MODEL ANSWERS TO THE SEVENTH HOMEWORK

8.3.4. We have

$$a + 2\sqrt{ab} + b = (\sqrt{a} + \sqrt{b})^2 \in \mathbb{Q}(\sqrt{a} + \sqrt{b}).$$

It follows that $\sqrt{ab} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$. It follows that

$$a\sqrt{b} + b\sqrt{a} = \sqrt{ab}(\sqrt{a} + \sqrt{b}) \in \mathbb{Q}(\sqrt{a} + \sqrt{b}).$$

Subtracting $b(\sqrt{a} + \sqrt{b})$ it follows that

$$\sqrt{b} \in \mathbb{Q}(\sqrt{a} + \sqrt{b}) \qquad \text{so that} \qquad \sqrt{a} \in \mathbb{Q}(\sqrt{a} + \sqrt{b}).$$

Suppose that $\sqrt{b} \in \mathbb{Q}(\sqrt{a})$. Then

$$\sqrt{b} = p + q\sqrt{a}.$$

Squaring both sides gives

$$p^2 + 2pq\sqrt{a} + q^2 = b \in \mathbb{Q}.$$

Thus

$$\sqrt{a} \in \mathbb{Q},$$

a contradiction. It follows that $\mathbb{Q}(\sqrt{a}, \sqrt{b}) \neq \mathbb{Q}(\sqrt{a})$. It follows that

$$1 < [\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}(\sqrt{a})] \leq 2 = \mathbb{Q}(\sqrt{b}) : \mathbb{Q}].$$

so that

$$[\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}(\sqrt{a})] = 2.$$

By the tower law we have

$$\begin{aligned} [\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}] &= [\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}(\sqrt{a})] \cdot [\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] \\ &= 2 \cdot 2 \\ &= 4. \end{aligned}$$

Let

$$\alpha = \sqrt{2} + \sqrt{3}.$$

Then

$$\alpha^2 = 2 + 3 + 2\sqrt{6},$$

so that

$$2\sqrt{6} = \alpha^2 - 5.$$

If we multiply by α we get

$$\begin{aligned} \alpha^3 - 5\alpha &= 2\sqrt{6}(\sqrt{2}+\sqrt{3}) \\ &= 4\sqrt{3} + 6\sqrt{2}. \end{aligned}$$

Subtracting 4α gives

$$2\sqrt{2} = \alpha^3 - 9\alpha.$$

8.4.1. As M is a submodule that properly contains $\mathbb{Z}$, it must contain an element of the form $k\omega$. Let m be the smallest positive multiple of ω contained in M.

Suppose that $\alpha \in M$. Then $\alpha = a + b\omega$. As $\mathbb{Z} \subset M$ we must have $b\omega \in M$. We may write

$$b = qm + r,$$

where $0 \leq r < m$. Note that

$$r\omega = b\omega - q(m\omega) \in M.$$

By minimality of m it follows that $r = 0$. Thus 1 and ω generate M. $m = 1$ if $d \equiv 2$ or 3 modulo 4 and $m = 2$ if $d \equiv 1 \mod 4$.

8.4.4. (a) Note that

$$\zeta = e^{2\pi i/3}.$$

It follows that $\zeta^3 = 1$. We have

$$\begin{aligned} \bar{\zeta} &= e^{-2\pi i/3} \\ &= e^{4\pi i/3} \\ &= \zeta^2. \end{aligned}$$

On the other hand,

$$\begin{aligned} 0 &= \zeta^3 - 1 \\ &= (\zeta - 1)(\zeta^2 + \zeta + 1). \end{aligned}$$

As $\zeta \neq 1$ it follows that

$$\zeta^2 = \zeta + 1.$$

(b) If

$$\alpha = a + b\zeta.$$

then

$$\begin{aligned} N(\alpha) &= \alpha\bar{\alpha} \\ &= (a + b\zeta)(a + b\bar{\zeta}) \\ &= (a + b\zeta)(a + b\zeta^2) \\ &= a^2 + ab(\zeta + \zeta^2) + b^2\zeta^3 \\ &= a^2 - ab + b^2. \end{aligned}$$

If $|a| \leq 1/2$ and $|b| \leq 1/2$ then

$$\begin{aligned} N(\alpha) &\leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} \\ &= \frac{3}{4} \\ &< 1. \end{aligned}$$

(c) Suppose $\alpha = a + b\zeta$ is an algebraic integer. We will show that a and $b \in \mathbb{Z}$.
Subtracting integer multiples of 1 and ζ we may assume that $|a| \in [0, 1/2)$ and $|b| \in [0, 1/2)$, so that $N(\alpha) < 1$.
We must have $N(\alpha) \in \mathbb{Z}$. It follows that $a = b = 0$.
Thus 1 and ζ are a basis for the ring of integers.
(d) We want

$$a^2 - ab + b^2 = \pm 1.$$

Thus

$$a^2 + b^2 = ab \pm 1.$$

Note that a and b cannot have the same parity. If $ab < 0$ then $ab \pm 1 \leq 1$ and so either $ab = 0$, a contradiction. Thus $ab \geq 0$. If $ab = 0$ then $a^2 + b^2 = 1$ and either $a = 0$ and $b = \pm 1$ or $b = 0$ and $a = \pm 1$. Suppose that $ab > 0$. Then $ab \geq 1$. On the other hand, $a^2 + b^2 \geq 2ab$ with equality only if $a = b$. Thus $ab = 1$ and $a = b$. Thus $a = b = 1$ or $a = b = -1$.
This gives ± 1, $\pm\zeta$, $\pm\zeta^2$. These are all clearly units.
(e) Define $d = N$ the norm. Suppose we are given α and $\beta \in \mathbb{Z}(F)$. We have to find $q \in \mathbb{Z}(F)$ such that

$$\beta = q\alpha + r,$$

where either $r = 0$ or $N(r) < N(\alpha)$. Let

$$\gamma = \frac{\beta}{\alpha}.$$

The components of γ are rational numbers; we approximate γ with an integer q. The error r/α then has coefficients at most $1/2$. (b) implies that

$$N(r) < N(\alpha).$$

It follows that $\mathbb{Z}(F)$ is a Euclidean domain.
(f) If $\alpha = a + b\zeta \in \mathbb{Z}(F)$. Consider

$$N(\alpha) = a^2 - ab + b^2 \mod 3.$$

If a, $b \equiv 0$ modulo 3 then $N(\alpha) \equiv 0 \mod 3$. If $a \equiv \pm 1$ and $b \equiv 0$ modulo 3 then $N(\alpha) \equiv 1 \mod 3$. If $a \equiv 1$ and $b \equiv 1$ modulo 3 then

$N(\alpha) \equiv 0 \mod 3$. If $a \equiv 2$ and $b \equiv 2$ modulo 3 then $N(\alpha) \equiv 0 \mod 3$. If $a \equiv 2$ and $b \equiv 1$ modulo 3 then $N(\alpha) \equiv 1 \mod 3$.
It follows that $N(\alpha) \neq 2 \mod 3$.
Suppose $p \in \mathbb{Z}$ is a prime and suppose that $p = \alpha\beta$. Then

$$p^2 = N(\alpha)N(\beta).$$

If $p \equiv 2 \mod 3$ then neither $N(\alpha)$ nor $N(\beta) = p$ and so either $N(\alpha)$ or $N(\beta) = 1$. But then p is a prime in $\mathbb{Z}(F)$.
(g) By what we just proved $\mathbb{Z}(F)$ is a UFD. We look for primes.

$$N(1 - \zeta) = 2$$

and so $1 - \zeta$ is prime. We already saw that if $p \equiv 2 \mod 3$ then p is a prime.
Suppose that $p \equiv 1 \mod 3$. As

$$\begin{aligned} \left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \\ &= \left(\frac{p}{3}\right) \\ &= \left(\frac{1}{3}\right) \\ &= 1, \end{aligned}$$

it follows that -3 is a quadratic residue of p. By 7.2.c it follows that we may find a and $b \in \mathbb{Z}$ such that $a^2 + 3b^2 = p$. Let $d = 2b$ and $c = a + b$. Then

$$\begin{aligned} a^2 + 3b^2 &= (c - b)^2 + 3b^2 \\ &= c^2 - 2cb + 4b^2 \\ &= c^2 - cd + d^2, \end{aligned}$$

so that

$$p = (c + d\zeta)(c + d\bar{\zeta}).$$

Now suppose that $\alpha \in \mathbb{Z}(F)$. Then $N(\alpha) = m \in \mathbb{Z}$ and so $\alpha | m$. We can factor m into a product of ordinary primes and then into a product of the primes above. As we have a UFD, α is then a product of some of those primes.
Thus we have exhausted the list of primes.
8.4.5. Suppose we want to divide α into β. Let

$$\xi = \frac{\alpha}{\beta} \in \mathbb{Q}(F).$$

Let $\gamma \in D$ be the closest point. Then

$$\beta = \gamma\alpha + \rho,$$

where

$$\rho = \alpha \cdot (\xi - \gamma).$$

Thus

$$N(\rho) < N(\alpha) \qquad \text{if and only if} \qquad N(\xi - \gamma) < 1.$$

Following the notation of the question, we have

$$\xi - \alpha = u + v\omega \qquad \text{and we want} \qquad N(\xi - \alpha) < 1.$$

This gives

$$N(u + b\omega) < 1.$$

There are two cases. If $d \equiv 2$ or $3 \mod 4$ then this reduces to

$$|u^2 - dv^2| < 1.$$

If $d \equiv 1 \mod 4$ then this reduces to

$$\left| \left(u + \frac{v}{2}\right)^2 - d\left(\frac{v}{2}\right)^2 \right| < 1.$$

We first suppose that $0 \leq u \leq 1/2$ and $0 \leq v \leq 1/2$. It enough then to show that the maximum of the LHS is less than one.
If $d \equiv 2$ or $3 \mod 4$ and $d > 0$ then clearly the worse case is when $u = 0$ and $v = 1/2$. We have the cases $d = 2$ or 3; $d = 3$ is the worse case when we get

$$\frac{3}{4} < 1.$$

If $d < 0$ then the worse case is $u = v = 1/2$. We have the cases $d = -1$ or $d = -2$; $d = -2$ is the worse case when we get

$$\frac{1}{4} + \frac{2}{4} = 34 < 1.$$

Now suppose $d \equiv 1 \mod 4$. There are two cases. If $d > 0$ then we consider the optimisation problem:

$$\max \left| \left(u + \frac{v}{2}\right)^2 - d\left(\frac{v}{2}\right)^2 \right| \qquad \text{subject to} \qquad 0 \leq u, v \leq \frac{1}{2}.$$

Setting the partial derivatives equal to zero gives

$$2u + v = 0 \qquad \text{and} \qquad v = 0.$$

Thus the maximum occurs on the boundary. We have to consider the maximum of the absolute value of

$$u^2 \qquad (d-1)\frac{v^2}{4} \qquad \left(u + \frac{1}{4}\right)^2 - \frac{d}{16} \qquad \text{and} \qquad \left(\frac{v}{2} + \frac{1}{2}\right)^2 - \frac{dv^2}{4}.$$

Thus the maximum either occurs at one of the four boundary corners or at the critical point of the fourth function, where

$$\frac{v}{2} + \frac{1}{2} - \frac{dv}{2} = 0 \qquad \text{so that} \qquad v = \frac{1}{d-1}.$$

The maximum at the four corners is

$$\frac{d-1}{16}.$$

This is less than one for $d < 16$. If $d > 3$ the critical point is at an interior point. If $d = 5$ the critical point is $v = 1/4$ and we get

$$\left(\frac{1}{2} + \frac{1}{8}\right)^2 - \frac{5}{16} < 1.$$

If $d = 13$ the critical point is $v = 1/12$ and we get

$$\left(\frac{1}{2} + \frac{1}{24}\right)^2 - \frac{13}{4 \cdot 12^2} < 1.$$

If $d < 0$ then we consider a slightly different optimisation problem:

$$\max \left| \left(-u + \frac{v}{2}\right)^2 + |d| \left(\frac{v}{2}\right)^2 \right| \qquad \text{subject to} \qquad 0 \le u, v \le \frac{1}{2}.$$

It is again enough to show that the maximum is less than one; we just choose $x - a < 0$. We have flipped the sign of u as a matter of convenience.
The maximum at the four corners is

$$\frac{|d| + 1}{16}.$$

This is less than one, provided

$$|d| < 15.$$

The function has no critical point in the interior. We have to consider the maximum of the absolute value of

$$u^2 \qquad (|d| + 1)\frac{v^2}{4} \qquad \left(u - \frac{1}{4}\right)^2 + \frac{|d|}{16} \qquad \text{and} \qquad \left(\frac{v}{2} - \frac{1}{2}\right)^2 + \frac{|d|v^2}{4}.$$

All of these have their maximum at one of the corners.