

# Correction feuille 5

## 1 Corps quadratiques

Soit  $K = \mathbb{Q}(\sqrt{d})$  un corps quadratique, de discriminant  $D$  égal à  $d$  ou  $4d$  selon que  $d$  est congru ou non à 1 modulo 4. Notons  $p_1, \dots, p_k$  les diviseurs premiers distincts de  $D$ , c'est-à-dire les nombres premiers de  $\mathbb{Z}$  qui se ramifient dans  $K$  et, pour chacun d'eux, notons  $\mathfrak{p}_i$  l'unique idéal premier de  $\mathcal{O}_K$  qui divise  $p_i$ , de sorte que  $p_i \mathcal{O}_K = \mathfrak{p}_i^2$ . Notons encore  $x \mapsto \bar{x}$  l'unique automorphisme non trivial de  $K$ , appelé conjugaison, même dans le cas réel ( $d > 0$ ).

**Exercice 1.** *Trouver un exemple de deux entiers d'un corps quadratique qui ont même norme sans être ni conjugués ni associés.*

*Preuve :* Dans l'anneau  $\mathbb{Z}[i]$  des entiers de Gauß, qui est l'anneau des entiers de  $\mathbb{Q}[i]$  et qui est principal, un nombre premier  $p$  est décomposé si et seulement si il est congru à 1 modulo 4. Dans ce cas, il se décompose en produit de deux entiers conjugués entre eux et premiers entre eux. par exemple  $5 = (1 + 2i)(1 - 2i)$ . Pour répondre à la question, on pourrait se contenter de prendre  $\alpha = 1 + 2i$  et  $\beta = i(1 - 2i) = 2 - i$ , mais ce serait tricher:  $\beta$  est associé au conjugué de  $\alpha$ . Mais si nous prenons un autre nombre premier décomposé, par exemple  $13 = (2 + 3i)(2 - 3i)$ , il suffit de prendre  $\alpha = (1 + 2i)(2 + 3i) = -4 + 7i$  et  $\beta = (1 + 2i)(2 - 3i) = 8 + i$  pour avoir un exemple:  $65 = 5.13 = 4^2 + 7^2 = 8^2 + 1$  s'écrit comme somme de deux carrés de deux façons essentiellement différentes, contrairement à 5 et à 13.

**Exercice 2.** *Montrer que, si  $\epsilon \in \mathbb{Q}(\sqrt{d})$  est une unité de norme 1 d'un corps quadratique, il existe un entier  $\gamma$  tel que  $\epsilon = \frac{\gamma'}{\gamma}$ , où  $\gamma'$  est le conjugué de  $\gamma$ .*

*Preuve :* Soit  $\alpha$  un entier quelconque de  $K$ . On pose  $\gamma = \alpha + \alpha'\epsilon$ . On a  $\epsilon\gamma' = \epsilon(\alpha' + \alpha\epsilon') = \gamma$ . Pour conclure, il reste à prouver que l'on peut choisir  $\alpha$  de façon à ce que  $\gamma$  ne soit pas nul. Si  $\epsilon \neq -1$ , on peut prendre  $\alpha = 1$ , sinon on prend  $\alpha = \sqrt{d}$ .

**Exercice 3.** *On considère le corps  $K = \mathbb{Q}(\sqrt{-43})$ . On pose  $\omega = \frac{-1 + \sqrt{-43}}{2}$ , et on rappelle que l'anneau des entiers de  $K$  admet  $\{1, \omega\}$  comme base sur  $\mathbb{Z}$ .*

- (1) *Calculer le polynôme minimal de  $\omega$  sur  $\mathbb{Q}$ . Montrer que 2 et 3 sont inertes dans  $K$ .*
- (2) *Calculer la constante de Minkowski de  $K$ . Montrer que  $\mathcal{O}$  est principal.*
- (3) *Soit  $\alpha \notin \mathbb{Z}$  un élément de  $\mathcal{O}$  qui engendre un idéal premier. Montrer que  $N_{L/\mathbb{Q}}(\alpha)$  est un nombre premier.*
- (4) *Soit  $x$  et  $y \neq 0$  deux entiers premiers entre eux tels que  $x^2 + xy + 11y^2$  soit strictement inférieur à 121. Montrer que  $x^2 + xy + 11y^2$  est un nombre premier.*

*Preuve :* (1) On a  $Tr(\omega) = \omega + \omega' = -1$  et  $N(\omega) = \omega\omega' = 11$ . Le polynôme minimal de  $\omega$  est donc  $X^2 + X + 11$ . Modulo 2 ou 3, ce polynôme est irréductible. La première proposition permet de conclure: 2 et 3 sont encore premiers dans  $K$ .

(2) Ici,  $n = 2$ ,  $t = 1$  et  $D_K = 43$ . La formule donne donc

$$M_K = \frac{4}{\pi} \frac{2}{4} \sqrt{43} = \frac{2\sqrt{43}}{\pi} < 5.$$

On vient de voir qu'il n'y a pas d'idéal de norme 2 ou 3, et que le seul idéal entier de norme 4 est  $2\mathcal{O}$ , qui est principal. Le théorème de Minkowski permet donc de conclure que  $K$  est principal.

(3) La norme d'un idéal premier d'un corps quadratique est soit un nombre premier ramifié ou décomposé, soit le carré  $p^2$  d'un nombre premier inerte  $p$ . Mais dans ce dernier cas, l'idéal en question est forcément  $p\mathcal{O}$ . Si  $\alpha\mathcal{O}$  et  $p\mathcal{O}$  sont égaux,  $\alpha/p$  est une unité de  $\mathcal{O}$ . Or, les seules unités de  $\mathcal{O}$  sont 1 et  $-1$ . Cela contredirait l'hypothèse selon laquelle  $\alpha$  n'appartient pas à  $\mathbb{Z}$ .

(4) La norme d'un entier de  $K$  qui n'est pas dans  $\mathbb{Z}$  vaut  $\frac{u^2+43v^2}{4} \geq \frac{43}{4}$ , et comme c'est un entier, elle vaut au moins 11. Considérons l'entier  $\alpha = x + y\omega$ . Il n'appartient pas à  $\mathbb{Z}$  puisque  $y \neq 0$ . Sa norme vaut  $\alpha\alpha' = x^2 + xy + 11y^2 < 121$ . Si ce n'était pas un nombre premier, il y aurait un diviseur premier de  $\alpha$  de norme inférieure à 11, et, d'après ce qui précède, son générateur  $a$  serait dans  $\mathbb{Z}$ . Mais si un entier rationnel  $a$  divise  $\alpha$ , il divise  $x$  et  $y$ , une contradiction.

On en déduit en particulier que  $x^2 + x + 11$  est un nombre premier pour  $x$  compris entre 0 et 9. Le même raisonnement avec  $\mathbb{Q}(\sqrt{-163})$  montre que  $x^2 + x + 41$  est premier pour  $x$  allant de 0 à 39.

**Exercice 4.** Soit  $K = \mathbb{Q}(\sqrt{-23})$  et  $\alpha = \frac{1+\sqrt{-23}}{2}$ .

(1) Calculer le polynôme minimal de  $\alpha$ , le discriminant  $D_K$  de  $K$  et la constante de Minkowski  $M_K$  de  $K$ .

(2) Montrer que les idéaux  $\mathfrak{p} = (2, \alpha)$  et  $\mathfrak{q} = (3, \alpha)$  sont premiers et non principaux.

(3) Donner la factorisation de  $2\mathcal{O}_K$  et  $3\mathcal{O}_K$  en produit d'idéaux premiers.

(4) Montrer que  $\mathfrak{p}^3$  est principal.

(5) Calculer le nombre de classes  $h_K$ . On pourra commencer par montrer que  $h_K$  est inférieur ou égal à 5.

*Preuve :* (1) La trace et la norme de  $\alpha$  valent respectivement 1 et 6. Le polynôme minimal de  $\alpha$  est donc  $P = X^2 - X + 6$ . Le discriminant de  $K$  est celui de  $\mathbb{Z}[\alpha]$  ou encore celui du polynôme, c'est-à-dire  $-23$ . La constante de Minkowski vaut

$$M_K = \left(\frac{4}{\pi}\right)^1 \frac{2!}{2^2} \sqrt{23} \approx 3.05.$$

(2) et (3) la décomposition dans  $K$  de 2 et de 3 reflète celle du polynôme  $P$  modulo 2 ou 3. On a  $P \equiv X(X-1) \pmod{2}$  et  $\pmod{3}$ , donc les idéaux  $\mathfrak{p} = (2, \alpha)$ ,  $\mathfrak{p}' = (2, \alpha - 1)$ ,  $\mathfrak{q} = (3, \alpha)$ ,  $\mathfrak{q}' = (3, \alpha - 1)$  sont premiers de norme respective 2, 2, 3 et 3, et l'on a  $2\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$  et  $3\mathcal{O}_K = \mathfrak{q}\mathfrak{q}'$ . Si  $\mathfrak{p}$  (resp.  $\mathfrak{q}$ ) était premier, il serait engendré par un entier de norme 2 (resp. 3). Il existerait donc une solution  $(a, b)$  entière à l'équation  $a^2 + 23b^2 = 8$  (resp.  $a^2 + 23b^2 = 12$ ), ce qui n'est pas le cas.

(4) L'équation  $a^2 + 23b^2 = 32$  a pour solutions entières  $(\pm 3, \pm 1)$ . On en déduit que  $\alpha + 1$  et  $2 - \alpha$  engendrent les seuls idéaux principaux de norme 8. Or les idéaux de norme 8 sont  $\mathfrak{p}^3$ ,  $\mathfrak{p}'^3$ ,  $2\mathfrak{p}$ ,  $2\mathfrak{p}'$ , et seuls les deux premiers peuvent être principaux. Reste à voir que  $2 - \alpha$  appartient à  $\mathfrak{p}$  pour en déduire

$$\mathfrak{p}^3 = (2 - \alpha)\mathcal{O}_K.$$

(5) Toute classe d'idéaux contient un idéal entier de norme inférieure ou égale à 3. Il y a exactement 5 tels idéaux: 1,  $\mathfrak{p}$ ,  $\mathfrak{p}'$ ,  $\mathfrak{q}$  et  $\mathfrak{q}'$ . Le nombre de classes  $h_K$  vaut donc au plus 5. Mais la question précédente montre que c'est un multiple de 3, d'où le résultat  $h_K = 3$ .

**Exercice 5.** Soit  $K = \mathbb{Q}(\sqrt{-5})$  et  $L = K(\sqrt{2})$ .

(1) Montrer que l'idéal  $\mathfrak{p} = (2, 1 + \sqrt{-5})$  de  $\mathcal{O}_K$  n'est pas principal, mais que son carré l'est. Calculer le nombre de classes de  $K$ .

(2) Montrer que  $\beta = \frac{1+\sqrt{-5}}{\sqrt{2}}$  est un entier de  $L$ . Montrer que l'idéal  $\mathfrak{p}' = \mathfrak{p}\mathcal{O}_L$  de  $\mathcal{O}_L$  est principal.

(3) Montrer que pour tout idéal  $\mathfrak{a}$  de  $\mathcal{O}_K$ ,  $\mathfrak{a}\mathcal{O}_L$  est principal.

*Preuve :* (1) Comme dans l'exercice précédent, on calcule la constante de Minkowski

$$M_K = (2/\pi)\sqrt{20} \approx 2.84.$$

Il suffit donc de considérer la décomposition de 2: modulo 2, on a  $X^2 + 5 \equiv (X + 1)^2$ , donc  $(2) = \mathfrak{p}^2$ , où  $\mathfrak{p} = (2, \sqrt{-5} + 1)$  est un idéal premier de norme 2, qui ne peut être principal puisque l'équation  $a^2 + 5b^2 = 2$  n'a pas de solution entière. Toute classe contient (1) ou  $\mathfrak{p}$  et le nombre de classes est 2.

(2) Comme  $\beta^2 = -2 + \sqrt{-5}$  est entier, il en est de même de  $\beta$ . Dans le groupe des idéaux fractionnaires de  $L$ , on a l'identité

$$(\mathfrak{p}\mathcal{O}_L)^2 = \mathfrak{p}^2\mathcal{O}_L = 2\mathcal{O}_L = (\sqrt{2}\mathcal{O}_L)^2.$$

Comme ce groupe est abélien libre, deux idéaux qui ont même carré sont égaux, donc  $\mathfrak{p}\mathcal{O}_L = \sqrt{2}\mathcal{O}_L$  est principal.

(3) Tout idéal  $\mathfrak{a}$  de  $\mathcal{O}_K$  est soit principal, soit équivalent à  $\mathfrak{p}$ , c'est-à-dire qu'il existe un élément  $\alpha$  de  $K^*$  tel que  $\mathfrak{a}$  soit égal à  $\alpha\mathcal{O}_K$  ou à  $\mathfrak{a} = \alpha\mathfrak{p}$ . Dans le premier cas, on a  $\mathfrak{a}\mathcal{O}_L = \alpha\mathcal{O}_L$  et dans le second  $\mathfrak{a}\mathcal{O}_L = \alpha\sqrt{2}\mathcal{O}_L$ .

*Remarque:* Cet exercice est un exemple simple du théorème suivant: pour tout corps de nombres  $K$ , il existe une extension abélienne finie  $L$  (le corps de classes de Hilbert) de  $K$  telle que tout idéal de  $K$  devienne principal dans  $L$ .

**Exercice 6.** Montrer que, si  $\mathfrak{a}$  est un idéal entier de  $K$  stable par conjugaison, c'est-à-dire si  $\mathfrak{a} = \bar{\mathfrak{a}}$ , alors il existe une partie  $H$  de  $\{1 \dots k\}$  et un entier naturel  $m$  tel que

$$\mathfrak{a} = m \prod_{i \in H} \mathfrak{p}_i.$$

*Preuve :* Dans l'écriture de  $\mathfrak{a}$  comme produit de puissances d'idéaux premiers, regroupons séparément les idéaux inertes, qui proviennent d'entiers naturels, les idéaux ramifiés, qui font partie des  $\mathfrak{p}_i$ , et les couples d'idéaux qui décomposent des nombres entiers. La condition sur  $\mathfrak{a}$  dit seulement que, dans une composante du type  $\mathfrak{p}^{n_p}\bar{\mathfrak{p}}^{n'_p}$ , on a  $n_p = n'_p$  et la composante vaut  $p^{n_p}\mathcal{O}_K$ . On trouve donc un produit de nombres entiers naturels pour les deux derniers types de contribution. Restent les  $\mathfrak{p}_i$ . La condition  $\mathfrak{p}_i\mathcal{O}_K = \bar{\mathfrak{p}}_i$  permet de réduire leurs exposants modulo 2, ce qui donne bien la forme annoncée ( $H$  est l'ensemble des  $i$  tels que  $\mathfrak{p}_i$  apparaisse à une puissance impaire dans la décomposition de  $\mathfrak{a}$ ).

**Exercice 7.** Démontrer un cas très particulier du théorème 90 de Hilbert: si  $x$  est un élément de norme 1 dans  $K$ , il existe un élément  $y$  de  $K^*$  tel que  $x = y/\bar{y}$ . On pourra chercher  $y$  sous la forme  $z + x\bar{z}$ .

*Preuve :* Posons  $y = z + x\bar{z}$ . On voit que  $x\bar{y} = x\bar{z} + x\bar{x}\bar{z} = y$ . Pour conclure, il faut prouver qu'il est possible de choisir  $z$  de façon que  $y$  ne soit pas nul. Si  $x \neq -1$  on peut prendre  $z = x$ . Pour  $x = -1$ , on peut prendre pour  $z$  n'importe quel élément non réel. En résumé, on a  $x = (x+1)/(\bar{x}+1)$  pour le cas général et  $-1 = \sqrt{d}/\sqrt{d}$  dans un cas particulier.

On notera  $Cl_K[2]$  le groupe des classes d'idéaux de carré trivial de  $K$ . C'est un  $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel.

**Exercice 8.** Soit  $\mathfrak{a}$  un idéal représentant d'un élément de  $Cl_K[2]$ , c'est-à-dire un idéal dont le carré est principal. Montrer qu'il existe un élément  $\alpha$  de  $K^*$  tel que  $\bar{\mathfrak{a}} = \alpha\mathfrak{a}$ . Montrer que  $\alpha$  ou  $\alpha^2$  est de norme 1 et en déduire l'existence d'un élément  $\beta$  de  $K^*$  tel que  $\beta\mathfrak{a}$  soit stable par conjugaison. En déduire que  $Cl_K[2]$  est engendré par les classes des idéaux  $\mathfrak{p}_i$ . Montrer que son ordre est un diviseur de  $2^{k-1}$ .

*Preuve :* Comme la norme  $\mathfrak{a}\bar{\mathfrak{a}}$  de  $\mathfrak{a}$  est engendré par un rationnel, c'est un idéal principal. Il en est de même par hypothèse de l'idéal  $\mathfrak{a}^2$ . Il en est donc encore de même de leur quotient  $\bar{\mathfrak{a}}/\mathfrak{a}$  qui est donc engendré par  $\alpha$ . On a donc  $\mathfrak{a} = \bar{\mathfrak{a}} = \alpha\bar{\mathfrak{a}} = \alpha\bar{\alpha}\mathfrak{a}$ . L'élément  $\alpha\bar{\alpha}$  est donc une unité rationnelle. C'est donc 1 ou -1 et la norme de  $\alpha^2$  vaut 1.

D'après l'exercice précédent, il existe un  $\beta$  dans  $K^*$  tel que  $\alpha^2 = \bar{\beta}/\beta$ . On en déduit que  $\beta\mathfrak{a}$  est un idéal stable par conjugaison, et le premier exercice nous permet d'écrire

$$\beta\mathfrak{a} = m \prod_{i \in H} \mathfrak{p}_i$$

et la classe de  $\mathfrak{a}$  est produit des classes des  $\mathfrak{p}_i$  pour  $i$  dans  $H$ .

On a donc trouvé un système générateur à  $k$  éléments du  $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel  $Cl_K[2]$ . Il reste à voir que ces éléments ne sont pas indépendants. En effet, si  $d$  est congru à 1 ou 2 modulo 4, le produit de tous les  $\mathfrak{p}_i$  est engendré par  $\sqrt{d}$ . Si  $d$  est congru 3 modulo 4,  $\sqrt{d}$  engendre le produit de tous les  $\mathfrak{p}_i$  sauf celui qui divise 2. Dans tous les cas, on a donc une relation non triviale entre les classes correspondantes dans  $Cl_K[2]$ .

**Exercice 9.** Acheter la démonstration du théorème 1 du cours: montrer que si  $D < 0$ , l'ordre de  $Cl_K[2]$  vaut exactement  $2^{k-1}$ , et que dans tous les cas, les groupes  $Cl_K[2]$  et  $Cl_K/2Cl_K$  sont isomorphes.

*Preuve :* Il est démontré dans le cours que si  $D < 0$ , il y a exactement une relation entre les classes des  $\mathfrak{p}_i$ . Le sous-groupe de  $Cl_K$  qu'ils engendrent, et qui est  $Cl_K[2]$ , est donc bien d'ordre  $2^{k-1}$ . Enfin, si  $A$  est un groupe abélien fini, et  $n$  un entier naturel, les groupes  $A[n]$  et  $A/nA$  sont toujours (non canoniquement) isomorphes: en effet, comme  $A$  est un produit de groupes cycliques, il suffit de le montrer pour  $A = \mathbb{Z}/m\mathbb{Z}$ . Il est facile de voir que dans ce cas, ces groupes sont tous deux isomorphes à  $\mathbb{Z}/d\mathbb{Z}$ , où  $d$  est le PGCD de  $m$  et  $n$ .

**Exercice 10.** Soit  $K = \mathbb{Q}(\sqrt{d})$  un corps quadratique réel, et  $\epsilon = \frac{x+y\sqrt{d}}{2}$  son unité fondamentale. Montrer que  $x$  et  $y$  sont positifs. Montrer que  $y$  est le plus petit entier naturel tel que  $dy^2$  diffère d'un carré par  $\pm 4$ . Calculer les unités fondamentales de  $\mathbb{Q}(\sqrt{d})$  pour  $d \in \{2, 3, 5, 6, 7, 10\}$ .

*Preuve :* Le conjugué  $\bar{\epsilon} = \frac{x-y\sqrt{d}}{2}$  de  $\epsilon$  est aussi une unité, et on a

$$\epsilon\bar{\epsilon} = \frac{x^2 - dy^2}{4} = \pm 1.$$

Comme  $\epsilon > 1$ , on en déduit  $|\bar{\epsilon}| < \epsilon$ , donc  $x = \epsilon + \bar{\epsilon} > 0$  et  $y\sqrt{d} = \epsilon - \bar{\epsilon} > 0$ . Les autres unités supérieures à 1 de  $K$  s'écrivent  $\epsilon^n = \frac{x_n + y_n\sqrt{d}}{2}$  et on a la relation de récurrence:

$$\begin{cases} x_{n+1} = \frac{xx_n + dy_n y_n}{2} \\ y_{n+1} = \frac{xy_n + yx_n}{2} \end{cases}$$

Si  $x \geq 2$ , on en déduit que la suite  $y_n$  est croissante. Si  $x = 1$ , l'équation  $x^2 - dy^2 = \pm 4$  implique que  $y = 1$ . Dans tous les cas,  $y$  est la plus petite valeur de la suite  $(y_n)_{n \in \mathbb{N}}$ . Comme toute solution en entiers de  $X^2 = dY^2 \pm 4$  correspond à un élément de la suite  $(\epsilon^n)_{n \in \mathbb{N}}$ , le résultat est démontré.

Pour  $d = 2, 3, 5, 6, 7, 10$ , les plus petites valeurs de  $y$  sont respectivement 2, 2, 1, 4, 6 et 2. Il n'y a qu'une valeur possible pour  $x$ , sauf pour  $d = 5$ , où on prend la plus petite. Finalement, les unités fondamentales sont  $1 + \sqrt{2}$ ,  $2 + \sqrt{3}$ ,  $\frac{1+\sqrt{5}}{2}$ ,  $5 + 2\sqrt{6}$ ,  $8 + 3\sqrt{7}$  et  $3 + \sqrt{10}$ , de norme respective  $-1, 1, -1, 1, 1$  et  $-1$ .

**Exercice 11.** On considère le corps quadratique imaginaire  $K = \mathbb{Q}(\sqrt{-13})$ , et on note  $\sigma$  son automorphisme non trivial.

(1) Démontrer les assertions suivantes:

- (a) L'anneau des entiers de  $K$  est  $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-13}$  et son discriminant vaut  $-52$ .
- (b)  $2\mathcal{O} = \mathfrak{p}^2$ , où  $\mathfrak{p} = \sigma(\mathfrak{p})$  est un idéal premier de  $\mathcal{O}$  qui n'est pas principal.
- (c)  $13\mathcal{O} = \mathfrak{q}^2$ , où  $\mathfrak{q} = \sigma(\mathfrak{q})$  est l'idéal premier engendré par  $\sqrt{-13}$ .
- (d)  $3\mathcal{O}$  est un idéal premier de  $\mathcal{O}$ .
- (e) Les seules unités de  $\mathcal{O}$  sont 1 et -1.

(2) Montrer que toute classe d'idéaux de  $K$  admet parmi ses représentants un idéal entier de norme inférieure à 5. Dédurre de ce qui précède que le nombre de classes de  $K$  vaut 2.

(3) Montrer que pour tout entier rationnel  $y$ , l'idéal  $\mathfrak{d}$  de  $\mathcal{O}$  engendré par  $y + \sqrt{-13}$  et  $y - \sqrt{-13}$  admet au plus  $\mathfrak{p}$  et  $\mathfrak{q}$  comme diviseurs premiers — autrement dit,  $\mathfrak{p}$  et  $\mathfrak{q}$  sont les seuls idéaux premiers pouvant contenir  $\mathfrak{d}$ .

(4) Soient  $\alpha, \beta$  des entiers naturels tels que  $(y + \sqrt{-13})\mathcal{O} = \mathfrak{c}\mathfrak{p}^\alpha\mathfrak{q}^\beta$ , où  $\mathfrak{c}$  est un idéal de  $\mathcal{O}$  qui n'est divisible ni par  $\mathfrak{p}$  ni par  $\mathfrak{q}$ . Montrer que  $\mathfrak{c}$  et  $\sigma(\mathfrak{c})$  n'ont pas de diviseur premier commun.

On désigne désormais par  $(x, y) \in \mathbb{Z}^2$  une solution en entiers rationnels de l'équation

$$Y^2 = X^3 - 13 \quad (*).$$

(5) Dédurre de la relation  $(x)^3 = (y + \sqrt{-13})(y - \sqrt{-13})$  l'existence d'un idéal  $\mathfrak{c}$  de  $\mathcal{O}$  et de deux entiers naturels  $a$  et  $b$  tels que

$$(y + \sqrt{-13})\mathcal{O} = (\mathfrak{c}\mathfrak{p}^a\mathfrak{q}^b)^3.$$

(6) Montrer que  $\mathfrak{c}\mathfrak{p}^a\mathfrak{q}^b$  est un idéal principal.

(7) En déduire qu'il existe des entiers rationnels  $u, v$  tels que

$$y = u^3 - 39uv^2 \quad , \quad 1 = v(3u^2 - 13v^2).$$

(8) Dans le taxi qui l'amène à la mairie-préfecture où il doit épouser Alice, Bernard s'aperçoit qu'en soustrayant le carré du dernier nombre de la plaque minéralogique de la voiture au cube de l'âge de sa fiancée, il pourrait se croire à Marseille. Alice est-elle en âge de se marier, et si oui, dans quelle ville sera célébré l'heureux événement ?

*Preuve :* Le corps  $K$  est corps de rupture du polynôme  $P = X^2 + 13$ .

(1) On a vu en cours le calcul de l'anneau des entiers d'un corps quadratique. Le (a) est donc déjà connu. Pour calculer la décomposition des idéaux premiers, il suffit d'après le (complément de) cours, de réduire le polynôme  $P$ . On a  $P \equiv (X + 1)^2 \pmod{2}$ ,  $P \equiv X^2 \pmod{13}$ , et  $P$  irréductible  $\pmod{3}$ . Ceci démontre les (b), (c) et (d), à part le fait que  $\mathfrak{p}$  n'est pas principal. Mais s'il l'était, un générateur  $x + y\sqrt{13}$  donnerait une solution entière à l'équation  $x^2 + 13y^2 = 2$  qui n'en a pas. De même, l'équation en entiers  $x^2 + 13y^2 = \pm 1$  n'a que les solutions triviales  $(1, 0)$  et  $(-1, 0)$ , d'où le v).

(2) Avec les notations du cours, on a  $n = 2$  et  $t = 1$ . La constante de Minkowski de  $K$  vaut donc

$$M_K = \frac{4}{\pi} \cdot \frac{2}{4} \cdot \sqrt{52} = \frac{4\sqrt{13}}{\pi} \approx 4.6 < 5,$$

d'où la première affirmation. Les seuls idéaux entiers de norme inférieure à 5 sont  $\mathcal{O}$ ,  $\mathfrak{p}$  et  $2\mathcal{O}$ . Il y a donc au plus une classe non principale (celle de  $\mathfrak{p}$ ), et comme on a vu qu'elle ne l'était effectivement pas, il y a exactement deux classes distinctes.

(3) Un tel idéal doit contenir leur différence  $2\sqrt{13}$ , donc  $\mathfrak{d} \mid 2\sqrt{13}\mathcal{O} = \mathfrak{p}^2\mathfrak{q}$ , donc les seuls (idéaux) diviseurs premiers de  $\mathfrak{d}$  sont au plus  $\mathfrak{p}$  et  $\mathfrak{q}$ .

(4) On a  $(y - \sqrt{-13})\mathcal{O} = \sigma((y + \sqrt{-13})\mathcal{O}) = \sigma(\mathfrak{c}\mathfrak{p}^\alpha\mathfrak{q}^\beta) = \sigma(\mathfrak{c})\mathfrak{p}^\alpha\mathfrak{q}^\beta$ . Tout (idéal) premier facteur commun entre  $\mathfrak{c}$  et  $\sigma(\mathfrak{c})$  serait un facteur commun entre  $y - \sqrt{-13}$  et  $y + \sqrt{-13}$ , donc  $\mathfrak{p}$  ou  $\mathfrak{q}$ , qui ne peuvent diviser  $\mathfrak{c}$ .

(5) Ecrivons comme au (4)  $(y + \sqrt{-13})\mathcal{O} = \mathfrak{c}'\mathfrak{p}^\alpha\mathfrak{q}^\beta$ , où  $\mathfrak{c}'$  est un idéal de  $\mathcal{O}$  qui n'est divisible ni par  $\mathfrak{p}$  ni par  $\mathfrak{q}$ . On a

$$(x)^3 = (y + \sqrt{-13})\mathcal{O}\sigma((y + \sqrt{-13})\mathcal{O}) = \mathfrak{c}'\mathfrak{p}^\alpha\mathfrak{q}^\beta\sigma(\mathfrak{c}'\mathfrak{p}^\alpha\mathfrak{q}^\beta) = \mathfrak{c}'\sigma(\mathfrak{c}')\mathfrak{p}^{2\alpha}\mathfrak{q}^{2\beta},$$

cette dernière décomposition étant en quatre facteurs premiers entre eux deux à deux. On en déduit que chacun des quatre facteurs est lui-même le cube d'un idéal entier,  $\mathfrak{c}' = \mathfrak{c}^3$ ,  $\alpha = 3a$  et  $\beta = 3b$ , d'où le résultat.

(6) Le groupe des classes d'idéaux a deux éléments; la multiplication par 3 est donc l'identité sur ce groupe: un idéal est principal si et seulement si son cube l'est. C'est donc le cas de  $\mathfrak{c}\mathfrak{p}^a\mathfrak{q}^b$  dont le cube est engendré par  $y + \sqrt{-13}$ .

(7) Notons  $u + v\sqrt{-13}$  un générateur de l'idéal  $\mathfrak{c}\mathfrak{p}^a\mathfrak{q}^b$ . Le cube de cet entier est un générateur de  $(y + \sqrt{-13})\mathcal{O}$ , c'est-à-dire qu'il vaut  $\pm((y + \sqrt{-13}))$ . En changeant au besoin les signes de  $u$  et  $v$ , on choisit le signe +, d'où l'équation  $y + \sqrt{-13} = (u + v\sqrt{-13})^3$  qui donne celles du texte.

(8) La deuxième équation impose  $v = -1$  et  $u = \pm 2$ , et la première  $y = \pm 70$ , d'où  $x = u^2 + 13v^2 = 17$ . Alice a 17 ans et le mariage a lieu à Vesoul.

## 2 Corps de nombres

**Exercice 1.** Dans  $K = \mathbb{Q}(\theta = \sqrt[4]{5})$ , calculer les discriminants

$$\Delta(1, \theta, \theta^2, \theta^3),$$

$$\Delta(1 + \theta, 1 + \theta^2, 1 + \theta^3, 1 + \theta^4)$$

$$\Delta(1, \theta, \frac{1 + \theta^2}{2}, \frac{\theta + \theta^3}{2}).$$

*Preuve :* Comme indiqué dans le cours, le discriminant de la base  $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$  où  $\theta$  est racine d'un polynôme  $F$  irréductible de degré  $n$  vaut  $(-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(F'(\theta))$ . Ici  $F = X^4 - 5$ , donc  $F'(\theta) = 4\theta^3$  et

$$\Delta(1, \theta, \theta^2, \theta^3) = N_{K/\mathbb{Q}}(F'(\theta)) = 4^4 N_{K/\mathbb{Q}}(\theta)^3 = 4^4 \cdot (-5)^3 = -32000.$$

Compte tenu de l'égalité  $\theta^4 = 5$ , la matrice de passage de la première base à la deuxième est

$$\begin{pmatrix} 1 & 0 & 0 & 6 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

et son déterminant est  $-6$ . On en déduit

$$\Delta(1 + \theta, 1 + \theta^2, 1 + \theta^3, 1 + \theta^4) = 6^2 \cdot \Delta(1, \theta, \theta^2, \theta^3) = -1152000.$$

De même, la matrice

$$\begin{pmatrix} 1 & 0 & 1/2 & 0 \\ 0 & 1 & 0 & 1/2 \\ 0 & 0 & 1/2 & 0 \\ 0 & 0 & 0 & 1/2 \end{pmatrix}$$

a pour déterminant  $1/4$ , ce qui donne

$$\Delta\left(1, \theta, \frac{1 + \theta^2}{2}, \frac{\theta + \theta^3}{2}\right) = 4^{-2} \cdot \Delta(1, \theta, \theta^2, \theta^3) = -2000.$$

**Exercice 2.** *Montrer qu'un entier algébrique dont tous les conjugués (dans  $\mathbb{C}$ ) sont de module strictement inférieur à 1 est forcément nul.*

*Preuve :* Soit  $\alpha$  un tel entier, de degré  $n$ ,  $\kappa < 1$  le plus grand module d'un conjugué de  $\alpha$  et  $k$  un entier tel que  $\kappa^k < 2^{-n}$ . Considérons l'entier algébrique  $\beta = \alpha^k$ . Les coefficients de son polynôme caractéristique sont sommes de produits de conjugués de  $\beta$ : chaque conjugué est de module inférieur à  $\kappa^k$  et chaque somme comporte moins de  $2^n$  termes. Ces coefficients sont donc des entiers rationnels de valeur absolue strictement inférieure à 1, c'est-à-dire qu'ils sont nuls. Le polynôme caractéristique de  $\beta$  est  $X^n$  et  $\alpha = \beta = 0$ .

**Exercice 3.** *Montrer qu'un entier algébrique dont tous les conjugués (dans  $\mathbb{C}$ ) sont de module inférieur ou égal à 1 est une racine de l'unité ou est nul.*

*Preuve :* Soit  $\alpha$  un tel entier, de degré  $n$ . Pour tout entier naturel  $k$ , considérons l'entier algébrique  $\beta = \alpha^k$ . Les coefficients de son polynôme caractéristique sont sommes de produits de conjugués de  $\beta$ . Chaque conjugué est inférieur ou égal à 1 et chaque somme comporte moins de  $2^n$  termes. Ces coefficients sont donc des entiers rationnels de valeur absolue inférieure à  $2^n$ . Il n'y a qu'un nombre fini de tels polynômes, donc la suite  $\alpha^k$  ne prend qu'un nombre fini de valeurs distinctes, d'où le résultat.

**Exercice 4.** *Montrer que, dans un corps de nombres  $K$  de degré  $n$ , tout idéal (entier) non nul contient une infinité d'entiers naturels mais que, si  $b$  est un entier naturel non nul, il n'est pas contenu dans plus de  $b^n$  idéaux entiers.*

*Preuve :* Tout idéal entier non nul  $\mathfrak{a}$  contient sa norme, qui est un entier naturel non nul. Il contient aussi tous les multiples de cette norme, qui sont en nombre infini. Inversement, comme indiqué dans l'introduction, tout idéal qui contient  $b$  est engendré par  $b$  et un autre entier, disons  $x$ . Exprimons  $x$  dans une base d'entiers, et réduisons ses composantes modulo  $b$ . Le nombre de valeurs possibles de  $x$  est inférieur ou égal à  $b^n$ , d'où le résultat. Il est facile de voir que, même pour  $n = 1$ , cette majoration est grossière.

**Exercice 5.** *Dans tout le problème,  $K$  désigne le corps  $\mathbb{Q}(\alpha)$ , avec  $\alpha^3 = 17$ , et  $A$  désigne l'anneau des entiers de  $K$*

(1) *Donner la décomposition en idéaux premiers de  $17A$ .*

- (2) Donner la forme de la décomposition en idéaux premiers de  $7A$ ,  $5A$  et  $2A$ . Dans chaque cas, on calculera le nombre de diviseurs premiers distincts, leur indice de ramification et leur degré résiduel.
- (3) On pose  $\beta = \frac{1-\alpha+\alpha^2}{3}$ . Calculer  $(\alpha+1)\beta$ . En déduire que  $\beta$  est racine du polynôme  $P = X^3 - X^2 + 6X - 12$ . Calculer les discriminants des bases  $\{1, \alpha, \alpha^2\}$  et  $\{1, \alpha, \beta\}$  de  $K/\mathbb{Q}$ . En déduire que cette dernière est une base de  $A$  comme  $\mathbb{Z}$ -module.
- (4) Montrer que  $\beta - 1$  n'appartient à aucun idéal premier de degré résiduel 2. À l'aide des idéaux premiers énumérés au b), trouver la décomposition en produit d'idéaux premiers de  $(\beta - 2)A$  et  $(\alpha - 3)A$ . En déduire que les idéaux premiers en question sont tous principaux.
- (5) Écrire la décomposition en produit d'idéaux premiers des idéaux  $\beta A$  et  $(\beta - 1)A$ , et trouver des générateurs de deux idéaux premiers divisant  $3A$ . Calculer  $\frac{(\beta-1)\beta^2}{2(\beta-2)}$  et en déduire la décomposition en produit d'idéaux premiers de  $3A$ .
- (6) Montrer que les idéaux fractionnaires de  $A$  sont tous principaux.
- (7) On pose  $\gamma = \frac{3}{\alpha-2}$ . Décomposer en produit d'idéaux premiers l'idéal  $(\alpha+1)A$ , puis  $\gamma A$ . Calculer le polynôme minimal  $Q$  de  $\gamma$  sur  $\mathbb{Q}$  et montrer que  $\{1, \gamma, \gamma^2\}$  est une base du  $\mathbb{Z}$ -module  $A$ . Trouver la décomposition en produit d'idéaux premiers de  $Q'(\gamma)A$  et calculer  $|N_{K/\mathbb{Q}}(Q'(\gamma))|$ .

*Preuve :* (1) Soit  $\mathfrak{p}_{17}$  un idéal premier divisant  $\alpha A$ . De l'identité  $17A = \alpha^3 A = (\alpha A)^3$  on tire que  $\mathfrak{p}_{17}^3$  divise  $17A$ . Mais la décomposition de  $17A$  est de la forme  $\prod_{i=1}^g \mathfrak{p}_i^{e_i}$ , avec  $\sum_{i=1}^g e_i f_i = 3$ . On en déduit que  $g = 1 = f_1$  et  $e_1 = 3$ , c'est-à-dire que  $\alpha A = \mathfrak{p}_{17}$  est premier et  $17A = \mathfrak{p}_{17}^3$ . On dit que 17 est *totalelement ramifié* dans  $K$ .

(2) Commençons par calculer la décomposition en produit de polynômes irréductibles du polynôme  $X^3 - 17$  modulo 2, 5 et 7. On trouve

$$X^3 - 17 \equiv \begin{cases} (X+1)(X^2+X+1) \pmod{2} \\ (X+2)(X^2+2X+1) \pmod{5} \\ X^3+4 \pmod{7} \end{cases}$$

c'est-à-dire que, dans chaque cas, le polynôme est scindé modulo  $p$ . D'après l'introduction, la décomposition des nombres premiers reflète directement celle du polynôme:

$$2A = \mathfrak{p}_2 \mathfrak{p}_4, \quad 5A = \mathfrak{p}_5 \mathfrak{p}_{25},$$

où  $\mathfrak{p}_k$  est de norme  $k$  et 7 est inerte dans  $A$ . Les degrés résiduels sont 1 pour  $\mathfrak{p}_2$  et  $\mathfrak{p}_5$ , 2 pour  $\mathfrak{p}_4$  et  $\mathfrak{p}_{25}$  et 3 pour 7. Enfin, tous les indices de ramification valent 1.

(3) On a  $(\alpha+1)\beta = (1+\alpha^3)/3 = 6$ . On a donc directement  $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$  et  $0 = (6/\beta - 1)^3 - 17 = 216/\beta^3 - 108/\beta^2 + 18/\beta - 18$ . En multipliant par  $-\beta^3/18$ , on trouve  $\beta^3 - \beta^2 + 6\beta - 12 = 0$  et  $\beta$  appartient à  $A$ . Le discriminant de  $\{1, \alpha, \alpha^2\}$  vaut  $D(1, \alpha, \alpha^2) = -N_{K/\mathbb{Q}}(3\alpha^2) = 3^3 17^2$ . Le déterminant de la matrice de passage de  $\{1, \alpha, \alpha^2\}$  à  $\{1, \alpha, \beta\}$  valant  $1/3$ , on en déduit que  $D(1, \alpha, \beta) = -3 \cdot 17^2$ . Comme 17 est ramifié dans  $K$  (voir a)), il doit diviser le discriminant de  $K$ . Le seul facteur carré restant ne peut être retiré, donc le discriminant de  $K$  vaut  $-3 \cdot 17^2$  et  $\{1, \alpha, \beta\}$  est une base d'entiers.

(4) Comme  $P$  est le polynôme minimal de  $\beta$ , la norme de  $\beta - 1$  vaut  $-P(1) = 6$ , qui n'est pas divisible par un carré d'entier autre que 1. La décomposition en idéaux premiers de  $(\beta - 1)A$  fait intervenir un diviseur de 2: ce ne peut être que  $\mathfrak{p}_2$ , donc  $(\beta - 1) \in \mathfrak{p}_2$ . De même, de  $P(2) = 4$ , on déduit que  $\beta - 2$  appartient à  $\mathfrak{p}_2$  ou  $\mathfrak{p}_4$ . Mais si  $\beta - 2$  appartenait à  $\mathfrak{p}_2$ ,  $1 = (\beta - 1) - (\beta - 2)$  aussi, ce qui est impossible. Donc  $\mathfrak{p}_4 = (\beta - 2)A$  et  $\mathfrak{p}_2 = \frac{2}{\beta-2}A$  sont principaux. Enfin, la norme de  $\alpha - 3$  vaut  $-(3^3 - 17) = -10$ , ce qui donne une décomposition  $(\alpha - 3)A = \mathfrak{p}_2 \mathfrak{p}_5$ , donc  $\mathfrak{p}_5 = \frac{(\alpha-3)(\beta-2)}{2}A$  et  $\mathfrak{p}_{25} = \frac{10}{(\alpha-3)(\beta-2)}A$ .

(5) Comme  $N(\beta) = 12$ ,  $\beta$  appartient à  $\mathfrak{p}_2$  ou  $\mathfrak{p}_4$ . Mais  $\beta$  appartient à  $\mathfrak{p}_2$ , donc  $\beta$  ne peut pas lui appartenir, donc  $\beta$  est un multiple du générateur  $\beta - 2$  de  $\mathfrak{p}_4$ . Le calcul des normes montre que  $\mathfrak{p}_3 = \frac{\beta}{\beta-2}A$  est un idéal premier de norme 3. Le même raisonnement, en remplaçant  $\beta$  par  $\beta - 1$ , montre que  $\mathfrak{p}'_3 = \frac{(\beta-1)(\beta-2)}{2}A$  est un idéal premier de norme 3 qui contient  $\beta - 1$ . Il ne peut être égal à  $\mathfrak{p}_3$  puisque  $\beta$  et  $\beta - 1$  ne peuvent appartenir au même idéal premier. Un calcul direct montre que  $\frac{(\beta-1)\beta^2}{2(\beta-2)} = \frac{12-6\beta}{2(\beta-2)} = -3$ , donc

$$3A = \frac{(\beta-1)\beta^2}{2(\beta-2)}A = \left(\frac{\beta}{\beta-2}\right)^2 \cdot \frac{(\beta-1)(\beta-2)}{2}A = \mathfrak{p}_3^2 \mathfrak{p}'_3.$$

(6) Le corps  $K$  a un plongement réel et deux plongements complexe. la borne de Minkowski vaut ici

$$\frac{4}{\pi} \cdot \frac{6}{27} \cdot 17 \cdot \sqrt{3} \sim 8,3 < 9.$$

On a vu que tous les idéaux premiers de norme inférieure à 9 était principaux. Il en est de même des idéaux entiers de norme inférieure à 9 et, d'après le Théorème de Minkowski, de tous les idéaux.

(8) De  $(\alpha + 1 = 6/\beta)$ , on tire

$$(\alpha + 1)A = \frac{2A \cdot 3A}{\beta A} = \frac{\mathfrak{p}_2 \mathfrak{p}_4 \mathfrak{p}_3^2 \mathfrak{p}'_3}{\mathfrak{p}_4 \mathfrak{p}_3} = \mathfrak{p}_2 \mathfrak{p}_3 \mathfrak{p}'_3.$$

On en déduit que  $\alpha - 2 = \alpha + 1 - 3$  appartient à  $\mathfrak{p}_3 \mathfrak{p}'_3$ , ce qui donne, en comparant les normes  $(\alpha - 2)A = \mathfrak{p}_3 \mathfrak{p}'_3$  et

$$\gamma A = \frac{3A}{(\alpha - 2)A} = \frac{\mathfrak{p}_3^2 \mathfrak{p}'_3}{\mathfrak{p}_3 \mathfrak{p}'_3} = \mathfrak{p}_3.$$

De  $\alpha = 3/\gamma + 2$  on tire comme au c) le polynôme minimal  $Q(X) = X^3 - 4X^2 - 6X + 3$ . Le discriminant de la base  $\{1, \gamma, \gamma^2\}$  est le déterminant de la matrice  $Tr_{K/\mathbb{Q}}(\gamma^{i+j})$ , c'est-à-dire

$$\begin{vmatrix} 3 & 4 & 28 \\ 4 & 28 & 145 \\ 28 & 145 & 760 \end{vmatrix} = -3 \cdot 17^2 = D_K.$$

On en déduit que  $\{1, \gamma, \gamma^2\}$  est une base d'entiers de  $K$ . Le discriminant de cette base vaut  $-N_{K/\mathbb{Q}}(Q'(\gamma))$ , donc la norme de l'idéal  $Q'(\gamma)A$  vaut  $3 \cdot 17^2$ . la décomposition de  $Q'(\gamma)A$  ne peut donc être que  $\mathfrak{p}_3 \cdot \mathfrak{p}_{17}^2$  ou  $\mathfrak{p}'_3 \mathfrak{p}_{17}^2$ . On peut vérifier que la première possibilité est la bonne par le calcul de  $Q'(\gamma) = 3\gamma^2 - 8\gamma - 6 \in \gamma A = \mathfrak{p}_3$ . Cet idéal  $Q'(\gamma)A$  est appelé la *différente* de l'extension  $K/\mathbb{Q}$ . Ses diviseurs premiers sont précisément ceux qui sont ramifiés au dessus de  $\mathbb{Q}$ , et sa norme absolue est le déterminant de  $K$ .

**Exercice 6.** Soit  $\theta$  une racine d'un polynôme  $F$  de  $\mathbb{Z}[X]$  unitaire de degré  $n$  irréductible sur  $\mathbb{Q}$ ,  $K = \mathbb{Q}(\theta)$ ,  $\mathcal{O}$  l'anneau des entiers de  $K$ , et  $D$  le discriminant de  $K$ . On note  $k$  l'indice  $[\mathcal{O} : R]$  de l'anneau  $R = \mathbb{Z}[\theta]$  dans  $\mathcal{O}$ , et  $D_\theta$  le discriminant de la base  $\{1, \theta, \dots, \theta^{n-1}\}$  de  $K$  sur  $\mathbb{Q}$ .

- (1) Exprimer  $D_\theta$  en fonction de  $D$  et de  $k$ . Montrer que, si un nombre premier  $q$  ne divise pas  $D_\theta$ , il ne divise pas non plus  $k$ .
- (2) Soit  $p$  un nombre premier. On suppose que  $F$  est un polynôme d'Eisenstein relativement à  $p$  ( $p$  divise tous les coefficients sauf le coefficient dominant, et  $p^2$  ne divise pas le coefficient constant). On note  $\mathfrak{p}$  l'idéal de  $\mathcal{O}$  engendré par  $p$  et  $\theta$ . Montrer que la norme  $N\mathfrak{p}$  de  $\mathfrak{p}$  divise  $p^n$  et  $N_{K/\mathbb{Q}}(\theta)$ . En déduire que  $N\mathfrak{p} = p$ , que  $\mathfrak{p}$  est un idéal premier de degré résiduel 1 et que  $\mathfrak{p}\mathcal{O} = \mathfrak{p}^n$ .
- (3) Montrer que  $\theta^{n-1}$  n'appartient pas à  $\mathfrak{p}^n$ . En déduire que pour tout entier  $i$  compris entre 1 et  $n$ ,  $\theta^i$  n'appartient pas à  $\mathfrak{p}^{i+1}$ , et que tout élément de  $\mathcal{O}$  est congru modulo le sous-groupe  $\mathfrak{p}\mathcal{O}$  à un élément de  $R$ .
- (4) Montrer que  $p$  ne divise pas l'indice  $k$  de  $R$  dans  $\mathcal{O}$ .
- (5) On considère désormais le cas  $\theta = \sqrt[5]{2}$ . Montrer que l'indice  $k$  de  $R$  dans  $\mathcal{O}$  n'est pas divisible par 2.
- (6) Calculer le polynôme minimal de  $\theta - 2$ . Montrer que 5 ne divise pas  $k$ .
- (7) Montrer que dans ce cas  $\mathcal{O}$  est égal à  $R$ .

*Preuve :* (1) Soit  $\{\omega_1, \dots, \omega_n\}$  une base d'entiers de  $K$ , et  $P$  la matrice de passage de la base  $\{\omega_1, \dots, \omega_n\}$  à la base  $\{1, \theta, \dots, \theta^{n-1}\}$ . Cette matrice est à coefficients entiers, et son déterminant est égal, au signe près, à l'indice  $k$  de  $R$  dans  $\mathcal{O}$ . On a donc  $|\det(P)| = k$  et la proposition 2 du cours donne

$$D_\theta = \text{disc}(1, \theta, \dots, \theta^{n-1}) = \text{disc}(\omega_1, \dots, \omega_n)(\det(P))^2 = k^2 D.$$



On en déduit que, si  $q$  est un nombre premier qui divise  $k$ , alors  $q^2$  divise  $D_\theta$ .

(2) L'idéal  $\mathfrak{p}$  contient  $p$  et  $\theta$ . Sa norme divise donc  $p^n = N_{K/\mathbb{Q}}(p)$  et  $N_{K/\mathbb{Q}}(\theta)$  qui est, au signe près, le coefficient constant de  $F$ . Elle divise donc leur pgcd, qui est  $p$  puisque  $F$  est un polynôme d'Eisenstein. De la relation  $F(\theta) = 0$  on tire que  $\theta^n$  appartient à  $p\mathcal{O}$ . Donc  $(\mathfrak{p})^n \subset p\mathcal{O}$ , donc  $p^n = N(p\mathcal{O})$  divise  $N(\mathfrak{p}^n) = (N\mathfrak{p})^n$ , donc  $p$  divise  $N\mathfrak{p}$ , et finalement  $N\mathfrak{p} = p$ . L'idéal  $\mathfrak{p}^n$  divise  $p\mathcal{O}$  et a même norme que lui: il lui est égal. La décomposition de  $p\mathcal{O}$  en idéaux premiers est donc  $n$  fois celle de  $\mathfrak{p}$ . Or on sait que la somme des  $e_i f_i$  vaut  $n$ . On en déduit qu'il n'y a qu'un idéal premier au dessus de  $p$  et que  $e_1 = n$  et  $f_1 = 1$ .

(3) La norme de  $\theta^i$  est divisible par  $p^i$  mais pas par  $p^{i+1}$ . On en déduit que  $\theta^i$  appartient à  $\mathfrak{p}^i$  mais pas à  $\mathfrak{p}^{i+1}$ . Un élément  $\sum_{i=0}^{n-1} \theta^i$  de  $R$  qui appartient à  $p\mathcal{O}$  vérifie donc  $p|a_0$ , puis  $p|a_1$  et ainsi de suite jusqu'à  $p|a_{n-1}$ . On en déduit que les  $p^n$  éléments de  $R$  dont les coordonnées  $a_i$  sont toutes comprises entre 0 et  $p-1$  appartiennent à des classes différentes modulo  $p\mathcal{O}$ . Or il y a  $N(p\mathcal{O}) = p^n$  classes distinctes. Ces éléments forment donc un système de représentants de  $\mathcal{O}/p\mathcal{O}$ : tout élément de  $\mathcal{O}$  est congru modulo  $p$  à un et un seul élément de  $R$  à coordonnées dans la base  $\{1, \theta, \dots, \theta^{n-1}\}$  comprises entre 0 et  $p-1$ .

(4) Supposons que  $p$  divise l'indice  $k$  de  $R$  dans  $\mathcal{O}$ . le groupe  $\mathcal{O}/R$  a pour ordre  $k$ , et contient donc un élément d'ordre  $p$ . Il existe donc un élément  $\alpha$  de  $\mathcal{O}$  qui n'est pas dans  $R$  mais tel que  $p\alpha$  soit dans  $R$ . D'après la question précédente, l'intersection de  $p\mathcal{O}$  et de  $R$  est  $pR$ . On en déduit que  $p\alpha$  appartient à  $pR$  et  $\alpha$  appartient à  $R$ , une contradiction.

(5) On pose  $F = X^5 - 2$  et  $p = 2$ . On a bien un polynôme d'Eisenstein, et on peut appliquer le résultat de la question 4.

(6) Le polynôme minimal de  $\theta - 2$  est  $F(X + 2) = X^5 + 10X^4 + 40X^3 + 80X^2 + 80X + 30$ . C'est un polynôme d'Eisenstein pour  $p = 5$ , donc 5 ne divise pas l'indice dans  $\mathcal{O}$  de  $\mathbb{Z}[\theta - 2] = \mathbb{Z}[\theta]$ .

(7) Le discriminant de  $F$  vaut  $N_{K/\mathbb{Q}}F'(\theta) = 5^5(N_{K/\mathbb{Q}}(\theta))^4 = 50000$  et a pour seuls facteurs premiers 2 et 5. On a vu à la question 1 que seuls 2 et 5 pourraient diviser  $k$ , et aux questions 5 et 6 que  $k$  n'est pas non plus divisible par 2 ni par 5. Le nombre entier naturel  $k$  n'a aucun diviseur premier. Donc  $k$  égale 1 et  $\mathcal{O}$  égale  $R$ .

**Exercice 7.** On note  $\zeta = e^{\frac{2i\pi}{23}}$  et  $L = \mathbb{Q}(\zeta)$ . On rappelle que le degré de  $L$  sur  $\mathbb{Q}$  est 22. Le but de ce problème est de montrer que l'anneau  $\mathcal{O}$  des entiers de  $L$  n'est pas principal.

(1) Montrer que  $2^{23} - 1$  est divisible par 47 mais pas par 47<sup>2</sup>. Calculer  $N_{L/\mathbb{Q}}(\zeta - 2)$ .

(2) Notons  $\mathfrak{a}$  l'idéal de  $\mathcal{O}$  engendré par 47 et  $\zeta - 2$ . Montrer que, pour tout élément  $\beta$  de  $\mathfrak{a}$ , 47 divise  $N_{L/\mathbb{Q}}(\beta)$ .

(3) On suppose que  $\mathfrak{a}$  est principal, engendré par  $\alpha$ . Montrer que la norme  $N(\alpha)$  divise 47<sup>22</sup> et  $N(\zeta - 2)$ . Calculer  $N(\alpha)$ .

(4) Montrer que  $L$  contient un corps  $K$  quadratique sur  $\mathbb{Q}$  et un seul.

(5) Posons  $\omega = N_{L/K}(\alpha)$ . Montrer que  $\omega$  est un entier de  $K$  et que sa norme est 47.

(6) On sait, grâce à une formule de Gauß (cf. feuille d'exercices), que  $K = \mathbb{Q}(\sqrt{-23})$ . Montrer que  $K$  ne contient pas d'entier de norme 47, et conclure.

*Preuve :* (1) On a  $2^{23} - 1 = 8388607 = 47 \cdot 178481$  et 47 ne divise pas 178481... Le polynôme minimal de  $\zeta$  est  $F(X) = (X^{23} - 1)/(X - 1)$  et la norme de  $\zeta - 2$  est sa valeur au point 2, c'est-à-dire  $2^{23} - 1$ .

(2) De façon générale, si  $m$  est un entier rationnel,  $\alpha$  un entier algébrique, et  $p$  le pgcd de  $m$  et de  $N(\alpha)$ , la norme de tout élément de l'idéal engendré par  $m$  et  $\alpha$  est divisible par  $p$ . Une façon de le prouver est de remarquer que si  $x = my + \alpha z$ , la norme de  $x$  est un produit de conjugués de  $x$ . Un tel conjugué s'écrit  $ny' + \alpha' z'$ , où  $y'$ ,  $\alpha'$  et  $z'$  sont les conjugués correspondants de  $y$ ,  $\alpha$  et  $z$  respectivement. En développant le produit et en rassemblant tous les termes où  $m$  apparaît, on trouve  $N(x) = mt + N(\alpha)N(z)$ . Comme  $N(x)$ ,  $N(\alpha)$  et  $N(z)$  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  $N(x)$  appartient à l'idéal de  $\mathbb{Z}$  engendré par  $m$  et  $N(\alpha)$ . Ici le pgcd vaut 47, qui divise tout élément de l'idéal  $\mathfrak{a}$  engendré par 47 et  $\zeta - 2$ .

(3) Comme  $\mathfrak{a}$  contient  $47\mathcal{O}$  et  $(\zeta - 2)\mathcal{O}$ , sa norme divise celle de chacun d'eux, c'est-à-dire 47<sup>22</sup> et  $2^{23} - 1$ . Elle divise donc leur pgcd 47. D'après la question précédente,  $\mathfrak{a}$  ne contient pas 1, donc sa norme n'est pas 1. On a donc montré  $N\mathfrak{a} = 47$ . Si  $\mathfrak{a} = \alpha\mathcal{O}$  on en déduit  $N\alpha = \pm 47$ . Montrons que la norme absolue de tout élément  $x$  de

$L$  est positive. Notons  $L^+ = \mathbb{Q}(\zeta + \zeta^{-1}) = L \cap \mathbb{R}$  le sous-corps réel de  $L$ . La norme  $y = N_{L/L^+}(x)$  est un élément de  $L^+$  qui est *totalelement positif*, c'est-à-dire que tous ses conjugués sont positifs. En effet, comme le groupe de Galois de  $L/\mathbb{Q}$  est commutatif, chacun de ces conjugués est produit d'un conjugué de  $x$  par son conjugué complexe (la conjugaison complexe commute aux automorphismes de  $L$ ). On en déduit que  $N_{L/\mathbb{Q}}(x) = N_{L^+/\mathbb{Q}}(y)$ , qui est le produit de ces conjugués, est lui aussi positif. En conclusion, on a démontré que  $N(\alpha) = 47$ .

(4), (5) et (6) On a vu dans le cours et dans les feuilles d'exercices que le groupe cyclique d'ordre 22  $\text{Gal}(L/\mathbb{Q})$  a un seul sous-groupe d'indice 2. Le corps correspondant par la théorie de Galois est un corps quadratique, engendré par la somme de Gauss  $\sqrt{-23}$ . On doit avoir

$$47 = N_{L/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(N_{L/K}(\alpha)) = N_{K/\mathbb{Q}}(\omega).$$

Comme  $\omega$  est une norme d'entier, c'est un entier. On a vu que l'anneau des entiers de  $\mathbb{Q}(\sqrt{-23})$  est engendré comme  $\mathbb{Z}$ -module par 1 et  $\frac{1+\sqrt{-23}}{2}$ , on peut donc écrire  $\omega = \frac{a+b\sqrt{-23}}{2}$ , où  $a$  et  $b$  sont deux entiers rationnels de même parité. L'équation  $47 = N_{K/\mathbb{Q}}(\omega)$  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  $4$ , etc.).

**Exercice 8.** Dans le corps  $K = \mathbb{Q}(\sqrt{-47})$ , on note  $\omega = (1 + \sqrt{-47})/2$  et  $\mathfrak{D} = \mathbb{Z}[\omega]$  l'anneau des entiers. On se propose d'étudier le groupe  $C$  des classes d'idéaux fractionnaires de  $K$ .

(1) Montrer que si  $\mathfrak{p}$  est l'idéal engendré par 2 et  $\omega$ ,  $\mathfrak{p}$  est un idéal de norme 2 distinct de son conjugué  $\bar{\mathfrak{p}}$  et que l'on a  $2\mathfrak{D} = \mathfrak{p}\bar{\mathfrak{p}}$ .

(2) Montrer que si  $A$  est la norme d'un idéal entier principal  $\mathfrak{a}$ , alors l'équation

$$x^2 + 47y^2 = 4A$$

admet une solution  $(x, y)$  dans  $\mathbb{Z}^2$ . Montrer que  $\mathfrak{p}$ ,  $\mathfrak{p}^2$ ,  $\mathfrak{p}^3$  et  $\mathfrak{p}^4$  ne sont pas principaux.

(3) Montrer qu'il existe deux idéaux principaux de norme 32. Donner la liste des idéaux entiers de norme 32 et montrer que  $\mathfrak{p}^5$  est principal.

(4) Montrer qu'il y a au plus huit idéaux entiers de norme inférieure ou égale à 4. À l'aide du théorème de Minkowski, montrer que  $C$  est cyclique d'ordre 5.

(5) Montrer que l'idéal  $\mathfrak{q}$  engendré par 3 et  $\omega$  est de norme 3. Pour quelles valeurs de  $n$  l'idéal  $\mathfrak{p}^n\mathfrak{q}$  est-il principal ?

*Preuve :* Le polynôme minimal de  $\omega$  est  $f = X^2 - X + 12$ .

(1) Modulo 2, on a  $f \equiv X(X+1)$ . On peut donc appliquer la proposition 7: 2 se décompose en deux facteurs, dont l'un, noté  $\mathfrak{p}$ , est engendré par 2 et  $\omega$ .

(2) Supposons donc  $\mathfrak{a}$  principal, engendré par l'entier  $\alpha = a + b\omega$ . La norme  $A$  de  $\mathfrak{a}$  est la valeur absolue de celle de  $\alpha$ , soit  $A = (a + b\omega)(a + b\bar{\omega}) = a^2 + ab + 12b^2$ , donc  $4A = (2a + b)^2 + 47b^2$ , d'où le résultat en posant  $x = 2a + b$  et  $y = b$ . Il est facile de voir que les équations  $x^2 + 47y^2 = m$  n'ont pas de solution entière pour  $m = 8$  ou  $m = 32$ , donc  $\mathfrak{p}$  et  $\mathfrak{p}^3$  ne sont pas principaux, et que les seules solutions pour  $m = 16$  ou  $m = 64$  sont données par  $x = \pm 4, y = 0$  et  $x = \pm 8, y = 0$  respectivement, correspondant aux idéaux 2 et 4, donc  $\mathfrak{p}^2$  et  $\mathfrak{p}^4$  ne sont pas principaux.

(3) Pour  $m = 128$ , on trouve les solutions  $x = \pm 9, y = \pm 1$ , qui correspondent à deux idéaux principaux entiers de norme 32. Les idéaux entiers de norme 32 sont  $\mathfrak{p}^5, 2\mathfrak{p}^3, 4\mathfrak{p}, 4\bar{\mathfrak{p}}, 2\bar{\mathfrak{p}}^3$  et  $\bar{\mathfrak{p}}^5$ . Seuls les deux extrêmes peuvent être principaux: ils le sont donc.

(4) Modulo 3, on a aussi  $f \equiv X(X+1)$ , donc on peut appliquer la proposition 7: 3 se décompose en deux facteurs, dont l'un, noté  $\mathfrak{q}$ , est engendré par 3 et  $\omega$ . La liste complète des idéaux entiers de norme au plus 4 est donc la suivante:  $\{1, \mathfrak{p}, \bar{\mathfrak{p}}, \mathfrak{q}, \bar{\mathfrak{q}}, \mathfrak{p}^2, \bar{\mathfrak{p}}^2, 2\}$ . La constante de Minkowski du corps est  $2/\pi\sqrt{47} \approx 4.364445271138074545056000371 < 5$ . On déduit du théorème 5 que le nombre de classes de  $K$  est inférieur ou égal à 8. Comme la classe  $\mathfrak{p}$  est d'ordre 5 dans ce groupe,  $C$  est cyclique d'ordre 5.

(5) L'élément  $\omega$  est de norme 12, et il est contenu dans  $\mathfrak{p}$  et  $\mathfrak{q}$ . L'idéal engendré par  $\omega$  est donc  $\mathfrak{p}^2\mathfrak{q}$  ou bien  $2\mathfrak{q}$ . Comme  $\mathfrak{q}$  n'est pas principal ( $x^2 + 47y^2 = 12$  n'a pas de solution entière), c'est  $\mathfrak{p}^2\mathfrak{q}$ . De la structure de groupe, on tire immédiatement que  $\mathfrak{p}^n\mathfrak{q}$  est principal si et seulement si  $n \equiv 2 \pmod{5}$ .

### 3 Loi de réciprocité supérieure

Soit  $L/K$  une extension finie; on note  $\mathcal{O}_K$  et  $\mathcal{O}_L$  les anneaux d'entiers. Pour  $\mathfrak{p}$  un idéal premier non nul de  $\mathcal{O}_K$ . On écrit

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{b}_1^{e_1} \cdots \mathfrak{b}_r^{e_r}$$

où les  $\mathfrak{b}_i$  sont des idéaux premiers distincts non nuls de  $\mathcal{O}_L$  et les  $e_i$  des entiers  $\geq 1$ . On note en outre  $f_i$  le degré de l'extension de corps résiduel  $\kappa(\mathfrak{b}_i)/\kappa(\mathfrak{p})$ . On rappelle que  $\sum_i e_i f_i = [L : K] = n$ . En outre si l'extension  $L/K$  est galoisienne,  $e_i = e$  et  $f_i = f$  sont constants. Quand  $r = 1$  (resp.  $r = n$ ), on dit que  $\mathfrak{p}$  est inerte (resp. totalement décomposé). Quand tous les  $e_i = 1$ , on dit que  $\mathfrak{p}$  est non ramifié. On note  $\text{Spl}(L/K)$  l'ensemble des idéaux premiers de  $K$  totalement décomposés dans  $L$ .

**Exercice 1.** Soit  $K$  un corps quadratique et  $a \in \mathbb{Z}$  un entier sans carré tel que  $K = \mathbb{Q}[\sqrt{a}]$ .

(1) Montrer que pour tout premier  $p$ ,  $\mathcal{O}_K/p\mathcal{O}_K \simeq \mathbb{F}_p[X]/(X^2 - a)$ .

(2) En déduire que tout  $p$  ne divisant pas  $2a$ ,  $(p)$  est non ramifié dans  $K$  puis que pour  $p \nmid 2a$ ,  $(p)$  est complètement décomposé si et seulement si  $\left(\frac{a}{p}\right) = 1$ .

(3) Montrer que  $\text{Spl}(\mathbb{Q}[\sqrt{a}]/\mathbb{Q})$  est l'ensemble des premiers contenus dans une certaine réunion de classes non nulles modulo  $4a$ , auquel il faut éventuellement ajouter des diviseurs premiers de  $2a$ .

*Preuve :* (1) On rappelle que  $\mathcal{O}_K = \mathbb{Z}[\omega]$  avec suivant la valeur de  $a$ ,  $\omega = \sqrt{a}$  ou  $\omega = \frac{1+\sqrt{a}}{2}$ ; dans ce dernier cas, pour  $\alpha + \beta\omega \in \mathcal{O}_K$  qui n'est pas dans  $R = \mathbb{Z}[\sqrt{a}]$ ,  $\beta$  est impair et donc congru à  $\alpha + (\beta + p)\omega \in R$  modulo  $p$ . Ainsi dans tous les cas on a

$$\mathcal{O}_K/p\mathcal{O}_K \simeq R/pR \simeq \mathbb{Z}[X]/(X^2 - a, p) \simeq \mathbb{F}_p[X]/(X^2 - a)$$

(2) Si  $p\mathcal{O}_K = \mathfrak{b}_1^{e_1} \cdots \mathfrak{b}_r^{e_r}$ , le théorème chinois donne

$$\mathcal{O}_K/p\mathcal{O}_K \simeq \bigoplus_{i=1}^r \mathcal{O}_K/\mathfrak{b}_i^{e_i}$$

L'algèbre  $\mathbb{F}_p[X]/(X^2 - a)$  étant sans élément nilpotent,  $(p)$  est donc non ramifiée dans  $K$  et  $\mathcal{O}_K/p\mathcal{O}_K$  est la somme de  $r = 1, 2$  corps qui sont des extensions de  $\mathbb{F}_p$ .

Selon que  $X^2 - a$  est irréductible sur  $\mathbb{F}_p$ , i.e. selon la valeur de  $\left(\frac{a}{p}\right)$ ,  $(p)$  ne se décompose pas ou se décompose complètement dans  $K$ .

(3) Cela découle de la loi de réciprocité quadratique; en effet  $\left(\frac{a}{p}\right)$  est déterminé à un signe explicite près, par la classe de  $p$  modulo  $a$ .

**Exercice 2.** Soit  $\zeta_n$  une racine primitive  $n$ -ième de l'unité. Soit  $K = \mathbb{Q}[\zeta_n]$  d'anneau des entiers  $\mathcal{O}_K = \mathbb{Z}[\zeta_n] \simeq \mathbb{Z}[X]/(\Phi_n(X))$ .

(1) Montrer que pour tout  $p$  ne divisant pas  $n$ ,  $(p)$  est non ramifié dans  $K$  et se décompose en idéaux premiers de même degré résiduel  $f$  égal à l'ordre de  $p$  dans  $(\mathbb{Z}/n\mathbb{Z})^\times$ .

(2) Montrer que  $\text{Spl}(K/\mathbb{Q})$  est l'ensemble des premiers congrus à 1 modulo  $n$ .

*Preuve :* (1) On a  $\mathcal{O}_K/p\mathcal{O}_K \simeq \mathbb{F}_p[X]/(\overline{\Phi_n(X)})$ . On rappelle que  $\overline{\Phi_n(X)}$  se décompose en un produit de  $\phi(n)/f$  facteurs irréductibles, tous de même degré  $f$  qui est égal à l'ordre de  $p$  dans  $(\mathbb{Z}/n\mathbb{Z})^\times$ , d'où le résultat.

(2)  $p$  est totalement décomposé si et seulement si  $f = 1$  i.e.  $p \equiv 1 \pmod{n}$ .

**Exercice 3.** Soit  $\mathfrak{p}$  un idéal premier non nul de  $K$  et soit  $\mathfrak{b}$  un idéal de  $L$  au dessus de  $\mathfrak{p}$ .

(1) Montrer que l'ordre du stabilisateur  $G_{\mathfrak{b}}$  est égal à  $ef$ .

(2) Dans le cas où  $\mathfrak{p}$  est non ramifié,  $e = 1$ , montrer que  $G_{\mathfrak{b}}$  s'identifie au groupe de Galois de l'extension de corps finis  $\kappa(\mathfrak{b})/\kappa(\mathfrak{p})$ .

(3) Dans le cas où  $G$  est abélien, construire un élément  $\left(\frac{L/K}{\mathfrak{p}}\right)$  associé au Frobenius de  $\kappa(\mathfrak{b})/\kappa(\mathfrak{p})$ . C'est le **symbole d'Artin**.

(4) Calculer le symbole d'Artin pour  $K = \mathbb{Q}$  et  $L = \mathbb{Q}[\zeta_n]$  (resp.  $L = \mathbb{Q}[\sqrt{m}]$ ) pour  $p$  non ramifié.

(5) Soit  $L = \mathbb{Q}[\zeta_l]$  et  $H = (\mathbb{F}_l^\times)^2 \subset \text{Gal}(L/\mathbb{Q})$  et  $M = L^H$ .

(i) Montrer que  $M = \mathbb{Q}[\sqrt{l^*}]$  avec  $l^* = (-1)^{(l-1)/2}l$ .

(ii) Montrer que  $p \neq l$  est non ramifié dans  $L$  et  $M$  et que la restriction à  $M$  de  $\left(\frac{L/\mathbb{Q}}{p}\right)$  est  $\left(\frac{M/\mathbb{Q}}{p}\right) = \left(\frac{p}{l}\right)$ .

(iii) En déduire une nouvelle preuve de la loi de réciprocité quadratique.

*Preuve :* (1) Cela découle du fait que le groupe de Galois opère transitivement sur les  $\mathfrak{b}_i$ .

(2) C'est du cours.

(3) À  $\mathfrak{b}_i$ , on associe donc un élément  $\phi_{\mathfrak{b}_i} \in G_{\mathfrak{b}_i}$  qui correspond au morphisme de Frobenius de  $\kappa(\mathfrak{b}_i)/\kappa(\mathfrak{p})$ . Pour  $\sigma \in G$ , on a  $\phi_{\sigma\mathfrak{b}_i} = \sigma\phi_{\mathfrak{b}_i}\sigma^{-1}$  de sorte que si  $G$  est abélien  $\phi_{\mathfrak{b}_i}$  ne dépend pas du choix de  $\mathfrak{b}_i$  au dessus de  $\mathfrak{p}$ : on le note  $(\frac{L/K}{\mathfrak{p}})$ .

(4) Pour  $K = \mathbb{Q}$ ,  $L = \mathbb{Q}[\zeta_n]$  (resp.  $L = \mathbb{Q}[\sqrt{m}]$ ) et  $p$  non ramifié, on a  $(\frac{L/K}{\mathfrak{p}})$  est défini par  $\zeta_n \mapsto \zeta_n^p$  (resp. par  $(\frac{m}{p})$  en identifiant le groupe de Galois à  $\{\pm 1\}$ ).

(5) (i) On considère la somme de Gauß:  $\tau = \sum_{x \in \mathbb{F}_l^\times} (\frac{x}{l})\zeta_l^x$ . On rappelle que  $\tau^2 = (\frac{-1}{l})l = l^*$ , de sorte que  $\mathbb{Q}[\tau]/\mathbb{Q}$  est une extension quadratique. Par ailleurs si  $\mathbb{Q} \subset K \subset L$  est une extension quadratique alors  $p$  est le seul premier qui peut se ramifier ce qui impose  $K = \mathbb{Q}[\sqrt{\pm l}]$ . Supposons que  $\mathbb{Q}[il^*]$  soit contenu dans  $L$ , on en déduit alors que  $i \in L$  ce qui n'est pas car  $p$  est impair.

(ii)  $(\frac{M/\mathbb{Q}}{p})$  est l'identité si et seulement s'il est dans  $H$  d'où  $(\frac{M/\mathbb{Q}}{p}) = (\frac{p}{l})$ .

(iii) Le résultat découle des égalités  $(\frac{M/\mathbb{Q}}{p}) = (\frac{l^*}{p}) = (\frac{p}{l})$ .

**Loi de réciprocité d'Artin:** Pour  $\mathfrak{m}$  un idéal de  $K$ , on note  $J_K^{\mathfrak{m}}$  le groupe des idéaux fractionnaires premiers à  $\mathfrak{m}$  et  $P_K^{\mathfrak{m}}$  le sous-groupe des idéaux principaux engendré par les idéaux principaux engendré par les  $\alpha \equiv 1 \pmod{\mathfrak{m}}$  qui est d'indice fini.

Pour  $L/K$  une extension finie abélienne, il existe un idéal  $\mathfrak{m}$  de  $K$  tel que le morphisme

$$(\frac{L/K}{\mathfrak{m}}) : J_K^{\mathfrak{m}} \rightarrow \text{Gal}(L/K)$$

est surjectif et son noyau  $H^{\mathfrak{m}}$  contient  $P_K^{\mathfrak{m}}$  que l'on peut exprimer explicitement grâce au morphisme norme  $N_{L/K}$ . On obtient ainsi, pour toutes les extensions abéliennes, une description en termes de congruences de la décomposition des idéaux premiers non ramifiés: par exemple pour  $K = \mathbb{Q}$ , pour  $m$  un générateur de  $\mathfrak{m}$ , on a  $J_{\mathbb{Q}}^{\mathfrak{m}}/P_{\mathbb{Q}}^{\mathfrak{m}} \simeq (\mathbb{Z}/m\mathbb{Z})^\times$  et donc le groupe  $H^{\mathfrak{m}}$  qui est, aux premiers ramifiés près,  $\text{Spl}(L/\mathbb{Q})$ , est une réunion de classes de congruences modulo  $m$ .

On peut définir aussi le symbole de Jacobi de puissance  $n$ -ième  $(\frac{a}{b})_n$  donné par le symbole d'Artin d'une extension de la forme  $K(\sqrt[n]{a})/K$  avec  $K = \mathbb{Q}[\zeta_n]$ . On peut alors énoncer une loi de réciprocité pour les puissances  $n$ -ièmes.

**Le cas non abélien:** la loi de réciprocité d'Artin s'exprime comme suit: pour tout corps  $k$ , il existe un groupe abélien  $C_K$  naturellement associé à  $K$  de sorte que pour toute extension galoisienne  $L$  de  $K$ , on dispose d'un morphisme naturel

$$N_{L/K} : C_L \longrightarrow C_K$$

ainsi qu'un isomorphisme canonique définie par les symboles d'Artin:

$$\text{Gal}(L/K)^{ab} \simeq C_K/N_{L/K}C_L$$

On peut rêver d'un analogue non abélien, i.e. d'un groupe  $\mathfrak{C}_K$ , d'une famille de morphismes  $\mathfrak{N}_{L/K}$  tels que l'on ait des isomorphismes  $\text{Gal}(L/K) \simeq \mathfrak{C}_K/\mathfrak{N}_{L/K}\mathfrak{C}_L$ . Pour l'instant on ne connaît rien de tel, par contre on sait associer certaines fonctions analytiques à des représentations des groupes de Galois des extensions de  $K$ , ainsi qu'à des représentations de  $GL_n(\mathbb{A}_K)$  d'un certain anneau  $\mathbb{A}_K$  dont  $C_K$  est un quotient de  $GL_1(\mathbb{A}_K)$ . R. P. Langlands, dans les années 60 et 70, a formulé un important faisceau de conjectures concernant ces fonctions analytiques qui établissent un lien entre les représentations galoisiennes et les représentations des groupes linéaires. Ces conjectures ont été en partie prouvées récemment et fournissent ainsi une "loi de réciprocité non-abélienne".