. Le groupe de Galois G est cyclique d'ordre $\varphi(p) = p-1$, isomorphe au groupe des unités de $\mathbf{Z}/p\mathbf{Z}$. Un élément de G est déterminé par sa valeur en ζ. Un isomorphisme de $(\mathbf{Z}/p\mathbf{Z})^\times$ sur G est l'application qui à une classe h modulo p avec $\mathrm{pgcd}(h,p) = 1$ associe l'automorphisme φ_h de k défini par $\varphi_h(\zeta) = \zeta^h$.

3) Comme $\pi = \zeta - 1$ et $\zeta = \pi + 1$ on a $\mathbf{Q}(\zeta) = \mathbf{Q}(\pi)$. Le polynôme irréductible de π est

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + pX^{p-2} + \binom{p}{2} X^{p-3} + \cdots + \binom{p}{p-2} X + p.$$

Les conjugués de π sont $\pi_h = \zeta^h - 1$, $(1 \le h \le p-1)$. La norme de π est le produit de ces conjugués, c'est aussi le coefficient constant du polynôme irréductible, à savoir p :

$$\mathrm{N}_{k/\mathbf{Q}}(\pi) = \prod_{h=1}^{p-1} \pi_h = p.$$

La trace de π est la somme des conjugués, c'est aussi le produit du coefficient de X^{p-2} par -1 :

$$\mathrm{Tr}_{k/\mathbf{Q}}(\zeta) = \sum_{h=1}^{p-1} \pi_h = -p.$$

4) Cela résulte de la relation

$$\zeta^{p-1} = -1 - \zeta - \cdots - \zeta^{p-2}.$$

Écrire les matrices de passage d'une des trois bases à une autre. Vérifier que les coefficients sont dans $\mathbf{Z}$ *et que les déterminants valent* ± 1.

5) Pour h entier positif on a

$$\frac{\zeta^h - 1}{\zeta - 1} = 1 + \zeta + \zeta^2 + \cdots + \zeta^{h-1} \in \mathbf{Z}[\zeta].$$

Soit h un entier dans l'intervalle $1 \leq h \leq p-1$. Alors h est premier avec p, donc il existe un entier j tel que $hj \equiv 1 \pmod{p}$. Par conséquent

$$\frac{\zeta - 1}{\zeta^h - 1} = \frac{(\zeta^h)^j - 1}{\zeta^h - 1} = 1 + \zeta^h + (\zeta^h)^2 + \cdots + (\zeta^h)^{j-1} \in \mathbf{Z}[\zeta].$$

Ceci montre que le quotient de π par un conjugué π' est une unité de $\mathbf{Z}[\zeta]$. En d'autres termes les deux idéaux principaux $\pi\mathbf{Z}[\zeta]$ et $\pi'\mathbf{Z}[\zeta]$ de l'anneau $\mathbf{Z}[\zeta]$ coïncident.

6) Pour $1 \leq h \leq p-1$ le quotient $\epsilon_h = \pi_h/\pi$ est une unité de $\mathbf{Z}[\zeta]$, donc $p = \mathrm{N}_{k/\mathbf{Q}}(\pi) = \epsilon\pi^{p-1}$ avec $\epsilon = \epsilon_1 \cdots \epsilon_{p-1} \in \mathbf{Z}[\zeta]^\times$.
`Correction du 25 Mai 2007 : dans la version distribuée le 24 Mai il était écrit` $\epsilon = \epsilon_1 \cdots \epsilon_{p-1} \in \mathbf{Z}_k^\times$. `C'est vrai mais ça ne suffit pas : c'est une unité de` $\mathbf{Z}[\zeta]$

7) Comme $p = \pi\alpha$ avec $\alpha = \pi_2 \cdots \pi_{p-1} \in \mathbf{Z}_k$, on a $p \in \pi\mathbf{Z}[\zeta]$, donc $p\mathbf{Z} \subset \pi\mathbf{Z}[\zeta] \cap \mathbf{Z}$.
Inversement, soit $n \in \pi\mathbf{Z}[\zeta] \cap \mathbf{Z}$. On écrit $n = \pi\gamma$ avec $\gamma \in \mathbf{Z}_k$. Alors la norme de π divise $\mathrm{N}_{k/\mathbf{Q}}(n) = n^{p-1}$, donc p divise n. On en déduit $p\mathbf{Z} = \pi\mathbf{Z}[\zeta] \cap \mathbf{Z}$.

8) Quand on compose l'injection de $\mathbf{Z}$ dans $\mathbf{Z}_k$ avec la surjection de $\mathbf{Z}_k$ sur le quotient par l'idéal $\pi\mathbf{Z}_k$, on obtient un homomorphisme d'anneaux de $\mathbf{Z}$ dans $\mathbf{Z}_k/\pi\mathbf{Z}_k$ de noyau $p\mathbf{Z}$. On en déduit un homomorphisme injectif ψ de $\mathbf{Z}/p\mathbf{Z}$ dans $\mathbf{Z}_k/\pi\mathbf{Z}_k$. Mais $\mathbf{Z}_k/\pi\mathbf{Z}_k$ a aussi $\mathrm{N}_{k/\mathbf{Q}}(\pi) = p$ éléments, donc ψ est un isomorphisme. En conclusion l'anneau $\mathbf{Z}_k/\pi\mathbf{Z}_k$ est un corps à p éléments et $\pi\mathbf{Z}_k$ est un idéal maximal de $\mathbf{Z}_k$.

9) a) On a

$$\alpha\pi = a_0\pi + a_1\zeta\pi + \cdots + a_{p-2}\zeta^{p-2}\pi.$$

La trace de π est $-p$ et celle de $\zeta^j\pi$ est nulle pour $1 \leq j \leq p-2$ car $\zeta^j\pi = \zeta^{j+1} - \zeta^j$. Donc

$$\mathrm{Tr}_{k/\mathbf{Q}}(\pi\alpha) = -pa_0 \in \mathbf{Z}.$$

Comme $\alpha\zeta^{-1}$ est entier et que

$$\alpha\zeta^{-1} = a_1 + a_2\zeta + \cdots + a_{p-2}\zeta^{p-3} + a_0\zeta^{p-1} = (a_1 - a_0) + (a_2 - a_0)\zeta + \cdots + (a_{p-2} - a_0)\zeta^{p-3} - a_0\zeta^{p-2},$$

on en déduit $pa_1 \in \mathbf{Z}$. Par récurrence on trouve $pa_j \in \mathbf{Z}$ pour $1 \leq h \leq p-2$.

b) On a

$$p\alpha = pa_0 + pa_1\zeta + \cdots + pa_{p-2}\zeta^{p-2}$$

avec $pa_i \in \mathbf{Z}$. En changeant de base (voir la question 4)) on trouve

$$p\alpha = b_0 + b_1\pi + \cdots + b_{p-2}\pi^{p-2}$$

avec $b_i \in \mathbf{Z}$ pour $0 \leq i \leq p-2$.
Dans $\mathbf{Z}[\zeta]$, π divise tous les $b_j\pi^j$ pour $1 \leq j \leq p-2$. Il divise aussi $p\alpha$. Il en résulte que π divise b_0. D'après la question 7), p divise b_0. Maintenant dans $\mathbf{Z}[\zeta]$, π^2 divise tous les $b_j\pi^j$ pour $2 \leq j \leq p-2$ et aussi pour $j = 0$, donc π^2 divise $b_1\pi$ et par conséquent π divise b_1. On montre en poursuivant que p divise $b_1, \ldots, b_{p-2}$.

c) Comme ζ est un entier algébrique, on a $\mathbf{Z}[\zeta] \subset \mathbf{Z}_k$. Nous venons de démontrer l'inclusion inverse

$$\mathbf{Z}_k \subset \mathbf{Z} + \mathbf{Z}\pi + \mathbf{Z}\pi^2 + \cdots + \mathbf{Z}\pi^{p-2} = \mathbf{Z}[\zeta].$$

II.

1) On a $47 \equiv -1 \mod 16$, donc $47^2 - 1 \equiv 0 \mod 16$, de sorte que $(-1)^{(47^2-1)/8} = 1$. La loi de réciprocité quadratique en 2 donne la valeur du symbole de Legendre

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Pour $p = 47$ on en déduit que 2 est un carré modulo 47, donc $2^{(47-1)/2} \equiv 1 \pmod{47}$, soit $2^{23} \equiv 1 \pmod{47}$.

2) Modulo $47^2 = 2209$ on a $2^{11} = 2048 \equiv -161$, d'où $2^{22} \equiv 161^2 \equiv 1622$ et donc $2^{23} \equiv 3244 \not\equiv 0$.

3) Le polynôme minimal de ζ est $F(X) = (X^{23} - 1)/(X - 1)$ et la norme de $\zeta - 2$ est sa valeur au point 2, c'est-à-dire $2^{23} - 1$.

4) Soit $\beta \in \mathfrak{a}$. On peut écrire $\beta = 47y + (\zeta - 2)z$ avec y et z dans $\mathbf{Z}_k$. La norme de β est le produit des conjugués ; on développe et on met 47 en facteur ; on obtient

$$\mathrm{N}_{k/\mathbf{Q}}(\beta) = 47t + \mathrm{N}_{k/\mathbf{Q}}(\zeta - 2)\mathrm{N}_{k/\mathbf{Q}}(z)$$

avec $t \in \mathbf{Z}_k \cap \mathbf{Q} = \mathbf{Z}$. Maintenant $\mathrm{N}_{k/\mathbf{Q}}(z)$ est un entier rationnel et 47 divise la norme de $\zeta - 2$, donc 47 divise $\mathrm{N}_{k/\mathbf{Q}}(\beta)$.
`Remarque`. *De façon générale, si m est un entier rationnel, α un entier algébrique, et p le pgcd de m et de $\mathrm{N}_{k/\mathbf{Q}}(\alpha)$, la norme de tout élément β de l'idéal engendré par m et α est divisible par p. En effet si $\beta = my + \alpha z$, la norme de β est un produit de conjugués de β. Un tel conjugué s'écrit $my' + \alpha' z'$, où y', α' et z' sont les conjugués correspondants de y, α et z respectivement. En développant le produit et en rassemblant tous les termes où m apparaît, on trouve $\mathrm{N}_{k/\mathbf{Q}}(\beta) = mt + \mathrm{N}_{k/\mathbf{Q}}(\alpha)\mathrm{N}_{k/\mathbf{Q}}(z)$. Comme $\mathrm{N}_{k/\mathbf{Q}}(\beta)$, $\mathrm{N}_{k/\mathbf{Q}}(\alpha)$ et $\mathrm{N}_{k/\mathbf{Q}}(z)$ sont rationnels, il en est de même de t. D'autre part, t est une somme de produits d'entiers algébriques, c'est donc un entier algébrique. En fin de compte, t est un entier rationnel, et $\mathrm{N}_{k/\mathbf{Q}}(\beta)$ appartient à l'idéal de $\mathbf{Z}$ engendré par m et $\mathrm{N}_{k/\mathbf{Q}}(\alpha)$. Ici $m = 47$, $\alpha = \zeta - 2$, le pgcd vaut $p = 47$, qui divise tout élément de l'idéal $\mathfrak{a}$ engendré par 47 et $\zeta - 2$.*

5) Comme $\mathfrak{a}$ contient $47\mathbf{Z}_k$ et $(\zeta - 2)\mathbf{Z}_k$, sa norme divise celle de chacun d'eux, c'est-à-dire 47^{22} et $2^{23} - 1$. Elle divise donc leur pgcd 47. D'après la question 4), $\mathfrak{a}$ ne contient pas 1, donc sa norme n'est pas 1. On a donc montré $\mathrm{N}(\mathfrak{a}) = 47$. Si $\mathfrak{a} = \alpha\mathbf{Z}_k$ on en déduit $\mathrm{N}_{k/\mathbf{Q}}(\alpha) = \pm 47$. Montrons que la norme absolue de tout élément x de k est positive. Notons $k^+ = \mathbf{Q}(\zeta + \zeta^{-1}) = k \cap \mathbf{R}$ le sous-corps réel de k. La norme $y = \mathrm{N}_{k/k^+}(x)$ est un élément de k^+ qui est *totalement positif*, c'est-à-dire que tous ses conjugués sont positifs. En effet, comme le groupe de Galois de $k/\mathbf{Q}$ est commutatif, chacun de ces conjugués est produit d'un conjugué de x par son conjugué complexe (la conjuguaison complexe commute aux automorphisme de k). On en déduit que $\mathrm{N}_{k/\mathbf{Q}}(x) = \mathrm{N}_{k^+/\mathbf{Q}}(y)$, qui est le produit de ces conjugués, est lui aussi positif. En conclusion, on a démontré que $\mathrm{N}_{k/\mathbf{Q}}(\alpha) = 47$.

6) Le groupe cyclique $\mathrm{Gal}(k/\mathbf{Q})$ d'ordre 22 a un seul sous-groupe d'indice 2. Le sous-corps correspondant par la théorie de Galois est un corps quadratique, engendré par la somme de Gauß $\sqrt{-23}$.

7) On a

$$47 = \mathrm{N}_{k/\mathbf{Q}}(\alpha) = \mathrm{N}_{K/\mathbf{Q}}(\mathrm{N}_{k/K}(\alpha)) = \mathrm{N}_{K/\mathbf{Q}}(\omega).$$

8) Comme ω est la norme d'un entier algébrique, c'est un entier algébrique. On sait que l'anneau des entiers de $\mathbf{Q}(\sqrt{-23})$ est engendré comme $\mathbf{Z}$-module par 1 et $(1+\sqrt{-23})/2$, on peut donc écrire $\omega = (a + b\sqrt{-23})/2$, où a et b sont deux entiers rationnels de même parité. L'équation $47 = \mathrm{N}_{K/\mathbf{Q}}(\omega)$ s'écrit alors $188 = a^2 + 23b^2$ et il est facile de voir qu'elle n'a pas de solution (on aurait $b^2 < 9$, donc $b^2 = 0$, 1 ou 4).