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.

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

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 $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$.

(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,

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

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

(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)

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

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. 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 $\mathbb{Z}$. Thus, the result follows from previous conclusions. □

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 $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Let $\alpha = a + b\sqrt{-5}$. Then, we may conclude that α or β is a unit in $\mathbb{Z}[\sqrt{-5}]$.

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 them.

[1]The inverse image of prime ideal in .

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

End.