Chapter 1: A Special Case of Fermat's Conjecture

Author: Meng-Gen Tsai
Email: plover@gmail.com

Exercise 1.1-1.9: Define $N : \mathbb{Z}[i] \to \mathbb{Z}$ by $N(a+bi) = a^2 + b^2$.

Exercise 1.1. *Verify that for all $\alpha, \beta \in \mathbb{Z}[i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$, either by direct computation or using the fact that $N(a+bi) = (a+bi)(a-bi)$. Conclude that if $\alpha \mid \gamma$ in $\mathbb{Z}[i]$, then $N(\alpha) \mid N(\gamma)$ in $\mathbb{Z}$.*

Proof.

(1) *Direct computation.* Write $\alpha = a+bi, \beta = c+di$ where $a, b, c, d \in \mathbb{Z}$. Thus,

$$\begin{aligned}
N(\alpha\beta) &= N((a+bi)(c+di)) \\
&= N((ac-bd) + (ad+bc)i) \\
&= (ac-bd)^2 + (ad+bc)^2 \\
&= (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) \\
&= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2, \\
N(\alpha)N(\beta) &= N(a+bi)N(c+di) \\
&= (a^2+b^2)(c^2+d^2) \\
&= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2.
\end{aligned}$$

Therefore, $N(\alpha\beta) = N(\alpha)N(\beta)$. (Note that we also get the identity $(a^2 + b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$.)

(2) *Using the fact that $N(a+bi) = (a+bi)(a-bi)$*, or $N(\alpha) = \alpha\overline{\alpha}$ for any $\alpha \in \mathbb{Z}[i]$. Thus,

$$\begin{aligned}
N(\alpha\beta) &= \alpha\beta\overline{\alpha\beta} \\
&= \alpha\beta\overline{\alpha}\overline{\beta} \\
&= \alpha\overline{\alpha}\beta\overline{\beta} \\
&= N(\alpha)N(\beta).
\end{aligned}$$

(3) *Show that if $\alpha \mid \gamma$ in $\mathbb{Z}[i]$, then $N(\alpha) \mid N(\gamma)$ in $\mathbb{Z}$.* Write $\gamma = \alpha\beta$ for some $\beta \in \mathbb{Z}[i]$. So $N(\gamma) = N(\alpha)N(\beta) \in \mathbb{Z}$, or $N(\alpha) \mid N(\gamma)$ in $\mathbb{Z}$.

□

Exercise 1.2. *Let $\alpha \in \mathbb{Z}[i]$. Show that α is a unit iff $N(\alpha) = 1$. Conclude that the only unit are ± 1 and $\pm i$.*

Proof.

(1) ($\Longrightarrow$) Since α is a unit, there is $\beta \in \mathbb{Z}[i]$ such that $\alpha\beta = 1$. By Exercise 1.1, $N(\alpha\beta) = N(1)$, or $N(\alpha)N(\beta) = 1$. Since the image of N is nonnegative integers, $N(\alpha) = 1$.

(2) ($\Longleftarrow$) By Exercise 1.1, $N(\alpha) = \alpha\overline{\alpha}$, or $1 = \alpha\overline{\alpha}$ since $N(\alpha) = 1$. That is, $\overline{\alpha} \in \mathbb{Z}[i]$ is the inverse of $\alpha \in \mathbb{Z}[i]$. (Or by (1), we solve the equation $N(\alpha) = a^2 + b^2 = 1$, and show that all four solutions (± 1 and $\pm i$) are unit.)

Conclusion: a unit $\alpha = a+bi$ of $\mathbb{Z}[i]$ is satisfying the equation $N(\alpha) = a^2+b^2 = 1$ by (1)(2). That is, the only unit of $\mathbb{Z}[i]$ are ± 1 and $\pm i$. $\square$

Exercise 1.3. *Let $\alpha \in \mathbb{Z}[i]$. Show that if $N(\alpha)$ is a prime in $\mathbb{Z}$ then α is irreducible in $\mathbb{Z}[i]$. Show that the same conclusion holds if $N(\alpha) = p^2$, where p is a prime in $\mathbb{Z}$, $p \equiv 3 \pmod 4$.*

Proof.

(1) *Show that if $N(\alpha)$ is a prime in $\mathbb{Z}$ then α is irreducible in $\mathbb{Z}[i]$.* Write $\alpha = \beta\gamma$. Then $N(\alpha) = N(\beta)N(\gamma)$ is a prime in $\mathbb{Z}$. Since each integer prime is irreducible, $N(\beta) = 1$ or $N(\gamma) = 1$. So that β is unit or γ is unit by Exercise 1.2. Hence, α is irreducible.

(2) *Show that α is irreducible in $\mathbb{Z}[i]$ if $N(\alpha) = p^2$, where p is a prime in $\mathbb{Z}$, $p \equiv 3 \pmod 4$.* Assume $\alpha = \beta\gamma$ were not irreducible. Similar to (1), $N(\alpha) = N(\beta)N(\gamma) = p^2$. Since β and γ are proper factors of α,

$$N(\beta) = N(\gamma) = p.$$

Since any square $a^2 \equiv 0, 1 \pmod 4$, any $N(a + bi) = a^2 + b^2 \equiv 0, 1, 2 \pmod 4$. Especially, $N(\beta) \equiv 0, 1, 2 \pmod 4$, contrary to $N(\beta) = p \equiv 3 \pmod 4$ by the assumption. Therefore, α is irreducible in $\mathbb{Z}[i]$.

$\square$

Supplement.

(1) The prime 2 is reducible in $\mathbb{Z}[i]$ (Exercise 1.4).

(2) Every prime $p \equiv 1 \pmod 4$ is reducible in $\mathbb{Z}[i]$ (Exercise 1.8).

Exercise 1.4. *Show that $1 - i$ is irreducible in $\mathbb{Z}$ and that $2 = u(1-i)^2$ for some unit u.*

Proof.

(1) *$1 - i$ is irreducible.* Since $N(1-i) = 2$ is a prime in $\mathbb{Z}$, $1 - i$ is irreducible by Problem 1.3.

(2) $2 = i(1-i)^2$ where i is unit in $\mathbb{Z}$.

□

Exercise 1.5. *Notice that $(2+i)(2-i) = 5 = (1+2i)(1-2i)$. How is this consistent with unique factorization?*

Proof. Since $2+i = i(1-2i)$ and $2-i = (-i)(1+2i)$, the factorization is unique up to order and multiplication of primes by units. □

Exercise 1.6. *Show that every nonzero, non-unit Gaussian integer α is a product of irreducible elements, by induction on $N(\alpha)$.*

Proof. Induction on $N(\alpha)$.

(1) $n = 2$. Given $\alpha \in \mathbb{Z}[i]$ with $N(\alpha) = 2$. Since $N(\alpha) = 2$ is a prime in $\mathbb{Z}$, α is irreducible (Exercise 1.3).

(2) *Suppose the result holds for $n \leq k$.* Given $\alpha \in \mathbb{Z}[i]$ with $N(\alpha) = k+1$. There are only two possible cases.

   (a) *α is irreducible.* Nothing to do.

   (b) *α is reducible.* Write $\alpha = \beta\gamma$ where neither factor is unit. Since $N(\alpha) = N(\beta)N(\gamma)$ and neither factor is unit,

   $$2 \leq N(\beta), N(\gamma) \leq k.$$

   By the induction hypothesis, each factor of α (β and γ) is a product of irreducible elements. So that α again is a product of irreducible elements.

   In any cases, α is a product of irreducible elements.

By induction, the result is established. □

Exercise 1.7. *Show that $\mathbb{Z}[i]$ is a principal ideal domain (PID); i.e., every ideal I is principal. (As shown in Appendix 1, this implies that $\mathbb{Z}[i]$ is a UFD.)*

Suggestion: Take $\alpha \in I - \{0\}$ such that $N(\alpha)$ is minimized, and consider the multiplies $\gamma\alpha$, $\gamma \in \mathbb{Z}[i]$; show that these are the vertices of an infinite family of squares which fill up the complex plane. (For example, one of the squares has vertices 0, α, $i\alpha$, and $(1+i)\alpha$; all others are translates of this one.) Obviously I contains all $\gamma\alpha$; show by a geometric argument that if I contains anything else then minimality of $N(\alpha)$ would be contradicted.

Proof (without geometric intuition). Define N on $\mathbb{Q}[i]$ by $N(a+bi) = a^2 + b^2$ where $a + bi \in \mathbb{Q}[i]$ as usual.

(1) *Show that $\mathbb{Z}[i]$ is a Euclidean domain.* Given $\alpha = a + bi \in \mathbb{Z}[i]$ and $\gamma = c + di \in \mathbb{Z}[i]$ with $\gamma \neq 0$. It suffices to show there exist δ and ρ such that the identity $\alpha = \gamma\delta + \rho$ holds and either $\rho = 0$ or $N(\rho) < N(\gamma)$.

  (a) *Pick $\delta \in \mathbb{Z}[i]$. (Intuition: Pick the 'integer part' of $\frac{\alpha}{\gamma}$ as we did in integer numbers.)* Write $\frac{\alpha}{\gamma} = r + si \in \mathbb{Q}[i]$. Then we pick $\delta = m + ni \in \mathbb{Z}[i]$ such that $|r - m| \leq \frac{1}{2}$ and $|s - n| \leq \frac{1}{2}$. Therefore,

$$\begin{aligned} N\left(\frac{\alpha}{\gamma} - \delta\right) &= (r-m)^2 + (s-n)^2 \\ &\leq \frac{1}{4} + \frac{1}{4} \\ &= \frac{1}{2}. \end{aligned}$$

  (b) *Pick $\rho \in \mathbb{Z}[i]$.* Clearly we can pick $\rho = \alpha - \gamma\delta \in \mathbb{Z}[i]$. Therefore, $\rho = 0$ or

$$\begin{aligned} N(\rho) &= N(\alpha - \gamma\delta) \\ &= N\left(\gamma\left(\frac{\alpha}{\gamma} - \delta\right)\right) \\ &= N(\gamma)N\left(\frac{\alpha}{\gamma} - \delta\right) \\ &\leq \frac{1}{2}N(\gamma) \\ &< N(\gamma). \end{aligned}$$

(2) *Show that every Euclidean domain R is a PID.* Given any ideal I of R. Take $\alpha \in I - \{0\}$ such that $N(\alpha)$ is minimized.

  (a) $R\alpha \subseteq I$ clearly.

  (b) Conversely, for any $\beta \in I$, there are $\delta, \rho \in R$ such that $\beta = \alpha\delta + \rho$, where either $\rho = 0$ or $N(\rho) < N(\alpha)$. Since $\rho = \beta - \alpha\delta \in I$, we cannot have $N(\rho) < N(\alpha)$ by the minimality of $N(\alpha)$. Therefore, $\rho = 0$ and $\beta = \alpha\delta \in R\alpha$, or $R\alpha \supseteq I$.

By (1)(2), $\mathbb{Z}[i]$ is a PID. $\square$

Exercise 1.8. *We will use the unique factorization in $\mathbb{Z}[i]$ to prove that every prime $p \equiv 1 \pmod 4$ is a sum of two squares.*

(a) Use the fact that the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of integers mod p is cyclic to show that if $p \equiv 1 \pmod 4$ then $n^2 \equiv -1 \pmod p$ for some $n \in \mathbb{Z}$.

(b) Prove that p cannot be irreducible in $\mathbb{Z}[i]$. (Hint: $p \mid n^2+1 = (n+i)(n-i)$.)

(c) Prove that p is a sum of two squares. (Hint: (b) shows that $p = (a+bi)(c+di)$ with neither factor a unit. Take norms.)

Proof of (a). Since the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of integers mod p is cyclic, $(\mathbb{Z}/p\mathbb{Z})^\times$ is generated by (a primitive root) $g \in \mathbb{Z}/p\mathbb{Z}$. $g^{p-1} = 1$, or

$$(g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1) = 0$$

since p is odd. Since $\mathbb{Z}/p\mathbb{Z}$ is an integral domain, $g^{\frac{p-1}{2}} - 1 = 0$ or $g^{\frac{p-1}{2}} + 1 = 0$. g cannot satisfy $g^{\frac{p-1}{2}} - 1 = 0$ since g is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. So,

$$g^{\frac{p-1}{2}} + 1 = 0.$$

Let $n = g^{\frac{p-1}{4}} \in \mathbb{Z}$ since $p \equiv 1 \pmod 4$. So $n^2 + 1 = 0 \pmod p$. $\square$

Proof of (b). Since $n^2 + 1 \equiv 0 \pmod p$ by (a), $p \mid n^2 + 1 = (n+i)(n-i)$. If p were irreducible in $\mathbb{Z}[i]$, $p \mid (n+i)$ or $p \mid (n-i)$ by using the unique factorization in $\mathbb{Z}[i]$. Hence

$$\frac{n+i}{p} = \frac{n}{p} + \frac{1}{p}i \notin \mathbb{Z}[i], \frac{n-i}{p} = \frac{n}{p} - \frac{1}{p}i \notin \mathbb{Z}[i],$$

contrary to the assumption. Therefore, p is reducible in $\mathbb{Z}[i]$. $\square$

Proof of (c). Since p is reducible in $\mathbb{Z}[i]$ by (b), write $p = (a+bi)(c+di)$ with neither factor a unit. Take norms,

$$p^2 = N(p) = N(a+bi)N(c+di).$$

Since neither factor of p is unit, $N(a+bi) = p$, or $a^2 + b^2 = p$, or p is a sum of two squares. $\square$

Exercise 1.9. *Describe all irreducible elements in $\mathbb{Z}[i]$.*

Notice that α is irreducible if and only if $\overline{\alpha}$ is irreducible. (Write $\alpha = \beta\gamma$, then $\overline{\alpha} = \overline{\beta}\overline{\gamma}$. Besides, $\overline{\overline{\alpha}} = \alpha$.)

Proof. Show that all irreducible elements in $\mathbb{Z}[i]$ (up to units) are

(1) $1+i$.

(2) $\pi = a + bi$ *for each integer prime* $p \equiv 1 \pmod 4$ *with* $p = a^2 + b^2$.

(3) p *for each integer prime* $p \equiv 3 \pmod 4$.

Let α be any irreducible element in $\mathbb{Z}[i]$. Consider $N(\alpha) = \alpha\overline{\alpha}$. $N(\alpha) \neq 1$ since α is not unit. By the unique factorization theorem in $\mathbb{Z}$, $N(\alpha) \in \mathbb{Z}$ is a product of primes in $\mathbb{Z}$.

There are three possible cases.

(a) $2 \mid N(\alpha)$. Write $(1+i)(1-i) \mid \alpha\overline{\alpha}$ in $\mathbb{Z}[i]$. Notice that $1+i$, $1-i$, α and $\overline{\alpha}$ are all irreducible (Exercise 1.4). By the unique factorization theorem in $\mathbb{Z}[i]$, $\alpha = 1+i$ (up to units).

(b) $p \mid N(\alpha)$ *for some prime* $p \equiv 3 \pmod 4$. Write $p \mid \alpha\overline{\alpha}$ in $\mathbb{Z}[i]$. Notice that p, α and $\overline{\alpha}$ are all irreducible (Exercise 1.3). By the unique factorization theorem in $\mathbb{Z}[i]$, $\alpha = p$ (up to units) or $\overline{\alpha} = p$ (up to units). So in any cases $\alpha = p$ (up to units). (Note that $\overline{p} = p$.)

(c) $p \mid N(\alpha)$ *for some prime* $p \equiv 1 \pmod 4$. For such p, there is an irreducible $\pi \in \mathbb{Z}[i]$ satisfying $p = \pi\overline{\pi}$ (Exercise 1.8). Now we write $\pi\overline{\pi} \mid \alpha\overline{\alpha}$ in $\mathbb{Z}[i]$. Notice that π, $\overline{\pi}$, α and $\overline{\alpha}$ are all irreducible. By the unique factorization theorem in $\mathbb{Z}[i]$, $\alpha = \pi$ or $\alpha = \overline{\pi}$. In any cases, $\alpha = a+bi$ for integer prime $p \equiv 1 \pmod 4$ with $p = a^2 + b^2$.

$\square$

Exercise 1.10 - 1.14: Let $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. *Define* $N : \mathbb{Z}[\omega] \to \mathbb{Z}$ *by* $N(a + b\omega) = a^2 - ab + b^2$.

Exercise 1.10. *Show that if $a + b\omega$ is written in the form $u + vi$ where u and v are real, then $N(a + b\omega) = u^2 + v^2$.*
Proof. By $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, write

$$a + b\omega = \left(a - \frac{1}{2}b\right) + \left(\frac{\sqrt{3}}{2}b\right) i.$$

Here $u = a - \frac{1}{2}b \in \mathbb{R}$ and $v = \frac{\sqrt{3}}{2}b \in \mathbb{R}$. Hence $u^2 + v^2 = (a - \frac{1}{2}b)^2 + (\frac{\sqrt{3}}{2}b)^2 = a^2 - ab + b^2 = N(a + b\omega)$. $\square$

Exercise 1.11. *Show that for all $\alpha, \beta \in \mathbb{Z}[\omega]$, $N(\alpha\beta) = N(\alpha)N(\beta)$, either by direct computation or by using Exercise 1.10. Conclude that if $\alpha \mid \gamma$ in $\mathbb{Z}[\omega]$, then $N(\alpha) \mid N(\gamma)$ in $\mathbb{Z}$.*

Proof.

(1) *Direct computation.* Note that $1 + \omega + \omega^2 = 0$ or $\omega^2 = -1 - \omega$. Write $\alpha = a + b\omega, \beta = c + d\omega$ where $a, b, c, d \in \mathbb{Z}$. Thus,

$$\begin{aligned}
N(\alpha\beta) &= N((a + b\omega)(c + d\omega)) \\
&= N(ac + (ad + bc)\omega + bd\omega^2) \\
&= N(ac + (ad + bc)\omega + bd(-1 - \omega)) \\
&= N((ac - bd) + (ad + bc - bd)\omega) \\
&= (ac - bd)^2 - (ac - bd)(ad + bc - bd) + (ad + bc - bd)^2 \\
&= (a^2 - ab + b^2)(c^2 - cd + d^2), \\
N(\alpha)N(\beta) &= N(a + b\omega)N(c + d\omega) \\
&= (a^2 - ab + b^2)(c^2 - cd + d^2).
\end{aligned}$$

(2) *Exercise 1.10.* The result is established by Exercise 1.10 and Exercise 1.1.

(3) *Using the fact that $N(a+b\omega) = (a+b\omega)\overline{(a + b\omega)}$.* Similar to the argument of Exercise 1.1.

(4) *Show that if $\alpha \mid \gamma$ in $\mathbb{Z}[\omega]$, then $N(\alpha) \mid N(\gamma)$ in $\mathbb{Z}$.* Similar to the argument of Exercise 1.1.

$\square$

Exercise 1.12. *Let $\alpha \in \mathbb{Z}[\omega]$. Show that α is a unit iff $N(\alpha) = 1$, and find all units in $\mathbb{Z}[\omega]$. (There are six of them.)*

Proof.

(1) ($\Longrightarrow$) Since α is a unit, there is $\beta \in \mathbb{Z}[\omega]$ such that $\alpha\beta = 1$. By Exercise 1.11, $N(\alpha\beta) = N(1)$, or $N(\alpha)N(\beta) = 1$. Since the image of N is nonnegative integers, $N(\alpha) = 1$.

(2) ($\Longleftarrow$) By Exercise 1.10, $N(\alpha) = \alpha\overline{\alpha}$, or $1 = \alpha\overline{\alpha}$ since $N(\alpha) = 1$. That is, $\overline{\alpha} \in \mathbb{Z}[\omega]$ is the inverse of $\alpha \in \mathbb{Z}[\omega]$.

(3) By (1), we solve the equation $N(\alpha) = a^2-ab+b^2 = 1$, or $4 = (2a-b)^2+3b^2$. There are 2 possible cases.

    (a) $2a - b = \pm 1$, $b = \pm 1$.

(b) $2a - b = \pm 2$, $b = \pm 0$.

Solve these 6 pairs of equations yields the result $\pm 1, \pm\omega, \pm\omega^2$.

$\square$

Exercise 1.13. *Show that $1 - \omega$ is irreducible in $\mathbb{Z}[\omega]$, and that $3 = u(1-\omega)^2$ for some unit u.*

3 is not irreducible in $\mathbb{Z}[\omega]$.

Proof.

(1) $N(1-\omega) = 3$ is an integer prime. Similar to the argument in Exercise 1.3, $1 - \omega$ is irreducible in $\mathbb{Z}[\omega]$.

(2) Note that $1 + \omega + \omega^2 = 0$. So $(1-\omega)^2 = 1 - 2\omega + \omega^2 = 3(-\omega)$, or $(-\omega^2)(1-\omega)^2 = 3$. By Exercise 1.12, $-\omega^2$ is unit. Hence $3 = u(1-\omega)^2$ for some unit $u = -\omega^2$.

$\square$

Exercise 1.14. *Modify Exercise 1.7 to show that $\mathbb{Z}[\omega]$ is a PID, hence a UFD. Here the squares are replaced by parallelograms; one of them has vertices $0, \alpha, \omega\alpha, (\omega+1)\alpha$, and all others are translates of this one. Use Exercise 1.10 for the geometric argument at the end.*

Similar to Exercise 1.7.

Proof (without geometric intuition). Define N on $\mathbb{Q}[\omega]$ by $N(a+b\omega) = a^2 - ab + b^2$ where $a + b\omega \in \mathbb{Q}[\omega]$ as usual.

(1) *Show that $\mathbb{Z}[\omega]$ is a Euclidean domain.* Given $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ and $\gamma = c + d\omega \in \mathbb{Z}[\omega]$ with $\gamma \neq 0$. It suffices to show there exist δ and ρ such that the identity $\alpha = \gamma\delta + \rho$ holds and either $\rho = 0$ or $N(\rho) < N(\gamma)$.

(a) *Pick $\delta \in \mathbb{Z}[\omega]$. (Intuition: Pick the 'integer part' of $\frac{\alpha}{\gamma}$ as we did in integer numbers.)* Write $\frac{\alpha}{\gamma} = r + s\omega \in \mathbb{Q}[\omega]$. Then we pick $\delta = m + n\omega \in \mathbb{Z}[\omega]$ such that $|r - m| \leq \frac{1}{2}$ and $|s - n| \leq \frac{1}{2}$. Therefore,

$$\begin{aligned} N\left(\frac{\alpha}{\gamma} - \delta\right) &\leq |r-m|^2 + |r-m||s-n| + |s-n|^2 \\ &\leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} \\ &= \frac{3}{4}. \end{aligned}$$

(b) *Pick* $\rho \in \mathbb{Z}[\omega]$. Clearly we can pick $\rho = \alpha - \gamma\delta \in \mathbb{Z}[\omega]$. Therefore, $\rho = 0$ or

$$\begin{aligned} N(\rho) &= N(\alpha - \gamma\delta) \\ &= N\left(\gamma\left(\frac{\alpha}{\gamma} - \delta\right)\right) \\ &= N(\gamma)N\left(\frac{\alpha}{\gamma} - \delta\right) \\ &\leq \frac{3}{4}N(\gamma) \\ &< N(\gamma). \end{aligned}$$

(2) *Show that every Euclidean domain R is a PID.* Given any ideal I of R. Take $\alpha \in I - \{0\}$ such that $N(\alpha)$ is minimized.

(a) $R\alpha \subseteq I$ clearly.

(b) Conversely, for any $\beta \in I$, there are $\delta, \rho \in R$ such that $\beta = \alpha\delta + \rho$, where either $\rho = 0$ or $N(\rho) < N(\alpha)$. Since $\rho = \beta - \alpha\delta \in I$, we cannot have $N(\rho) < N(\alpha)$ by the minimality of $N(\alpha)$. Therefore, $\rho = 0$ and $\beta = \alpha\delta \in R\alpha$, or $R\alpha \supseteq I$.

By (1)(2), $\mathbb{Z}[\omega]$ is a PID. $\square$

Exercise 1.15. *Here is a proof of Fermat's conjecture for $n = 4$: If $x^4 + y^4 = z^4$ has a solution in positive integers, then so does $x^4 + y^4 = w^2$. Let x, y, w be a solution with smallest possible w. Then x^2, y^2, w is a primitive Pythagorean triple. Assuming (without loss of generality) that x is odd, we can write*

$$x^2 = m^2 - n^2, y^2 = 2mn, w = m^2 + n^2$$

with m and n are relatively prime positive integers, not both odd.

(a) *Show that*

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

with r and s are relatively prime positive integers, not both odd.

(b) *Show that r, s and m are pairwise relatively prime. Using $y^2 = 4rsm$, conclude that r, s and m are all squares, say a^2, b^2 and c^2.*

(c) *Show that $a^4 + b^4 = c^2$, and that this contradicts minimality of w.*

Proof of (a). Write $x^2 + n^2 = m^2$ by moving n^2 of $x^2 = m^2 - n^2$ to the left side. Notice that x is odd, and thus $x = r^2 - s^2, n = 2rs, m = r^2 + s^2$ with r and s are relatively prime positive integers, not both odd. $\square$

Proof of (b).

(1) It suffices to show that $(r,m)=1$. By assumption, $(r,s)=1$. So $(r,s)=1 \Rightarrow (r,s^2)=1 \Rightarrow (r,r^2+s^2)=1$ and note that $m=r^2+s^2$ to get the result.

(2) $y^2=2mn=2m(2rs)=4rsm$ by (a). Since r,s and m are pairwise relatively prime, r,s and m are all squares.

□

Proof of (c). By (b), $r=a^2$, $s=b^2$, $m=c^2$. By (a), $m=r^2+s^2$, or $c^2=(a^2)^2+(b^2)^2=a^4+b^4$. However, $w=m^2+n^2>m^2>m=c^2>c$, contrary to the minimality of w. □

Exercise 1.16-1.28: Let p be an odd prime, $\omega=e^{\frac{2\pi i}{p}}$.

Exercise 1.16. *Show that*

$$(1-\omega)(1-\omega^2)\cdots(1-\omega^{p-1})=p$$

by considering equation $t^p-1=(t-1)(t-\omega)(t-\omega^2)\cdots(t-\omega^{p-1})$.

Proof. Note that $t^p-1=(t-1)(t^{p-1}+t^{p-2}+\cdots+t+1)$. Cancel out $t-1$ of Equation (2),

$$t^{p-1}+t^{p-2}+\cdots+t+1=(t-\omega)(t-\omega^2)\cdots(t-\omega^{p-1}).$$

Put $t=1$ to get $p=(1-\omega)(1-\omega^2)\cdots(1-\omega^{p-1})$. □

Exercise 1.17. *Let $x^p+y^p=z^p$. Suppose that $\mathbb{Z}[\omega]$ is a UFD and $\pi \mid x+y\omega$, and π is a prime in $\mathbb{Z}[\omega]$. Show that π does not divide any of the other factors on the left side of*

$$(x+y)(x+y\omega)(x+y\omega^2)\cdots(x+y\omega^{p-1})=z^p$$

by showing that if it did, then π would divide both z and yp (Hint: Use Exercise 1.16); but z and yp are relatively prime (assuming p divides none of x,y,z), hence $zm+ypn=1$ for some $m,n\in\mathbb{Z}$. How is this a contradiction?

Proof. Write

$$z=u\pi_1^{e_1}\cdots\pi_m^{e_m}$$

where u is unit and π_k $(1\le k\le m)$ are distinct primes in $\mathbb{Z}[\omega]$ and $e_k\in\mathbb{Z}^+$ $(1\le k\le m)$. Since $\mathbb{Z}[\omega]$ is a UFD by assumption, the factorization of z is unique up to order and units.

(1) *Show that $\pi \mid z$.* Since $\pi \mid x + y\omega$, $\pi \mid z^p$. The factorization of z^p is

$$z^p = u^p \pi_1^{pe_1} \cdots \pi_m^{pe_m}.$$

u^p is unit, and $\pi | z^p$ implies that $\pi = \pi_k$ for some k, that is, $\pi \mid z$.

(2) *Show that $\pi \mid yp$ if π were divide any of the other factors on the left side of $(x+y)(x+y\omega)(x+y\omega^2)\cdots(x+y\omega^{p-1}) = z^p$.* Say $\pi \mid x + y\omega^k$ for some $k \neq 1$. So that $\pi \mid ((x+y\omega) - (x+y\omega^k))$, or $\pi \mid y(\omega - \omega^k)$. Since $k \neq 1$, there are two possible cases.

   (a) $k > 1$. $\pi \mid y\omega(1-\omega^{k-1})$. By Exercise 1.16, $\pi \mid y\omega p$, or $\pi \mid yp$ since ω is unit. (ω^{p-1} is the inverse of ω since $\omega \cdot \omega^{p-1} = 1$.)

   (b) $k = 0$. $\pi \mid y(\omega - 1)$, or $\pi \mid y(1-\omega)$. By Exercise 1.16, $\pi \mid yp$.

   In any case, $\pi \mid yp$.

(3) Note that z and yp are integers, and they are relatively prime by the assumption that p divides none of x, y, z. Therefore, on $\mathbb{Z}$ we have $zm + ypn = 1$ for some $m, n \in \mathbb{Z}$.

(4) $zm + ypn = 1$ is also true in $\mathbb{Z}[\omega]$. Therefore, by (1)(2) we have $\pi \mid (zm + ypn)$ or $\pi \mid 1$, or π is unit, contrary to the primality of π.

□

Exercise 1.18. *Use Exercise 1.17 to show that if $\mathbb{Z}[\omega]$ is a UFD then $x + y\omega = u\alpha^p$, $\alpha \in \mathbb{Z}[\omega]$, u a unit in $\mathbb{Z}[\omega]$.*

Proof.

(1) Write $z = u\pi_1^{e_1} \cdots \pi_m^{e_m}$ as Exercise 1.17. So

$$z^p = u^p \pi_1^{pe_1} \cdots \pi_m^{pe_m}.$$

(2) Factorize $x + y\omega = vq_1^{f_1} \cdots q_n^{f_n}$, where v is unit and all q_h ($1 \leq h \leq n$) are distinct primes in $\mathbb{Z}[\omega]$ and $f_h \in \mathbb{Z}^+$. Since $\mathbb{Z}[\omega]$ is a UFD, for every $q_h \mid x + y\omega$, there is some $k(h)$ such that $q_h = \pi_{k(h)}$ and also $q_h^{f_h} = \pi_{k(h)}^{pe_{k(h)}}$ or $f_h = pe_{k(h)}$.

(3) Hence,

$$x + y\omega = v\left(\pi_{k(1)}^{e_{k(1)}} \cdots \pi_{k(n)}^{e_{k(n)}}\right)^p,$$

where $\alpha = \pi_{k(1)}^{e_{k(1)}} \cdots \pi_{k(n)}^{e_{k(n)}} \in \mathbb{Z}[\omega]$ and v is unit.

□

Exercise 1.19. *Dropping the assumption that $\mathbb{Z}[\omega]$ is a UFD but using the fact that ideals factor uniquely (up to order) into prime ideals, show that the principal ideal $(x + y\omega)$ has no prime ideal factor in common with any of the other principal ideals on the left side of the equation*

$$(x + y)(x + y\omega)(x + y\omega^2) \cdots (x + y\omega^{p-1}) = (z)^p$$

in which all factors are interpreted as principal ideals. (Hint: Modify the proof of Exercise 1.17 appropriately, using the fact that if A is an ideal dividing another ideal B, then $A \supseteq B$.)

Proof. Write

$$(z) = \pi_1^{e_1} \cdots \pi_m^{e_m}$$

where π_k $(1 \leq k \leq m)$ are distinct prime ideals of $\mathbb{Z}[\omega]$ and $e_k \in \mathbb{Z}^+$ $(1 \leq k \leq m)$. By assumption that $\mathbb{Z}[\omega]$ is a Dedekind domain, the factorization of z is unique up to order.

(1) *Show that $\pi \mid (z)$.* Since $\pi \mid (x + y\omega)$, $\pi \mid (z)^p$. The factorization of $(z)^p$ is

$$(z)^p = \pi_1^{pe_1} \cdots \pi_m^{pe_m}.$$

$\pi | (z)^p$ implies that $\pi = \pi_k$ for some k, that is, $\pi \mid (z)$.

(2) *Show that $\pi \mid (yp)$ if π were divide any of the other factors on the left side of $(x + y)(x + y\omega)(x + y\omega^2) \cdots (x + y\omega^{p-1}) = (z)^p$.* Say $\pi \mid (x + y\omega^k)$ for some $k \neq 1$. So that $x + y\omega \in \pi$ and $x + y\omega^k \in \pi$, or $y(\omega - \omega^k) \in \pi$. Since $k \neq 1$, there are two possible cases.

   (a) $k > 1$. $y\omega(1 - \omega^{k-1}) \in \pi$. By Exercise 1.16, $y\omega p \in \pi$, or $yp \in \pi$ since ω is unit. (ω^{p-1} is the inverse of ω since $\omega \cdot \omega^{p-1} = 1$.)

   (b) $k = 0$. $y(\omega - 1) \in \pi$, or $y(1 - \omega) \in \pi$. By Exercise 1.16, $yp \in \pi$.

   In any case, $yp \in \pi$, or $\pi \mid (yp)$.

(3) Note that z and yp are integers, and they are relatively prime by the assumption that p divides none of x, y, z. Therefore, on $\mathbb{Z}$ we have $zm + ypn = 1$ for some $m, n \in \mathbb{Z}$.

(4) $zm + ypn = 1$ is also true in $\mathbb{Z}[\omega]$. Therefore, by (1)(2) we have $z \in \pi$ and $yp \in \pi$. So $zm + ypn \in \pi$ since π is an ideal. So $1 \in \pi$ or $\pi = (1)$, contrary to the primality of π.

□

Exercise 1.20. *Use Exercise 1.19 to show that $(x+y\omega) = I^p$ for some ideal I.*

Proof.

(1) Write $(z) = \pi_1^{e_1} \cdots \pi_m^{e_m}$ as Exercise 1.17. So

$$(z)^p = \pi_1^{pe_1} \cdots \pi_m^{pe_m}.$$

(2) Factorize $(x + y\omega) = q_1^{f_1} \cdots q_n^{f_n}$, where every q_h $(1 \leq h \leq n)$ are distinct prime ideals of $\mathbb{Z}[\omega]$ and $f_h \in \mathbb{Z}^+$. By assumption that $\mathbb{Z}[\omega]$ is a Dedekind domain, for every $q_h \mid (x + y\omega)$, there is some $k(h)$ such that $q_h = \pi_{k(h)}$ and also $q_h^{f_h} = \pi_{k(h)}^{pe_{k(h)}}$ or $f_h = pe_{k(h)}$.

(3) Hence,

$$(x + y\omega) = \left(\pi_{k(1)}^{e_{k(1)}} \cdots \pi_{k(n)}^{e_{k(n)}}\right)^p,$$

where $I = \pi_{k(1)}^{e_{k(1)}} \cdots \pi_{k(n)}^{e_{k(n)}}$ is an ideal of $\mathbb{Z}[\omega]$.

□

Exercise 1.21. *Show that every number of $\mathbb{Q}[\omega]$ is uniquely representable in the form*

$$a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2}, a_i \in \mathbb{Q} \ \forall\, i$$

by show that ω is a root of the polynomial

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

and that $f(t)$ is irreducible over $\mathbb{Q}$. (Hint: It is enough to show that $f(t+1)$ is irreducible, which can be established by Eisenstein's criterion. It helps to notice that $f(t+1) = \frac{(t+1)^p - 1}{t}$.)

Proof.

(1) *Given any number $\alpha \in \mathbb{Q}[\omega]$. Show that*

$$\alpha = a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2}, a_i \in \mathbb{Q} \ \forall\, i.$$

Since $\omega^p = 1$, we can write

$$\alpha = a_0' + a_1'\omega + a_2'\omega^2 + \cdots + a_{p-2}'\omega^{p-2} + a_{p-1}'\omega^{p-1}, a_i \in \mathbb{Q} \ \forall\, i.$$

Note that $\omega^{p-1} + \omega^{p-2} + \cdots + \omega + 1 = 0$, and thus we can replace ω^{p-1} by $-\omega^{p-2} - \cdots - \omega - 1$.

(2) *Show that ω is a root of the polynomial $f(t) = t^{p-1} + t^{p-2} + \cdots + t + 1$.* $f(\omega) = \omega^{p-1} + \omega^{p-2} + \cdots + \omega + 1 = 0$.

(3) *Show that $f(t)$ is irreducible over $\mathbb{Q}$.* It suffices to show that $f(t+1)$ is irreducible over $\mathbb{Q}$. Write $(t-1)f(t) = t^p - 1$. So

$$\begin{aligned} tf(t+1) &= (t+1)^p - 1 && \text{(Put } t \mapsto t+1\text{)} \\ &= \left(\sum_{k=0}^{p} \binom{p}{k} t^k \right) - 1 && \text{(Binomial theorem)} \\ &= \sum_{k=1}^{p} \binom{p}{k} t^k, \\ f(t+1) &= \sum_{k=1}^{p} \binom{p}{k} t^{k-1} \\ &= t^{p-1} + pt^{p-2} + \cdots + \frac{p(p-1)}{2} t + p. \end{aligned}$$

By Eisenstein's criterion, $f(t+1)$ is irreducible over $\mathbb{Q}$.

(4) To show the uniqueness, it suffices to show that the relation

$$0 = a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2}$$

implies all $a_i = 0$. Say $g(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_{p-2}t^{p-2} \in \mathbb{Q}[t]$. Clearly $g(\omega) = 0$. By the minimality of $f(t)$, $g(t)$ is identical zero, or all $a_i = 0$.

$\square$

Exercise 1.22. *Use Exercise 1.21 to show that if $\alpha \in \mathbb{Z}[\omega]$ and $p \mid \alpha$, then (writing $\alpha = a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}$, $a_i \in \mathbb{Z}$) all a_i are divisible by p.*

Proof. Since $p \mid \alpha$, there is $\beta \in \mathbb{Z}[\omega]$ such that $\alpha = p\beta$. Write

$$\begin{aligned} \alpha &= a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}, \\ \beta &= b_0 + b_1\omega + \cdots + b_{p-2}\omega^{p-2}, \end{aligned}$$

where $a_i, b_j \in \mathbb{Z}$. By $\alpha = p\beta$ and Exercise 1.21, $a_i = pb_i$ for every $1 \leq i \leq p-2$. So all a_i are divisible by p. $\square$

Define congruence mod p for $\beta, \gamma \in \mathbb{Z}[\omega]$ as follows:

$$\beta \equiv \gamma \pmod{p} \textit{ iff } \beta - \gamma = \delta p \textit{ for some } \delta \in \mathbb{Z}[\omega].$$

(Equivalently, this is congruence mod the principal ideal $p\mathbb{Z}[\omega]$.

Exercise 1.23. *Show that if $\beta \equiv \gamma \pmod p$, then $\overline{\beta} \equiv \overline{\gamma} \pmod p$ where the bar denotes complex conjugation.*

Proof.

(1) *Show that $\overline{\delta} \in \mathbb{Z}[\omega]$ for any $\delta \in \mathbb{Z}[\omega]$.* Write

$$\delta = a_0 + a_1\omega + \cdots + a_{p-1}\omega^{p-1}$$

where $a_0, \ldots, a_{p-1} \in \mathbb{Z}$. Take the complex conjugation to get

$$\begin{aligned}\overline{\delta} &= \overline{a_0} + \overline{a_1} \cdot \overline{\omega} + \cdots + \overline{a_{p-1}} \cdot \overline{\omega}^{p-1} \\ &= a_0 + a_1\overline{\omega} + \cdots + a_{p-1}\overline{\omega}^{p-1} && (\text{Every } a_k \in \mathbb{Z}) \\ &= a_0 + a_1\omega^{p-1} + \cdots + a_{p-1}\omega \in \mathbb{Z}[\omega]. && (\omega^p = 1)\end{aligned}$$

(2)

$$\begin{aligned}&\beta \equiv \gamma \pmod p \\ \Longleftrightarrow &\beta - \gamma = \delta p \text{ for some } \delta \in \mathbb{Z}[\omega] \\ \Longleftrightarrow &\overline{\beta} - \overline{\gamma} = \overline{\delta} p \text{ for some } \delta \in \mathbb{Z}[\omega] && (\text{Complex conjugation}) \\ \Longleftrightarrow &\overline{\beta} - \overline{\gamma} = \delta' p \text{ for some } \delta' \in \mathbb{Z}[\omega] && ((1)) \\ \Longleftrightarrow &\overline{\beta} \equiv \overline{\gamma} \pmod p\end{aligned}$$

□

Exercise 1.24. *Show that $(\beta + \gamma)^p \equiv \beta^p + \gamma^p \pmod p$ and generalize this to sums of arbitrarily many terms by induction.*

Proof.

(1) Binomial theorem gives us

$$(\beta + \gamma)^p = \sum_{k=0}^{p} \binom{p}{k} \beta^k \gamma^{p-k} = \beta^p + \gamma^p + \sum_{k=1}^{p-1} \binom{p}{k} \beta^k \gamma^{p-k}.$$

(2) Note that every binomial coefficient $\binom{p}{k}$ is divided by p in $\mathbb{Z}$ for $1 \leq k \leq p-1$. Also, every term $\beta^k \gamma^{p-k}$ is in $\mathbb{Z}[\omega]$. So $(\beta+\gamma)^p - \beta^p - \gamma^p = \delta p$ for some $\delta \in \mathbb{Z}[\omega]$. Hence the result holds.

(3) *In general,*

$$\left(\sum_{k=1}^{n} \alpha_k \right)^p \equiv \sum_{k=1}^{n} \alpha_k^p \pmod p.$$

Induction by $(\alpha_1+\alpha_2)^p \equiv \alpha_1^p+\alpha_2^p \pmod p$ and $\left(\sum_{k=1}^{n+1} \alpha_k\right)^p \equiv \left(\sum_{k=1}^{n} \alpha_k\right)^p + \alpha_{n+1}^p \equiv \left(\sum_{k=1}^{n} \alpha_k^p\right) + \alpha_{n+1}^p \equiv \sum_{k=1}^{n+1} \alpha_k^p \pmod p$.

□

Exercise 1.25. *Show that for all $\alpha \in \mathbb{Z}[\omega]$, α^p is congruent $\pmod p$ to some $a \in \mathbb{Z}$. (Hint: Write α in terms of ω and use Exercise 1.24.)*

Proof (Hint). Write

$$\alpha = a_0 + a_1\omega + \cdots + a_{p-1}\omega^{p-1}$$

where $a_0, \ldots, a_{p-1} \in \mathbb{Z}$. By Exercise 1.24,

$$\begin{aligned}
\alpha^p &\equiv a_0^p + (a_1\omega)^p + \cdots + (a_{p-1}\omega^{p-1})^p \\
&\equiv a_0^p + a_1^p\omega^p + \cdots + a_{p-1}^p(\omega^{p-1})^p \\
&\equiv a_0^p + a_1^p\omega^p + \cdots + a_{p-1}^p(\omega^p)^{p-1} \\
&\equiv a_0^p + a_1^p + \cdots + a_{p-1}^p. && (\omega^p = 1)
\end{aligned}$$

Here $a_0^p + a_1^p + \cdots + a_{p-1}^p \in \mathbb{Z}$, and thus α^p is congruent $\pmod p$ to some integer. □

Exercise 1.26-1.28: Now assume $p \geq 5$. We will show that if $x + y\omega = u\alpha^p \pmod p$, $\alpha \in \mathbb{Z}[\omega]$, u a unit in $\mathbb{Z}[\omega]$, x and y integers not divisible by p, then $x \equiv y \pmod p$. For this we will need the following result, proved by Kummer, on the units of $\mathbb{Z}[\omega]$:

Lemma: If u is a unit in $\mathbb{Z}[\omega]$ and $\overline{u}$ is its complex conjugate, then $u/\overline{u}$ is a power of ω. (For the proof, see Exercise 2.12.)

Exercise 1.26. *Show that $x + y\omega \equiv u\alpha^p \pmod p$ implies*

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

for some $k \in \mathbb{Z}$. (Use the Lemma on units and Exercise 1.23 and 1.25. Note that $\overline{\omega} = \omega^{-1}$.)

Proof (Hint).

$$
\begin{aligned}
& x + y\omega \equiv u\alpha^p \pmod p \\
\Longrightarrow & x + y\omega \equiv ua \pmod p \text{ for some } a \in \mathbb{Z} && \text{(Exercise 1.25)} \\
\Longrightarrow & \overline{x + y\omega} \equiv \overline{ua} \pmod p && \text{(Exercise 1.23)} \\
\Longrightarrow & x + y\overline{\omega} \equiv \overline{u}a \pmod p \\
\Longrightarrow & x + y\omega^{-1} \equiv \overline{u}a \pmod p && (\overline{\omega} = \omega^{-1}) \\
\Longrightarrow & x + y\omega^{-1} \equiv u\omega^{-k}a \pmod p \text{ for some } k \in \mathbb{Z} && \text{(Lemma)} \\
\Longrightarrow & ua \equiv (x + y\omega^{-1})\omega^k \pmod p \\
\Longrightarrow & x + y\omega \equiv (x + y\omega^{-1})\omega^k \pmod p.
\end{aligned}
$$

□

Exercise 1.27. *Use Exercise 1.22 to show that a contradiction results unless* $k \equiv 1 \pmod p$. *(Recall that* $p \nmid xy$, $p \geq 5$, *and* $\omega^{p-1} + \omega^{p-2} + \cdots + \omega + 1 = 0$.*)*

Proof. Exercise 1.26 shows

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

Multiply ω on the both sides to get $x\omega + y\omega^2 \equiv y\omega^k + x\omega^{k+1} \pmod p$, or

$$p \mid (x\omega + y\omega^2 - y\omega^k - x\omega^{k+1}).$$

If k were satisfying $k \not\equiv 1 \pmod p$, then by Exercise 1.22 and $p \geq 5$ we have $p \mid x$ or $p \mid y$, contrary to the assumption that x and y are integers not divisible by p. □

Exercise 1.28. *Finally, show* $x \equiv y \pmod p$.

Proof. In the argument of Exercise 1.27 we have

$$p \mid ((x - y)\omega + (y - x)\omega^2)$$

by replacing $k = 1$. By Exercise 1.22 and $p \geq 5$, $x - y$ is divisible by p, or $x \equiv y \pmod p$ as integers. □

Exercise 1.29. *Let* $\omega = \exp(\frac{2\pi i}{23})$. *Verify that the product*

$$(1 + \omega^2 + \omega^4 + \omega^5 + \omega^6 + \omega^{10} + \omega^{11})(1 + \omega + \omega^5 + \omega^6 + \omega^7 + \omega^9 + \omega^{11})$$

is divisible by 2 *in* $\mathbb{Z}[\omega]$, *although neither factor is. It can be shown (Exercise 3.17) that* 2 *is an irreducible element in* $\mathbb{Z}[\omega]$; *it follows that* $\mathbb{Z}[\omega]$ *cannot be a*

UFD.

Proof. Note that $\sum_{k=0}^{22} \omega^k = 0$. So

$$\begin{aligned}
&(1+\omega^2+\omega^4+\omega^5+\omega^6+\omega^{10}+\omega^{11})(1+\omega+\omega^5+\omega^6+\omega^7+\omega^9+\omega^{11}) \\
=&2(\omega^5+\omega^6+\omega^7+\omega^9+\omega^{10}+3\omega^{11}+\omega^{12}+\omega^{13}+\omega^{15}+\omega^{16}+\omega^{17})
\end{aligned}$$

is divisible by 2 in $\mathbb{Z}[\omega]$, although neither factor is. □

Exercise 1.30-1.32: R is an integral domain (commutative ring with 1 and no zero divisors).

Exercise 1.30. *Show that two ideals in R are isomorphic as R-modules iff they are in the same ideal class.*

Proof. Given any two ideals A, B in an commutative integral domain R.

(1) ($\Longrightarrow$) Let $\varphi : A \to B$ be an R-module isomorphism. Given any nonzero $\alpha \in A$, we have

$$\begin{aligned}
\varphi(\alpha)A &= \{\varphi(\alpha)a : a \in A\} \\
&= \{\varphi(\alpha a) : a \in A\} && (\varphi \text{ is a homomorphism}) \\
&= \{\alpha\varphi(a) : a \in A\} && (\varphi \text{ is a homomorphism}) \\
&= \{\alpha b : b \in B\} && (\varphi \text{ is an isomorphism}) \\
&= \alpha B.
\end{aligned}$$

Notice that $\varphi(\alpha) \neq 0$ since $\alpha \neq 0$ and φ is injective. Therefore, $A \sim B$.

(2) ($\Longleftarrow$) Given $A \sim B$, there are nonzero $\alpha, \beta \in R$ such that $\alpha A = \beta B$. Define a map $\varphi : A \to B$ by $\varphi(a) = b$ if $\alpha a = \beta b$.

- (a) *φ is well-defined.*
  - (i) *Existence of b.* Since $\alpha a \in \alpha A = \beta B$, there is $b \in B$ such that $\alpha a = \beta b$.
  - (ii) *Uniqueness of b.* If $\alpha a = \beta b_1 = \beta b_2$, $\beta(b_1 - b_2) = 0$. Since R is an integral domain and $\beta \neq 0$, $b_1 - b_2 = 0$ or $b_1 = b_2$.
- (b) *φ is an R-module homomorphism.*
  - (i) *Show that $\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)$.* Write $\varphi(a_1) = b_1$ and $\varphi(a_2) = b_2$.

$$\begin{aligned}
&\varphi(a_1) = b_1 \text{ and } \varphi(a_2) = b_2 \\
\Longrightarrow&\alpha a_1 = \beta b_1 \text{ and } \alpha a_2 = \beta b_2 && (\text{Definition of } \varphi) \\
\Longrightarrow&\alpha a_1 + \alpha a_2 = \beta b_1 + \beta b_2 && (\text{Add together}) \\
\Longrightarrow&\alpha(a_1 + a_2) = \beta(b_1 + b_2) \\
\Longrightarrow&\varphi(a_1 + a_2) = b_1 + b_2 = \varphi(a_1) + \varphi(a_2). && (\text{Definition of } \varphi)
\end{aligned}$$

(ii) *Show that $\varphi(ra) = r\varphi(a)$.* Write $\varphi(a) = b$.

$$\begin{aligned}
\varphi(a) = b &\Longrightarrow \alpha a = \beta b && \text{(Definition of } \varphi\text{)} \\
&\Longrightarrow r\alpha a = r\beta b && \text{(Multiply } r\text{)} \\
&\Longrightarrow \alpha(ra) = \beta(rb) && (R \text{ is commutative}) \\
&\Longrightarrow \varphi(ra) = rb = r\varphi(a). && \text{(Definition of } \varphi\text{)}
\end{aligned}$$

(c) *φ is injective.* Given $\varphi(a) = 0$. Then $\alpha a = \beta b = \beta 0 = 0$. Since R is an integral domain and $\alpha \neq 0$, $a = 0$.

(d) *φ is surjective.* Given any $b \in B$. $\beta b \in \beta B = \alpha A$. There is $a \in A$ such that $\beta b = \alpha a$. Such a satisfies $\varphi(a) = b$.

Therefore, $\varphi : A \to B$ is an R-module isomorphism.

□

Exercise 1.31. *Show that if A is an ideal in R and if αA is principal for some nonzero $\alpha \in R$, then A is principal. Conclude that the principal ideals form an ideal class.*

Proof.

(1) Write $\alpha A = (b)$ for some $b \in \alpha A$. That is, there is $a \in A$ such that

$$b = \alpha a.$$

(2) *Show that $A = (a)$ is principal.* $(a) \subseteq A$ holds trivially since $a \in A$ and A is an ideal. Given any $x \in A$. $\alpha x \in \alpha A = (b)$, and thus there is $y \in R$ such that $\alpha x = by$. Replace b by $b = \alpha a$ to get $\alpha x = \alpha a y$ or

$$\alpha(x - ay) = 0.$$

Since $\alpha \neq 0$ and R is an integral domain, $x - ay = 0$ or $x = ay \in (a)$ or $A \subseteq (a)$. Hence $A = (a)$ is principal.

(3) *Show that the principal ideals form an ideal class.* Given any $A = (a) \neq 0$ and $B = (b) \neq 0$, we have $bA = aB = (ab)$ for $a, b \in R$ or $A \sim B$.

□

Exercise 1.32. *Show that the ideal classes in R form a group iff for every ideal A there is an ideal B such that AB is principal.*

Note. The Picard group of the spectrum of a Dedekind domain is its ideal class group.

Proof. Let $[A]$ be the ideal class representing by a nonzero ideal A of R. Let

$$\mathrm{Pic}(R) = \{[A] : A \text{ is an ideal of } R\}$$

be the set of all ideal classes. Define the operation $\cdot : \mathrm{Pic}(R) \times \mathrm{Pic}(R) \to \mathrm{Pic}(R)$ by $[A] \cdot [B] \mapsto [AB]$.

(1) *(Closure) Show that the operation $[A] \cdot [B] \mapsto [AB]$ is well-defined.* Trivial due to the definition of the ideal class. Note that $[A] \cdot [B] = [B] \cdot [A]$ by the commutativity of R.

(2) *(Associativity) Show that $([A] \cdot [B]) \cdot [C] = [A] \cdot ([B] \cdot [C])$.* Trivial due to the definition of the ideal class.

(3) *(Identity element) Show that the non-zero principal ideals form the ideal class $[1]$.* Exercise 1.30 and note that (1) is principal too.

(4) *Show that the set Pic(R) forms an (abelian) group with $[1]$ as the identity element if and only if every $[A]$ has an inverse in Pic(R).* By (1)(2)(3), the set $\mathrm{Pic}(R)$ forms an (abelian) group iff every element has an inverse element. The conclusion is established.

□