Marlon Hu Stege

Number theory - Exercises

23.10.23

Ex. 1

(i) show: $\mathcal{O}_K^\times = \{ x \in \mathcal{O}_K \mid N_{K/\mathbb{Q}}(x) = \pm 1 \}$

Pf: write the minimal polynomial of $\alpha \in \mathcal{O}_K^\times$ as:

$$p(x) = a_0 + a_1 x + \dots + x^n$$

Then note that

$$(*) \quad \alpha^{-n} p(\alpha) = a_0 \alpha^{-n} + a_1 \alpha^{-(n-1)} + \dots + a_n = 0$$

Then $(*)$ is a polynomial with coefficients over $\mathbb{Z}$ of smallest degree possible for α to satisfy and all the coefficients a_i are already known to be coprime. So after dividing everything by a_0 this is the minimal polynomial over $\mathbb{Q}$ for α^{-1} and by definition this is an algebraic integer, i.e. α is a unit $\Leftrightarrow$ the minimal polynomial of α has coefficients in $\mathbb{Z}$, i.e. $a_0 \mid a_i \ \forall\, 1 \leq i \leq n$.

But if they are coprime and still a_0 divides all the others, we know $a_0 = \pm 1$ by the fundamental theorem of arithmetic. $\Rightarrow N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

Alternative way:

"$\Rightarrow$": If $u \in \mathcal{O}_K$ is a unit $\Rightarrow N_{K/\mathbb{Q}}(u) N_{K/\mathbb{Q}}(u^{-1}) = 1$, an equation in $\mathbb{Z}$. $\Rightarrow$ Hence $N_{K/\mathbb{Q}}(u) = \pm 1$ #

"$\Leftarrow$": Conversely if $u \in \mathcal{O}_K$ has norm ± 1, as an algebraic integer u is a root of a polynomial of form $X^n + \dots + a_1 X \pm 1 \in \mathbb{Z}[X]$.
Hence $\pm(u^{n-1} + \dots + a_1) \in \mathcal{O}_K$ is the inverse of u
$\Rightarrow$ u invertible in $\mathcal{O}_K$. #

(ii) we know from lecture, that for a squarefree integer $m \in \mathbb{N}$ we have the following: for $K = \mathbb{Q}(\sqrt{-m})$

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \frac{1+\sqrt{m}}{2}\mathbb{Z} = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right], & \text{as } m \equiv 1 \bmod 4 \\ \mathbb{Z} + \sqrt{m}\,\mathbb{Z} = \mathbb{Z}[\sqrt{m}], & \text{as } m \equiv 2,3 \bmod 4 \end{cases}$$

So we are looking for the inverses of elements in $\mathcal{O}_K$ in both cases:

Case $m \equiv 1 \bmod 4$:

$\forall x \in \mathcal{O}_K$ we have $a, b \in \mathbb{Z}$:

$$x = a + b \cdot \frac{1+\overset{\circ}{i}\sqrt{m}}{2}$$

For ~~another~~ $\mathcal{O}_K \ni x' = \overset{\in \mathbb{Z}}{c + d}\,\frac{1+\overset{\circ}{i}\sqrt{m}}{2}$ we get

$$1 \overset{?}{=} x x' = \Big(\underbrace{(ac) + \frac{ad}{2} + \frac{bc}{2} - \frac{bdm}{4} + \frac{bd}{4}}_{=1 \in \mathbb{Z}}\Big) + \underbrace{\left(\frac{1}{2}ad + \frac{1}{2}bc + \frac{1}{2}bd\right)}_{\overset{!}{=} 0 \in \mathbb{Z}} \overset{\circ}{i}\sqrt{m}$$

So we get the conditions:

① $ac + \frac{1}{2}(ad + bc) + \frac{bd}{4}(1+m) = 1$

② $ad + bc + bd = 0$

$\Rightarrow$ ② in ①: $ac + \frac{1}{2}(-bc) + \frac{bd}{4}(1+m) = 1$

But we have from (i), that:

$$\pm 1 \overset{!}{=} N_{K/\mathbb{Q}}(x) = N_{K/\mathbb{Q}}\left(a + b\left(\frac{1+\overset{\circ}{i}\sqrt{m}}{2}\right)\right)$$

~~And we have $x x' = \left(ac + \frac{1}{2}ad + \frac{1}{2}bc + \frac{1}{2}bd\right)$~~

And we have in $K^2 \cong \mathbb{Q}(\sqrt{-m})$ basis:

$$x x' = \begin{pmatrix} ac - \frac{1}{4}(1+m) \cdot bd \\ ad + bc + bd \end{pmatrix}$$

So $\underbrace{\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}}_{A_x} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = x x' \Rightarrow A_x = \begin{pmatrix} c & -d\left(\frac{1+m}{4}\right) \\ d & c+d \end{pmatrix}$

$$\Rightarrow N_{K/\mathbb{Q}}(x) = \det(A_x) = c(c+d) + d^2\left(\frac{1+m}{4}\right) \overset{!}{=} \pm 1$$

Now we have the condition:

$$d^2 = 4 \cdot \frac{\pm 1 - c(c+d)}{1+m} \quad (*)$$

So we want to solve the equation for $m > 0$ (otherwise we would have ∞-many solutions of $(*)$).

Case $m = 2,3 \bmod 4$ $\Rightarrow$ ~~These~~ are all possible units in $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$

So we want to have

$$N_{u|\mathbb{Q}}(a + b\sqrt{-d}) = a^2 + m b^2 = \pm 1$$

$$\Rightarrow b^2 = \frac{\pm 1 - a^2}{m} \quad \text{for } m > 0$$

so $b^2 > 0$ and therefore

$$a^2 \in \{0, 1\}$$

but because of $m = 4 \cdot \overset{\text{new}}{n} + \{2, 3\}$

we just have for ~~0~~ $a = \pm 1$:

$$b^2 = \frac{\pm 1 - (\pm 1)^2}{m} = 0 \Rightarrow b = 0 \in \mathbb{Z}$$

So $x = \pm 1 \in \mathbb{Z}(-\sqrt{m})$ are the only invertible elements of $\mathcal{O}^{\times}_{\mathbb{Q}(\sqrt{m})}$ - $\forall m > 1$ #

If $m = 1$ then we have:

$a^2 + b^2 = \pm 1 \Rightarrow 4$ solutions:

$(a, b) = (0, 1), (0, -1), (1, 0), (-1, 0)$

so the only invertible elements in $\mathcal{O}^{\times}_{\mathbb{Q}(-\sqrt{m})}$ are:

$x = \pm 1$ or $\pm i\sqrt{m}$ $\forall m = 1$ #

ex. 2

show: $\varphi(\mathcal{O}_K) \subset \mathcal{O}_L$ for K, L numb. fields and $\varphi: K \to L$ rings. homom.

<u>Pf</u>: $\forall x \in \mathcal{O}_K$ we have:

$$\exists p \in \mathbb{Z}[x]: \quad p(x) = 0 \underset{\text{i.e.}}{=} a_0 + a_1 x^1 + \dots + x^n \quad (*)$$

If we multiply $(*)$ with x we get:

$$+x = -\left(\frac{a_1}{a_0} x^2 + \frac{a_2}{a_0} x^3 + \dots + \frac{a_n}{a_0} x^n + \frac{x^{n+1}}{a_0}\right)$$

So when we apply $\varphi(x)$ then we get:

$$\varphi(a_0 x) \underset{\substack{RH \\ \text{Scalar}}}{=} a_0 \varphi(x) \underset{\substack{RH \\ \text{Scalar}}}{=} -\varphi(a_1 x^2 + \dots + a_n x^n + x^{n+1})$$

$$\underset{\substack{RH \\ \text{linear} \\ +\text{multiplicative}}}{=} -\left(a_1 \varphi(x)^2 + \dots + a_n \varphi(x)^n + \varphi(x)^{n+1}\right)$$

So we optain by dividing through $\varphi(x)$:

$$\Rightarrow 0 = a_0 + a_1 \varphi(x) + \dots + a_n \varphi(x)^{n-1} + \varphi(x)^n$$

$$= p(\varphi(x)) \in \mathbb{Z}[\varphi(x)]$$

So $p(\varphi(x)) = 0$ and therefore every $y = \varphi(x) \in L$ (for $x \in K$) is algebraic over $\mathbb{Z}$

$$\Rightarrow \varphi(x) \in \mathcal{O}_L$$

$$\Rightarrow \varphi(\mathcal{O}_K) \subset \mathcal{O}_L \quad \#$$

ex. 3

(i) show: $\Delta_{K/\mathbb{Q}}(1, x, x^2) = -3^3 m^2$

Pf.: Calculate

$$\Delta_{K/\mathbb{Q}}(1,x,x^2) = \det\begin{pmatrix} Tr_{K/\mathbb{Q}}(1\cdot 1) & Tr_{K/\mathbb{Q}}(1\cdot x) & Tr_{K/\mathbb{Q}}(1\cdot x^2) \\ Tr_{K/\mathbb{Q}}(x\cdot 1) & Tr_{K/\mathbb{Q}}(x\cdot x) & Tr_{K/\mathbb{Q}}(x\cdot x^2) \\ Tr_{K/\mathbb{Q}}(x^2\cdot 1) & Tr_{K/\mathbb{Q}}(x^2\cdot x) & Tr_{K/\mathbb{Q}}(x^2\cdot x^2) \end{pmatrix}$$

$$= \det\begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 3m \\ 0 & 3m & 0 \end{pmatrix} = -(3m\cdot 3m\cdot 3) = -3^3 m^2 \quad \square$$

because $\forall y \in \operatorname{Im}(1,x,x^2)$: $\exists\, a,b,c \in \mathbb{Q}$:

$$y = a + bx + cx^2 = \begin{pmatrix} a \\ b \\ c \end{pmatrix} \in \mathbb{Q}^3 \text{ identified}$$

$$Tr_{K/\mathbb{Q}}(1) = Tr\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 3$$

$$Tr_{K/\mathbb{Q}}(x) = Tr\begin{pmatrix} 0 & 0 & m \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = 0$$

$$A_x\cdot\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} cm \\ a \\ b \end{pmatrix} \quad (x^3 = m) \text{ for } K = \mathbb{Q}[x]/(x^3 - m)$$

$$Tr_{K/\mathbb{Q}}(x^2) = Tr\begin{pmatrix} 0 & m & 0 \\ 0 & 0 & m \\ 1 & 0 & 0 \end{pmatrix} = 0$$

$$A_{x^2}\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} bm \\ cm \\ a \end{pmatrix}$$

$$Tr_{K/\mathbb{Q}}(x^3) = Tr\begin{pmatrix} m & 0 & 0 \\ 0 & m & 0 \\ 0 & 0 & m \end{pmatrix} = 3m$$

$$A_{x^3}\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} am \\ bm \\ cm \end{pmatrix}$$

$$Tr_{K/\mathbb{Q}}(x^4) = Tr(mx) = Tr\begin{pmatrix} 0 & 0 & m^2 \\ m & 0 & 0 \\ 0 & m & 0 \end{pmatrix} = 0$$

$$A_{x^4}\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} m^2 c \\ ma \\ mb \end{pmatrix}$$

(ii) Compute $N_{K/\mathbb{Q}}(\overbrace{a + bx + cx^2}^{y}) \hat{=} \begin{pmatrix} a \\ b \\ c \end{pmatrix}$ for $a, b, c \in \mathbb{Q}$

$$N_{K/\mathbb{Q}}(y) = \det(A_y) = \det\begin{pmatrix} a & ac & bm \\ a & bc & cm \\ c & c^2 & a \end{pmatrix} = \begin{array}{l} abc + accm\cdot c \\ + bmbc^2 - cbc\cdot bm \\ - c^2cma - abac \end{array}$$

$$= 0 \quad \Big(\text{Norm } N_{K/\mathbb{Q}}(y) = 0 \Big) \; \#$$

K as above ($x^3 = m$)

$A_y : K \to K : k \mapsto y\cdot k$

we have $y \cdot k = y\cdot(d + gx + fx^2) = \begin{pmatrix} acg + ad + bfm \\ bcg + bd + cfm \\ af + c^2 g + cd \end{pmatrix}$

So we get: $A_y\begin{pmatrix} d \\ g \\ f \end{pmatrix} \overset{!}{=} y\cdot k \Rightarrow A_y = \begin{pmatrix} a & ac & bm \\ b & bc & cm \\ c & c^2 & a \end{pmatrix}$

ex. 4

(i) Show: For $K = \mathbb{Q}(\alpha) = \mathbb{Q}\left(\sqrt{59-24\sqrt{2}}\right)$ has $[K:\mathbb{Q}] = 4$ and $\left(1, \sqrt{59-24\sqrt{2}}, \sqrt{2}, \sqrt{2}\sqrt{59-24\sqrt{2}}\right)$ is a $\mathbb{Q}$-basis of K

<u>Pf:</u> The minimal polynomial of α is in $\mathbb{Q}[X]$, i.e. in $\mathbb{Z}[X]$:

$$\mu_{\alpha,\mathbb{Q}} = X^4 - 118X^2 + 2329 \in \mathbb{Z}[X]$$

~~Because of Eisenstein's criterion we have~~

$\mu_{\alpha,\mathbb{Q}}$ has roots $\pm\sqrt{59-24\sqrt{2}}$ and $\pm\sqrt{59+24\sqrt{2}}$, so $\mu_{\alpha,\mathbb{Q}}$ is irreducible over $\mathbb{Q}$.

(and $\mu_{\alpha,\mathbb{Q}}$ is the minimal polynom.)

$$\Rightarrow [K:\mathbb{Q}] = 4 = \deg(\mu_{\alpha,K})$$

For the tuple $B = (b_1, b_2, b_3, b_4) = \left(1, \sqrt{59-24\sqrt{2}}, \sqrt{2}, \sqrt{2}\sqrt{59-24\sqrt{2}}\right)$ we have for $x, y \in \mathrm{Lin}(B)$:

$$x \cdot y = (ab_1 + bb_2 + cb_3 + db_4)\cdot(fb_1 + gb_2 + hb_3 + jb_4)$$

$$\underset{\text{as } K^4}{=} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \cdot \begin{pmatrix} f \\ g \\ h \\ j \end{pmatrix} = \begin{pmatrix} af + 59bg - 48bj + 2ch - 48cg + 118dj \\ ag + bf + 59bj + 2cj + 2dh \\ ah + 24bg + cf + 59dg - 48dj \\ aj + bh + cg + df \end{pmatrix}$$

So we get $x \cdot y \in \mathrm{Lin}(B)$ $\forall x, y \in \mathrm{Lin}(B)$

And because $\mathbb{Q}(\alpha) \subseteq \mathrm{Lin}(B)$ we have

$K = \mathbb{Q}(\alpha) = \mathrm{Lin}(B)$ so B is a basis of K.

(ii) Show: $\beta = \left((-1+\sqrt{59-24\sqrt{2}})/\sqrt{2}\right) \in \mathcal{O}_K$

<u>Pf.</u> Minimal polynomial of β is:

$$\mu_{\beta,\mathbb{Q}} = X^4 - 60X^2 - 48X + 553 \in \mathbb{Z}[X],$$

which is irreducible because its roots are $\pm\beta$ and $\pm\frac{1}{\sqrt{2}}(\alpha - 1)$, so we have $\mu_{\beta,\mathbb{Q}} \in \mathbb{Z}[X]$

$\Rightarrow \beta \in \mathcal{O}_K$ ⨳

$\sqrt{\ } = \gamma = 2\alpha^2$

(iii) Show: $2\cdot(59-24\sqrt{2})\,\mathcal{O}_K \subset \mathcal{O}_F[\beta]$ for $F=\mathbb{Q}(\sqrt{2})$

<u>Pf:</u> we have $\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}(\sqrt{2})$

So we have $\mathcal{O}_F[\beta] = \mathbb{Z}(\sqrt{2},\beta)$

$\forall x \in \mathcal{O}_K$ we have: $\exists p \in \mathbb{Z}[X]$:

$p(x) = 0 = a_0 + a_1 x + \dots + x^n \in \mathbb{Z}[X]$

i.e. $\Longrightarrow x = \frac{1}{-a_0}(a_1 x^2 + \dots + x^{n+1})$

If we multiply by $2\alpha^2$ we get for $x' = 2\alpha^2 x$

~~$p(2\alpha^2 x) = 2\alpha^2 \cdot 0 = 0$~~

optimal

$$2\alpha^2 x = -\frac{2\alpha^2}{2a_0}\cdot(a_1x^2 + \dots + x^{n+1})$$

$\uparrow \in \mathbb{Z}$

and

$$p(2\alpha^2 x) = a_0 + 2\alpha^2 a_1 x + \dots + (2\alpha^2)^n x^n$$

we know, that $\mathcal{B}$ basis of $K = \mathbb{Q}(\alpha)$,
So we want to check $\forall x \in K$:
$(\exists a,b,c,d \in \mathbb{Q})$: $x = a + b\alpha + c\sqrt{2} + d\sqrt{2}\alpha$

If minimal polynomial $\mu_{x,\mathbb{Q}} \in \mathbb{Z}[X]$

$\Longrightarrow a,b,c,d \in \mathbb{Z}$

$\Longrightarrow \forall x \in \mathcal{O}_{\mathbb{Q}(\alpha)}$: $x = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \in \mathbb{Z}^4$

But we have for $x,y \in \mathcal{O}_{\mathbb{Q}(\alpha)}$:

$2\alpha^2 x = 2\alpha^2 \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$ and $2\alpha^2 y = 2\alpha \begin{pmatrix} f \\ g \\ h \\ j \end{pmatrix}$

$$x\cdot y = 4\alpha^4 \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}\begin{pmatrix} f \\ g \\ h \\ j \end{pmatrix} = \underbrace{A \circ \beta + B \cdot \sqrt{2}}_{\in \mathbb{Z}} \in \mathbb{Z}(\sqrt{2},\beta)$$

So we have $\forall x \in 2\alpha^2\mathcal{O}_K \Rightarrow x \in \mathbb{Z}(\sqrt{2},\beta) \subseteq \mathcal{O}_F[\beta] = \mathbb{Z}(\sqrt{2})[\beta]$ $\blacksquare$