Summary for Modern Algebra II

SEUNGWOO HAN

David S. Dummit, Richard M. Foote. *Abstract Algebra*.
3rd ed., Wiley, 2003.

Contents

Chapter 1

Integral Domains

1.1 Basics of Integral Domains

Definition 1.1.1: Integral Domain

A ring R is an *integral domain* if R is a commutative ring with identity which has no zero divisor.

Note

Here are some basic facts regarding an integral domain R.

(1) If $ac = bc$ and $c \neq 0$, then $a = b$.

(2) Let $c_1, \cdots, c_n \in R$.

$$(c_1, \cdots, c_n) \triangleq \{ r_1c_1 + \cdots + r_nc_n \mid r_i \in R \} \subseteq R$$

is called the *ideal generated by* $c_1, \cdots, c_n$. If $n = 1$, then it is called a *principal ideal*.

(3) For $a, b \in R$ with $a \neq 0$, we write $a \mid b$ if $b = ad$ for some $d \in R$.

(4) For $a, b \in R \setminus \{0\}$, $d \in R$ is a *greatest common divisor* if

  (i) $d \mid a$ and $d \mid b$; and

  (ii) if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

(5) $u \in R$ is a *unit* in R if $uv = 1$ for some $v \in R$. v is called the *inverse* of u and is denoted u^{-1}.

(6) For $a, b \in R$, a is an *associate* of b if $a = bu$ for some $u \in R$, or equivalently, if $(a) = (b)$.

(7) For a non-unit $p \in R \setminus \{0\}$, p is *irreducible* if $p = ab$ implies a or b is a unit, or equivalently, only divisors of p are associates of p and units.

(8) For a non-unit $p \in R \setminus \{0\}$, p is *prime* in R if $p \mid ab$ implies $p \mid a$ or $p \mid b$, or equivalently, p is prime if (p) is a prime ideal of R.

(9) $R^* \triangleq \{ u \in R \mid u \text{ is a unit in } R \}$ is a group under "$\cdot$".

Theorem 1.1.2

Let R be an integral domain. If $p \in R$ is prime, then it is irreducible.

Proof. Suppose $p = ab$. WLOG, $p \mid a$. Then, $a = pr$ for some $r \in R$. Hence, $p = prb$, which implies $rb = 1$; b is a unit. □

Example 1.1.3

(i) $\mathbb{Z}$ is an integral domain. $\mathbb{Z}^* = \{\pm 1\}$. For nonzero $n \in \mathbb{Z}$, n and $-n$ are associate. $p \in \mathbb{Z}$ is a prime number if and only if $\pm p$ is prime in $\mathbb{Z}$.

(ii) $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Then, $\pm 1 + \sqrt{2}$ are units in $\mathbb{Z}[\sqrt{2}]$. $\sqrt{2}$ and $2 - \sqrt{2}$ are associate. There is no $a, b \in \mathbb{Z}$ such that $(a + b\sqrt{2})\sqrt{2} = 2b + a\sqrt{2} = 1$. Hence, $\sqrt{2}$ is not a unit in $\mathbb{Z}[\sqrt{2}]$.

Now, we prove that $\sqrt{2}$ is irreducible in $\mathbb{Z}[\sqrt{2}]$. Suppose $(a+b\sqrt{2})(c+d\sqrt{2}) = \sqrt{2}$ for some $a, b, c, d \in \mathbb{Z}$. Then, we get $ac + 2bd = 0$ and $ad + bd = 1$. Hence,

$$\begin{aligned} -2 &= (ac + 2bd)^2 - 2(ad + bc)^2 \\ &= (a^2 - 2b^2)(c^2 - 2d^2). \end{aligned}$$

WLOG, $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 = \pm 1$; thus $a + b\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$.

Definition 1.1.4

$d \in \mathbb{Z} \setminus \{0, 1\}$ is *square-free* if $c^2 \nmid d$ for all $c \in \mathbb{Z}_{\geq 2}$.

$$\mathbb{Q}(\sqrt{d}) \triangleq \{a + b\sqrt{d} \mid a + b \in \mathbb{Q}\}$$

is a field. Now, we introduce a function called *norm*:

$$\begin{aligned} N : \mathbb{Q}(\sqrt{d}) &\longrightarrow \mathbb{Q} \\ a + b\sqrt{d} &\longmapsto (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d. \end{aligned}$$

Note that for $d < 0$, $N(\alpha) \geq 0$ for all $\alpha \in \mathbb{Q}(\sqrt{d})$.

Theorem 1.1.5

Let d be a square-free integer. Let $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$.

(i) $N(\alpha) = 0 \iff \alpha = 0$

(ii) $N(\alpha\beta) = N(\alpha)N(\beta)$

Definition 1.1.6: Ring of Quadratic Integer

Let d be a square-free integer. Then,

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} \triangleq \begin{cases} \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} & \text{if } d \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{ a + \frac{1+\sqrt{d}}{2} b \;\middle|\; a, b \in \mathbb{Z} \right\} & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

is an integral domain. As $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a subring of $\mathbb{Q}(\sqrt{d})$, we may apply the norm function N for $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

Note

The weird definition follows from the fact that $\mathbb{Z}[\sqrt{d}]$ when $d \equiv 1 \pmod 4$ is not integrally closed.

Theorem 1.1.7

Let d be a square-free integer.

(i) $\forall \alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, $N(\alpha) \in \mathbb{Z}$

(ii) $\forall u \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, ($u$ is a unit $\iff N(u) = \pm 1$)

(iii) $\forall \alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, ($N(\alpha)$ is prime in $\mathbb{Z} \implies \alpha$ is irreducible in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$)

(iv) If $\pi \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is prime, then $N(\pi) \in \{\pm p^2, \pm p\}$ for some prime $p \in \mathbb{Z}$. Either p is irreducible in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ (in which $N(\pi) = \pm p^2$) or $p = \pi\pi'$ for some irreducible π' (in which $N(\pi) = \pm p$).

Proof. For simplicity, let

$$\omega \triangleq \begin{cases} \sqrt{d} & \text{if } d \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4 \end{cases} \quad \text{and} \quad \overline{\omega} \triangleq \begin{cases} -\sqrt{d} & \text{if } d \equiv 2,3 \pmod 4 \\ \frac{1-\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

so that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\omega]$.

(i)

$$N(a+b\omega) = \begin{cases} a^2 - db^2 & \text{if } d \equiv 2,3 \pmod 4 \\ a^2 + ab + \frac{1-d}{4} b^2 d & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

is an integer.

(ii) If $u \in \mathbb{Z}[\omega]$ is a unit, then $1 = N(1) = N(uu^{-1}) = N(u)N(u^{-1})$. Hence, by (i), $N(u) = \pm 1$. If $N(a+b\omega) = \pm 1$, then $(a+b\omega)(a-b\omega) = \pm 1$. Hence, $a + b\omega$ is a unit.

(iii) Suppose $\alpha = \beta\gamma$ where $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$ and let $N(\alpha) = p$ is prime in $\mathbb{Z}$. Then, $p = N(\alpha) = N(\beta)N(\gamma)$ and $N(\beta), N(\gamma) \in \mathbb{Z}$ by (i). Hence, $N(\beta) = \pm 1$ or $N(\gamma) = \pm 1$, which implies β or γ is a unit in $\mathbb{Z}[\omega]$ by (ii).

(iv) Let $(\pi) \subseteq \mathbb{Z}[\omega]$ be a prime ideal. π is irreducible by Theorem 1.1.2. Let

$$\begin{aligned} \iota : \mathbb{Z} &\longrightarrow \mathbb{Z}[\omega] \\ a &\longmapsto a + 0\omega \end{aligned}$$

be an injective ring homomorphism. Then, $\iota^{-1}\big((\pi)\big) = (\pi) \cap \mathbb{Z} \subseteq \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$.[1] Hence, $(\pi) \cap \mathbb{Z} = (p)$ for some prime $p \in \mathbb{Z}$, and thus $p = \pi\pi'$ for some $\pi' \in \mathbb{Z}[\omega]$. Therefore, we get $N(\pi)N(\pi') = N(p) = p^2$ in $\mathbb{Z}$. As $N(\pi) \in (\pi) \cap \mathbb{Z}$, we have $p \mid N(\pi)$. Thus, $N(\pi) \in \{\pm p^2, \pm p\}$.

If $N(\pi) = \pm p^2$, then π' is a unit by (ii), i.e., p is an associate of π and hence p is irreducible. If $N(\pi) = \pm p$, then $N(\pi') = \pm p$; hence π' is irreducible by (iii). □

Example 1.1.8

(i) $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$ is the *ring of Gaussian integers*. $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$. $N(1 \pm i) = 2$; $1 \pm i$ is irreducible in $\mathbb{Z}[i]$.

(ii) Consider $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$. $N(1+\sqrt{-5}) = 6$; hence $1+\sqrt{-5}$ is not prime in $\mathbb{Z}[\sqrt{-5}]$ by Theorem 1.1.7 (iv).

Suppose $1 + \sqrt{-5} = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Then, $6 = N(1+\sqrt{-5}) = N(\alpha\beta) = N(\alpha)N(\beta)$. Write $\alpha = a + b\sqrt{-5}$ so that $N(\alpha) = a^2 + 5b^2 \in \{1,2,3,6\}$. As $a, b \in \mathbb{Z}$, $N(\alpha) \in \{1, 6\}$. If $N(\alpha) = 6$, then $N(\beta) = 1$. Then, we may conclude that

[1] Given a ring homomorphism between commutative rings with identity, the inverse image of prime ideal is a prime ideal.

α or β is a unit in $\mathbb{Z}[\sqrt{-5}]$ by Theorem 1.1.5 (ii). Hence, $1+\sqrt{-5}$ is irreducible but not prime, which is a counterexample of the converse of Theorem 1.1.7 (iii).

Moreover there is no gcd of 6 and $2+2\sqrt{-5}$. Note that $6=(1+\sqrt{-5})(1-\sqrt{-5})=2\cdot 3$. Hence, $1+\sqrt{-5}$ and 2 are common divisors of 6 and $2+2\sqrt{-5}$. Suppose $d=a+b\sqrt{-5}$ is a gcd of 6 and $2+2\sqrt{-5}$ for the sake of contradiction. Then, by Theorem 1.1.5 (ii), $N(1+\sqrt{-5})=6$ and $N(2)=4$ both divide $N(d)=a^2+5b^2$. Hence, $12 \mid N(d)=a^2+5b^2$. On the other hand, as d divides both 6 and $2+2\sqrt{-5}$, $N(d)=a^2+5b^2$ divides $N(6)=36$ and $N(2+2\sqrt{-5})=24$. Hence, $N(d)=a^2+5b^2=12$; but there is no such $a,b\in\mathbb{Z}$.

1.2 Euclidean Domains

Definition 1.2.1: Euclidean Domain

An integral domain R is a *Euclidean domain* if R has a *Euclidean function* $\delta : R\setminus\{0\}\to\mathbb{Z}_{\geq 0}$ satisfying

(EF1) If $a,b\in R\setminus\{0\}$, then $\delta(a)\leq\delta(ab)$.

(EF2) If $a\in R$ and $b\in R\setminus\{0\}$, then there exist $q,r\in R$ such that $a=bq+r$ with $r=0$ or $\delta(r)<\delta(b)$.

Note

The condition (EF1) is reduntant. If $\delta' : R\setminus\{0\}\to\mathbb{Z}_{\geq 0}$ is a function that satisfies (EF2), then

$$\begin{aligned}\delta : R\setminus\{0\} &\longrightarrow \mathbb{Z}_{\geq 0}\\ r &\longmapsto \min\{\,\delta'(rx)\mid x\in R\setminus\{0\}\,\}\end{aligned}$$

is a Euclidean function. By definition, δ evidently satisfies (EF1).

To see how δ satisfies (EF2), take any $a\in R$ and $b\in R\setminus\{0\}$. Then, there exist $q,r\in R$ such that $a=bq+r$ and either $r=0$ or $\delta'(r)<\delta'(b)$. If $r=0$, then we are done; hence assume $b\nmid a$. By definition, $\delta(b)=\delta'(bx)$ for some $x\in R$. There exist $q'\in R$ and $r'\in R\setminus\{0\}$ such that $a=(bx)q'+r'$ and $\delta'(r')<\delta'(bx)$. Now, we have $\delta(r')\leq\delta'(r')<\delta'(bx)=\delta(b)$ and $a=b(xq')+r'$.

Example 1.2.2

(i) Every field F is a Euclidean domain, since $a=(a/b)b$ for all $a,b\in F\setminus\{0\}$. The Euclidean function is $a\mapsto 0$.

(ii) $\mathbb{Z}$ is a Euclidean domain. The Euclidean function is $n\mapsto |n|$. The pairs q,r may not be unique; $10=(-7)(-1)+3=(-7)(-2)+(-4)$.

(iii) Let F be a field. Then, $F[x]$ is a Euclidean domain. The Euclidean function is $f(x)\mapsto \deg f(x)$. Moreover, the quotient and the remainder of any division is unique.

(iv) $\mathbb{Z}[i]$ is a Euclidean domain with the function $a+bi\mapsto a^2+b^2$ (the norm of $\mathbb{Z}[i]$). (EF1) is satisfied by Theorem 1.1.5 (ii).

To check (EF2), take any $a+bi\in\mathbb{Z}[i]$ and $c+di\in\mathbb{Z}[i]\setminus\{0\}$. Then, in $\mathbb{Q}(i)$, $\frac{a+bi}{c+di}=t'+s'i$ for some $t',s'\in\mathbb{Q}$. Let $t\triangleq\lfloor t'\rceil$ and $s\triangleq\lfloor s\rceil$ so that $|t-t'|,|s-s'|\leq$

1/2.[2] Let $q \triangleq t + si \in \mathbb{Z}[i]$ and

$$\begin{aligned} r &\triangleq (a+bi) - (c+di)q \\ &= (a+bi) - (c+di)\{(t'+s'i) + \big((t-t') + (s-s')i\big)\} \\ &= (c+di)\big((t-t') + (s-s')i\big) \end{aligned}$$

so that $a + bi = (c+di)q + r$. Now, as

$$\begin{aligned} \delta(r) &= \delta(c+di)\delta((t-t') + (s-s')i) \\ &= \delta(c+di)\big((t-t')^2 + (s-s')^2\big) \\ &\le \frac{1}{2}\delta(c+di) < \delta(c+di), \end{aligned}$$

(EF2) is verified.

(v) $\mathcal{O}_{\mathbb{Q}(\sqrt{-19})} = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is not a Euclidean domain. Let $\omega \triangleq \frac{1+\sqrt{-19}}{2}$. Here are some facts easy to verify:

(1) $N(a+b\omega) = a^2 + ab + 5b^2 = (a+b/2)^2 + \frac{19}{4}b^2$.

(2) $N(\alpha) \ge 5$ if $\alpha \notin \{0, \pm 1, \pm 2\}$.

(3) $N(a+b\omega) \notin \{2, 3\}$.

(4) $\mathbb{Z}[\omega]^* = \{\pm 1\}$.

2 is irreducible in $\mathbb{Z}[\omega]$. If $2 = \alpha\beta$ in $\mathbb{Z}[\omega]$, Then, $4 = N(2) = N(\alpha)N(\beta)$; thus one of α and β is a unit by (3) and Theorem 1.1.7 (ii). Similarly, 3 is irreducible in $\mathbb{Z}[\omega]$.

Suppose $\mathbb{Z}[\omega]$ is a Euclidean domain with $\delta\colon \mathbb{Z}[\omega] \setminus \{0\} \to \mathbb{Z}_{\ge 0}$. Choose $m \in \mathbb{Z}[\omega] \setminus \{0, \pm 1\}$ such that $\delta(m)$ is smallest. Note that m is not a unit by (4). There exists $q, r \in \mathbb{Z}[\omega]$ with $2 = mq + r$ with $r = 0$ or $\delta(r) < \delta(m)$. We have $r \in \{0, \pm 1\}$.

- If $r = 0$, then $m \mid 2$; hence $m \in \{\pm 2\}$ as 2 is irreducible.
- If $r = 1$, then $m \mid 1$, which is impossible.
- If $r = -1$, then $m \mid 3$; hence $m \in \{\pm 3\}$ as 3 is irreducible.

Hence, $m \in \{\pm 2, \pm 3\}$.

Now, write $\omega = mq' + r'$ for some $q', r' \in R$ with $r' = 0$ or $\delta(r') < \delta(m)$. This means $r' \in \{0, \pm 1\}$. We have

$$N(\omega - r') = N(mq') = N(m)N(q') \in \{4N(q'), 9N(q')\}$$

while

$$N(\omega - r') = (r')^2 - r' + 5 \in \{5, 7\},$$

which is a contridiction.

[2] $\lfloor x \rceil$ for $x \in \mathbb{R}$ is an integer closest to x.

Theorem 1.2.3

Let R be a Euclidean domain with the Euclidean function $\delta\colon R \setminus \{0\} \to \mathbb{Z}_{\ge 0}$. Let $u \in R \setminus \{0\}$. TFAE.

(i) u is a unit in R.

(ii) $\delta(u) = \delta(1)$.

(iii) There exists $c \in R \setminus \{0\}$ such that $\delta(c) = \delta(uc)$.

Proof.

(i) $\Rightarrow$ (ii) $\delta(1) \le \delta(1 \cdot u) = \delta(u) \le \delta(uu^{-1}) = \delta(1)$.

(ii) $\Rightarrow$ (iii) Take $c = 1$.

(iii) $\Rightarrow$ (i) There exist $q, r \in R$ such that $c = (uc)q + r$ with $r = 0$ or $\delta(r) < \delta(uc) = \delta(c)$. If $r \neq 0$, then

$$\delta(uc) = \delta(c) \le \delta(c(1-uq)) = \delta(c - ucq) = \delta(r) < \delta(uc),$$

which is a contridiction. Hence, $c = ucq$, i.e., $uq = 1$. $\square$

Theorem 1.2.4

Let R be a Euclidean domain with the Euclidean function $\delta : \mathbb{R} \setminus \{0\} \to \mathbb{Z}_{\ge 0}$. Let $I \subseteq R$ be a nonzero ideal in R. Then, there exists $d \in I \setminus \{0\}$ such that $\forall a \in I \setminus \{0\}$, $\delta(d) \le \delta(a)$ and $I = (d)$.

Proof. Choose $d \in I \setminus \{0\}$ such that $\delta(d)$ is minimized. Take any $a \in I$. Then, there exist $q, r \in R$ such that $a = dq + r$ with $r = 0$ or $\delta(r) < \delta(d)$. As $r = a - dq \in I$, $r = 0$ by the choice of d. Hence, $a = dq \in (d)$. $\square$

Theorem 1.2.5

Le t R be an integral domain. Let $a, b \in R \setminus \{0\}$. Assume $(a, b) = (d)$ for some $d \in R$. Then,

(i) d is a greatest common divisor of a and b.

(ii) If d' is a greatest common divisor of a and b, then $(a, b) = (d')$.

Proof.

(i) Since $a, b \in (a, b) = (d)$, it follows that $d \mid a, b$ so that d is a common divisor of a and b. If $m \mid a, b$, then $(d) = (a, b) \subseteq (m)$ so that $m \mid d$.

(ii) $d' \mid d$, i.e., $(d) \subseteq (d')$. On the other hand, $d \mid d'$, i.e., $(d') \subseteq (d)$. Therefore, $(d') = (d) = (a, b)$. $\square$

Note

The assumption that there exists $d \in R$ such that $(a, b) = (d)$ in Theorem 1.2.5 is critical. For instance in the integral domain $\mathbb{Z}[x]$, elements 2 and x are prime and thus irreducible; thus 1 is a greatest common divisor of 2 and x but $(2, x) \neq (1)$.

Lemma 1.2.6

Let R be a Euclidean domain with the Euclidean function $\delta : \mathbb{R} \setminus \{0\} \to \mathbb{Z}_{\ge 0}$. Let $a, b \in R \setminus \{0\}$. Let $q, r \in R$ satisfy $a = bq + r$ with $r = 0$ or $\delta(r) < \delta(b)$. Then, $(a, b) = (b, r)$.

Proof. By Theorem 1.2.4, there exist $d, d' \in R$ such that $(a, b) = (d)$ and $(b, r) = (d')$. By Theorem 1.2.5, d and d' are greatest common divisors of a, b and b, r, respecitvely. We have $d \mid a - bq = r$ so d is a common divisor of b and r; thus $d \mid d'$. On the other hand, we have $d' \mid bq + r = a$, so d' is a common divisor of a and b; thus $d' \mid d$. Hence, $(d) = (d')$. $\square$

Definition 1.2.7: Euclidean Algorithm

Let R be a Euclidean domain and let $\delta : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ be its Euclidean function. The following algorithm is called *Euclidean algorithm*. For CS majors, assume that there is a Euclidean divison oracle for Line 3.

EUCLIDEAN ALGORITHM

```
1 Algorithm EUCLID(a, b)
    Input: a, b ∈ R
    Output: x, y ∈ R such that (a, b) = (ax + by)
2   if b = 0 then return (1, 0)
3   Find q, r ∈ R such that a = bq + r with r = 0 or δ(r) < δ(b).
4   (x, y) ← EUCLID(b, r)
5   return (y, x − qy)
```

Theorem 1.2.8

Let R be a Euclidean domain and let $\delta : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ be its Euclidean function.

(i) EUCLIDEAN ALGORITHM terminates in a finite number of recursions.

(ii) The result of EUCLIDEAN ALGORITHM is correct.

(iii) For any greatest common divisor d of a and b, there exist $x, y \in R$ such that $d = ax + by$.

Proof.

(i) At Line 4, $\delta(\cdot)$ value of the right argument strictly decreases. Hence, in at most $\delta(b)$ recursions, the algorithm falls into the base case at Line 2.

(ii) We first make sure that Line 2 is evidently correct; and hence the case in which $r = 0$ at Line 3 is correct.

Now, we conduct the induction on $\delta(b)$; assume the algorithm is correct for all inputs (a', b') such that $b' \neq 0$ or $\delta(b') < \delta(b)$. Then, the algorithm will reach Line 3 with $r = 0$ or $\delta(r) < \delta(b)$. If $r = 0$, then it is done; in the other case, by the induction hypothesis and Lemma 1.2.6,

$$(a, b) = (b, r) = (bx + ry) = (bx + (a - bq)y) = (ay + b(x - qy)).$$

The result follows by the mathematical induction.

(iii) It is a direct consequence of Theorem 1.2.4 and Theorem 1.2.5. □

1.3 Principal Ideal Domains

Definition 1.3.1: Principal Ideal Domain

A *principal ideal domain* is an integral domain in which every ideal is principal.

Note

By Theorem 1.2.4, as the zero ideal is principal, every Euclidean domain is a principal ideal domain.

Example 1.3.2

(i) $\mathbb{Z}$, $F[x]$, and $\mathbb{Z}[i]$ are principal ideal domains.

(ii) $\mathcal{O}_{\mathbb{Q}(\sqrt{-19})}$ is not a Euclidean domain but is a principal ideal domain. In Example 1.2.2 (v), we already showed that $\mathcal{O}_{\mathbb{Q}(\sqrt{-19})}$ is not a Euclidean domain.

Let $\omega = \frac{1+\sqrt{-19}}{2}$ and let $I \subsetneq \mathbb{Z}[\omega]$ be a proper nonzero ideal of $\mathbb{Z}[\omega]$. Choose $\beta \in I \setminus \{0\}$ such that $N(\beta)$ is the smallest. Suppose there exists $\alpha \in I \setminus (\beta)$ for the sake of contradiction. To this end, it is enough to show that there exists $s, t \in \mathbb{Z}[\omega]$ such that

$$0 < N\left(\frac{\alpha}{\beta}s - t\right) < 1,$$

which contradicts the minimality of β. Write

$$\frac{\alpha}{\beta} = \frac{a + b\sqrt{-19}}{c} \in \mathbb{Q}(\sqrt{-19})$$

with $a, b, c \in \mathbb{Z}$, $c > 0$, and they have no common divisor. Note that, if $c = 1$, then $\beta \mid \alpha$, i.e., $\alpha \in (\beta)$, which is a contradiction. We have four cases: $c \geq 5$, $2 \leq c \leq 4$.

- Assume $c \geq 5$. There exist $x, y, z \in \mathbb{Z}$ such that $ax + by + cz = 1$. There exist $q, r \in \mathbb{Z}$ such that

$$ax - 19bx = cq + r \text{ with } |r| \leq c/2.$$

Let $s \triangleq y + x\sqrt{-19} \in \mathbb{Z}[\omega]$ and $t \triangleq q - z\sqrt{-19} \in \mathbb{Z}[\omega]$ so that

$$\begin{aligned}\frac{\alpha}{\beta}s - t &= \frac{(a + b\sqrt{-19})(y + x\sqrt{-19})}{c} - (q - z\sqrt{-19}) \\ &= \frac{(ay - 19bx) + (ax + by)\sqrt{-19}}{c} - \frac{cq - cz\sqrt{-19}}{c} \\ &= \frac{(ay - 19bx - cq) + (ax + by + cz)\sqrt{-19}}{c} = \frac{r + \sqrt{-19}}{c},\end{aligned}$$

and hence

$$0 < N\left(\frac{\alpha}{\beta}s - t\right) = \frac{r^2 + 19}{c^2} \leq \frac{1}{4} + \frac{19}{c^2}.$$

Then, when $c \geq 6$, we have $N\left(\frac{\alpha}{\beta}s - t\right) \leq \frac{7}{9}$, and when $c = 5$, we have $|r| \leq 2$ so that $N\left(\frac{\alpha}{\beta}s - t\right) \leq \frac{23}{25}$; we eventually reached the contradiction.

- Assume $2 \leq c \leq 4$. There exists $q, r \in \mathbb{Z}$ such that

$$a^2 + 19b^2 = cq + r \text{ with } 0 \leq r < c.$$

  - Consider the case in which $r \neq 0$. Let $s \triangleq a - b\sqrt{-19} \in \mathbb{Z}[\omega]$ and $t \triangleq q \in \mathbb{Z}[\omega]$. Then, we have

$$\frac{\alpha}{\beta}s - t = \frac{(a + b\sqrt{-19})(a - b\sqrt{-19})}{c} - q = \frac{a^2 + 19b^2 - cq}{c} = \frac{r}{c},$$

  so we have $0 < N\left(\frac{\alpha}{\beta}s - t\right) = \frac{r^2}{c^2} < 1$.

- Now, consider the case $r = 0$, which means $c \mid a^2 + b^2$ while a, b, and c have no common divisor.
  - ⋆ if $c = 2$, then $a^2 + 19b^2$ is even thus a and b are both odd. Then,

$$\frac{\alpha}{\beta} = \frac{a + b\sqrt{-19}}{2} = \frac{a-b}{2} + b\omega \in \mathbb{Z}[\omega],$$

    which is a contradiction.
  - ⋆ If $c = 3$, then $3 \nmid a$ or $3 \nmid b$ so that $a^2 + 19b^2 \equiv a^2 + b^2 \equiv 1$ or $2 \pmod 3$ while it must be $c \mid a^2 + 19b^2$.
  - ⋆ If $c = 4$, then a and b are both odd. As $a^2, b^2 \equiv 1 \pmod 8$, we have $a^2 + 19b^2 = 8k + 4$ for some $k \in \mathbb{Z}$. Let

$$s \triangleq \frac{a - b\sqrt{-19}}{2} = \frac{a+b}{2} - b\omega \in \mathbb{Z}[\omega] \text{ and } t \triangleq k \in \mathbb{Z}[\omega].$$

    Then, we have

$$\frac{\alpha}{\beta}s - t = \frac{(a + b\sqrt{-19})(a - b\sqrt{-19})}{8} - k = \frac{a^2 + 19b^2 - 8k}{8} = \frac{1}{2},$$

    hence $0 < N\left(\frac{\alpha}{\beta}s - t\right) = \frac{1}{4} < 1$.

Therefore, in all cases, $(\beta) \subsetneq I$ reached a contradiction. Hence, I is a principal ideal.

(iii) $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ is not a PID. We will show $I \triangleq (3, 2 + \sqrt{-5}) \subseteq \mathbb{Z}[-5]$ is not principal. I is an proper ideal. Otherwise, there exist $x, y, z, w \in \mathbb{Z}$ such that

$$\begin{aligned} 1 &= 3(x + y\sqrt{-5}) + (2 + \sqrt{-5})(z + w\sqrt{-5}) \\ &= (3x + 2z - 5w) + (3y + z + 2w)\sqrt{-5}, \end{aligned}$$

i.e., $3x + 2z - 5w = 1$ and $3y + z + 2w = 0$. Hence, it follows that

$$1 = 3x + 2(-3y - 2w) - 5w = 3(x - 2y - 3w),$$

which is a contradiction. Hence, I is a proper ideal.

Suppose $I = (a + b\sqrt{-5})$. Then, $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ for some $c, d \in \mathbb{Z}$. Then, we have

$$9 = N(3) = (a^2 + 5b^2)(c^2 + 5d^2).$$

$a^2 + 5b^2 \neq 1$ as I is not proper; hence $a^2 + 5b^2 = 9$ and $c^2 + 5d^2 = 1$, which implies $c + d\sqrt{-15}$ is a unit and $a + b\sqrt{-5}$ is an associate of 3. Therefore, $I = (3)$, which is a contradiction.

Theorem 1.3.3

Let R be a principal ideal domain. If $p \in R$ is irreducible, then $(p) \subseteq R$ is a maximal ideal.

Proof. Let $M \subseteq R$ be an ideal containing (p). As R is a PID, $M = (m)$ for some $m \in R$. Hence, $p = mr$ for some $r \in R$. If r is a unit, then $(p) = (m)$. If m is a unit, then $M = R$. □

1.4 Unique Factorization Domains

Definition 1.4.1: Unique Factorization Domain

A *unique factorization domain* is an integral domain R such that:

(i) Every nonzero nonunit element is a product of irreducible elements of R.

(ii) If $u = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ are two products of irreducible elements of R, then $r = s$, and (possibly after reordering) p_i is an associate of q_i for all $i \in [r]$.

Example 1.4.2

(i) $\mathbb{Z}$ is a unique factorization domain by Fundamental Theorem of Arithmetic.

(ii) $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ is not a unique factorization domain.

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

is a two different factorizations of 6 into irreducible elements.

Theorem 1.4.3

Let R be a UFD. Then, every irreducible element in R is prime.

Proof. Let $p \in R$ be irreducible. If $p \mid ab$, then $ab = pc$ for some $c \in R$. Since R is a UFD, a or b has a factor which is an associate of p, i.e., $p \mid a$ or $p \mid b$. □

Definition 1.4.4: Ascending Chain Condition on Principal Ideals

Let R be an integral domain. R is said to satisfy *ascending chain condition on principal ideals* if, for all infinite chains of principal ideals

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots,$$

then there exists $n \in \mathbb{N}$ such that $(a_n) = (a_{n+1}) = (a_{n+1}) = \cdots$.

Theorem 1.4.5

Let R be an integral domain. R is a unique factorization domain if and only if

(i) R satisfies ascending chain condition on principal ideals and

(ii) if p is irreducible in R, then p is prime in R.

Proof.

($\Rightarrow$) Thanks to Theorem 1.4.3, we only need to check (i).

Let $(a_1) \subseteq (a_2) \subseteq \cdots$ be an ascending chain of principal ideals. Let $a_1 = up_1^{e_1} \cdots p_n^{e_n}$ be an irreducible factorization. There are at most $e_1 + \cdots + e_n$ strict inclusions.

($\Leftarrow$) Take any nonunit $r \in R \setminus \{0\}$. We want to find an irreducible factorization of r. If r is already irreducible, then we are done.

Assume $r = r_1 r_1'$ for some nonunit $r_1, r_1' \in R \setminus \{0\}$ so that $(r) \subsetneq (r_1)$. Continue this to get an ascending chain $(r) \subsetneq (r_1) \subsetneq (r_2) \subseteq \cdots$. Hence, we get an irreducible factor r_k at some point. □

Corollary 1.4.6

Every principal ideal domain is a unique factorization domain.

Proof. By Theorem 1.3.3, every irreducible element in R is prime.

Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of principal ideals in R. Let $I \triangleq \bigcup_{i \geq 1} I_i$ so that I is an ideal in R. Then, as R is a principal ideal domain, $I = (c)$ for some $c \in R$. By definition, $c \in I_n$ for some $n \in \mathbb{Z}_{>0}$. Hence, $I = (c) \subseteq I_n \subseteq I_{n+1} \subseteq \cdots \subseteq I = (c)$. □

Theorem 1.4.7

Let $d \in \mathbb{Z}$ be a square-free integer. Every nonzero nonunit element in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a product of irreducible elements.

Proof. Let

$$S \triangleq \{\text{nonzero nonunit elements in } \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \text{ that are not a product of irreducible elements}\}.$$

Suppose $S \neq \varnothing$ for the sake of contradiction and choose $a \in S$ such that $|N(a)|$ is minimized. As a is not irreducible, then $a = bc$ for some nonunit $b, c \in R \setminus \{0\}$. If $b, c \notin S$, then b and c are products of irreducible elements; hence $b \in S$ or $c \in S$. WLOG, $b \in S$. Then, $|N(b)| < |N(a)|$, which contradicts the choice of a. □

1.5 Unique Factorizations in Polynomial Rings

Definition 1.5.1: Primitive Polynomial

Let R be a unique factorization domain. $f(x) \in R[x] \setminus \{0\}$ is *primitive* if, for $r \in R$, r is a unit whenever whenever a constant polynomial $r \in R[x]$ divides $f(x)$.

1.6 Irreducibility Criteria for Polynomials

1.7 Field Extensions and Minimal Polynomials

1.8 Integrally Closed Domains

Definition 1.8.1: R-module

Let R be a commutative ring with identity. An *R-module* M is an abelian group $(M, +)$ with $R \times M \to M$ $((r, m) \mapsto rm$; scalar multiplication) such that following hold for all $a, b \in R$ and $m, n \in M$.

(1) $(a + b)m = am + bm$.

(2) $a(m + n) = am + an$.

(3) $(ab)m = a(bm)$.

(4) $1 \cdot m = m$.

Example 1.8.2

(1) If G is an abelian group, then it is a $\mathbb{Z}$-module.

(2) If F is a field, then M is a F-module if and only if M is a vector space over F.

(3) Let R be a commutative ring with identity and I be a subring of R. Then, I is an R-module if and only if I is an ideal of R.

Definition 1.8.3: R-submodule

Let R be a commutative ring with identity and M be an R-module. Then, $N \subseteq M$ is an *R-submodule* if

(1) $(N,+)$ is a subgroup of $(M,+)$ and

(2) $\forall a \in R$, $\forall n \in N$, $an \in N$.

Let $S := \{s_1, s_2, \cdots, s_n\} \subseteq M$. The *submodule generated by S* is

$$\sum_{i=1}^{n} Rs_i = \{r_1s_1 + \cdots + r_ns_n \mid r_1, \cdots, r_n \in R\}.$$

M is *finitely generated* if it is generated by some finite subset of M.

Definition 1.8.4: Integral

Let R and S be integral domains with $R \subseteq S$. Then, $u \in S$ is *integral* over R if u is a root of monic polynomial $f(x) \in R[x]$. Moreover, S is *integral* over R if all elements of S are integral over R. If S is integral over R, then S is an R-module.

Let $u_1, \cdots, u_n \in S$. We define

$$R[u_1, \cdots, u_n] \triangleq \{f(u_1, \cdots, u_n) \mid f(x_1, \cdots, x_n) \in R[x_1, \cdots, x_n]\}.$$

Then, $R[u_1, \cdots, u_n]$ is the smallest subring of S containing $u_1, \cdots, u_n$. Furthermore, it is an R-submodule of S.

Note

In general, $R[u_1, \cdots, u_n]$ is *not* finitely generated R-module.

Theorem 1.8.5

Let R be an integral domain and L be a field. Let L be a subring of S. For each $u \in L$, TFAE.

(1) u is integral over R.

(2) $R[u]$ is a finitely generated R-module.

(3) There is a finitely generated nonzero R-submodule M of L such that $uM := \{um \mid m \in M\} \subseteq M$.

Proof.

(i) $\Rightarrow$ (ii) $u^n + a_{n-1}a^{n-1} + \cdots + a_1u + a_0 = 0$ for some $a_{n-1}, \cdots, a_1, a_0 \in R$.

Take any $i \in \mathbb{Z}_{\geq n}$. Then,

$$u^i = u^n u^{i-n} = -a_0u^{i-n} - a_1u^{i-n+1} - \cdots - a_{n-1}u^{i-1}.$$

Hence, by induction every, u^i is in $\sum_{j=0}^{n-1} Rs^j$. Therefore, $R[u] = \sum_{j=0}^{n-1} Rs^j$ is finitely generated.

(ii) ⇒ (iii) Set $M := R[u]$.

(iii) ⇒ (i) Write $M = \sum_{i=1}^{n} R\ell_i$ for some $\ell_1, \cdots, \ell_n \in L$. As $u\ell_i \in M$, write $u\ell_i = \sum_{j=1}^{n} b_{ij}\ell_j$ for some $b_{ij} \in R$. □

Corollary 1.8.6

Let R be an integral domain and L be a field. Let R be a subring of L. Then, $S \triangleq \{u \in L \mid u \text{ is integral over } R\}$ is a subring of L. In particular, if $u \in L$ is integral over R, then $R[u]$ is an integral extension of R.

Proof. If suffices to check if $u, v \in S$, then $u \pm v, uv \in S$. By Theorem 1.8.5, $R[u]$ and $R[v]$ are finitely generated R-modules. Write $R[u] = \sum_{i=1}^{n} Rf_i$ and $R[v] = \sum_{j=1}^{m} Rg_j$. Then, $R[u,v] = \sum_{1\le n 1 \le m} Rf_i g_j$. As $(u \pm v)R[u,v], uvR[uv] \subseteq R[u,v]$, by Theorem 1.8.5, they are integral over R. □

Definition 1.8.7: Integral Closure

Let R be an integral domain and L be a field. Let R be a subring of L. The set S defined in Corollary 1.8.6 is called the *integral closure* of R in L.

Definition 1.8.8: Integrally Closed Domain

We say R is an *integrally closed domain* if R is the integral closure of R in the fraction field of R.

Theorem 1.8.9

Every unique factorization domain is integrally closed.

Proof. Let R be a unique factorization domain and F be its fraction field. Take any $u \in F$ that is integral over R. Then, there are some $a_0, \cdots, a_{n-1} \in R$ with $u^n + a_{n-1}u^{n-1} + \cdots + a_1 u + a_0 = 0$. Write $u = b/c$ where $b, c \in R$ with $c \neq 0$ and $(1) = (b,c)$. Then,

$$c(a_{n-1}b^{n-1} + \cdots + a_1 bc^{n-2} + a_0 c^{n-1}) = -b^n.$$

Hence, c must be a unit; thus $u = b/c \in R$. □

Example 1.8.10

We showed that $\mathbb{C}[x,y,z,w]/(xy - zw)$ is not a unique factorization domain but is an integrally closed domain.

Lemma 1.8.11

Let R be an integrally closed domain and let F be its fraction field. Let K be an extension field of F. Let $u \in K$ is algebraic over F. Then, u is integral over R if and only if $\min_{u,F}(x) \in R[x]$.

Proof.

(⇒) There is a monic polynomial $f(x) \in R[x]$ such that $f(u) = 0$. There is some extension field L of F containing all roots of $p(x)$. Let $u_1 = u, u_2, \cdots, u_n$ be all roots of $p(x)$ in L. We have $p(x) = (x - u_1)(x - u_2)\cdots(x - u_n) \mid f(x)$ by the definition of minimal polynomial. Hence, $u_1, u_2, \cdots, u_n$ are integral over R.

($\Leftarrow$) As the minimal polynomial is monic, it is trivial. $\square$

Theorem 1.8.12

Let A, B, and C be integral domains with $A \subseteq B \subseteq C$. Then, C is integral over A if and only if C is integral over B and B is integral over A.

Proof.

($\Rightarrow$) As B is a subring of C, B is integral over A. As a monic polynomial over A is a monic polynomial over B, C is integral over B.

($\Leftarrow$) Take any $u \in C$. There is a polynomial $g(x) = x^n + b_{n-1}x^{n-1} + \cdots b_1 x + b_0 \in B[x]$ with $g(u) = 0$. Then $B' \triangleq A[b_0, \cdots, b_{n-1}, u] \subseteq B$ is a finitely generated A-module by Theorem 1.8.5. Then, $uB' \subseteq B'$; hence u is integral over A by Theorem 1.8.5. $\square$

Theorem 1.8.13

Let R be an integral domain and let F be its fraction field. Let K be an extension field of F with $\dim_F K < \infty$. Let S be the integral closure of R in K.

(1) $\forall u \in K, \exists (s, d) \in S \times D, u = s/d$. In particular, K is a fraction field of S.

(2) S is an integrally closed domain.

(3) If R is an integrally closed domain, then $S \cap F = R$.

We will show later $u \in K$ is algebraic over F.

Proof.

(1) Let $p(x) \triangleq \min_{u,F}(x) \in F[x]$. Write

$$p(x) = x^n + \frac{c_{n-1}}{d_{n-1}} x^{n-1} + \cdots \frac{c_1}{d_1} x + \frac{c_0}{d_0}$$

where $c_i, d_i \in R$ and $d_i \neq 0$. Let $d \triangleq d_0 \cdots d_{n-1}$. Then,

$$0 = d^n p(u) = (du)^n + \frac{c_{n-1}}{d_{n-1}} d(du)^{n-1} + \cdots \frac{c_1}{d_1} d^{n-1}(du) + \frac{c_0}{d_0} d^n,$$

i.e., $du \in S$.

(2) Let S' be the integral closure of S in K. Then, S' is integral over R by Theorem 1.8.12 so that $S' \subseteq S$. Hence, $S = S'$.

(3) Trivial. $\square$

Corollary 1.8.14

Let R be an integral domain and let F be its fraction field. Let K be a finite extension field of F. Let S be the integral closure of R in K. Then, there are $d_1, d_2, \cdots, d_n S$ such that $d_1, \cdots, d_n$ is a basis of K over F.

Example 1.8.15

Let $d \in \mathbb{Z}$ be square-free. Then, we claim that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$. Take any $u = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$.

- Suppose $b = 0$. Then, $\min_{u,\mathbb{Q}}(x) = x - a$. Thus, u is integral over $\mathbb{Z}$ if and only if $a \in \mathbb{Z}$.

- Suppose $b \neq 0$. Then, $\min_{u,\mathbb{Q}}(x) = x^2 - 2ax + (a^2 - b^2 d)$. u is integral over $\mathbb{Z}$ if and only if $2a, a^2 - b^2 d \in \mathbb{Z}$. By some elementary arguments, this is equivalent to $u \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

$\square$

Chapter 2

Field Extensions

2.1 Finite Extensions and Degree of Field Extension

Definition 2.1.1: Finite Extension

Let F be a field and K be an extension field over F. We say K is *finite* over F if $\dim_F K$ is finite. We also write $[K{:}F] \triangleq \dim_F K$ and call it the *degree* of K over F.

Example 2.1.2

(1) Let $d \in \mathbb{Z}$ be square-free. Then, $[\mathbb{Q}(\sqrt{d}){:}\mathbb{Q}] = 2$.

(2) If u is algebraic over F, then $[F(u){:}F] = \deg \min_{u,F}(x)$.

Lemma 2.1.3

Let F be a field, K be a finite extension field of K, and L be an extension field of F. If there is an isomorphism $f : K \xrightarrow{\approx} L$ such that $\forall c \in F,\ f(c) = c$, then $[K{:}F] = [L{:}F]$.

Proof. f is a bijective linear transformation between vector spaces K and L. □

Theorem 2.1.4

Let F be a field and K be a finite extension field of K. Then, every $u \in K$ is algebraic over F.

Proof. Let $n \triangleq [K{:}F]$. Then, $1, u, u^2, \cdots, u^{n-1}, u^n$ are linearly dependent over F. Hence, there are some $c_0, c_1, \cdots, c_n \in F$, not all zero, such that $c_0 + c_1 u + c_2 u^2 + \cdots + c_n u^n = 0$. □

Theorem 2.1.5

Let F, K, and L be fields with $F \subseteq K \subseteq L$. Then, L is finite over F if and only if L is finite over K and K is finite over F. Futhermore, $[L{:}F] = [L{:}K][K{:}F]$.

End.