Exercise (1.1).

Proof. Directly, we have:

$$N(\alpha\beta) = (\alpha\beta)\overline{(\alpha\beta)} = \alpha\beta\overline{\alpha}\overline{\beta} = (\alpha\overline{\alpha})(\beta\overline{\beta}) = N(\alpha)N(\beta)$$

So, if $\alpha \mid \gamma$ in $\mathbb{Z}[i]$, then there is $\beta \in \mathbb{Z}[i]$ with $\gamma = \alpha\beta$ and then $N(\gamma) = N(\alpha)N(\beta)$. Each of these norms is in $\mathbb{Z}$, so we have $N(\alpha) \mid N(\gamma)$. □

Exercise (1.2).

Proof. By the previous problem, if $\alpha \in Z[i]$ is a unit, then $\alpha \mid 1$ and so $N(\alpha)$ divides $N(1) = 1^2 + 0^2 = 1$. But $N(\alpha)$ is a nonnegative integer, so we must have $N(\alpha) = 1$. Conversely, if $\alpha \in Z[i]$ has $N(\alpha) = 1$, then $\alpha\overline{\alpha} = 1$, and $\overline{\alpha} \in Z[i]$ as well, so α is a unit (with inverse $\overline{\alpha}$).

Hence, to categorize units, we need to solve $a^2 + b^2 = 1$ for $a, b \in \mathbb{Z}$. The only solutions are $(a, b) = (\pm 1, 0)$ and $(a, b) = (0, \pm 1)$, corresponding to $\alpha = a + bi \in \{1, -1, i, -i\}$. □

Exercise (1.3).

Proof. Suppose $\alpha \in \mathbb{Z}[i]$ has $N(\alpha)$ prime, and write $\alpha = \beta\gamma$. Then $N(\beta)N(\gamma) = N(\alpha)$ is prime, so WLOG $N(\beta) = 1$. Hence β is a unit and since this factorization was arbitrary, α is irreducible.

Similarly, if $N(\alpha) = p^2$ for a prime p with $p \equiv 3 \pmod 4$, then for $\alpha = \beta\gamma$, we get that $N(\beta)N(\gamma) = p^2$. If either of these factors is 1, then we are done as above, and otherwise we have $N(\beta) = N(\gamma) = p$. But if $\beta = a + bi$, then this gives $p = a^2 + b^2$, which is a contradiction, since $a^2, b^2 \in \{0, 1\}$ modulo 4. □

Exercise (1.4).

Proof. Since

$$N(1 - i) = 1^2 + (-1)^2 = 2$$

is prime, the previous problem shows that $1 - i$ is irreducible. Directly, we have the second claim since:

$$i(1 - i)^2 = i(-2i) = 2$$

and i is a unit. □

Exercise (1.5).

Proof. This is consistent with unique factorization since the factors are unit multiples of one another. Namely:

$$-i(2 + i) = 1 - 2i \qquad \text{and} \qquad i(2 - i) = 1 + 2i$$

□

Exercise (1.6).

Proof. Suppose the claim is not true. Then, choose $\alpha \in \mathbb{Z}[i]$ such that α is a nonzero, nonunit Gaussian integer such that α is not a product of irreducibles, with $N(\alpha)$ as small as possible (by well-ordering of the nonnegative integers). We cannot have $N(\alpha) = 0$ or $N(\alpha) = 1$, since it would be zero or a unit in these cases, respectively. Further, α is not itself irreducible, else it would be a single product. So, there are nonunits β, γ with $\alpha = \beta\gamma$. Then $N(\alpha) = N(\beta)N(\gamma)$, and so $N(\beta), N(\gamma) < N(\alpha)$, since neither factor is equal to 1. By minimality, we can write β, γ as the product of irreducibles, but then α is the product of all of these irreducibles together. □

Exercise (1.7).

Proof. Let $I \subseteq \mathbb{Z}[i]$ be an ideal. If $I = (0)$, then it is clearly principal. Otherwise, I has nonzero elements, and so we can choose $\alpha \in I$ with $\alpha \neq 0$ and $N(\alpha)$ minimized. I claim $I = (\alpha)$.

So, let $\beta \in I$. We have that $\beta/\alpha \in \mathbb{Q}[i]$, so we can write $\beta/\alpha = x + yi$ for $x, y \in \mathbb{Q}$. Then, we can choose integers a, b with $|a - x|, |b - y| \leq \frac{1}{2}$ by rounding. Then, write $\gamma = \beta - \alpha(a + bi)$ and $\delta = (x - a) + (y - b)i$. Note that $\gamma \in I$ since $\alpha, \beta \in I$ and $a + bi \in \mathbb{Z}[i]$. Also note that

$$\delta\overline{\delta} = (x - a)^2 + (y - b)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

Further, we can compute the norm directly:

$$\begin{aligned} N(\gamma) &= \gamma\overline{\gamma} \\ &= (\beta - \alpha(a + bi))(\overline{\beta} - \overline{\alpha}(a - bi)) \\ &= \alpha\overline{\alpha}(x + yi - a - bi)(x - yi - a + bi) \\ &= N(\alpha)\delta\overline{\delta} \\ &< N(\alpha) \end{aligned}$$

So, by minimality of $N(\alpha)$ among nonzero elements of I, we must have $N(\gamma) = 0$, and so $\gamma = 0$. I.e. $\beta = \alpha(a+bi) \in (\alpha)$. □

Exercise (1.8).

Proof. As noted, $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p - 1$, so there is some $g \in \mathbb{Z}/p\mathbb{Z}$ that generates the group. If $p \equiv 1 \pmod 4$, then $p - 1$ is divisible by 4, and so $r = (p - 1)/4$ is an integer. But then $(g^r)^2 \equiv -1 \pmod 4$. Indeed, $g^{4r} = g^{p-1} = 1$, so g^{2r} is a root of $x^2 - 1$, i.e. g^{2r} is one of ± 1 since these are the only roots in the field $\mathbb{F}_p$. But we cannot have $g^{2r} = 1$, since g has order $4r$.

Now, we have that p divides $n^2 + 1 = (n + i)(n - i)$ for $n = g^r$. But p does not divide either of $n + i$ or $n - i$ in $\mathbb{Z}[i]$ since the imaginary component is not divisible by p. So p is not prime in $\mathbb{Z}[i]$ and so is not irreducible since $\mathbb{Z}[i]$ is a UFD and thus all irreducibles are prime.

So, we have that p is reducible, i.e. there are nonunits $\alpha, \beta \in \mathbb{Z}[i]$ with $p = \alpha\beta$. Taking norms, we have $p^2 = N(\alpha)N(\beta)$. Since they are nonunits, we must have $N(\alpha) = N(\beta) = p$. Hence, for $\alpha = a + bi$, we have $p = N(\alpha) = a^2 + b^2$ is the sum of two squares. □

Exercise (1.9).

Proof. Note that if $\alpha \in \mathbb{Z}[i]$ is such that $N(\alpha) = p$ is prime or $N(\alpha) = p^2$ for a prime $p \equiv 3 \pmod 4$, then α is irreducible by problem 3 above. I claim this is a complete list.

Indeed, suppose α is irreducible. Then $\alpha\overline{\alpha} = N(\alpha)$ is its unique factorization. So, if we factorize $N(\alpha)$ over $\mathbb{Z}$, then first we note that no prime can occur with an exponent of 3 or higher, else $N(\alpha)$ would have at least three irreducible factors.

Further, it cannot have distinct factors p, q. For then, counting the irreducible factors gives that these would have to themselves be irreducible. So, up to unit multiples, we have $p = \alpha$ and $q = \overline{alpha}$. Taking norms gives $p^2 = N(\alpha) = N(\overline{\alpha}) = q^2$.

The only remaining case is that $N(\alpha) = p$ for some prime, or that $N(\alpha) = p^2$. These are precisely the cases above, unless $N(\alpha) = 2^2$ or $N(\alpha) = p^2$ for $p \equiv 1 \pmod 4$. But we've already seen in these cases that p factors as the product of (at least) two irreducible factors, whence $p^2 = N(\alpha)$ has at least four irreducible factors, again contradicting unique factorization. □

Exercise (1.10).

Proof. Note that

$$\overline{\omega} = e^{-2\pi i/3} = e^{4\pi i/3} = \omega^2$$

and that

$$1 + \omega + \omega^2 = \frac{\omega^3 - 1}{\omega - 1} = 0$$

So, for $a, b \in \mathbb{R}$, we have:

$$(a + b\omega)\overline{(a + b\omega)} = (a + b\omega)(a + b\omega^2) = a^2 + ab(\omega + \omega^2) + b^2\omega^3 = a^2 - ab + b^2$$

So, for $a, b \in \mathbb{Z}$, we have $N(a + b\omega) = |a + b\omega|^2$. □

Exercise (1.11).

Proof. Exactly as before: for $\alpha, \beta \in \mathbb{Z}[\omega]$, we have

$$N(\alpha\beta) = (\alpha\beta)\overline{(\alpha\beta)} = \alpha\beta\overline{\alpha}\overline{\beta} = (\alpha\overline{\alpha})(\beta\overline{\beta}) = N(\alpha)N(\beta)$$

So, if $\alpha \mid \gamma$ in $\mathbb{Z}[\omega]$, then there is $\beta \in \mathbb{Z}[\omega]$ with $\gamma = \alpha\beta$ and then $N(\gamma) = N(\alpha)N(\beta)$. Each of these norms is in $\mathbb{Z}$, so we have $N(\alpha) \mid N(\gamma)$. □

Exercise (1.12).

Proof. Again, exactly as before: if $N(\alpha) = 1$, then $\alpha\overline{\alpha} = 1$, so α is a unit, and if α is a unit, then $\alpha\beta = 1$, so $N(\alpha) = 1$ since it is a positive integer divisor of 1.

So, to find units, we solve for $a^2 - ab + b^2 = 1$. Multiplying by 4 gives

$$4 = 4a^2 - 4ab + 4b^2 = (2a - b)^2 + 3b^2$$

So, $|b| < 2$, else $(2a - b)^2 + 3b^2 \geq 0 + 12$. If $b = \pm 1$, then we have $(2a - b)^2 = 1$, and so $2a = b \pm 1$. This gives the solutions $(a, b) = (1, 1), (0, 1), (0, -1), (-1, -1)$. Otherwise $b = 0$ and then we have $a^2 = 1$, so $a = \pm 1$, i.e. we have the solutions $(1, 0), (-1, 0)$. Since $1 + \omega = -\omega^2$, this gives the full list of units:

$$\pm 1, \pm\omega, \pm\omega^2$$

□

Exercise (1.13).

Proof. As before, we have:

$$N(1 - \omega) = 1 + 1 + 1 = 3$$

which is prime. So, $1 - \omega$ is irreducible. Similarly, directly, we get:

$$-\omega^2(1 - \omega)^2 = -\omega^2(1 - 2\omega + \omega^2) = 3$$

□

Exercise (1.14).

Proof. Let $I \subseteq \mathbb{Z}[\omega]$ be an ideal. If $I = (0)$, then I is principal. Otherwise, choose an element $\alpha \in I$ with $\alpha \neq 0$ and $N(\alpha)$ minimized. Again, I claim $I = (\alpha)$. So, let $\beta \in I$.

Again, we can take quotients to get $\beta/\alpha \in \mathbb{Q}[\omega]$, so $\beta/\alpha = x + y\omega$ for $x, y \in \mathbb{Q}$. Choose a, b by rounding so $|x - a|, |y - b| \leq \frac{1}{2}$. Then, let $\gamma = \beta - \alpha(a + b\omega)$ and $\delta = (x - a) + (y - b)\omega$. Then,

$$|\delta|^2 = (x - a)^2 - (x - a)(y - b) + (y - b)^2 \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} < 1$$

So, the rest of the proof goes exactly as before: $\gamma \in I$ and

$$N(\gamma) = N(\alpha)|\delta|^2 < N(\alpha)$$

and so by minimality $\gamma = 0$. Hence $\beta \in (\alpha)$ as claimed. □

Exercise (1.15).

Proof. Note that (n, x, m) is a primitive Pythagorean triple. Indeed, if p divides all of these, then it also divides $y^2 = 2mn$ and $w = m^2 + n^2$, but (x^2, y^2, w) is primitive. Since x is assumed odd, we thus conclude

$$x = r^2 - s^2 \qquad n = 2rs \qquad m = r^2 + s^2$$

for r, s coprime and not both odd.

For the second claim, note that if p divides any two of r, s, m, then it divides the third since $m = r^2 + s^2$. But r, s are coprime, so this cannot be. Hence, as noted, since $y^2 = 2mn = 2m(2rs) = 4mrs$, we get that m, r, s are all perfect squares by unique factorization (each prime must occur to an even power since it does in the LHS).

Hence, for $r = a^2, s = b^2, m = c^2$, we get $c^2 = m = r^2 + s^2 = a^4 + b^4$. But $c \leq c^2 = m \leq m^2 < m^2 + n^2 = w$, so this contradicts the minimality of w. □

Exercise (1.16).

Proof. The roots of $x^p - 1$ are $1, \omega, \ldots, \omega^{p-1}$, and so

$$x^p - 1 = \prod_{i=0}^{p-1}(x - \omega^i)$$

Dividing through $x - 1$ gives:

$$1 + x + \cdots + x^{p-1} = \prod_{i=1}^{p-1}(x - \omega^i)$$

Evaluating at $x = 1$ gives:

$$p = \prod_{i=1}^{p-1}(1 - \omega^i)$$

as claimed. □

Exercise (1.17).

Proof. Suppose that π also divides $x + y\omega^i$ for some $i = 2, \ldots, p$. Then π divides the difference: $(x + y\omega^i) - (x + y\omega) = y\omega(\omega^{i-1} - 1)$. Multiplying through by the remaining factors of the form $\omega^j - 1$ and by ω^{p-1} gives that π divides yp. On the other hand, π divides z^p and so π divides z since it's prime. Since p does not divide z, we have that z and yp are coprime, so we cannot have a common divisor π. □

Exercise (1.18).

Proof. Let P be the set of prime divisors of $x + y\omega$. Then, each $\pi \in P$ also divides z^p and so z. Thus, the unique factorization of z gives an integer n with $\pi^n \mid z$ and $\pi^{n+1} \nmid z$. Since π does not divide any of the other terms in the product, we have that π^{np} divides $x + y\omega$ but no higher power. Hence, each prime divisor of $x + y\omega$ has an exponent which is a multiple of p. I.e. $x + y\omega = u\alpha^p$, where α is the product of π^n over all $\pi \in P$ (and corresponding exponents n), and u is the unit in the factorization. □

Exercise (1.19).

Proof. The proof works the same way: if π is a prime ideal factor of both $(x+y\omega)$ and $(x+y\omega^i)$ for some $i \neq 1$, then π contains both z and yp, and hence 1 since they are coprime. I.e. π is not proper, so certainly not prime. □

Exercise (1.20).

Proof. This proof also works the same way. Writing P as the set of prime ideal factors of $(x + y\omega)$, each π contains z, and the factorization of (z) includes π^n as a multiplicand for some n. Then $(x + y\omega) = I^p$ where I is the product of π^n over all π. □

Exercise (1.21).

Proof. Note that $f(t)(t - 1) = t^p - 1$. Then $f(\omega)(\omega - 1) = \omega^p - 1 = 0$, so $f(\omega) = 0$, since $\omega \neq 1$. So, ω has degree at most $p - 1$, and to see that it has degree $p - 1$ exactly, we check that f is irreducible.

But

$$f(t+1)t = (t+1)^p - 1 = t^p + \binom{p}{1}t^{p-1} + \cdots + \binom{p}{p-1}t + 1 - 1$$

So, subtracting and dividing by t gives:

$$f(t+1) = t^{p-1} + \binom{p}{1}t^{p-2} + \cdots + \binom{p}{p-1}$$

By Eisenstein's criterion, this is irreducible as long as p divides $\binom{p}{k}$ for $k = 1, \ldots, p-1$ and $p^2 \nmid \binom{p}{p-1}$. The first is clear, since $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ and p divides the numerator but not the denominator. The second is also clear, since $\binom{p}{p-1} = p$. □

Exercise (1.22).

Proof. Suppose that p divides α. Then,

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

On the other hand, $\alpha/p \in \mathbb{Z}[\omega]$, and so we can write:

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

for integers b_i (note that we can only use terms up to ω^{p-2} since higher terms can be reduced using f from the previous problem). But the uniqueness we proved above gives $b_i = a_i/p$, i.e. $a_i = pb_i$ is a multiple of p. □

Exercise (1.23).

Proof. If $\beta \equiv \gamma \pmod{p}$, then $\beta - \gamma = \delta p$ for some $\delta \in \mathbb{Z}[\omega]$. Then, taking conjugates gives:

$$\overline{\beta} - \overline{\gamma} = \overline{\delta} p$$

Since δ is a $\mathbb{Z}$-linear combination of powers of ω, and $\overline{\omega} = \omega^{p-1}$ is also in $\mathbb{Z}[\omega]$, we get that $\overline{\delta} \in \mathbb{Z}[\omega]$. So, $\overline{\beta} \equiv \overline{\gamma} \pmod{p}$. □

Exercise (1.24).

Proof. Note that:

$$(\beta+\gamma)^p - (\beta^p + \gamma^p) = \binom{p}{1}\beta\gamma^{p-1} + \cdots + \binom{p}{p-1}\beta^{p-1}\gamma$$

and the right hand side is divisible by p since each binomial coefficient is. By induction, we have

$$\left(\sum_{i=1}^{n} \beta_i\right)^p \equiv \sum_{i=1}^{n} \beta_i^p$$

since the above gives the case $n = 2$ and each additional term also follows from the above case. □

Exercise (1.25).

Proof. As suggested, write $\alpha = a_0 + \cdots + a_{p-2}\omega^{p-2}$. Then, we have:

$$\alpha^p = \left(\sum_{i=0}^{p-2} a_i\omega^i\right)^p \equiv \sum_{i=0}^{p-2} (a_i\omega^i)^p = \sum_{i=0}^{p-2} a_i^p$$

since $\omega^p = 1$. The right hand side is an integer, so this completes the argument. □

Exercise (1.26).

Proof. Suppose $x + y\omega \equiv u\alpha^p \pmod{p}$ for $x, y \in \mathbb{Z}$, a unit u, and some $\alpha \in \mathbb{Z}[\omega]$. Then, we've shown that $\alpha^p \equiv a \pmod{p}$ for some $a \in \mathbb{Z}$, i.e. $x + y\omega \equiv ua \pmod{p}$. Then, we've also shown that

$$x + y\omega^{-1} = \overline{x + y\omega} \equiv \overline{u}a = u\omega^{-k}a \pmod{p}$$

for some k, where we've used $u/\overline{u} = \omega^k$ by Kummer's result on units. Multiplying through by ω^k gives:

$$(x + y\omega^{-1})\omega^k \equiv ua \equiv x + y\omega \pmod{p}$$

as claimed. □

Exercise (1.27).

Proof. We may assume, without loss of generality, that $0 \leq k < p$. If $k = 0$, then we get that p divides $y - y\omega^2$, but problem 22 implies that $p \mid y$, contrary to assumption. If $2 \leq k \leq p-2$, we get that p divides

$$x + y\omega - x\omega^k - y\omega^{k-1}$$

and again, problem 22 implies that p divides each coefficient, including, say, x. Finally, if $k = p-1$, we have that p divides

$$x + y\omega - x\omega^{p-1} - y\omega^{p-2}$$

and so it also divides (multiplying by ω^2):

$$x\omega^2 + y\omega^3 - x\omega - y$$

and so it divides y. The only remaining possibility is that $k = 1$, as claimed. □

Exercise (1.28).

Proof. Finally, we have:

$$x + y\omega \equiv x\omega + y \pmod{p}$$

and so p divides $(x-y)+(y-x)\omega$. Hence, by problem 22, we get that p divides $x-y$, i.e. $x \equiv y \pmod{p}$. □

Exercise (1.29).

Proof. We compute blindly:

$$\begin{aligned}
&(1+\omega^2+\omega^4+\omega^5+\omega^6+\omega^{10}+\omega^{11})(1+\omega+\omega^5+\omega^6+\omega^7+\omega^9+\omega^{11}) \\
&\quad = 1+\omega+\omega^2+\omega^3+\omega^4+3\omega^5+3\omega^6+3\omega^7+\omega^8+3\omega^9+3\omega^{10}+7\omega^{11} \\
&\qquad +3\omega^{12}+3\omega^{13}+\omega^{14}+3\omega^{15}+3\omega^{16}+3\omega^{17}+\omega^{18}+\omega^{19}+\omega^{20}+\omega^{21}+\omega^{22} \\
&\quad = 2\omega^5+2\omega^6+2\omega^7+2\omega^9+2\omega^{10}+6\omega^{11}+2\omega^{12}+2\omega^{13}+2\omega^{15}+2\omega^{16}+2\omega^{17}
\end{aligned}$$

which is divisible by 2 in $\mathbb{Z}[\omega]$. On the other hand, $1, \omega, \ldots, \omega^{21}$ is a basis for $\mathbb{Q}(\omega)$ over $\mathbb{Q}$, so each factor is not divisible by 2 since the coefficients aren't. □

Exercise (1.30).

Proof. Suppose that A, B are ideals of R in the same ideal class, so there are nonzero elements $a, b \in R$ with $aA = bB$. Note that the map $A \to aA$ given by $x \mapsto ax$ is an R-module isomorphism. Indeed, it is a group homomorphism since $a(x+y) = ax + ay$, and it is compatible with multiplication in R: $a(rx) = r(ax)$. Finally, it is surjective essentially by definition and injective since R is a domain and a is nonzero. The same proof shows that $B \cong bB$. But $bB = aA$, and so we have $A \cong B$.

On the other hand, suppose that $f : A \to B$ is an R-module isomorphism of ideals A, B of R. If $A = 0$, then clearly $B = 0$ as well, and so $A = B$ are obviously in the same ideal class. Otherwise, choose a nonzero element $x \in A$, and let $y = f(x)$. I claim $yA = xB$.

First, let $xb \in xB$. Then, since f is an isomorphism, there is $a \in A$ with $f(a) = b$. Then $xb = xf(a) = f(xa) = af(x) = ay \in yA$. So, $xB \subseteq yA$. The same argument using f^{-1} shows $yA \subseteq xB$. This completes the proof. □

Exercise (1.31).

Proof. Note that this is false unless we assume $\alpha \neq 0$. With this assumption, now assume that $\alpha A = \beta R$. Then in particular, there is $a \in A$ with $\alpha a = \beta$. I claim $A = aR$. One containment is obvious, and for the other, suppose $x \in A$. Then $\alpha x \in \beta R$ so there is $r \in R$ with $\alpha x = \beta r = \alpha a r$. Since α is nonzero and R is a domain, we get $x = ar \in aR$ as claimed.

So, indeed, the principal ideals form an ideal class. For any two principal ideals are clearly in the same class, and the previous argument shows that if A is in the same class as a principal ideal, then it is itself principal. □

Exercise (1.32).

Proof. Suppose that multiplication of ideal classes forms a group. Since $R \cdot R = R$, we have that principal ideals must be the identity element of this group. Hence, if A is any ideal, then the ideal class of A has an inverse, i.e. another class such that the product of the representatives gives a representative of the identity. I.e. we get an ideal B such that AB is principal as desired.

Conversely, suppose that every ideal has an inverse in this sense. Then multiplication of ideal classes is associative and the principal ideals act as identity clearly, and the inverse condition is satisfied by our assumption. □