Solutions to the book:
Marcus, Number Fields

Meng-Gen Tsai
plover@gmail.com

October 16, 2021

Contents

Chapter 1: A Special Case of Fermat's Conjecture

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. $\square$

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 $\alpha \in I \setminus \{0\}$ 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 $\alpha \in I \setminus \{0\}$ 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.

□

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

□

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 $\alpha \in I \setminus \{0\}$ 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. $\Box$

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. $\Box$

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.

$\square$

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. $\square$

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

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 $(1 \leq k \leq m)$ are distinct primes in $\mathbb{Z}[\omega]$ and $e_k \in \mathbb{Z}^+$ $(1 \leq k \leq m)$. 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.

$\square$

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.

$\square$

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 $\mathbb{Z}[\omega]$.

$\square$

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 $a_i = 0$.

□

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. □

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

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

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

□

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. $\square$

Exercise 1.29.

Let $\omega = \exp\left(\frac{2\pi i}{23}\right)$. 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. $\square$

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 $\varphi(a) = b$.

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

(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.

$\square$

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.

□

Chapter 2: Number Fields and Number Rings

Exercise 2.1.

(a) *Show that every number field of degree 2 over $\mathbb{Q}$ is one of the quadratic fields $\mathbb{Q}[\sqrt{m}]$, $m \in \mathbb{Z}$.*

(b) *Show that the fields $\mathbb{Q}[\sqrt{m}]$, m squarefree, are pairwise distinct. (Hint: Consider the equation $\sqrt{m} = a + b\sqrt{n}$); use this to show that they are in fact pairwise non-isomorphic.*

Proof of (a). Let $f(x) = ax^2 + bx + c$, $a, b, c \in \mathbb{Z}$ $(a \neq 0)$ and assume f is irreducible over $\mathbb{Q}$. Let α be a root of $f(x)$. So

$$\alpha = \frac{-b \pm \sqrt{m}}{2a}$$

where $m = b^2 - 4ac \in \mathbb{Z}$. Therefore,

$$\mathbb{Q}[\alpha] = \mathbb{Q}\left[\frac{-b \pm \sqrt{m}}{2a}\right] = \mathbb{Q}[\sqrt{m}].$$

$\square$

Proof of (b). Show that $\mathbb{Q}[\sqrt{m}]$ and $\mathbb{Q}[\sqrt{n}]$ are not isomorphic as fields if m and n are squarefree and $m \neq n$. Reductio ad absurdum.

(1) If $\varphi : \mathbb{Q}[\sqrt{m}] \to \mathbb{Q}[\sqrt{n}]$ were an isomorphism as fields, then φ is an identity map on $\mathbb{Q}$, and

$$\begin{aligned} &\varphi(\sqrt{m}) = a + b\sqrt{n} \text{ for some } a, b \in \mathbb{Q} \\ \Longrightarrow &\varphi(\sqrt{m})\varphi(\sqrt{m}) = (a + b\sqrt{n})^2 \\ \Longrightarrow &\varphi(\sqrt{m}\sqrt{m}) = (a + b\sqrt{n})^2 \\ \Longrightarrow &\varphi(m) = a^2 + nb^2 + 2ab\sqrt{n} \\ \Longrightarrow &m = a^2 + nb^2 + 2ab\sqrt{n}. \end{aligned}$$

If $2ab \neq 0$, then $\sqrt{n} = \frac{m - a^2 - nb^2}{2ab} \in \mathbb{Q}$, contrary to the assumption that n is squarefree. Hence $2ab = 0$.

(2) $a = 0$. Write $b = \frac{r}{s} \in \mathbb{Q}$ where $r, s \in \mathbb{Z}$ and $(r, s) = 1$. So

$$ms^2 = nr^2.$$

Hence

$$\begin{aligned} b \neq 0 &\Longrightarrow s^2 > 0 \text{ and } r^2 > 0 \\ &\Longrightarrow m \text{ and } n \text{ have the same sign} \\ &\Longrightarrow (\exists \text{ prime } p \mid m,\ p \nmid n) \text{ or } (\exists \text{ prime } q \mid n,\ q \nmid m) \text{ since } m \neq n. \end{aligned}$$

(a) *There is a prime $p \mid m$ but $p \nmid n$.*

$$\begin{aligned}
p \mid m &\Longrightarrow \text{Write } m = pm_1 \text{ for some } m_1 \in \mathbb{Z} \\
&\Longrightarrow (pm_1)s^2 = nr^2 && (ms^2 = nr^2) \\
&\Longrightarrow p \mid nr^2 \\
&\Longrightarrow p \mid r^2 && (p \nmid n \text{ by assumption}) \\
&\Longrightarrow p \mid r && (p \text{ is a prime}) \\
&\Longrightarrow \text{Write } r = pr_1 \text{ for some } r_1 \in \mathbb{Z} \\
&\Longrightarrow (pm_1)s^2 = n(pr_1)^2 && (ms^2 = nr^2) \\
&\Longrightarrow m_1 s^2 = npr_1^2 \\
&\Longrightarrow p \mid m_1 s^2 \\
&\Longrightarrow p \mid m_1 && ((r,s) = 1 \text{ and } p \mid r) \\
&\Longrightarrow \text{Write } m_1 = pm_2 \text{ for some } r_2 \in \mathbb{Z} \\
&\Longrightarrow m = p^2 m_2,
\end{aligned}$$

contrary to the assumption that m is squarefree.

(b) *There is a prime $q \mid n$ but $q \nmid m$.* Similar to (a).

(3) $b = 0$. $m = a^2$. Write $a = \frac{r}{s} \in \mathbb{Q}$ where $r, s \in \mathbb{Z}$ and $(r,s) = 1$. Hence $ms^2 = r^2$. Similar to the argument in (2).

(4) By (2)(3), no such isomorphism φ, that is, $\mathbb{Q}[\sqrt{m}]$ and $\mathbb{Q}[\sqrt{n}]$ are not isomorphic as fields.

$\square$

Supplement. (Isomorphic as vector spaces)

Show that $\mathbb{Q}[\sqrt{m}]$ and $\mathbb{Q}[\sqrt{n}]$ are isomorphic as $\mathbb{Q}$-vector spaces.

Proof. $[\mathbb{Q}[\sqrt{m}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{n}] : \mathbb{Q}] = 2$. There is a natural map $\varphi : \mathbb{Q}[\sqrt{m}] \to \mathbb{Q}[\sqrt{n}]$ defined by $\varphi(a + b\sqrt{m}) = a + b\sqrt{n}$. Clearly φ is well-defined, linear, injective and surjective. $\square$

Exercise 2.2.

Let I be the ideal generated by 2 and $1+\sqrt{-3}$ in the ring $\mathbb{Z}[\sqrt{-3}] = \{a+b\sqrt{-3} : a, b \in \mathbb{Z}\}$. Show that $I \neq (2)$ but $I^2 = 2I$. Conclude that ideals in $\mathbb{Z}[\sqrt{-3}]$ do not factor uniquely into prime ideals. Show moreover that I is the unique prime ideal containing (2) and conclude that (2) is not a product of prime ideals.

Proof.

(1) *Show that* $I \neq (2)$.

   (a) *Show that* $I \supseteq (2)$. $2 \in (2, 1+\sqrt{-3}) = I$.

   (b) *Show that* $I \not\subseteq (2)$. Consider $1+\sqrt{-3} \in I$. (Reductio ad absurdum) If $1+\sqrt{-3}$ were in (2), then there exists $a+b\sqrt{-3}$ such that

$$1+\sqrt{-3} = 2(a+b\sqrt{-3}) = 2a+2b\sqrt{-3}.$$

   Thus, $a = \frac{1}{2}$ and $b = \frac{1}{2}$, which is absurd.

(2) *Show that* $I^2 = 2I$.

   (a) *Show that* $I^2 \supseteq 2I$. Since $2 \in (2, 1+\sqrt{-3}) = I$, $2I \subseteq I^2$.

   (b) *Show that* $I^2 \subseteq 2I$. All elements of I^2 are generated by

$$2 \cdot 2, 2(1+\sqrt{-3}) \text{ and } (1+\sqrt{-3})^2.$$

   Clearly, $2 \cdot 2, 2(1+\sqrt{-3}) \in 2I$. Besides,

$$(1+\sqrt{-3})^2 = -2+2\sqrt{-3} = 2(-(2)+(1+\sqrt{-3})) \in 2I.$$

   Hence $I^2 \subseteq 2I$.

(3) *Show that ideals in* $\mathbb{Z}[\sqrt{-3}]$ *do not factor uniquely into prime ideals.* It is followed by $I^2 = 2I$ and $I \neq (2)$.

(4) *Show that* I *is the unique prime ideal containing* (2).

   (a) *Show that* $I = (2, 1+\sqrt{-3})$ *is a prime ideal containing* (2). Note that

$$\mathbb{Z}[\sqrt{-3}]/(2) = (\mathbb{Z}/2\mathbb{Z})[\sqrt{-3}] = \{0, 1, \sqrt{-3}, 1+\sqrt{-3}\}$$

   and

$$I/(2) = (1+\sqrt{-3})$$

   is an ideal of $\mathbb{Z}[\sqrt{-3}]/(2)$. So

$$\mathbb{Z}[\sqrt{-3}]/I = (\mathbb{Z}[\sqrt{-3}]/(2))/(I/(2)) = \{0, 1\} = \mathbb{Z}/2\mathbb{Z}$$

   is an integral domain. Hence I is a prime ideal containing (2).

   (b) Suppose I' is a prime ideal containing (2). Similar to part (a),

$$\begin{aligned}\mathbb{Z}[\sqrt{-3}]/I' &= (\mathbb{Z}[\sqrt{-3}]/(2))/(I'/(2)) \\ &= \{0, 1, \sqrt{-3}, 1+\sqrt{-3}\}/(I'/(2))\end{aligned}$$

   must be an integral domain.

   (c) Since $\{0, 1, \sqrt{-3}, 1+\sqrt{-3}\}$ is not an integral domain, $I'/(2) \neq (0)$ or $I' \neq (2)$. Also, $I'/(2) \neq \{0, 1, \sqrt{-3}, 1+\sqrt{-3}\}$ implies that $I'/(2) \neq (1) = (\sqrt{-3})$. Therefore we must have $I'/(2) = (1+\sqrt{-3})$. Here the existence is guaranteed by part (a).

(5) *Show that* (2) *is not a product of prime ideals.* (Reductio ad absurdum) Suppose (2) were a product of prime ideals. By part (4), we might write $(2) = I^n$ for some positive integer n. Since $I \neq (2)$ and $I^2 = 2I$,

$$(2) = (2)I^{n-1} \subseteq (2)I.$$

for some $n \geq 2$.

(6) Take $2 \in (2) \subseteq (2)I$. Write

$$2 = 2a_1 + \cdots + 2a_k = 2\underbrace{(a_1 + \cdots + a_k)}_{:=a \in I}$$

where $a_1, \ldots, a_k \in I$. We take the norm of the both sides to get $N(a) = 1$. a is a unit in $\mathbb{Z}[\sqrt{-3}]$. $I = \mathbb{Z}[\sqrt{-3}]$, which is absurd. Therefore (2) is not a product of prime ideals.

□

Exercise 2.3.

Complete the proof of Corollary 2, Theorem 2.1.

Corollary 2: Let m be a squarefree integer. The set of algebraic integers in the quadratic field $\mathbb{Q}[\sqrt{m}]$ is

$$\{a + b\sqrt{m} : a, b \in \mathbb{Z}\} \text{ if } m \equiv 2, 3 \pmod 4,$$
$$\left\{\frac{a + b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod 2\right\} \text{ if } m \equiv 1 \pmod 4.$$

Proof.

(1) Let $\alpha = r + s\sqrt{m}$, $r, s \in \mathbb{Q}$. If $s \neq 0$, then the monic irreducible polynomial over $\mathbb{Q}$ having α as a root is

$$x^2 - 2rx + r^2 - ms^2.$$

Thus α is an algebraic integer iff $2r$ and $r^2 - ms^2$ are both integers.

(2) Hence $4(r^2 - ms^2) = (2r)^2 - m(2s)^2 \in \mathbb{Z}$. $m(2s)^2 \in \mathbb{Z}$ since $2r \in \mathbb{Z}$. Hence $2s \in \mathbb{Z}$ since m is squarefree. Let $a = 2r, b = 2s \in \mathbb{Z}$. Then $a^2 - mb^2 = 4(r^2 - ms^2) \equiv 0 \pmod 4$. Note that a square $\equiv 0, 1 \pmod 4$ and thus we consider the following two cases.

(3) If $m \equiv 1 \pmod 4$, then

$$\begin{aligned} &a^2 - mb^2 \equiv a^2 - b^2 \pmod 4 \\ \Longrightarrow\ & a \text{ and } b \text{ has the same parity} \\ \Longrightarrow\ & \alpha = r + s\sqrt{m} = \frac{a + b\sqrt{m}}{2}, a, b \in \mathbb{Z}, a \equiv b \pmod 2. \end{aligned}$$

(4) If $m \equiv 2, 3 \pmod 4$, then

$$\begin{aligned} &a^2 - mb^2 \equiv a^2 + 2b^2 \text{ or } a^2 + b^2 \pmod 4 \\ \Longrightarrow\ & \text{both } a \text{ and } b \text{ are even} \\ \Longrightarrow\ & \text{both } r \text{ and } s \text{ are rational integers} \\ \Longrightarrow\ & \alpha = r + s\sqrt{m}, r, s \in \mathbb{Z}. \end{aligned}$$

□

Supplement.

(Exercise I.2.4 in [Jürgen Neukirch, *Algebraic Number Theory*].) *Let D be a squarefree rational integer $\neq 0, 1$ and d the discriminant of the quadratic number field $K = \mathbb{Q}(\sqrt{D})$. Show that*

$$d = \begin{cases} D & \text{if } D \equiv 1 \pmod 4, \\ 4D & \text{if } D \equiv 2, 3 \pmod 4. \end{cases}$$

and that an integral basis of K is given by $\{1, \sqrt{D}\}$ in the second case, by $\left\{1, \frac{1+\sqrt{D}}{2}\right\}$ in the first case, and by $\left\{1, \frac{d+\sqrt{d}}{2}\right\}$ in both case.

Proof.

(1) The Galois group of $K|\mathbb{Q}$ has two elements, the identity and an automorphism sending $\sqrt{D}$ to $-\sqrt{D}$.

(2) Note that $\alpha \in \mathcal{O}_K$ iff $\mathrm{Tr}_{K|\mathbb{Q}}(\alpha), N_{K|\mathbb{Q}}(\alpha) \in \mathbb{Z}$ (by noting that the equation $x^2 - \mathrm{Tr}_{K|\mathbb{Q}}(\alpha)x + N_{K|\mathbb{Q}}(\alpha) = 0$ has a root $x = \alpha$). So given $\alpha = x + y\sqrt{D} \in \mathcal{O}_K$, we have

$$\begin{aligned} \mathrm{Tr}_{K|\mathbb{Q}}(\alpha) &= 2x \in \mathbb{Z}, \\ N_{K|\mathbb{Q}}(\alpha) &= x^2 - Dy^2 \in \mathbb{Z}. \end{aligned}$$

(3) So $4(x^2 - Dy^2) = (2x)^2 - D(2y)^2 \in \mathbb{Z}$. So $D(2y)^2 \in \mathbb{Z}$ since $2x \in \mathbb{Z}$. So $2y \in \mathbb{Z}$ since D is squarefree $\neq 0, 1$. Let $r = 2x, s = 2y$. Then $r^2 - Ds^2 = 4(x^2 - Dy^2) \equiv 0 \pmod 4$. Note that a square $\equiv 0, 1 \pmod 4$ and thus we consider the following two cases.

(4) If $D \equiv 1 \pmod 4$, then

$$\begin{aligned}
& r^2 - Ds^2 \equiv r^2 - s^2 \pmod 4 \\
\Longrightarrow\, & r \text{ and } s \text{ has the same parity} \\
\Longrightarrow\, & \mathcal{O}_K = \left\{ \frac{r+s\sqrt{D}}{2} : r \equiv s \pmod 2 \right\} \\
\Longrightarrow\, & \mathcal{O}_K = \left\{ \frac{r-s}{2} + s \cdot \frac{1+\sqrt{D}}{2} : r \equiv s \pmod 2 \right\} \\
\Longrightarrow\, & \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{D}}{2}.
\end{aligned}$$

So $\left\{1, \frac{1+\sqrt{D}}{2}\right\}$ is an integral basis of K. Hence

$$d = \begin{vmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{vmatrix}^2 = D.$$

(5) If $D \equiv 2, 3 \pmod 4$, then

$$\begin{aligned}
& r^2 - Ds^2 \equiv r^2 + 2s^2 \text{ or } r^2 + s^2 \pmod 4 \\
\Longrightarrow\, & \text{both } r \text{ and } s \text{ are even} \\
\Longrightarrow\, & \text{both } x \text{ and } y \text{ are rational integers} \\
\Longrightarrow\, & \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{D}.
\end{aligned}$$

So $\{1, \sqrt{D}\}$ is an integral basis of K. Hence

$$d = \begin{vmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{vmatrix}^2 = 4D.$$

(6) By (4)(5), $\left\{1, \frac{d+\sqrt{d}}{2}\right\}$ is an integral basis of K for any case.

□

Exercise 2.4.

Suppose $a_0, \ldots, a_{n-1}$ are algebraic integers and α is a complex number satisfying

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Show that the ring $\mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$ has a finitely generated additive group. (Hint: Consider the products $a_0^{m_0} a_1^{m_1} \cdots a_{n-1}^{m_{n-1}} \alpha^m$ and show that only finitely many values of the exponents are needed.) Conclude that α is an algebraic *integer.*

Proof. Let $V = \mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$. Let n_k be the degree of the algebraic integer a_k where $0 \leq k \leq n-1$.

(1) *Show that V is finitely generated as an additive subgroup of $\mathbb{C}$. It suffices to show that V is generated by*

$$a_0^{m_0} a_1^{m_1} \cdots a_{n-1}^{m_{n-1}} \alpha^m$$

where $0 \leq m_k < n_k$ *and* $0 \leq m < n$. Given any $x \in V$, x is a finite sum of the product $a_0^{m_0} a_1^{m_1} \cdots a_{n-1}^{m_{n-1}} \alpha^m$ with $m_k \geq 0$ and $m \geq 0$.

If $m \geq n$, replace α^m by

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

Repeat this process to reduce the degree of α^m less than n. Therefore, we can write x as a finite sum of the product $a_0^{m_0'} a_1^{m_1'} \cdots a_{n-1}^{m_{n-1}'} \alpha^{m'}$ with $m_k' \geq 0$ and $0 \leq m' < n$.

Once the degree of α^m is reduced, continue to reduce the degree of each $a_k^{m_k'}$ without affecting other a_h ($h \neq k$) and α. Now replace $a_k^{m_k'}$ by

$$a_k^{m_k'} = \sum_{i=0}^{n_k - 1} b_{k,i} a_k^i$$

where $b_{k,i} \in \mathbb{Z}$. Therefore, we can write x as a finite sum of the product $a_0^{m_0''} a_1^{m_1''} \cdots a_{n-1}^{m_{n-1}''} \alpha^{m'}$ with $0 \leq m_k'' < n_k$ and $0 \leq m' < n$.

(4) *Show that α is an algebraic integer.* Since $\alpha \in V$, $\alpha V \subseteq V$. Thus α is an algebraic integer (Theorem 2.2).

□

Exercise 2.5.

Show that if f is any polynomials over $\mathbb{Z}/p\mathbb{Z}$ (p a prime) then $f(x^p) = (f(x))^p$. (Suggestion: Use induction on the number of terms.)

Proof.

(1) *Let*

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

be a binomial coefficient. If $1 \leq k \leq p-1$*, show that* p *divides* $\binom{p}{k}$.

(a) If $1 \leq k \leq p-1$, then $p \nmid k!$ and $p \nmid (p-k)!$ since p is a prime.

(b) Write $a = \frac{p!}{k!(p-k)!} \in \mathbb{Z}$. Hence,

$$\begin{aligned} a = \frac{p!}{k!(p-k)!} &\Longleftrightarrow p! = ak!(p-k)! \\ &\Longrightarrow p \mid p! \text{ or } p \mid ak!(p-k)! \\ &\Longrightarrow p \mid a \quad \text{by (a)}. \end{aligned}$$

Hence p divides $\binom{p}{k}$ if $1 \leq k \leq p-1$.

(2) Note that $a^p = a \in \mathbb{Z}/p\mathbb{Z}$ for all $a \in \mathbb{Z}/p\mathbb{Z}$.

(3) Write

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}/p\mathbb{Z}[x].$$

Induction on n.

(a) $n = 0$. So $f(x) = a_0$, and thus $f(x)^p = a_0^p = a_0$ by (2).

(b) $n = 1$. By $f(x) = a_1 x + a_0$,

$$\begin{aligned} f(x)^p &= (a_1 x + a_0)^p \\ &= a_1^p x^p + \sum_{k=1}^{p-1} \binom{p}{k} (a_1 x)^k a_0^{p-k} + a_0^p && \text{(Binomial theorem)} \\ &= a_1^p x^p + a_0^p && \text{((1))} \\ &= a_1 x^p + a_0 && \text{((2))} \\ &= f(x^p). \end{aligned}$$

(c) If the statement holds for $n-1$, then

$$\begin{aligned} f(x)^p &= (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)^p \\ &= [a_n x^n + (a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)]^p \\ &= (a_n x^n)^p + (a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)^p && \text{(Same as (b))} \\ &= a_n (x^p)^n + (a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)^p && \text{((2))} \\ &= a_n (x^p)^n + a_{n-1}(x^p)^{n-1} + \cdots + a_1 x^p + a_0 && \text{(Induction hypothesis)} \\ &= f(x^p). \end{aligned}$$

The inductive step is established.

By induction, $f(x)^p = f(x^p)$ holds for any $n \geq 0$.

$\square$

Exercise 2.6.

Show that if f and g are polynomials over a field K and $f^2 \mid g$ in $K[x]$, then $f \mid g'$. (Hint: Write $g = f^2 h$ and differentiate.)

Proof (Hint). Since $f^2 \mid g$ in $K[x]$, there exists $h \in K[x]$ such $g = f^2 h$. Differentiate to get $g' = 2ff'h + f^2h' = f(2f'h + fh')$, or $f \mid g'$ in $K[x]$. $\square$

Exercise 2.7.

Complete the proof of Corollary 2, Theorem 2.3.

Corollary 2: The galois group of $\mathbb{Q}[\omega]$ over $\mathbb{Q}$ is isomorphic to the multiplicative group of integer $\pmod{m}$

$$(\mathbb{Z}/m\mathbb{Z})^* = \{k : 1 \leq k \leq m, (k, m) = 1\}.$$

For each $k \in (\mathbb{Z}/m\mathbb{Z})^*$, the corresponding automorphism in the galois group sends ω to ω^k (and hence $g(\omega) \to g(\omega^k)$ for each $g \in \mathbb{Z}[x]$).

Proof.

(1) An automorphism of $\mathbb{Q}[\omega]$ is uniquely determined by the image of ω, and Theorem 2.3 shows that ω can be sent to any of the ω^k, $(k, m) = 1$. (Clearly it can't be sent anywhere else.) This established the one-to-one correspondence between the galois group and the multiplicative group of integer $\pmod{m}$, say

$$\alpha : \mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q}) \to (\mathbb{Z}/m\mathbb{Z})^*.$$

(2) The composition of automorphisms corresponds to multiplication $\pmod{m}$ in the natural way. That is, if $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$ with $\sigma(\omega) = \omega^k$ and $\tau(\omega) = \omega^h$, then

$$(\sigma\tau)(\omega) = \sigma(\omega^h) = \omega^{kh} \xrightarrow{\alpha} kh.$$

Hence α is a group homomorphism.

$\square$

Exercise 2.8.

(a) *Let $\omega = e^{\frac{2\pi i}{p}}$, p an odd prime. Show that $\mathbb{Q}[\omega]$ contains $\sqrt{p}$ if $p \equiv 1 \pmod 4$, and $\sqrt{-p}$ if $p \equiv 3 \pmod 4$. (Hint: Recall that we have shown that $\mathrm{disc}(\omega) = \pm p^{p-2}$ with $+$ holding iff $p \equiv 1 \pmod 4$.) Express $\sqrt{-3}$ and $\sqrt{5}$ as polynomials in the appropriate ω.*

(b) *Show that the eighth cyclotomic field contains $\sqrt{2}$.*

(c) *Show that every quadratic field is contained in a cyclotomic field: In fact, $\mathbb{Q}[\sqrt{m}]$ is contained in the d-th cyclotomic field, where $d = \mathrm{disc}(\mathcal{O}_{\mathbb{Q}[\sqrt{m}]})$. (More generally, Kronecker and Weber proved that every abelian extension of $\mathbb{Q}$ (normal with abelian Galois group) is contained in a cyclotomic field. See the Chapter 4 exercises. Hilbert and others investigated the abelian extensions of an arbitrary number field; their results are known as **class field theory**, which will be discussed in Chapter 8.)*

Proof of (a).

(1) Recall that we have shown that

$$\mathrm{disc}(\omega) = \prod_{1 \leq r < s \leq p} (\omega_r - \omega_s)^2 = (-1)^{\frac{p-1}{2}} p^{p-2} = (-1)^{\frac{p-1}{2}} p \cdot p^{p-3}$$

where $\omega_1 = \omega, \ldots, \omega_p$ are the conjugates of ω over $\mathbb{Q}$. Hence

$$\prod_{1 \leq r < s \leq p} (\omega_r - \omega_s) = \pm\sqrt{(-1)^{\frac{p-1}{2}} p} \cdot p^{\frac{p-3}{2}} \in \mathbb{Q}[\omega].$$

Note that $p^{\frac{p-3}{2}} \in \mathbb{Q}$ as $p \geq 3$ is odd and $\pm$ is unrelated as $\mathbb{Q}[\omega]$ is a field. Therefore

$$\sqrt{(-1)^{\frac{p-1}{2}} p} \in \mathbb{Q}[\omega].$$

(2) *Express $\sqrt{-3}$ as polynomials in the appropriate ω.* Take $\omega = e^{\frac{2\pi i}{3}}$. A direct computing shows that

$$\begin{aligned}
\prod_{1 \leq r < s \leq 3} (\omega_r - \omega_s) = \prod_{1 \leq r < s \leq 3} (\omega^r - \omega^s) &\\
&= (1-\omega)(1-\omega^2)(\omega - \omega^2) \\
&= 3(-\omega^2 + \omega) \\
&= 3\sqrt{-3}.
\end{aligned}$$

Hence $\sqrt{-3} = -\omega^2 + \omega$.

(3) *Express* $\sqrt{5}$ *as polynomials in the appropriate* ω. Take $\omega = e^{\frac{2\pi i}{5}}$. A direct computing shows that

$$\begin{aligned}\prod_{1 \leq r < s \leq 5} (\omega_r - \omega_s) &= \prod_{1 \leq r < s \leq 5} (\omega^r - \omega^s) \\ &= 3(\omega - \omega^2) \\ &= -25(\omega^4 - \omega^3 - \omega^2 + \omega) \\ &= -25\sqrt{5}.\end{aligned}$$

Hence $\sqrt{5} = \omega^4 - \omega^3 - \omega^2 + \omega$.

(4) (Another proof) The quadratic Gauss sum shows that

$$\sum_{n=0}^{p-1} e^{\frac{2\pi i n^2}{p}} = \sqrt{(-1)^{\frac{p-1}{2}} p}.$$

So $\sqrt{-3} = 2\omega_3 + 1$ and $\sqrt{5} = 2\omega_5^4 + 2\omega_5 + 1$.

□

Proof of (b).

(1) A root of eighth unity is $\omega = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i$.

(2) Hence

$$\omega + \omega^{-1} = \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{-2}}{2} \right) + \left(\frac{\sqrt{2}}{2} - \frac{\sqrt{-2}}{2} \right) = \sqrt{2} \in \mathbb{Q}[\omega].$$

□

Proof of (c).

(1) Note that $\mathbb{Q}[\omega_a, \omega_b] = \mathbb{Q}[\omega_{ab}]$ if $a, b \in \mathbb{Z}$ are relatively prime. Might assume that m is squarefree since $\mathbb{Q}[\sqrt{ab^2}] = \mathbb{Q}[\sqrt{a}]$. Consider the following four cases.

(2) Suppose $m > 0$ and $2 \nmid m$. Write

$$m = p_1 \cdots p_r \cdot q_1 \cdots q_s$$

as a product of distinct primes where $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$. Part (a) shows that

$$\sqrt{p_1}, \ldots, \sqrt{p_r}, \sqrt{-q_1}, \cdots, \sqrt{-q_s} \in \mathbb{Q}[\omega_{p_1}, \ldots, \omega_{p_r}, \omega_{q_1}, \ldots, \omega_{q_s}].$$

So $\sqrt{(-1)^s m} \in \mathbb{Q}[\omega_m]$. If s is even, then $\sqrt{m} \in \mathbb{Q}[\omega_m]$ or $\mathbb{Q}[\sqrt{m}] \subseteq \mathbb{Q}[\omega_m]$. If s is odd, then $\sqrt{m} \in \mathbb{Q}[\omega_m, \omega_4] = \mathbb{Q}[\omega_{4m}]$ (since $\sqrt{-1} \in \mathbb{Q}[\omega_4]$). In any case, $\mathbb{Q}[\sqrt{m}]$ is contained in the d-th cyclotomic field, where $d = \mathrm{disc}(\mathcal{O}_{\mathbb{Q}[\sqrt{m}]})$. (See Supplement to Exercise 2.3.)

(3) Suppose $m < 0$ and $2 \nmid m$. Similar to (2).

(4) Suppose $m > 0$ and $2 \mid m$. Write

$$m = 2 \cdot p_1 \cdots p_r \cdot q_1 \cdots q_s$$

as a product of distinct primes where $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$. Parts (a)(b) show that

$$\sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{-q_1}, \cdots, \sqrt{-q_s} \in \mathbb{Q}[\omega_8, \omega_{p_1}, \dots, \omega_{p_r}, \omega_{q_1}, \dots, \omega_{q_s}].$$

So $\sqrt{(-1)^s m} \in \mathbb{Q}[\omega_{4m}]$. Note that $\sqrt{(-1)^s} \in \mathbb{Q}[\omega_4] \subseteq \mathbb{Q}[\omega_{4m}]$. Hence $\sqrt{m} \in \mathbb{Q}[\omega_{4m}]$ is contained in the d-th cyclotomic field, where $d = 4m = \operatorname{disc}(\mathcal{O}_{\mathbb{Q}[\sqrt{m}]})$.

(5) Suppose $m < 0$ and $2 \mid m$. Same as (4).

□

Exercise 2.9.

With notation as in the proof of Corollary 3, Theorem 2.3, show that there exist integers u and v such that $e^{\frac{2\pi i}{r}} = \omega^u \theta^v$.

Proof.

(1) Recall $\omega = e^{\frac{2\pi i}{m}}$, $\theta = e^{\frac{2\pi i}{k}}$ and r is the least common multiple of k and m.

(2) As r is the least common multiple of k and m, there exist coprime integers a and b such that $r = am = bk$. As $(a, b) = 1$, there exist integers u and v such that $au + bv = 1$.

(3) Hence,

$$\begin{aligned} \omega^u \theta^v &= e^{\frac{2\pi i u}{m}} \cdot e^{\frac{2\pi i v}{k}} \\ &= e^{\frac{2\pi i a u}{r}} \cdot e^{\frac{2\pi i b v}{r}} \\ &= e^{\frac{2\pi i (au+bv)}{r}} \\ &= e^{\frac{2\pi i}{r}}. \end{aligned}$$

□

Exercise 2.10.

Complete the proof of Corollary 3 to Theorem 2.3, by showing if m is even, $m \mid r$, and $\varphi(r) \leq \varphi(m)$, then $r = m$.

Proof.

(1) Since m is even, write the unique factorization of m as

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where $p_1 = 2$, all $\alpha_i \geq 1$ $(1 \leq i \leq k)$, and all p_i $(1 \leq i \leq k)$ are distinct prime numbers.

(2) Since $m \mid r$, write $r = mm_1$ for some $m_1 \in \mathbb{Z}$. Thus we can write the unique factorization of r as

$$m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} q_1^{\gamma_1} \cdots q_h^{\gamma_h}$$

where all $\beta_i \geq \alpha_i \geq 1$ $(1 \leq i \leq k)$ and all p_i $(1 \leq i \leq k)$ and q_j $(1 \leq j \leq h)$ are distinct prime numbers. Here h might be zero if $m_1 = 1$, and all $q_j \mid m_1$ but $q_j \nmid m$.

(3) Thus,

$$\begin{aligned}
\varphi(m) &= m\left(1 - \frac{1}{2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
\varphi(r) &= mm_1\left(1 - \frac{1}{2}\right) \cdots \left(1 - \frac{1}{p_k}\right)\left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_h}\right) \\
&= \varphi(m)m_1\left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_h}\right) \\
&\geq \varphi(m)(q_1 \cdots q_h)\left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_h}\right) \\
&\geq \varphi(m)(q_1 - 1) \cdots (q_h - 1).
\end{aligned}$$

(4) Since all $q_j \neq 2$ $(1 \leq j \leq h)$, $q_j - 1 > 1$. Hence by (3) and assumption that $\varphi(r) \leq \varphi(m)$, $h = 0$ or $m_1 = 1$ or $r = m$.

□

Exercise 2.11.

(a) *Suppose all roots of a monic polynomial $f \in \mathbb{Q}[x]$ has absolute value 1. Show that the coefficient of x^r has absolute value $\leq \binom{n}{r}$, where n is the degree of f and $\binom{n}{r}$ is the binomial coefficient.*

(b) *Show that there are only finitely many algebraic integers α of fixed degree n, all of whose conjugates (including α) have absolute value 1. (Note: If you don't use Theorem 2.1, your proof is probably wrong.)*

(c) *Show that α must be a root of 1. (Show that its powers are restricted to a finite set.)*

Proof of (a).

(1) Write $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ where $\alpha_i \in \mathbb{C}$, $|\alpha_i| = 1$ for $i = 1, 2, \ldots, n$.

(2) So
$$f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1) s_n$$
where
$$s_r = \sum_{1 \leq j_1 < \cdots < j_r \leq n} \alpha_{j_1} \cdots \alpha_{j_r} \in \mathbb{C}.$$
Let $c_r = (-1)^r s_{n-r}$ be the coefficient of x^r.

(3)
$$\begin{aligned}
|c_r| &= |(-1)^r s_{n-r}| \\
&= \left| \sum_{1 \leq j_1 < \cdots < j_{n-r} \leq n} \alpha_{j_1} \cdots \alpha_{j_{n-r}} \right| \\
&\leq \sum_{1 \leq j_1 < \cdots < j_{n-r} \leq n} \left| \alpha_{j_1} \cdots \alpha_{j_{n-r}} \right| \\
&= \sum_{1 \leq j_1 < \cdots < j_{n-r} \leq n} |\alpha_{j_1}| \cdots |\alpha_{j_{n-r}}| \\
&= \sum_{1 \leq j_1 < \cdots < j_{n-r} \leq n} 1 \\
&= \binom{n}{n-r} \\
&= \binom{n}{r}.
\end{aligned}$$

□

Proof of (b).

(1) Let f be an irreducible monic polynomial over $\mathbb{Z}$ of degree n such that $f(\alpha) = 0$. So f is irreducible over $\mathbb{Q}$ (Theorem 2.1), and thus all the conjugates of α (including α) are roots of f.

(2) By (a), all the coefficient of x^r has absolute value $\leq \binom{n}{r}$. Since all the coefficient of x^r are integers, there are finitely many irreducible monic polynomials $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$ with $|\alpha| = 1$.

(3) For each such f, there are only finitely many roots. Therefore, there are only finitely many such algebraic integers α.

$\square$

Proof of (c).

(1) If $\alpha_1, \ldots, \alpha_n$ are the roots of f of degree n over $\mathbb{Q}$, then for every $r \in \mathbb{Z}^+$, $\alpha_1^r, \ldots, \alpha_n^r$ are all the roots of some monic polynomial f_r of degree n over $\mathbb{Q}$ (Fundamental theorem of symmetric polynomials).

(2) Now we consider the powers of α. All the powers of α (α^r) are algebraic integers (Theorem 2.2), and of degree at most n. (Let $g \in \mathbb{Z}[x]$ be the minimal polynomial of α^r over $\mathbb{Q}$. By (1), $f_r(\alpha^r) = 0$, and thus $g \mid f_r$. Hence $\deg(g) \leq \deg(f_r) = n$.)

(3) By (b), the powers of α are restricted to a finite set, say $\alpha^r = \alpha^s$ for some $s > r \geq 1$. So $\alpha^{s-r} = 1$ with $s - r \geq 1$. That is, α is a root of unity.

$\square$

Exercise 2.12. (Kummer's Lemma)

Now we can prove Kummer's lemma on units in the p-th cyclotomic field, as stated before Exercise 1.26: Let $\omega = e^{\frac{2\pi i}{p}}$, p an odd prime, and suppose u is a unit in $\mathbb{Z}[\omega]$.

(a) *Show that $u/\overline{u}$ is a root of 1. (Use Exercise 2.11(c) above and observe that complex conjugation is a member of the Galois group of $\mathbb{Z}[\omega]$ over $\mathbb{Q}$.) Conclude that $u/\overline{u} = \pm\omega^k$ for some k.*

(b) *Show that the $+$ sign holds: Assuming $u/\overline{u} = -\omega^k$, we have $u^p = -\overline{u^p}$; show that this implies that u^p is divisible by p in $\mathbb{Z}[\omega]$. (Use Exercise 1.23 and 1.25) But this is impossible since u^p is a unit.*

Proof of (a). Write $\alpha = u/\overline{u}$. Then

$$\begin{aligned} |\alpha| = 1 &\Longrightarrow \alpha \text{ is a root of unity} && \text{(Exercise 2.11)} \\ &\Longrightarrow \alpha \text{ is a } 2p\text{-th root of unity} && \text{(Corollary 3 to Theorem 2.3)} \\ &\Longrightarrow \alpha = \pm\omega^k \text{ for some } k \in \mathbb{Z} \end{aligned}$$

$\square$

Proof of (b). (Reductio ad absurdum) Assume that $u/\overline{u} = -\omega^k$, then

$$\begin{aligned} u/\overline{u} = -\omega^k &\Longrightarrow (u/\overline{u})^p = (-\omega^k)^p \\ &\Longrightarrow u^p/\overline{u}^p = (-1)^p\omega^{pk} = -1 && (p \text{ is odd}) \\ &\Longrightarrow u^p = -\overline{u}^p = -\overline{u^p} \end{aligned}$$

By Exercise 1.25, $u^p \equiv a \pmod p$ for some $a \in \mathbb{Z}$. By Exercise 1.23, $\overline{u^p} \equiv \overline{a} \equiv a \pmod p$. Thus

$$\begin{aligned} u^p = -\overline{u^p} &\Longrightarrow a \equiv -a \pmod p \\ &\Longrightarrow 2a \equiv 0 \pmod p \\ &\Longrightarrow a \equiv 0 \pmod p && (p \text{ is odd}) \end{aligned}$$

or $u^p \equiv 0 \pmod p$, contradicts the assumption that u is a unit. Hence $u/\overline{u} = \omega^k$ for some k. $\square$

Exercise 2.13.

Show that 1 *and* -1 *are the only units in the ring* $\mathcal{O}_{\mathbb{Q}[\sqrt{m}]}$, *m squarefree,* $m < 0$, $m \neq -1, -3$. *What if* $m = -1$ *or* -3*?*

Proof.

(1) Let $K = \mathbb{Q}[\sqrt{m}]$. Define a norm N on K by

$$N(a + b\sqrt{m}) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 + |m|b^2.$$

(2) Corollary 2 to Theorem 2.1 shows that

$$\mathcal{O}_K = \begin{cases} \{a + b\sqrt{m} : a, b \in \mathbb{Z}\} & (m \equiv 2, 3 \pmod 4), \\ \left\{\frac{a+b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod 2\right\} & (m \equiv 1 \pmod 4). \end{cases}$$

Clearly, N maps $\mathcal{O}_K$ to nonnegative integers. That is, u is a unit in $\mathcal{O}_K$ if and only if $N(u) = 1$ (by the fact that $N(u) = u\overline{u}$).

(3) If $m \equiv 2, 3 \pmod 4$ and $u = a + b\sqrt{m} \in \mathcal{O}_K$ is a unit ($a, b \in \mathbb{Z}$), then

$$N(u) = 1 = a^2 + |m|b^2.$$

(a) $m = -1$ *or* $|m| = 1$. $1 = a^2 + b^2$ or $(a, b) = (\pm 1, 0), (0, \pm 1)$. Hence all units in $\mathcal{O}_K$ are

$$\pm 1, \pm\sqrt{-1}.$$

(b) $m < -1$ *or* $|m| > 1$. $1 = a^2 + |m|b^2$ implies that $b^2 = 0$. Hence all units in $\mathcal{O}_K$ are ± 1.

(4) If $m \equiv 1 \pmod 4$ and $u = \frac{a+b\sqrt{m}}{2} \in \mathcal{O}_K$ is a unit ($a, b \in \mathbb{Z}, a \equiv b \pmod 2$), then $N(u) = 1 = (\frac{a}{2})^2 + |m|(\frac{b}{2})^2$ or

$$4 = a^2 + |m|b^2.$$

(a) $m = -3$ *or* $|m| = 3$. $4 = a^2 + 3b^2$ or $(a, b) = (\pm 2, 0), (\pm 1, \pm 1)$. Hence all units in $\mathcal{O}_K$ are

$$\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}.$$

(b) $m < -3$ *or* $|m| > 3$. $4 = a^2 + |m|b^2$ implies that $b^2 = 0$. Hence all units in $\mathcal{O}_K$ are ± 1.

(5) By (3)(4), all units in $\mathcal{O}_K$ are

$$\begin{cases} \pm 1 & (m \neq -1, -3), \\ \pm 1, \pm\sqrt{-1} & (m = -1), \\ \pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2} & (m = -3). \end{cases}$$

□

Exercise 2.14.

Show that $1 + \sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$. Use the powers of $1 + \sqrt{2}$ to generate infinitely many solutions to the diophantine equation $a^2 - 2b^2 = \pm 1$. (It will be shown in Chapter 5 that all units in $\mathbb{Z}[\sqrt{2}]$ are of the form $\pm(1+\sqrt{2})^k$, $k \in \mathbb{Z}$.)

Might assume to find nonnegative solutions to the Pell's equation $a^2 - 2b^2 = \pm 1$.

Proof.

(1) *Show that $1 + \sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$.* There is $-1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ such that

$$(1 + \sqrt{2})(-1 + \sqrt{2}) = 1 \in \mathbb{Z}[\sqrt{2}].$$

Hence $1 + \sqrt{2}$ is a unit.

(2) $N(a + b\sqrt{2}) = |a^2 - 2b^2|$ *is a norm on* $\mathbb{Z}[\sqrt{2}]$. To prove this, use the same argument as Exercise 1.1 and note that

$$N(a + b\sqrt{2}) = |(a + b\sqrt{2})(a - b\sqrt{2})|.$$

(3) By (1)(2), all $(1+\sqrt{2})^k$ with $k \geq 0$ are distinct solutions to the diophantine equation $a^2 - 2b^2 = \pm 1$. Explicitly, let

$$\begin{aligned}
(a_0, b_0) &= (1, 0), \\
(a_1, b_1) &= (1, 1), \\
(a_2, b_2) &= (3, 2), \\
(a_3, b_3) &= (7, 5), \\
&\cdots \\
(a_k, b_k) &= (a_{k-1} + 2b_{k-1}, a_{k-1} + b_{k-1}), \\
&\cdots
\end{aligned}$$

Note that all (a_k, b_k) are distinct and satisfying $a_k^2 - 2b_k^2 = \pm 1$. Hence we get infinitely many solutions to the Pell's equation $a^2 - 2b^2 = \pm 1$.

Note. Suppose that all units in $\mathbb{Z}[\sqrt{2}]$ are of the form $\pm(1+\sqrt{2})^k$, $k \in \mathbb{Z}$. Note that $(1+\sqrt{2})^k = (-1+\sqrt{2})^{-k}$. Thus we can find all nonnegative solutions to the Pell's equation $a^2 - 2b^2 = \pm 1$ are exactly the same as (3). $\square$

Supplement. (Exercise I.1.6 in Jürgen Neukirch, *Algebraic Number Theory*)

Show that the ring $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d}$, for any squarefree rational integer $d > 1$, has infinitely many units.

Proof. The proof is quoted from Proposition 17.5.2 in the book: Ireland and Rosen, *A Classical Introduction to Modern Number Theory, 2nd Ed.*

(1) Define the norm of $z = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ by $N(z) = z\overline{z}$ or

$$N(x + y\sqrt{d}) = \underbrace{(x + y\sqrt{d})}_{=z}\underbrace{(x - y\sqrt{d})}_{:=\overline{z}} = x^2 - dy^2.$$

Note that a norm is multiplicative. Similar to Exercise I.1.1, $\alpha \in \mathbb{Z}[\sqrt{d}]$ is a unit if and only if $N(\alpha) = \pm 1$.

(2) To show $\mathbb{Z}[\sqrt{d}]$ has infinitely many units, it suffices to show the equation $x^2 - dy^2 = 1$ has infinitely many (x, y) solutions.

(3) *If ξ is irrational then there are infinitely many rational numbers $\frac{x}{y}$, $(x, y) = 1$ such that $\left|\frac{x}{y} - \xi\right| < \frac{1}{y^2}$.* It is followed by the pigeonhole principle.

(4) *If d is a positive squarefree integer then there is a constant $M := 2\sqrt{d} + 1$ such that $\left|x^2 - dy^2\right| < M$ has infinitely many solutions over $\mathbb{Z}$.* Write $x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d})$. By part (3), there exist infinitely many

pairs of relatively prime integers (x, y), $y > 0$ satisfying $\left|x - y\sqrt{d}\right| < \frac{1}{y}$. Hence

$$\begin{aligned}
\left|x^2 - dy^2\right| &= \left|x + y\sqrt{d}\right|\left|x - y\sqrt{d}\right| \\
&\leq \left(\left|x - y\sqrt{d}\right| + 2y\sqrt{d}\right)\left|x - y\sqrt{d}\right| \\
&\leq 2\sqrt{d} + 1.
\end{aligned}$$

(5) By part (4), there is an integer m such that $x^2 - dy^2 = m$ for infinitely many solutions over $\mathbb{Z}$. Here $m \neq 0$. We might assume $x, y > 0$ and x components of solutions are distinct.

(6) The pigeonhole principle shows that there are two distinct solutions (x_1, y_1), (x_2, y_2) with $x_1 \neq x_2$ such that

$$x_1 \equiv x_2 \pmod{|m|}, \qquad y_1 \equiv y_2 \pmod{|m|}.$$

Let $\alpha = x_1 - y_1\sqrt{d}$, $\beta = x_2 + y_2\sqrt{d}$ and $\gamma = \alpha\beta$. Hence

$$\begin{aligned}
\gamma &= (x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) \\
&= \underbrace{(x_1x_2 - dy_1y_2)}_{\equiv 0 \pmod{|m|}} + \underbrace{(x_1y_2 - x_2y_1)}_{\equiv 0 \pmod{|m|}}\sqrt{d} \\
&:= m(u + v\sqrt{d})
\end{aligned}$$

for some $u + v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Taking norms of $\gamma = \alpha\beta$ gives $N(\gamma) = N(\alpha)N(\beta)$ or

$$m^2(u + v\sqrt{d}) = m^2.$$

Hence $u + v\sqrt{d} = 1$. By construction of x_1, x_2, $v \neq 0$. Therefore the equation $x^2 - dy^2 = 1$ has one solution with $x, y > 0$.

(7) By part (6), we might take a unit $\varepsilon = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ with $x, y > 0$. Note that $\varepsilon \geq 1 + \sqrt{d} > 1$ (over the ordered field $\mathbb{R}$). Hence there are infinitely many units

$$\varepsilon, \varepsilon^2, \varepsilon^3, \ldots$$

in $\mathbb{Z}[\sqrt{d}]$.

□

Note. Furthermore, show that there is a unit ε such that every unit has the form $\pm\varepsilon^n$, $n \in \mathbb{Z}$.

Proof.

(1) By the well-ordering principle, there is a unit $\varepsilon = x_1 + y_1\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ such that $x_1, y_1 > 0$ and (x_1, y_1) is the smallest solution of $x^2 - dy^2 = \pm 1$ with $x, y > 0$.

(2) Now given any unit $\varepsilon' = x + y\sqrt{d}$, $x, y > 0$, it suffices to show that there is a positive integer n such that $\varepsilon' = \varepsilon^n$.

(3) (Reductio ad absurdum) If not, there were a positive integer n such that $\varepsilon^n < \varepsilon' < \varepsilon^{n+1}$. Hence $1 < \varepsilon^{-n}\varepsilon' < \varepsilon$. Say $\varepsilon^{-n}\varepsilon' := x' + y'\sqrt{d}$. As $\varepsilon^{-n}\varepsilon' > 1 > 0$, the inverse is satisfying $x' - y'\sqrt{d} > 0$. Hence $x' > 0$.

(4) As the inverse is satisfying $x' - y'\sqrt{d} < 1$, $y' \geq 0$. Note that $y' \neq 0$ (since $\varepsilon > 1$). Hence the existence of $\varepsilon^{-n}\varepsilon'$ contradicts the minimality of ε.

(5) Now suppose a unit $\varepsilon' = x + y\sqrt{d}$ is of the form $x > 0$, $y < 0$. Then $\varepsilon'^{-1} = x - y\sqrt{d} = \varepsilon^n$ for some positive integer n by (2)(3)(4). Hence $\varepsilon' = \varepsilon^{-n}$ for some positive integer n. Other two cases of $\varepsilon' = x + y\sqrt{d}$ are similar. Therefore, every unit has the form $\pm\varepsilon^n$, $n \in \mathbb{Z}$.

□

Supplement. (Exercise I.1.7 in Jürgen Neukirch, *Algebraic Number Theory*)

Show that the ring $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$ is euclidean. Show furthermore that its units are given by $\pm(1+\sqrt{2})^n$, $n \in \mathbb{Z}$, and determine its prime elements.

Proof.

(1) *Show that $\mathbb{Z}[\sqrt{2}]$ is euclidean with respect to the function $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{N} \cup \{0\}$, $\alpha \mapsto \alpha\overline{\alpha}$.* For $\alpha, \beta \neq 0 \in \mathbb{Z}[\sqrt{2}]$, one has to find $\gamma, \rho \in \mathbb{Z}[\sqrt{2}]$ such that
$$\alpha = \gamma\beta + \rho, \qquad N(\rho) < N(\beta).$$

(2) Extend the norm function N to $\mathbb{Q}[\sqrt{2}]$. Write
$$\frac{\alpha}{\beta} = x + y\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$
Take $\gamma = u + v\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ such that u, v are satisfying $|u - x| \leq \frac{1}{2}$, $|v - y| \leq \frac{1}{2}$. Now take $\rho = \alpha - \gamma\beta$.

(3) Hence,
$$N\left(\frac{\alpha}{\beta} - \gamma\right) = (u-x)^2 + 2(v-y)^2 \leq \left(\frac{1}{2}\right)^2 + 2 \cdot \left(\frac{1}{2}\right)^2 < 1$$
and thus
$$N(\rho) = N(\alpha - \gamma\beta) = N(\beta)N\left(\frac{\alpha}{\beta} - \gamma\right) < N(\beta).$$

(4) *Show that its units are given by* $\pm(1+\sqrt{2})^n$, $n \in \mathbb{Z}$. $\varepsilon = 1+\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is a unit such that $(1,1)$ is the smallest solution of $x^2 - 2y^2 = \pm 1$ with $x, y > 0$. By the note in Exercise I.1.6, all units are given by $\pm(1+\sqrt{2})^n$, $n \in \mathbb{Z}$.

(5) *For all prime numbers $p \neq 2$, one has $p = a^2 - 2b^2$ $(a, b \in \mathbb{Z})$ if and only if $p \equiv 1, 7 \pmod 8$.* Similar to the proof of Proposition I.1.1, it suffices to show that a prime number $p \equiv 1, 7 \pmod 8$ of $\mathbb{Z}$ does not remain a prime element in the ring $\mathbb{Z}[\sqrt{2}]$. (Reductio ad absurdum) Note that the congruence

$$2 \equiv x^2 \pmod p$$

admits a solution (by the law of quadratic reciprocity). Thus we have $p \mid x^2 - 2 = (x+\sqrt{2})(x-\sqrt{2})$. Hence $\frac{x}{p} \pm \frac{\sqrt{2}}{p} \in \mathbb{Z}[\sqrt{2}]$, which is absurd.

(6) *The prime element π of $\mathbb{Z}[\sqrt{2}]$, up to associated elements, are given as follows.*

   (i) $\pi = \sqrt{2}$,

   (ii) $\pi = a + \sqrt{2}b$ *with* $a^2 - 2b^2 = p$, $p \equiv 1, 7 \pmod 8$,

   (iii) $\pi = p$, $p \equiv 3, 5 \pmod 8$.

   Here, p denotes a prime number of $\mathbb{Z}$. The proof is exactly the same as Theorem I.1.4.

$\square$

Exercise 2.15.

(a) *Show that $\mathbb{Z}[\sqrt{-5}]$ contains no element whose norm is 2 or 3.*

(b) *Verify that $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ is an example of non-unique factorization in the number ring $\mathbb{Z}[\sqrt{-5}]$.*

Proof of (a). Since $N(a+b\sqrt{-5}) = a^2 + 5b^2 \equiv a^2 \equiv 0, 1, 4 \pmod 5$, there is no element whose norm is 2 or 3. $\square$

Proof of (b).

(1) *Show that* $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

$$2 \cdot 3 = 6 \text{ and } (1+\sqrt{-5})(1-\sqrt{-5}) = 6.$$

(2) *Show that* 2 *is irreducible.* Suppose $2 = \alpha\beta$ where $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Take norm to get

$$\begin{aligned} N(2) = N(\alpha)N(\beta) &\Longrightarrow 4 = N(\alpha)N(\beta) \\ &\Longrightarrow N(\alpha) = 1 \text{ or } N(\beta) = 1 \qquad\qquad ((1)) \\ &\Longrightarrow \alpha \text{ or } \beta \text{ is unit.} \end{aligned}$$

(3) *Show that* 3 *is irreducible.* Similar to (2).

(4) *Show that* $1 \pm \sqrt{-5}$ *is irreducible.* Since $N(1 \pm \sqrt{-5}) = 2$ is prime, $1 + \sqrt{-5}$ is irreducible.

Hence 6 has a non-unique factorization in the number ring $\mathbb{Z}[\sqrt{-5}]$. □

Exercise 2.16.

Set $\alpha = \sqrt[4]{2}$. *Use the trace* $T = T^{\mathbb{Q}[\alpha]}$ *to show that* $\sqrt{3} \notin \mathbb{Q}[\alpha]$. *(Hint: Write* $\sqrt{3} = a + b\alpha + c\alpha^2 + d\alpha^3$ *and successively show that* $a = 0$*;* $b = 0$ *(what is* $T\left(\frac{\sqrt{3}}{\alpha}\right)$*?);* $c = 0$*; and finally obtain a contradiction.)*

Proof.

(1) Let $K = \mathbb{Q}[\alpha]$. (Reductio ad absurdum) If $\sqrt{3} \in K$, then we can write $\sqrt{3} = a + b\alpha + c\alpha^2 + d\alpha^3$ for some integers a, b, c and d.

(2) Note that $K = \mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{3}]$ by assumption. Hence

$$\begin{aligned} & T^{\mathbb{Q}[\sqrt{3}]}(\sqrt{3}) = T^{\mathbb{Q}[\alpha]}(a + b\alpha + c\alpha^2 + d\alpha^3) \\ \Longrightarrow\ & 0 = 4a \\ \Longrightarrow\ & a = 0. \end{aligned}$$

So $\sqrt{3} = b\alpha + c\alpha^2 + d\alpha^3$.

(3) $\sqrt{3} = b\alpha + c\alpha^2 + d\alpha^3$ implies that

$$\underbrace{\sqrt{3}\alpha^3}_{=\sqrt[4]{72}} = 2b + 2c\alpha + 2d\alpha^2.$$

Since $\mathbb{Q}[\sqrt[4]{72}] \subseteq K$ and $[\mathbb{Q}[\sqrt[4]{72}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}] = 4$, $K = \mathbb{Q}[\sqrt[4]{72}]$. Hence

$$\begin{aligned} & T^{\mathbb{Q}[\sqrt[4]{72}]}(\sqrt[4]{72}) = T^{\mathbb{Q}[\alpha]}(2b + 2c\alpha + 2d\alpha^2) \\ \Longrightarrow\ & 0 = 8b \\ \Longrightarrow\ & b = 0. \end{aligned}$$

So $\sqrt{3} = c\alpha^2 + d\alpha^3$.

(4) Similar to (3). $\sqrt{3} = c\alpha^2 + d\alpha^3$ implies that

$$\underbrace{\sqrt{3}\alpha^2}_{=\sqrt{6}} = 2c + 2d\alpha.$$

Since $\mathbb{Q}[\sqrt{6}] \subseteq K$ and $[\mathbb{Q}[\sqrt{6}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = 2$, $K = \mathbb{Q}[\sqrt{6}]$. Hence

$$T^{\mathbb{Q}[\sqrt{6}]}(\sqrt{6}) = T^{\mathbb{Q}[\alpha]}(2c + 2d\alpha) \Longrightarrow 0 = 8c \Longrightarrow c = 0.$$

So $\sqrt{3} = d\alpha^3$.

(5) Similar to (3)(4), $d = 0$ and thus $\sqrt{3} = 0$, which is absurd.

$\square$

Proof (Field theory).

(1) (Reductio ad absurdum) If $\sqrt{3} \in \mathbb{Q}[\sqrt[4]{2}]$, then $\mathbb{Q}[\sqrt{3}, \sqrt{2}] \subseteq \mathbb{Q}[\sqrt[4]{2}]$. As $[\mathbb{Q}[\sqrt{3}, \sqrt{2}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}] = 4$, $\mathbb{Q}[\sqrt{3}, \sqrt{2}] = \mathbb{Q}[\sqrt[4]{2}]$.

(2) Note that $\mathbb{Q}[\sqrt{3}, \sqrt{2}]$ is normal over $\mathbb{Q}$ but $\mathbb{Q}[\sqrt[4]{2}]$ is not normal over $\mathbb{Q}$.

$\square$

Supplement.

(1) *Give an example of fields $F \subseteq K \subseteq L$ where L/K and K/F are normal but L/F is not normal.*

(2) *Show that $\sqrt[3]{3} \notin \mathbb{Q}[\sqrt[3]{2}]$.*

(3) *Show that $1 + 5\sqrt[3]{2} - \sqrt[3]{4}$ is not a perfect square in $\mathbb{Q}[\sqrt[3]{2}]$.*

Exercise 2.19. (Vandermonde determinant)

Let R be a commutative ring and fix elements $a_1, a_2, \ldots \in R$. We will prove by induction that the Vandermonde determinant

$$\begin{vmatrix} 1 & a_1 & \cdots & a_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} \end{vmatrix}$$

is equal to the product $\prod_{1 \le r < s \le n}(a_s - a_r)$. Assuming that the result holds for some n, consider the determinant

$$\begin{vmatrix} 1 & a_1 & \cdots & a_1^{n} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^{n} \\ 1 & a_{n+1} & \cdots & a_{n+1}^{n} \end{vmatrix}.$$

Show that this is equal to

$$\begin{vmatrix} 1 & a_1 & \cdots & f(a_1) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & f(a_n) \\ 1 & a_{n+1} & \cdots & f(a_{n+1}) \end{vmatrix}$$

for any monic polynomial f over R of degree n. Then choose f cleverly so that the determinant is easily calculated.

Proof.

(1) Let

$$V_n = \begin{pmatrix} 1 & a_1 & \cdots & a_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} \end{pmatrix}$$

be the Vandermonde matrix. We will apply the induction to show that $\det(V_n) = \prod_{1 \leq r < s \leq n}(a_s - a_r)$.

(2) Nothing to do for $n = 1, 2$. Now Assuming that the result holds for some n, consider the determinant

$$\det(V_{n+1}) = \begin{vmatrix} 1 & a_1 & \cdots & a_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^n \\ 1 & a_{n+1} & \cdots & a_{n+1}^n \end{vmatrix}.$$

(3) *Show that*

$$\det(V_{n+1}) = \begin{vmatrix} 1 & a_1 & \cdots & f(a_1) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & f(a_n) \\ 1 & a_{n+1} & \cdots & f(a_{n+1}) \end{vmatrix}$$

for any monic polynomial f over R of degree n. Note that $\det(V_{n+1})$ is unchanged by adding a multiple of one column of V_{n+1} to another column of V_{n+1}. In particular, we add a multiple of the i-th column of V_{n+1} to the last column of V_{n+1} for $i = 1, 2, \ldots, n$. Then we obtain the equation

$$\det(V_{n+1}) = \begin{vmatrix} 1 & a_1 & \cdots & f(a_1) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & f(a_n) \\ 1 & a_{n+1} & \cdots & f(a_{n+1}) \end{vmatrix}.$$

(4) In particular, we take

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_n).$$

Therefore

$$\begin{aligned}
\det(V_{n+1}) &= \begin{vmatrix} 1 & a_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & 0 \\ 1 & a_{n+1} & \cdots & \prod_{1 \le r \le n}(a_{n+1} - a_r) \end{vmatrix} \\
&= (-1)^{(n+1)+(n+1)} \prod_{1 \le r \le n} (a_{n+1} - a_r) \begin{vmatrix} 1 & a_1 & \cdots & a_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} \end{vmatrix} \\
&= \prod_{1 \le r \le n} (a_{n+1} - a_r) \prod_{1 \le r < s \le n} (a_s - a_r) \\
&= \prod_{1 \le r < s \le n+1} (a_s - a_r).
\end{aligned}$$

By induction, the result is established.

□

Exercise 2.20.

Let f be a monic irreducible polynomial over a number field K and let α be one of its roots in $\mathbb{C}$. Show that $f'(\alpha) = \prod_{\beta \neq \alpha}(\alpha - \beta)$ with the product taken over all roots $\beta - \alpha$. (Hint: Write $f(x) = (x - \alpha)g(x)$.)

Proof.

(1) Note that f has no repeated roots in $\mathbb{C}$ by the irreducibility of f. So we can write
$$f(x) = (x - \alpha)g(x) = (x - \alpha) \prod_{\beta \neq \alpha} (x - \beta).$$

(2) So
$$f'(x) = g(x) + (x - \alpha)g'(x)$$
by the Leibniz rule. Take $x = \alpha$ to get
$$f'(\alpha) = g(\alpha) = \prod_{\beta \neq \alpha} (\alpha - \beta).$$

□

Exercise 2.22. (Stickelberger's criterion)

Let K be a number field of degree n over $\mathbb{Q}$ and fix algebraic integers $\alpha_1, \ldots, \alpha_n \in K$. We know that $d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ is in $\mathbb{Z}$; we will show that $d \equiv 0$ or $1 \pmod 4$. Letting $\sigma_1, \ldots, \sigma_n$ denote the embeddings of K in $\mathbb{C}$, we know that d is the square of the determinant $|\sigma_i(\alpha_j)|$. This determinant is a sum of $n!$ terms, one for each permutation of $\{1, \ldots, n\}$. Let P denote the sum of the terms corresponding to even permutations, and let N denote the sum of the terms (without negative signs) corresponding to odd permutations. Thus $d = (P - N)^2 = (P + N)^2 - 4PN$. Complete the proof by showing that $P + N$ and PN are in $\mathbb{Z}$. (Suggestion: Show that they are algebraic integers and that they are in $\mathbb{Q}$; for the latter, extend all σ_i to some normal extension L of $\mathbb{Q}$ so that they become automorphisms of L.)

*In particular we have $\operatorname{disc}(\mathcal{O}_K) \equiv 0$ or $1 \pmod 4$. This is known as **Stickelberger's criterion**.*

Proof.

(1) Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$.

(2) Note that

$$\begin{aligned}
|\sigma_i \alpha_j| &= \sum_{\pi \in S_n} \left(\operatorname{sgn}(\pi) \prod_{i=1}^{n} \sigma_i \alpha_{\pi(i)} \right) \\
&= \underbrace{\sum_{\pi \in A_n} \prod_{i=1}^{n} \sigma_i \alpha_{\pi(i)}}_{:=P} - \underbrace{\sum_{\pi \in S_n - A_n} \prod_{i=1}^{n} \sigma_i \alpha_{\pi(i)}}_{:=N}
\end{aligned}$$

where S_n is the symmetric group of degree n and A_n is the alternating group of degree n.

(3) Note that $\sigma_i(P + N) = P + N$ and $\sigma_i(PN) = PN$ for all σ_i. Hence $P+N, PN \in \mathbb{Q}$ by extending all σ_i to some normal extension L of $\mathbb{Q}$ so that they become automorphisms of L. Therefore $P + N, PN \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$.

(4) By (2)(3),

$$\begin{aligned}
d &= |\sigma_i \omega_j|^2 \\
&= (P - N)^2 \\
&= (P + N)^2 - 4PN \\
&\equiv 0, 1 \pmod 4.
\end{aligned}$$

In particular, $\operatorname{disc}(\mathcal{O}_K) \equiv 0, 1 \pmod 4$.

$\square$

Supplement.

(Exercise I.2.7 (Stickelberger's discriminant relation) in [Jürgen Neukirch, *Algebraic Number Theory*].) *The discriminant d_K of an algebraic number field K is always $\equiv 0 \pmod 4$ or $\equiv 1 \pmod 4$. (Hint: The discriminant $\det(\sigma_i\omega_j)$ of an integral basis ω_j is a sum of terms, each prefixed by a positive or a negative sign. Writing P (resp. N) for the sum of the positive (resp. negative) terms, one find $d_K = (P-N)^2 = (P+N)^2 - 4PN$.)*

Proof (Hint).

(1) Let S_n be the symmetric group of degree n, and A_n be the alternating group of degree n. So

$$\begin{aligned}\det(\sigma_i\omega_j) &= \sum_{\pi\in S_n}\left(\operatorname{sgn}(\pi)\prod_{i=1}^{n}\sigma_i\omega_{\pi(i)}\right)\\ &= \underbrace{\sum_{\pi\in A_n}\prod_{i=1}^{n}\sigma_i\omega_{\pi(i)}}_{:=P} - \underbrace{\sum_{\pi\in S_n-A_n}\prod_{i=1}^{n}\sigma_i\omega_{\pi(i)}}_{:=N}.\end{aligned}$$

(2) Note that $\sigma_i(P+N) = P+N$ and $\sigma_i(PN) = PN$ for all σ_i. Hence $P+N, PN \in \mathbb{Q}$ by extending all σ_i to some normal extension L of $\mathbb{Q}$ so that they become automorphisms of L. Therefore $P+N, PN \in \mathbb{Q}\cap\mathcal{O}_K = \mathbb{Z}$.

(3) By (1)(2),

$$\begin{aligned}d_K &= \det(\sigma_i\omega_j)^2\\ &= (P-N)^2\\ &= (P+N)^2 - 4PN\\ &\equiv 0,1 \pmod 4.\end{aligned}$$

□

Exercise 2.24.

Let G be a free abelian group of rank n and let H be a subgroup. Without loss of generality we take $G = \mathbb{Z}\oplus\cdots\oplus\mathbb{Z}$ (n times). We will show by induction that H is a free abelian group of rank $\leq n$. First prove it for $n=1$. Then, assuming the result holds for $n-1$, let $\pi : G \to \mathbb{Z}$ denote the obvious projection of G on the first factor (so that an n-tuple of integers gets sent to its first component). Let K denote the kernel of π.

(a) *Show that $H \cap K$ is a free abelian group of rank $\leq n-1$.*

(b) *The image $\pi(H) \subseteq \mathbb{Z}$ is either $\{0\}$ or infinite cyclic. If it is $\{0\}$, then $H = H \cap K$; otherwise fix $h \in H$ such that $\pi(h)$ generates $\pi(H)$ and show that H is the direct sum of its subgroups $\pi(H) = \pi(h)\mathbb{Z}$ and $H \cap K$.*

Proof.

(1) Induction on n. If $n = 1$, then H is a subgroup of $G = \mathbb{Z}$. Thus $H = 0$ or $H = h\mathbb{Z} \cong \mathbb{Z}$ for some integer $h > 0$. In any case, H is a free abelian group of rank ≤ 1.

(2) Assume the result holds for $n - 1$. Suppose $G = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (n times). Let $\pi : G \to \mathbb{Z}$ denote the obvious projection of G on the first factor, say

$$\pi((g_1, \ldots, g_n)) \mapsto g_1.$$

So the kernel of π is

$$\{(g_1, \ldots, g_n) \in G : g_1 = 0\} = \{(0, g_2, \ldots, g_n) \in G\} \cong \mathbb{Z}^{n-1}$$

is a free abelian group of rank $n - 1$.

(3) *(Part (a)) Show that $H \cap K$ is a free abelian group of rank $\leq n - 1$.* Note that $H \cap K$ is a subgroup of a free abelian group $K = \ker(\pi)$ of rank $n - 1$. The induction hypothesis shows that $H \cap K$ is a free abelian group of rank $\leq n - 1$.

(4) *Show that the image $\pi(H) \subseteq \mathbb{Z}$ is either $\{0\}$ or infinite cyclic.* As π is a group homomorphism, $\pi(H)$ is a subgroup of $\mathbb{Z}$. Thus $\pi(H)$ is a free abelian group of rank ≤ 1.

(5) *Show that $H = \pi(H) \oplus (H \cap K)$.* If $\pi(H) = 0$, then $H = H \cap K = \pi(H) \oplus (H \cap K)$. If $\pi(H)$ is infinite cyclic, we might assume that $\pi(H)$ is generated by $\pi(h_0)$ for some $h_0 \in H$.

(6) Observe that

$$\pi|_H : H \to \pi(H)$$

is surjective and $\ker(\pi|_H) = K \cap H$. Given any $h \in H$. we have $\pi(h) = \pi(h_0) \cdot a = \pi(ah_0)$ for some integer a. So $h - ah_0 \in H \cap K$. Since $H \cap K$ is a free abelian group K of rank $\leq n - 1$, we might write

$$h - ah_0 = b_1 k_1 + \cdots + b_r k_r$$

where $\{k_1, \ldots, k_r\}$ is a basis of $H \cap K$ ($r \leq n - 1$) and $b_1, \ldots, b_r \in \mathbb{Z}$. Therefore

$$h = ah_0 + b_1 k_1 + \cdots + b_r k_r$$

is generated by a basis $\{h_0, k_1, \ldots, k_r\}$ (since $\pi(h_0) \neq 0$ by assumption). Hence $H = \pi(H) \oplus (H \cap K)$.

□

Exercise 2.25.

Show that for any algebraic number α, there exists $m \in \mathbb{Z}$, $m \neq 0$, such that $m\alpha$ is an algebraic integer. (Hint: Obtain $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$ and take m to be a power of the leading coefficient.) Use this to show that for every finite set of algebraic numbers α_i, there exists $m \in \mathbb{Z}$, $m \neq 0$, such that all $m\alpha_i \in \mathcal{O}_{\mathbb{Q}}$.

Proof.

(1) As α is an algebraic number, there is a monic polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x]$$

such that $f(\alpha) = 0$. Eliminating all denominators of $a_{n-1}, \ldots, a_0$, we might assume that

$$f(x) = mx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

such that $f(\alpha) = 0$ where $m \neq 0$.

(2) Hence

$$\begin{aligned} & m^n\alpha^n + m^{n-1}a_{n-1}\alpha^{n-1} + \cdots + m^{n-1}a_0 = 0 \\ \Longrightarrow\ & (m\alpha)^n + \underbrace{a_{n-1}}_{\in\mathbb{Z}}(m\alpha)^{n-1} + \underbrace{ma_{n-2}}_{\in\mathbb{Z}}(m\alpha)^{n-2} + \cdots + \underbrace{m^{n-1}a_0}_{\in\mathbb{Z}} = 0. \end{aligned}$$

Therefore $m\alpha$ ($m \neq 0$) is an algebraic integer.

(3) Given finitely many algebraic numbers $\alpha_1, \ldots, \alpha_r$. There exist $m_i \in \mathbb{Z}$, $m_i \neq 0$, such that $m_i\alpha_i \in \mathcal{O}_{\mathbb{Q}}$ for all $i = 1, \ldots, r$. Take $m = m_1 \cdots m_r$. Hence all $m\alpha_i$ are algebraic integers again.

$\square$

Exercise 2.28.

Let $f(x) = x^3 + ax + b$, a and $b \in \mathbb{Z}$, and assume f is irreducible over $\mathbb{Q}$. Let α be a root of f.

(a) *Show that $f'(\alpha) = -\frac{2a\alpha+3b}{\alpha}$.*

(b) *Show that $2a\alpha + 3b$ is a root of*

$$\left(\frac{x-3b}{2a}\right)^3 + a\left(\frac{x-3b}{2a}\right) + b.$$

Use this to find $N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(2a\alpha + 3b)$.

(c) *Show that* $disc(\alpha) = -(4a^3 + 27b^2)$.

(d) *Suppose* $\alpha^3 = \alpha + 1$. *Prove that* $\{1, \alpha, \alpha^2\}$ *is an integral basis for* $\mathcal{O}_{\mathbb{Q}[\alpha]}$. *(See Exercise 2.27(e).) Do the same if* $\alpha^3 + \alpha = 1$.

Proof of (a).

(1) *Show that* $\alpha \neq 0$. If α were 0, then $f(\alpha) = f(0) = b$. So $f(x) = x^3 + ax = x(x^2 + a)$ is reducible, contrary to the irreducibility of f.

(2) Since α be a root of f, $f(\alpha) = 0$, or $\alpha^3 + a\alpha + b = 0$, or $\alpha^3 = -a\alpha - b$.

(3)

$$
\begin{aligned}
f'(x) = 3x^2 + a \Longrightarrow f'(\alpha) &= 3\alpha^2 + a \\
\Longleftrightarrow \alpha f'(\alpha) &= 3\alpha^3 + a\alpha && (\alpha \neq 0) \\
\Longleftrightarrow \alpha f'(\alpha) &= 3(-a\alpha - b) + a\alpha && (\alpha^3 = -a\alpha - b) \\
\Longleftrightarrow \alpha f'(\alpha) &= -2a\alpha - 3b.
\end{aligned}
$$

So $f'(\alpha) = -\frac{2a\alpha + 3b}{\alpha}$.

□

Proof of (b).

(1) Since $\alpha^3 + a\alpha + b = 0$,

$$\left(\frac{(2a\alpha + 3b) - 3b}{2a}\right)^3 + a\left(\frac{(2a\alpha + 3b) - 3b}{2a}\right) + b = 0.$$

That is, $2a\alpha + 3b$ is a root of $\left(\frac{x-3b}{2a}\right)^3 + a\left(\frac{x-3b}{2a}\right) + b$.

(2) $N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(2a\alpha + 3b)$ is the product of three roots of $\left(\frac{x-3b}{2a}\right)^3 + a\left(\frac{x-3b}{2a}\right) + b$. Hence,

$$
\begin{aligned}
N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(2a\alpha + 3b) &= (2a)^3 \left[\left(\frac{-3b}{2a}\right)^3 + a \cdot \frac{-3b}{2a} + b\right] \\
&= 8a^3 \left[\frac{-27b^3}{8a^3} - \frac{b}{2}\right] \\
&= -27b^3 - 4a^3 b.
\end{aligned}
$$

□

Proof of (c).

$$\begin{aligned}
\operatorname{disc}(\alpha) &= (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(f'(\alpha)) && \text{(Theorem 2.8)} \\
&= -N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}\left(-\frac{2a\alpha+3b}{\alpha}\right) && (n = 3 \text{ and (a)}) \\
&= \frac{N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(2a\alpha+3b)}{N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\alpha)} \\
&= \frac{-27b^3-4a^3b}{b} && \text{((b))} \\
&= -27b^2-4a^3.
\end{aligned}$$

□

Proof of (d).

(1) Write $\alpha^3 = \alpha + 1$ as $\alpha^3 - \alpha - 1 = 0$. Note that $f(x) = x^3 - x - 1$ is irreducible over $\mathbb{Q}$ since $f(x)$ is irreducible over $\mathbb{Z}/3\mathbb{Z}$. So $\operatorname{disc}(\alpha) = -23$ (by (c)). Since $\operatorname{disc}(\alpha)$ is squarefree, the result is established (Exercise 2.27(e)).

(2) Similar to (1). Write $\alpha^3 + \alpha = 1$ as $\alpha^3 + \alpha - 1 = 0$. Note that $f(x) = x^3 + x - 1$ is irreducible over $\mathbb{Q}$ since $f(x)$ is irreducible over $\mathbb{Z}/2\mathbb{Z}$. So $\operatorname{disc}(\alpha) = -31$ (by (c)). Since $\operatorname{disc}(\alpha)$ is squarefree, the result is established (Exercise 2.27(e)).

□

Exercise 2.43.

Let $f(x) = x^5 + ax + b$, a and $b \in \mathbb{Z}$, and assume f is irreducible over $\mathbb{Q}$. Let α be a root of f.

(a) *Show that $\operatorname{disc}(\alpha) = 4^4a^5 + 5^4b^4$. (Suggestion: See Exercise 2.28.)*

(b) *Suppose $\alpha^5 = \alpha + 1$. Prove that $\mathcal{O}_{\mathbb{Q}[\alpha]} = \mathbb{Z}[\alpha]$. ($x^5 - x - 1$ is irreducible over $\mathbb{Q}$; this can be shown by reducing $\pmod 3$).*

Proof of (a)(Exercise 2.28).

(1) *Show that $f'(\alpha) = -\frac{4a\alpha+5b}{\alpha}$.*

   (a) *Show that $\alpha \neq 0$.* If α were 0, then $f(\alpha) = f(0) = b$. So $f(x) = x^5 + ax = x(x^4 + a)$ is reducible, contrary to the irreducibility of f.

   (b) Since α be a root of f, $f(\alpha) = 0$, or $\alpha^5 + a\alpha + b = 0$, or $\alpha^5 = -a\alpha - b$.

(c)

$$\begin{aligned}
f'(x) = 5x^4 + a \Longrightarrow f'(\alpha) &= 5\alpha^4 + a \\
\Longleftrightarrow \alpha f'(\alpha) &= 5\alpha^5 + a\alpha & (\alpha \neq 0) \\
\Longleftrightarrow \alpha f'(\alpha) &= 5(-a\alpha - b) + a\alpha & (\alpha^5 = -a\alpha - b) \\
\Longleftrightarrow \alpha f'(\alpha) &= -4a\alpha - 5b.
\end{aligned}$$

So $f'(\alpha) = -\frac{4a\alpha+5b}{\alpha}$.

(2) *Show that* $4a\alpha + 5b$ *is a root of*

$$\left(\frac{x-5b}{4a}\right)^5 + a\left(\frac{x-5b}{4a}\right) + b.$$

Use this to show that $N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(4a\alpha + 5b) = -4^4a^5b - 5^5b^5$.

(a) Since $\alpha^5 + a\alpha + b = 0$,

$$\left(\frac{(4a\alpha+5b)-5b}{4a}\right)^5 + a\left(\frac{(4a\alpha+5b)-5b}{4a}\right) + b = 0.$$

That is, $4a\alpha + 5b$ is a root of $\left(\frac{x-5b}{4a}\right)^5 + a\left(\frac{x-5b}{4a}\right) + b$.

(b) $N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(4a\alpha + 5b)$ is the product of 5 roots of $\left(\frac{x-5b}{4a}\right)^5 + a\left(\frac{x-5b}{4a}\right) + b$. Hence,

$$\begin{aligned}
N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(4a\alpha + 5b) &= (4a)^5\left[\left(\frac{-5b}{4a}\right)^5 + a\cdot\frac{-5b}{4a} + b\right] \\
&= 4^5a^5\left[\frac{-5^5b^5}{4^5a^5} - \frac{b}{4}\right] \\
&= -5^5b^5 - 4^4a^5b.
\end{aligned}$$

(3) *Show that disc*$(\alpha) = 4^4a^5 + 5^4b^4$.

$$\begin{aligned}
\operatorname{disc}(\alpha) &= (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(f'(\alpha)) & \text{(Theorem 2.8)} \\
&= N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}\left(-\frac{4a\alpha+5b}{\alpha}\right) & (n = 5 \text{ and } (1)) \\
&= -\frac{N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(4a\alpha+5b)}{N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\alpha)} \\
&= -\frac{-4^4a^5b - 5^5b^5}{b} & ((2)) \\
&= 4^4a^5 + 5^4b^4.
\end{aligned}$$

$\square$

Proof of (b)(Exercise 2.28). Write $\alpha^5 = \alpha + 1$ as $\alpha^5 - \alpha - 1 = 0$. Note that $f(x) = x^5 - x - 1$ is irreducible over $\mathbb{Q}$ since $f(x)$ is irreducible over $\mathbb{Z}/3\mathbb{Z}$. So $\mathrm{disc}(\alpha) = 881$ (by (a)). Since $\mathrm{disc}(\alpha)$ is squarefree (a prime number), the result is established (Exercise 2.27(e)). $\square$

Exercise 2.45.

Obtain a formula for disc(α) if α is a root of an irreducible polynomial $x^n + ax + b$ over $\mathbb{Q}$. Do the same for $x^n + ax^{n-1} + b$.

Assume that $n \geq 2$.

Proof of $x^n + ax + b$ (Exercise 2.28).

(1) *Show that $f'(\alpha) = -\frac{(n-1)a\alpha + nb}{\alpha}$.*

   (a) *Show that $\alpha \neq 0$.* If α were 0, then $f(\alpha) = f(0) = b$. So $f(x) = x^n + ax = x(x^{n-1} + a)$ is reducible, contrary to the irreducibility of f.

   (b) Since α be a root of f, $f(\alpha) = 0$, or $\alpha^n + a\alpha + b = 0$, or $\alpha^n = -a\alpha - b$.

   (c)
$$\begin{aligned} f'(x) = nx^{n-1} + a \Longrightarrow f'(\alpha) &= n\alpha^{n-1} + a \\ \Longleftrightarrow \alpha f'(\alpha) &= n\alpha^n + a\alpha && (\alpha \neq 0) \\ \Longleftrightarrow \alpha f'(\alpha) &= n(-a\alpha - b) + a\alpha && (\alpha^n = -a\alpha - b) \\ \Longleftrightarrow \alpha f'(\alpha) &= -(n-1)a\alpha - nb. \end{aligned}$$

   So $f'(\alpha) = -\frac{(n-1)a\alpha + nb}{\alpha}$.

(2) *Let $\beta = (n-1)a\alpha + nb$. Show that β is a root of*
$$\left(\frac{x - nb}{(n-1)a}\right)^n + a\left(\frac{x - nb}{(n-1)a}\right) + b.$$
Use this to show that
$$N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\beta) = -(n-1)^{n-1}a^n b + (-1)^n n^n b^n.$$

   (a) Since $\alpha^n + a\alpha + b = 0$,
$$\left(\frac{\beta - nb}{(n-1)a}\right)^n + a\left(\frac{\beta - nb}{(n-1)a}\right) + b = 0.$$
   That is, β is a root of $\left(\frac{x-nb}{(n-1)a}\right)^n + a\left(\frac{x-nb}{(n-1)a}\right) + b$.

(b) $N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\beta)$ is the product of n roots of $\left(\frac{x-nb}{(n-1)a}\right)^n + a\left(\frac{x-nb}{(n-1)a}\right) + b$. Hence,

$$\begin{aligned} N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\beta) &= ((n-1)a)^n \left[\left(\frac{-nb}{(n-1)a}\right)^n + a \cdot \frac{-nb}{(n-1)a} + b\right] \\ &= (n-1)^n a^n \left[\frac{(-1)^n n^n b^n}{(n-1)^n a^n} - \frac{b}{n-1}\right] \\ &= (-1)^n n^n b^n - (n-1)^{n-1} a^n b. \end{aligned}$$

(3) *Show that* $disc(\alpha) = (-1)^{\frac{(n-1)(n-2)}{2}}(n-1)^{n-1}a^n + (-1)^{\frac{n(n-1)}{2}} n^n b^{n-1}$.

$$\begin{aligned} \operatorname{disc}(\alpha) &= (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(f'(\alpha)) && \text{(Theorem 2.8)} \\ &= (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}\left(-\frac{(n-1)a\alpha + nb}{\alpha}\right) && ((1)) \\ &= (-1)^{\frac{n(n-1)}{2}} (-1)^n \frac{N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}((n-1)a\alpha + nb)}{N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\alpha)} \\ &= (-1)^{\frac{n(n-1)}{2}} (-1)^n \frac{-(n-1)^{n-1}a^n b + (-1)^n n^n b^n}{b} && ((2)) \\ &= (-1)^{\frac{(n-1)(n-2)}{2}} (n-1)^{n-1} a^n + (-1)^{\frac{n(n-1)}{2}} n^n b^{n-1}. \end{aligned}$$

□