5. Quadratic number fields

Definition: An algebraic number field K is called a quadratic number field [dt quadratischer Zahlkörper] if $[K:\mathbb{Q}]=2$.

Theorem 68 Let K be a quadratic number field. Then there is a uniquely determined squarefree $d\in\mathbb{Z}\setminus\{0,1\}$ such that $K=\mathbb{Q}(\sqrt{d})$.

Proof: By Corollary 54 there is an $\alpha\in\mathcal{O}_K$ such that $K=\mathbb{Q}(\alpha)$.
Let $m_{K,\alpha}(X)=X^2+bX+c\in\mathbb{Z}[X]$. Then $\alpha\in\left\{\frac{-b+\sqrt{b^2-4c}}{2},\frac{-b-\sqrt{b^2-4c}}{2}\right\}$. We have $b^2-4c=dk^2$ for some $k\in\mathbb{N}$ and some squarefree $d\in\mathbb{Z}\setminus\{0,1\}$. (It is impossible that $d\in\{0,1\}$ as this would imply $\alpha\in\mathbb{Q}$ and $[K:\mathbb{Q}]=1$.) Clearly $K=\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{d})$.
Suppose that $d_1,d_2\in\mathbb{Z}\setminus\{0,1\}$ are squarefree and $\mathbb{Q}(\sqrt{d_1})=\mathbb{Q}(\sqrt{d_2})$. Then there are $x,y\in\mathbb{Q}$ such that $\sqrt{d_2}=x+y\sqrt{d_1}$ which implies $d_2=x^2+y^2d_1+2xy\sqrt{d_1}$.
If $xy\neq 0$ then $\sqrt{d_1}=\frac{d_2-x^2-y^2d_1}{2xy}\in\mathbb{Q}$. If $y=0$ then $\sqrt{d_2}=x\in\mathbb{Q}$. Both are contradictions. Therefore $x=0$ and $\sqrt{d_2}=y\sqrt{d_1}$ which implies $d_2=y^2d_1$. As d_1 and d_2 are squarefree $y^2=1$ and $d_1=d_2$.

Remark: From now on, when we state "Let $K=\mathbb{Q}(\sqrt{d})$ be a quadratic number field," the d will always be the one from Theorem 68 (unless we explicitly demand something different).

Theorem 69 Let $K=\mathbb{Q}(\sqrt{d})$ be a quadratic number field. Then

$$\mathcal{O}_K=\begin{cases}\mathbb{Z}[\sqrt{d}] & \text{if } d\not\equiv 1 \pmod 4,\\[1ex] \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d\equiv 1 \pmod 4.\end{cases}$$

Proof: As $\sqrt{d}$ is root of $X^2-d\in\mathbb{Z}[X]$ we get $\sqrt{d}\in\mathcal{O}_K$ and therefore $\mathbb{Z}[\sqrt{d}]\subseteq\mathcal{O}_K$.
If $d\equiv 1 \pmod 4$ then $\frac{1+\sqrt{d}}{2}\in\mathcal{O}_K$ as it is a root of $X^2-X+\frac{1-d}{4}\in\mathbb{Z}[X]$.
Therefore $(\mathbb{Z}[\sqrt{d}]\subsetneqq)\,\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]\subseteq\mathcal{O}_K$ if $d\equiv 1 \pmod 4$. (Note that $\mathbb{Z}[\sqrt{d}]\subseteq\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ as $a+b\sqrt{d}=a-b+2b\frac{1+\sqrt{d}}{2}$ $\forall a,b\in\mathbb{Z}$ but $\mathbb{Z}[\sqrt{d}]\neq\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ as $\frac{1+\sqrt{d}}{2}\notin\mathbb{Z}[\sqrt{d}]$.)

23.11.2022

Now let $\alpha\in\mathcal{O}_K$. As $\alpha\in K$ there are $p,q\in\mathbb{Q}:\alpha=p+q\sqrt{d}$. We can rewrite this as $\alpha=\frac{a+b\sqrt{d}}{c}$ for some $a,b\in\mathbb{Z}$ and $c\in\mathbb{N}$ with $\gcd(a,b,c)=1$. Clearly α is a root of the polynomial $\left(X-\frac{a+b\sqrt{d}}{c}\right)\left(X-\frac{a-b\sqrt{d}}{c}\right)=X^2-\frac{2a}{c}X+\frac{a^2-b^2d}{c^2}\in\mathbb{Q}[X]$.

If $b \neq 0$ then $f = m_{\mathbb{Q},\alpha}$. If $b=0$ then $f = m^2_{\mathbb{Q},\alpha}$. As $\alpha \in \mathcal{O}_K$ we know $m_{\mathbb{Q},\alpha} \in \mathbb{Z}[X]$ (by Corollary 58) and therefore $f \in \mathbb{Z}[X]$, i.e., $\frac{2a}{c}, \frac{a^2-b^2d}{c^2} \in \mathbb{Z}$. Suppose that there is a prime p such that $p|a$ and $p|c$. Then $p^2 | b^2 d$ and (as d is squarefree) $p|b$, which is a contradiction. Therefore $\gcd(a,c)=1$ and $c \in \{1,2\}$.

If $c=1$ then $\alpha = a+b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ (and also $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ if $d \equiv 1 \pmod 4$).

Now suppose $c=2$. As $\gcd(a,c)=1$ we have $2 \nmid a$ and therefore $a^2 \equiv 1 \pmod 4$.

As $c^2 | (a^2-b^2d)$ we know $a^2 - b^2 d \equiv 0 \pmod 4$. Assuming $2|b$ would lead to $a^2 \equiv a^2 - db^2 \equiv 0 \pmod 4$ and thus to $2|a$, a contradiction. Therefore $2 \nmid b$ and $b^2 \equiv 1 \pmod 4$ which implies $d \equiv db^2 \equiv a^2 \equiv 1 \pmod 4$ and

$$\alpha = \frac{a+b\sqrt{d}}{2} = \frac{a-b}{2} + b\frac{1+\sqrt{d}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right].$$

Remark: Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field, $\sigma_1 : K \hookrightarrow \mathbb{C}$, $\sigma_1(a+b\sqrt{d}) = a+b\sqrt{d}$ and $\sigma_2 : K \hookrightarrow \mathbb{C}$, $\sigma_2(a+b\sqrt{d}) = a-b\sqrt{d}$ (with $a,b \in \mathbb{Q}$). If $d>0$ then $\mathbb{Q}(\sqrt{d})$ is totally real (i.e., $r(K)=2$, $s(K)=0$). If $d<0$ then $\mathbb{Q}(\sqrt{d})$ is totally imaginary (i.e., $r(K)=0$ and $s(K)=1$ as $\sigma_2 = \overline{\sigma_1}$).

Theorem 70 Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field.

(i) If $d \not\equiv 1 \pmod 4$ then $\{1, \sqrt{d}\}$ is an integral basis for K and $d_K = 4d$,

(ii) If $d \equiv 1 \pmod 4$ then $\{1, \frac{1+\sqrt{d}}{2}\}$ is an integral basis for K and $d_K = d$.

Proof: According to Theorem 69 $\{1,\sqrt{d}\}$ resp. $\{1, \frac{1+\sqrt{d}}{2}\}$ is an integral basis for K. (Note that $\{1,\sqrt{d}\}$ resp. $\{1,\frac{1+\sqrt{d}}{2}\}$ is a basis of K as a $\mathbb{Q}$-vector space.)

If $d \not\equiv 1 \pmod 4$ then $d_K = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = (-2\sqrt{d})^2 = 4d$.

If $d \equiv 1 \pmod 4$ then $d_K = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = \left(\frac{1-\sqrt{d}}{2} - \frac{1+\sqrt{d}}{2}\right)^2 = (-\sqrt{d})^2 = d$.

Corollary 71 If K is a quadratic number field, then $K = \mathbb{Q}(\sqrt{d_K})$.

Proof: Follows immediately from Theorem 70.

Remarks: 1) We could have calculated the discriminant d_K using Corollary 64. If $d \not\equiv 1 \pmod 4$ then $\{1,\sqrt{d}\}$ is an integral basis and $m_{\mathbb{Q},\sqrt{d}}(X) = X^2 - d$. Thus $m'_{\mathbb{Q},\sqrt{d}}(X) = 2X \Rightarrow m'_{\mathbb{Q},\sqrt{d}}(\sqrt{d}) = 2\sqrt{d} \Rightarrow d_K = -N_{K/\mathbb{Q}}(2\sqrt{d}) = -(2\sqrt{d})(-2\sqrt{d}) = 4d$.

If $d \equiv 1 \pmod 4$ then $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ is an integral basis and $m_{\mathbb{Q}, \frac{1+\sqrt{d}}{2}}(X) = X^2 - X + \frac{1-d}{4}$. Thus

$m'_{\mathbb{Q}, \frac{1+\sqrt{d}}{2}}(X) = 2X - 1 \Rightarrow m'_{\mathbb{Q}, \frac{1+\sqrt{d}}{2}}\left(\frac{1+\sqrt{d}}{2}\right) = \sqrt{d} \Rightarrow d_K = -N_{K/\mathbb{Q}}(\sqrt{d}) = -\sqrt{d}(-\sqrt{d}) = d.$

2) In order to prove that $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ is an integral basis if $d \equiv 1 \pmod 4$ we could have used the following argument: $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ is a basis of K (as a $\mathbb{Q}$-vector space) and $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$. As $\Delta_{K/\mathbb{Q}}\left(1, \frac{1+\sqrt{d}}{2}\right) = d$ is squarefree, Theorem 62 implies that $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ is an integral basis.

If $d \not\equiv 1 \pmod 4$ one can modify this argument as follows: $\{1, \sqrt{d}\}$ is a basis of K (as a $\mathbb{Q}$-vector space) and $\Delta_{K/\mathbb{Q}}(1, \sqrt{d}) = 4d$. The second remark after Theorem 62 implies $d_K \mid (4d)$ and that $\frac{4d}{d_K}$ is a square (in $\mathbb{Z}$) and thus $d_K \in \{d, 4d\}$.

If $d_K = d$ then $d_K \not\equiv 0 \pmod 4$ (as $4 \mid d_K \Rightarrow 4 \mid d \Rightarrow d$ is not squarefree) and $d_K \not\equiv 1 \pmod 4$ (as $d \not\equiv 1 \pmod 4$). This a contradiction to Corollary 66 and therefore $d_K = 4d$.

This shows that $\{1, \sqrt{d}\}$ is an integral basis.

3) Theorem 70 shows that the converse of Theorem 62 is not true. (An easy example is $K = \mathbb{Q}(i)$, i.e., $d = -1$ and $d_K = -4$ which is not squarefree.)

4) The discriminant of a quadratic number field determines the field, i.e., if one knows $[K:\mathbb{Q}] = 2$ and d_K one knows K.

<u>Theorem 72</u> Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field with $d < 0$. Then

$$\mathcal{O}_K^* = \begin{cases} \{1, -1, i, -i\} & \text{if } d = -1, \\ \{1, -1, \omega, -\omega, \omega^2, -\omega^2\} & \text{if } d = -3 \ (\text{where } \omega = e^{2\pi i/3} = \tfrac{1}{2}(-1+i\sqrt{3})), \\ \{1, -1\} & \text{if } d < 0 \text{ is a squarefree integer and } d \notin \{-1, -3\} \end{cases}$$

and

$$(\mathcal{O}_K^*, \cdot) \cong \begin{cases} (\mathbb{Z}/4\mathbb{Z}, +) & \text{if } d = -1, \\ (\mathbb{Z}/6\mathbb{Z}, +) & \text{if } d = -3, \\ (\mathbb{Z}/2\mathbb{Z}, +) & \text{if } d < 0 \text{ is a squarefree integer and } d \notin \{-1, -3\}. \end{cases}$$

<u>Proof</u>: By Theorem 59 (ii) $r + s\sqrt{d} \in \mathcal{O}_K^*$ (where $r, s \in \mathbb{Q}$) $\Leftrightarrow N_{K/\mathbb{Q}}(r + s\sqrt{d}) \in \{1, -1\}$

$\Leftrightarrow r^2 - s^2 d = r^2 + s^2 |d| \in \{1, -1\} \Leftrightarrow r^2 - s^2 d = 1.$

If $d = -1$ then $\alpha = a + bi \in \mathcal{O}_K^* = \mathbb{Z}[i]^*$ (with $a, b \in \mathbb{Z}$) $\Leftrightarrow a^2 + b^2 = 1$

$\Leftrightarrow (a, b) \in \{(1,0), (-1,0), (0,1), (0,-1)\} \Leftrightarrow \alpha \in \{1, -1, i, -i\}$

If $d \leq -2$ and $d \not\equiv 1 \pmod 4$ then $\alpha = a + b\sqrt{d} \in \mathcal{O}_K^* = \mathbb{Z}[\sqrt{d}]^*$ (with $a, b \in \mathbb{Z}$)

$\Leftrightarrow a^2 - db^2 = 1$. If $b \neq 0$ then $a^2 - db^2 = \underbrace{a^2}_{\geq 0} + \underbrace{|d|}_{\geq 2}\underbrace{b^2}_{\geq 1} \geq 2$ and therefore $b = 0$. Thus

$a^2 = 1 \Rightarrow a \in \{1,-1\} \Rightarrow \alpha \in \{1,-1\}$ (and of course $1, -1 \in \mathcal{O}_K^*$).

Now let $d \leq -3$ and $d \equiv 1 \pmod 4$. Then $\alpha = r + s\sqrt{d} \in \mathcal{O}_K^* = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]^*$ (with $r, s \in \mathbb{Q}$)

$\Leftrightarrow r^2 - s^2 d = 1$. If $r, s \in \mathbb{Z}$ then $s = 0$ (as in the case $d \not\equiv 1 \pmod 4$) and $\alpha \in \{1,-1\}$.

This leaves the case $r = \frac{a}{2}$, $s = \frac{b}{2}$ with $a, b \in \mathbb{Z}$ and $a \equiv b \equiv 1 \pmod 2$ (which was shown in the proof of Theorem 69). This implies $a^2 - db^2 = 4$.

If $d < -3$ (and thus $d \leq -7$) then $b = 0$ (as $b \neq 0 \Rightarrow a^2 - b^2 d = \underbrace{a^2}_{\geq 0} + \underbrace{|d|}_{\geq 7}\underbrace{b^2}_{\geq 1} \geq 7$). This implies $a^2 = 4$ and therefore $a \in \{2,-2\}$ which contradicts $2 \nmid a$. This shows $\alpha \in \{1,-1\}$ for $d \equiv 1 \pmod 4$ and $d < -3$.

If $d = -3$ the equation $a^2 + 3b^2 = 4$ (with $a \equiv b \equiv 1 \pmod 2$) has exactly the solutions $(a,b) \in \{(1,1), (1,-1), (-1,1), (1,1)\}$ which leads to

$\alpha \in \left\{1, -1, \frac{1+\sqrt{3}i}{2}, \frac{1-\sqrt{3}i}{2}, \frac{-1+\sqrt{3}i}{2}, \frac{-1-\sqrt{3}i}{2}\right\}$. As $\left(\frac{-1+\sqrt{3}i}{2}\right)^2 = \frac{-1-\sqrt{3}i}{2}$ this shows

$\alpha \in \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$.

<u>Remark:</u> If $K = \mathbb{Q}(i)$ then $\mathcal{O}_K^* = \{1,-1,i,-i\}$ by Theorem 72. This implies that the associates of $a+bi \in \mathcal{O}_K = \mathbb{Z}[i]$ are $a+bi, -a-bi, -b+ai, b-ai$. This gives us an example which shows that the converse of Theorem 59 (iii) is not true. Clearly $2+3i, 3+2i \in \mathbb{Z}[i]$ and $N_{\mathbb{Q}(i)/\mathbb{Q}}(2+3i) = N_{\mathbb{Q}(i)/\mathbb{Q}}(3+2i) = 13$ but $2+3i$ and $3+2i$ are not associates.

<u>Theorem 73</u> Let $K = \mathbb{Q}(\sqrt{2})$. Then $\mathcal{O}_K^* = \mathbb{Z}[\sqrt{2}]^* = \{\pm(1+\sqrt{2})^n \mid n \in \mathbb{Z}\}$ and therefore $(\mathcal{O}_K^*, \cdot) \cong ((\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}, +)$

<u>Proof</u>: For $n \in \mathbb{Z}$ we have $\pm(1+\sqrt{2})^n \in \mathbb{Z}[\sqrt{2}]^*$ as $(1+\sqrt{2})\cdot(-1+\sqrt{2}) = 1$ implies $(\pm(1+\sqrt{2})^n)(\pm(-1+\sqrt{2})^n) = ((1+\sqrt{2})(-1+\sqrt{2}))^n = 1^n = 1$.

We claim that there is no $\varepsilon \in \mathbb{Z}[\sqrt{2}]^*$ with $1 < \varepsilon < 1+\sqrt{2}$. $(*)$

Suppose that such an ε exists. Then $N_{K/\mathbb{Q}}(\varepsilon) \in \{1,-1\}$ by Theorem 59 (ii). Let $\sigma_1 : \mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{C}$, $\sigma_1(x+\sqrt{2}y) = x+\sqrt{2}y$ and $\sigma_2 : \mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{C}$, $\sigma_2(x+\sqrt{2}y) = x-\sqrt{2}y$ (with $x, y \in \mathbb{Q}$) and set $\varepsilon' = \sigma_2(\varepsilon)$, i.e., $N_{K/\mathbb{Q}}(\varepsilon) = \varepsilon\varepsilon' = \pm 1$.

<u>1st case</u> $N_{K/\mathbb{Q}}(\varepsilon)=1$. Then $\sqrt{2}-1=(1+\sqrt{2})^{-1}<\varepsilon^{-1}=\varepsilon'<1$. Addition of $(*)$ to these inequalities yields $\sqrt{2}<\varepsilon+\varepsilon'<2+\sqrt{2}$ and therefore $\frac{1}{\sqrt{2}}<\frac{\varepsilon+\varepsilon'}{2}<1+\frac{1}{\sqrt{2}}$. As $\frac{\varepsilon+\varepsilon'}{2}=\frac{1}{2}\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon)\in\mathbb{Z}$ we get $\frac{\varepsilon+\varepsilon'}{2}=1$. So we would have $\varepsilon\varepsilon'=1$ and $\varepsilon+\varepsilon'=2$. Thus

$\varepsilon(2-\varepsilon)=1 \Rightarrow (\varepsilon-1)^2=\varepsilon^2-2\varepsilon+1=0 \Rightarrow \varepsilon=\varepsilon'=1$ which contradicts $\varepsilon>1$.

<u>2nd case</u> $N_{K/\mathbb{Q}}(\varepsilon)=-1$. Then $\varepsilon'<0$ and $(*)$ implies $-1<\varepsilon'=-\varepsilon^{-1}<1-\sqrt{2}$. This implies $0<\varepsilon+\varepsilon'<2$ and therefore $0<\frac{\varepsilon+\varepsilon'}{2}<1$, which is impossible as $\frac{\varepsilon+\varepsilon'}{2}=\frac{1}{2}\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon)\in\mathbb{Z}$.

We proceed to show that every $\delta\in\mathbb{Z}[\sqrt{2}]^*$ has shape $\delta=\pm(1+\sqrt{2})^n$ for some $n\in\mathbb{Z}$.

<u>1st case</u> $\delta\geq 1+\sqrt{2}$. Then $\exists n\in\mathbb{N}:(1+\sqrt{2})^n\leq\delta<(1+\sqrt{2})^{n+1}$ and therefore

$1\leq\delta(1+\sqrt{2})^{-n}<1+\sqrt{2}$. As $\delta(1+\sqrt{2})^{-n}\in\mathbb{Z}[\sqrt{2}]^*$ we get $\delta(1+\sqrt{2})^{-n}=1$ and $\delta=(1+\sqrt{2})^n$.

<u>2nd case</u> $0<\delta<1$. Then $\delta^{-1}\in\mathbb{Z}[\sqrt{2}]^*$ and $\delta^{-1}>1$. The first case implies that $\exists n\in\mathbb{N}:\delta^{-1}=(1+\sqrt{2})^n$ and $\delta=(1+\sqrt{2})^{-n}$.

<u>3rd case</u> $-1<\delta<0$. Then $-\delta^{-1}\in\mathbb{Z}[\sqrt{2}]^*$ and $-\delta^{-1}>1$. The first case implies that $\exists n\in\mathbb{N}:-\delta^{-1}=(1+\sqrt{2})^n$ and $\delta=-(1+\sqrt{2})^{-n}$.

<u>4th case</u> $\delta<-1$. Then $-\delta\in\mathbb{Z}[\sqrt{2}]^*$ and $-\delta>1$. The first case implies that $\exists n\in\mathbb{N}:-\delta=(1+\sqrt{2})^n$ and $\delta=-(1+\sqrt{2})^n$.

<u>5th case</u> $\delta=\pm1$. Then $\delta=\pm(1+\sqrt{2})^0$.

28.11.2022

<u>Remark:</u> For all squarefree $d>1$ the unit group $\mathcal{O}^*_{\mathbb{Q}(\sqrt{d})}$ has always this shape, i.e., there is an $\varepsilon\in\mathcal{O}^*_{\mathbb{Q}(\sqrt{d})}$ such that $\mathcal{O}^*_{\mathbb{Q}(\sqrt{d})}=\{\pm\varepsilon^n\mid n\in\mathbb{Z}\}$. Such an $\varepsilon\in\mathcal{O}^*_{\mathbb{Q}(\sqrt{d})}$ is called a fundamental unit [dt. Fundamentaleinheit]. This implies $(\mathcal{O}^*_{\mathbb{Q}(\sqrt{d})},\cdot)\cong((\mathbb{Z}/2\mathbb{Z})\oplus\mathbb{Z},+)$. This is a special case of Dirichlet's unit theorem [dt. Dirichletscher Einheitensatz]. There is no simple formula for ε but an algorithm for its calculation.

<u>Definition:</u> An algebraic number field is called norm-euclidean [dt. normeuklidisch] if $\mathcal{O}_K$ is an euclidean domain with respect to the map $\varphi:\mathcal{O}_K\to\mathbb{N}\cup\{0\}$, $\varphi(\alpha)=|N_{K/\mathbb{Q}}(\alpha)|$.

(i.e., $\forall\alpha,\beta\in\mathcal{O}_K,\beta\neq0\ \exists\gamma,\delta\in\mathcal{O}_K:\alpha=\gamma\beta+\delta$ and $\delta=0$ or $|N_{K/\mathbb{Q}}(\delta)|<|N_{K/\mathbb{Q}}(\beta)|$.)

<u>Remarks:</u> 1) If K is norm-euclidean then $\mathcal{O}_K$ is a principal ideal domain and therefore a unique factorization domain (see algebra).

2) If $\alpha|\beta$ and $\beta\neq0$ (with $\alpha,\beta\in\mathcal{O}_K$) then $|N_{K/\mathbb{Q}}(\alpha)|\leq|N_{K/\mathbb{Q}}(\beta)|$. (The assumption $\alpha|\beta$ just says $\exists\gamma\in\mathcal{O}_K:\beta=\alpha\gamma$, where $\gamma\neq0$ as $\beta\neq0$. Therefore
$|N_{K/\mathbb{Q}}(\beta)|=|N_{K/\mathbb{Q}}(\alpha\gamma)|=|N_{K/\mathbb{Q}}(\alpha)\cdot N_{K/\mathbb{Q}}(\gamma)|=|N_{K/\mathbb{Q}}(\alpha)|\cdot\underbrace{|N_{K/\mathbb{Q}}(\gamma)|}_{\geq1}\geq|N_{K/\mathbb{Q}}(\alpha)|$.)

Lemma 74 Let K be an algebraic number field. Then the following are equivalent:

(i) $\forall \alpha, \beta \in \mathcal{O}_K, \beta \neq 0 \ \exists \gamma, \delta \in \mathcal{O}_K : \alpha = \beta\gamma + \delta$ and $\delta = 0$ or $|N_{K/\mathbb{Q}}(\delta)| < |N_{K/\mathbb{Q}}(\beta)|$,

(ii) $\forall \zeta \in K \ \exists \gamma \in \mathcal{O}_K : |N_{K/\mathbb{Q}}(\zeta - \gamma)| < 1$

Proof: (i) $\Rightarrow$ (ii) If $\zeta = 0$ let $\gamma = 0$. Then $|N_{K/\mathbb{Q}}(\zeta - \gamma)| = 0 < 1$.

Let $\zeta \neq 0$. By Lemma 53 there is a $c \in \mathbb{Z}\setminus\{0\}$ such that $c\zeta \in \mathcal{O}_K \setminus \{0\}$. We apply (i) with $\alpha = c\zeta$ and $\beta = c$, i.e., there are $\gamma, \delta \in \mathcal{O}_K$ such that $c\zeta = c\gamma + \delta$ and either $\delta = 0$ or $|N_{K/\mathbb{Q}}(\delta)| < |N_{K/\mathbb{Q}}(c)|$.

If $\delta = 0$ then $c\zeta = c\gamma$ and therefore $\zeta = \gamma$ and $|N_{K/\mathbb{Q}}(\zeta - \gamma)| = 0 < 1$.

If $|N_{K/\mathbb{Q}}(\delta)| < |N_{K/\mathbb{Q}}(c)|$ then $|N_{K/\mathbb{Q}}(\zeta - \gamma)| = \left|N_{K/\mathbb{Q}}\left(\frac{\delta}{c}\right)\right| = \dfrac{|N_{K/\mathbb{Q}}(\delta)|}{|N_{K/\mathbb{Q}}(c)|} < 1$

(ii) $\Rightarrow$ (i) Use (ii) with $\zeta = \frac{\alpha}{\beta}$. There is a $\gamma \in \mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\frac{\alpha}{\beta} - \gamma)| < 1$.

If $\frac{\alpha}{\beta} = \gamma$ we get $\alpha = \beta\gamma$ and we set $\delta = 0$. If $\frac{\alpha}{\beta} \neq \gamma$ then $\delta := \alpha - \beta\gamma \neq 0$. Therefore

$$\frac{|N_{K/\mathbb{Q}}(\delta)|}{|N_{K/\mathbb{Q}}(\beta)|} = \frac{|N_{K/\mathbb{Q}}(\alpha - \beta\gamma)|}{|N_{K/\mathbb{Q}}(\beta)|} = \left|N_{K/\mathbb{Q}}\left(\frac{\alpha}{\beta} - \gamma\right)\right| < 1 \text{ and } |N_{K/\mathbb{Q}}(\delta)| < |N_{K/\mathbb{Q}}(\beta)|.$$

Theorem 75 Let $d \in \mathbb{Z}$, $d < 0$ be squarefree. The quadratic number field $K = \mathbb{Q}(\sqrt{d})$ is norm-euclidean if $d \in \{-1, -2, -3, -7, -11\}$.

Proof: If $d \in \{-1, -2\}$ then $d \not\equiv 1 \pmod 4$ and $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. For $r + s\sqrt{d} \in K$ (with $r, s \in \mathbb{Q}$) choose $a, b \in \mathbb{Z}$ with $|r - a| \leq \frac{1}{2}$ and $|s - b| \leq \frac{1}{2}$. Then

$$|N_{K/\mathbb{Q}}((r + s\sqrt{d}) - (a + b\sqrt{d}))| = |N_{K/\mathbb{Q}}((r-a) + (s-b)\sqrt{d})| = (r-a)^2 - d(s-b)^2$$

$$= (r-a)^2 + |d|(s-b)^2 \leq \frac{1}{4} + 2 \cdot \frac{1}{4} = \frac{3}{4} = 1$$

and the assertion follows from Lemma 74.

If $d \in \{-3, -7, -11\}$ then $d \equiv 1 \pmod 4$ and $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}$. For $r + s\sqrt{d} \in K$ (with $r, s \in \mathbb{Q}$) choose $a, b \in \mathbb{Z}$ such that $|2s - b| \leq \frac{1}{2}$ and $|r - \frac{1}{2}b - a| \leq \frac{1}{2}$. Then

$$\left|N_{K/\mathbb{Q}}\left((r + s\sqrt{d}) - \left(a + b\frac{1+\sqrt{d}}{2}\right)\right)\right| = \left|N_{K/\mathbb{Q}}\left(\left(r - a - \frac{b}{2}\right) + \left(s - \frac{b}{2}\right)\sqrt{d}\right)\right|$$

$$= \left(r - a - \frac{b}{2}\right)^2 - d\left(s - \frac{b}{2}\right)^2 = \left(r - a - \frac{b}{2}\right)^2 + |d|\frac{(2s-b)^2}{4} \leq \frac{1}{4} + 11 \cdot \frac{1}{16} = \frac{15}{16} < 1$$

and the assertion follows from Lemma 74.

Theorem 76 Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field. If $d \in \{-5, -6, -10\}$ the ring $\mathcal{O}_K$ is not a unique factorization domain (and therefore not a euclidean domain).

Proof: If $K = \mathbb{Q}(i\sqrt{5})$ then $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}i\sqrt{5}$. We have $N_{K/\mathbb{Q}}(\alpha) \geq 0 \ \forall \alpha \in \mathcal{O}_K$ as $N_{K/\mathbb{Q}}(a + i\sqrt{5}b) = a^2 + 5b^2 \geq 0 \ \forall a, b \in \mathbb{Z}$.

There is no $\alpha \in \mathcal{O}_K$ such that $N_{K|\mathbb{Q}}(\alpha) \in \{2,3\}$. (Let $a, b \in \mathbb{Z}$. If $b \neq 0$ then $N_{K|\mathbb{Q}}(a+i\sqrt{5}b) = a^2+5b^2 \geq 5$. If $b=0$ then $N_{K|\mathbb{Q}}(a+i\sqrt{5}b) = a^2 \notin \{2,3\}$.)

We have $6 = 2\cdot 3 = (1+i\sqrt{5})\cdot(1-i\sqrt{5})$. We claim that $2, 3, 1+i\sqrt{5}$ and $1-i\sqrt{5}$ are all irreducible in $\mathcal{O}_K$:

2 reducible $\Rightarrow \exists \alpha, \beta \in \mathcal{O}_K \setminus \mathcal{O}_K^*: 2 = \alpha\beta \Rightarrow N_{K|\mathbb{Q}}(\alpha)\cdot N_{K|\mathbb{Q}}(\beta) = 4$

As $\alpha, \beta \notin \mathcal{O}_K^*$ this implies $N_{K|\mathbb{Q}}(\alpha) = N_{K|\mathbb{Q}}(\beta) = 2$, which is impossible.

3 reducible $\Rightarrow \exists \alpha, \beta \in \mathcal{O}_K \setminus \mathcal{O}_K^*: 3 = \alpha\beta \Rightarrow N_{K|\mathbb{Q}}(\alpha)\cdot N_{K|\mathbb{Q}}(\beta) = 9$

As $\alpha, \beta \notin \mathcal{O}_K^*$ this implies $N_{K|\mathbb{Q}}(\alpha) = N_{K|\mathbb{Q}}(\beta) = 3$, which is impossible.

$1 \pm i\sqrt{5}$ reducible $\Rightarrow \exists \alpha, \beta \in \mathcal{O}_K \setminus \mathcal{O}_K^*: 1 \pm i\sqrt{5} = \alpha\beta \Rightarrow N_{K|\mathbb{Q}}(\alpha)\cdot N_{K|\mathbb{Q}}(\beta) = 6$

As $\alpha, \beta \notin \mathcal{O}_K^*$ this implies $N_{K|\mathbb{Q}}(\alpha), N_{K|\mathbb{Q}}(\beta) \in \{2,3\}$, which is impossible.

As $\mathcal{O}_K^* = \{1,-1\}$ by Theorem 72, 2 is neither an associate of $1+i\sqrt{5}$ nor of $1-i\sqrt{5}$.

This shows that $\mathcal{O}_K$ is not a unique factorization domain.

If $K = \mathbb{Q}(i\sqrt{6})$ (resp. $K = \mathbb{Q}(i\sqrt{10})$) the proof runs along the same lines starting from $6 = 2\cdot 3 = i\sqrt{6}\cdot(-i\sqrt{6})$ (resp. $14 = 2\cdot 7 = (2+i\sqrt{10})(2-i\sqrt{10})$). (Exercise)

<u>Theorem 77</u> Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d < -11$ squarefree. Then $\mathcal{O}_K$ is not an euclidean domain.

<u>Proof</u>: Suppose there is a function $\varphi: \mathcal{O}_K \setminus \{0\} \to \mathbb{N} \cup \{0\}$ such that $\mathcal{O}_K$ is an euclidean domain with respect to φ. (Here $\varphi(\alpha) = |N_{K|\mathbb{Q}}(\alpha)|$ is possible but we do not restrict ourselves to this function.) Choose an $\alpha \in \mathcal{O}_K \setminus (\mathcal{O}_K^* \cup \{0\})$ with the property $\varphi(\alpha) = \min\{\varphi(x) \mid x \in \mathcal{O}_K \setminus (\mathcal{O}_K^* \cup \{0\})\}$. For all $\beta \in \mathcal{O}_K$ there are $\gamma, \delta \in \mathcal{O}_K$ such that $\beta = \alpha\gamma + \delta$ and either $\delta = 0$ or $\varphi(\delta) < \varphi(\alpha)$. As α was chosen such that $\varphi(\alpha)$ is minimal we have $\delta \in \mathcal{O}_K^* \cup \{0\}$ for all $\beta \in \mathcal{O}_K$. Theorem 72 implies $\delta \in \{-1,0,1\}$.

If $(\alpha) = \alpha\mathcal{O}_K$ denotes the principal ideal generated by α, this implies that each $\beta \in \mathcal{O}_K$ is contained in one of the three cosets $-1+(\alpha), (\alpha)$ and $1+(\alpha)$. This shows that the factor ring $\mathcal{O}_K/(\alpha)$ has the property $|\mathcal{O}_K/(\alpha)| \leq 3$.

We claim that $|\mathcal{O}_K/(\alpha)| = |N_{K|\mathbb{Q}}(\alpha)|$. 30.11.2022

By Theorem 61 $(\mathcal{O}_K, +)$ is a free abelian group of rank 2. As $((\alpha), +)$ is a subgroup of $(\mathcal{O}_K, +)$ Theorem 5 implies that $((\alpha), +)$ is a free abelian group of rank ≤ 2.

As $\mathcal{O}_K/(\alpha)$ is finite $((\alpha), +)$ has rank 2 (because of Corollary 6).

1st case $d \not\equiv 1 \pmod 4$. Then $\{1, \sqrt{d}\}$ is an integral basis for $\mathcal{O}_K$. If $\alpha = a + b\sqrt{d}$ (with $a, b \in \mathbb{Z}$) then $(\alpha) = \alpha\mathcal{O}_K = (a+b\sqrt{d})(\mathbb{Z} + \mathbb{Z}\sqrt{d}) = (a+b\sqrt{d})\mathbb{Z} + (bd + a\sqrt{d})\mathbb{Z}$.

We claim that $\{a+b\sqrt{d}, bd + a\sqrt{d}\}$ is linearly independent over $\mathbb{Z}$. Let

$x(a+b\sqrt{d}) + y(bd + a\sqrt{d}) = 0$ (with $x, y \in \mathbb{Z}$) $\Rightarrow xa + ybd + (xb + ya)\sqrt{d} = 0$

$$\Rightarrow \left.\begin{aligned} xa + ybd &= 0 \\ xb + ya &= 0 \end{aligned}\right\} \Rightarrow \begin{pmatrix} a & bd \\ b & a \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

As $\begin{vmatrix} a & bd \\ b & a \end{vmatrix} = a^2 - db^2 = N_{K/\mathbb{Q}}(\alpha) \neq 0$ (as $\alpha \neq 0$) we get $x = y = 0$.

This shows that $\{a+b\sqrt{d}, bd + a\sqrt{d}\}$ is a $\mathbb{Z}$-basis for $((\alpha), +)$ and Corollary 6 implies $\left|\mathcal{O}_K/(\alpha)\right| = \left|\det\begin{pmatrix} a & b \\ bd & a \end{pmatrix}\right| = |a^2 - b^2 d| = |N_{K/\mathbb{Q}}(\alpha)|$. This implies $a^2 - b^2 d \leq 3$.

If $b \neq 0$ then $a^2 - b^2 d \geq 13$. Therefore $b = 0$ and $a^2 \in \{0, 1\}$. Thus $\alpha = a \in \{-1, 0, 1\}$, i.e., $\alpha \in \mathcal{O}_K^* \cup \{0\}$, a contradiction.

2nd case $d \equiv 1 \pmod 4$. Then $\{1, \frac{1+\sqrt{d}}{2}\}$ is an integral basis for $\mathcal{O}_K$.

If $\alpha = a + b\frac{1+\sqrt{d}}{2}$ (with $a, b \in \mathbb{Z}$) then

$$(\alpha) = \alpha\mathcal{O}_K = \left(a + b\tfrac{1+\sqrt{d}}{2}\right)\left(\mathbb{Z} + \mathbb{Z}\tfrac{1+\sqrt{d}}{2}\right) = \left(a + b\tfrac{1+\sqrt{d}}{2}\right)\mathbb{Z} + \left(a + b\tfrac{1+\sqrt{d}}{2}\right)\tfrac{1+\sqrt{d}}{2}\mathbb{Z}$$

$$= \left(a + b\tfrac{1+\sqrt{d}}{2}\right)\mathbb{Z} + \left(a\tfrac{1+\sqrt{d}}{2} + b\tfrac{1+2\sqrt{d}+d}{4}\right)\mathbb{Z} = \left(a + b\tfrac{1+\sqrt{d}}{2}\right)\mathbb{Z} + \left(a\tfrac{1+\sqrt{d}}{2} + b\tfrac{d-1+2+2\sqrt{d}}{4}\right)\mathbb{Z}$$

$$= \left(a + b\tfrac{1+\sqrt{d}}{2}\right)\mathbb{Z} + \left(b\tfrac{d-1}{4} + (a+b)\tfrac{1+\sqrt{d}}{2}\right)\mathbb{Z}.$$

We claim that $\left\{a + b\frac{1+\sqrt{d}}{2}, b\frac{d-1}{4} + (a+b)\frac{1+\sqrt{d}}{2}\right\}$ is linearly independent over $\mathbb{Z}$. Let

$x\left(a + b\frac{1+\sqrt{d}}{2}\right) + y\left(b\frac{d-1}{4} + (a+b)\frac{1+\sqrt{d}}{2}\right) = 0$ (with $x, y \in \mathbb{Z}$)

$\Rightarrow xa + yb\frac{d-1}{4} + (xb + y(a+b))\frac{1+\sqrt{d}}{2} = 0$

$$\Rightarrow \left.\begin{aligned} xa + yb\tfrac{d-1}{4} &= 0 \\ xb + y(a+b) &= 0 \end{aligned}\right\} \Rightarrow \begin{pmatrix} a & b\frac{d-1}{4} \\ b & a+b \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

We have

$$N_{K/\mathbb{Q}}(\alpha) = \left(a + b\tfrac{1+\sqrt{d}}{2}\right)\left(a + b\tfrac{1-\sqrt{d}}{2}\right) = \left(a + \tfrac{b}{2} + \tfrac{b}{2}\sqrt{d}\right)\left(a + \tfrac{b}{2} - \tfrac{b}{2}\sqrt{d}\right)$$

$$= \left(a + \tfrac{b}{2}\right)^2 - \tfrac{b^2 d}{4} = a^2 + ab + \tfrac{b^2}{4} - \tfrac{b^2 d}{4} = a^2 + ab + b^2\tfrac{1-d}{4}.$$

As $\begin{vmatrix} a & b\frac{d-1}{4} \\ b & a+b \end{vmatrix} = a^2 + ab + b^2\frac{1-d}{4} = N_{K/\mathbb{Q}}(\alpha) \neq 0$ (as $\alpha \neq 0$) we get $x = y = 0$.

This shows that $\left\{a+b\frac{1+\sqrt{d}}{2},\ b\frac{d-1}{4}+(a+b)\frac{1+\sqrt{d}}{2}\right\}$ is a $\mathbb{Z}$-basis for $((\alpha),+)$ and Corollary 6 implies

$$\left|\mathcal{O}_K/(\alpha)\right| = \left|\det\begin{pmatrix} a & b \\ b\frac{d-1}{4} & a+b\end{pmatrix}\right| = \left|a^2+ab+b^2\frac{1-d}{4}\right| = \left|N_{K/\mathbb{Q}}(\alpha)\right|.$$ This implies

$a^2+ab+b^2\frac{1-d}{4} \leq 3$. If $b \neq 0$ then $a^2+ab+b^2\frac{1-d}{4} = \left(a+\frac{b}{2}\right)^2 - \frac{b^2 d}{4} \geq \frac{13}{4} > 3$. Therefore $b=0$ and $a^2 \in \{0,1\}$. Thus $\alpha = a \in \{-1,0,1\}$, i.e., $\alpha \in \mathcal{O}_K^* \cup \{0\}$, a contradiction.

Remarks: 1) Theorems 75, 76 and 77 together show the following fact: if $d<0$ is squarefree and $K=\mathbb{Q}(\sqrt{d})$ then $\mathcal{O}_K$ is euclidean if and only if $d \in \{-1,-2,-3,-7,-11\}$ (and $\mathbb{Q}(\sqrt{d})$ is norm-euclidean for those d).

2) There are four further squarefree $d<0$ for which $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a unique factorization domain (namely $-19,-43,-67,-163$), however, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is not euclidean in these cases. Gauß conjectured that there are no further squarefree $d<0$ such that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a unique factorization domain. HEEGNER (1952) gave an incomplete proof (which was completed later). The first complete proof was given by STARK (1967).

3) There are exactly 16 squarefree $d>1$ such that $\mathbb{Q}(\sqrt{d})$ is norm-euclidean, namely 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57 and 73. This is the work of many mathematicians and was completed by CHATLAND and DAVENPORT (1950). However, in contrast to the case $d<0$ there are squarefree $d>1$ such that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is euclidean but not norm-euclidean. This was first proved for $d=69$ by CLARK (1994) (i.e., $\mathbb{Z}\left[\frac{1+\sqrt{69}}{2}\right]$ is euclidean but not norm-euclidean). It has been conjectured that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is euclidean if it is a unique factorization domain. Among the 60 squarefree $d \in \{2,3,\dots,100\}$ there are exactly 38 for which $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a unique factorization domain. It is not known whether there are infinitely many squarefree $d>1$ such that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a unique factorization domain.

Theorem 78 (FERMAT) Let p be a prime. Then the following are equivalent:

(i) $\exists\, x,y \in \mathbb{Z}: x^2+y^2=p$,

(ii) $p=2$ or $p \equiv 1 \pmod 4$.

Proof: (i) $\Rightarrow$ (ii) If $2 \mid x$ then $x^2 \equiv 0 \pmod 4$ and if $2 \nmid x$ then $x^2 \equiv 1 \pmod 4$. This implies $p = x^2+y^2 \equiv 0 \pmod 4$ (which is impossible), $p = x^2+y^2 \equiv 2 \pmod 4$ (and therefore $p=2$) or $p = x^2+y^2 \equiv 1 \pmod 4$.

(ii) $\Rightarrow$ (i) $2 = 1^2 + 1^2$. If $p \equiv 1 \pmod 4$ we know from elementary number theory that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$. (Here $\left(\frac{-1}{p}\right)$ denotes the Legendre-symbol.) This says that there is an $m \in \mathbb{Z}$ such that $m^2 \equiv -1 \pmod p$ or equivalently $p \mid (m^2+1)$ (in $\mathbb{Z}$), which can be rewritten as $p \mid (m+i)(m-i)$ (in $\mathbb{Z}[i]$). As $\frac{m \pm i}{p} = \frac{m}{p} \pm \frac{1}{p} i \notin \mathbb{Z}[i]$ we see that $p \nmid (m \pm i)$ (in $\mathbb{Z}[i]$). This shows that p is not a prime element of $\mathbb{Z}[i]$ and is therefore reducible. Consequently there are $x, y, u, v \in \mathbb{Z}$ such that $p = (x+iy)(u+iv)$, where $x+iy, u+iv \notin \mathbb{Z}[i]^*$. Taking norms yields

$$p^2 = N_{\mathbb{Q}(i)/\mathbb{Q}}(p) = N_{\mathbb{Q}(i)/\mathbb{Q}}(x+iy) \cdot N_{\mathbb{Q}(i)/\mathbb{Q}}(u+iv) = (x^2+y^2)(u^2+v^2)$$

where $x^2+y^2, u^2+v^2 \notin \{1,-1\}$ (because of Theorem 59(iii)). Therefore $p = x^2+y^2 = u^2+v^2$

Theorem 79 The prime elements of $\mathbb{Z}[i]$ are

(a) $1+i$ (and its associates $-1+i, -1-i, 1-i$),

(b) $a+bi, a-bi$ (and $-a-bi, -b+ai, b-ai$ which are the associates of $a+bi$ and $-a+bi, b+ai, -b-ai$ which are the associates of $a-bi$)

where $a > b > 0$ and there is a prime $p \equiv 1 \pmod 4$ such that $a^2+b^2 = p$,

(c) p where $p \equiv 3 \pmod 4$ is a prime (and its associates $-p, ip, -ip$). 5.12.2022

Proof: As $N_{\mathbb{Q}(i)/\mathbb{Q}}(1+i) = 2$ Theorem 59 (iv) implies that $1+i$ is irreducible in $\mathbb{Z}[i]$. As $\mathbb{Z}[i]$ is a unique factorisation domain $1+i$ is a prime element of $\mathbb{Z}[i]$.
If $p \equiv 1 \pmod 4$ there are $a, b \in \mathbb{Z}$ such that $a^2+b^2 = p$. W.l.o.g. we can assume $a \geq b \geq 0$. As $b = 0$ ($\Rightarrow p = a^2$) and $a = b$ ($\Rightarrow p = 2a^2$) are impossible we can demand $a > b > 0$. Therefore we have $p = a^2+b^2 = (a+ib)(a-ib)$. As $N_{\mathbb{Q}(i)/\mathbb{Q}}(a+ib) = N_{\mathbb{Q}(i)/\mathbb{Q}}(a-ib) = a^2+b^2 = p$ both $a+ib$ and $a-ib$ are irreducible (and therefore prime) in $\mathbb{Z}[i]$ by Theorem 59(iv). However, $a+ib$ and $a-ib$ are not associates as there is no $\varepsilon \in \mathbb{Z}[i]^* = \{1,-1,i,-i\}$ such that $a-ib = \varepsilon(a+ib)$. As $\mathbb{Z}[i]$ is a unique factorisation domain a and b (with $a > b > 0$) are uniquely determined by p.
Let $p \equiv 3 \pmod 4$ be a prime. Suppose that p is not irreducible in $\mathbb{Z}[i]$. Then there are $\alpha, \beta \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^*$ such that $p = \alpha \cdot \beta$ and therefore $N_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha) \cdot N_{\mathbb{Q}(i)/\mathbb{Q}}(\beta) = N_{\mathbb{Q}(i)/\mathbb{Q}}(p) = p^2$. If $N_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha) \in \{1,-1\}$ or $N_{\mathbb{Q}(i)/\mathbb{Q}}(\beta) \in \{1,-1\}$ then $\alpha \in \mathbb{Z}[i]^*$ or $\beta \in \mathbb{Z}[i]^*$ which contradicts our assumption. Therefore $N_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha) = N_{\mathbb{Q}(i)/\mathbb{Q}}(\beta) = p$. If $\alpha = x+iy$ with $x, y \in \mathbb{Z}$

then $x^2+y^2 = N_{\mathbb{Q}(i)/\mathbb{Q}}(x+iy) = p$ which implies that $p=2$ or $p \equiv 1 \pmod 4$ by Theorem 78. This is a contradiction.

This shows that all elements given above are prime elements $\mathbb{Z}[i]$. It remains to check that there are no further prime elements in $\mathbb{Z}[i]$.

Let $\pi \in \mathbb{Z}[i]$ be a prime element and let $\pi\bar{\pi} = N_{\mathbb{Q}(i)/\mathbb{Q}}(\pi) = p_1 \cdots p_r$ be the prime factorisation of $N_{\mathbb{Q}(i)/\mathbb{Q}}(\pi)$ in $\mathbb{Z}$. As $\pi \mid (p_1 \cdots p_r)$ (in $\mathbb{Z}[i]$) there has to be an $i \in \{1, \ldots, r\}$ such that $\pi \mid p_i$ (in $\mathbb{Z}[i]$). I.e., there is a prime p such that $\pi \mid p$. This prime is uniquely determined. (Suppose that there two different primes p and q such that $\pi \mid p$ and $\pi \mid q$. As $\exists x, y \in \mathbb{Z}: px + qy = 1$ this would imply $\pi \mid 1$ and therefore $\pi \in \mathbb{Z}[i]^*$, a contradiction)

1st case: $p = 2$, i.e., $\pi \mid 2 \Rightarrow \pi \mid (2i) \Rightarrow \pi \mid (1+i)^2 \Rightarrow \pi \mid (1+i) \Rightarrow \pi$ is an associate of $1+i$

2nd case: $p \equiv 1 \pmod 4$. Then $p = a^2 + b^2 = (a+bi)(a-bi)$ for some $a, b \in \mathbb{Z}$, $a > b > 0$ and $a \pm bi$ irreducible in $\mathbb{Z}[i] \Rightarrow \pi \mid (a+bi)(a-bi) \Rightarrow \pi \mid (a+bi)$ or $\pi \mid (a-bi)$

$\Rightarrow \pi$ is an associate of $a+bi$ or π is an associate of $a-bi$

3rd case: $p \equiv 3 \pmod 4$. Then p is irreducible in $\mathbb{Z}[i]$ and $\pi \mid p$ implies that π is an associate of p.

Remark: Theorem 79 shows that the converse of Theorem 59 (iv) is not true. E.g., 3 is an irreducible element of $\mathbb{Z}[i]$ but $N_{\mathbb{Q}(i)/\mathbb{Q}}(3) = 3^2 = 9$ is not a prime.